PRESIDÊNCIA DA REPÚBLICA
TERMO DE ABERTURA DE PROJETO (TAP)

Processo nº 00261.000968/2021-06

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

1. **PROJETO**

Nome do Projeto:	Regulamentação da Transferência Internacional de Dados Pessoais
Áreas Responsáveis pelo Projeto:	Coordenação-Geral de Normatização (CGN) e Coordenação-Geral de Relações Internacionais e Institucionais (CGRII)

2. **IDENTIFICAÇÃO DA EQUIPE DE TRABALHO DA ANPD**

Áreas técnicas:	Coordenação-Geral de Normatização (CGN) e Coordenação-Geral de Relações Internacionais e Institucionais (CGRII)
Gerente do Projeto:	Isabela Maiolino (CGN)
Integrantes da equipe:	Sabrina Fernandes Maciel, Mariana Talouki, Ailana Linhares de Sousa Medeiros, Caroline Nazaré dos Santos Chucre Kappel
Unidade Demandante:	Conselho Diretor da ANPD

2.1. A Equipe de Projeto será constituída por servidores da Coordenação-Geral de Normatização (CGN) e da Coordenação-Geral de Relações Internacionais e Institucionais (CGRI), além de outros servidores que manifestarem interesse.

3. **OBJETIVO**

3.1. Regulamentar a transferência internacional de dados, nos termos do disposto nos arts. 33, 34, 35 e 36 da Lei nº 13.709, de 14 de agosto de 2018, que instituiu a Lei Geral de Proteção de Dados Pessoais (LGPD). Ou seja, apresentar proposição operacionalizadora das ações envolvidas nas transferências internacionais de dados pessoais com vistas das garantias jurídicas envolvidas no dever de atuação regulamentadora da Autoridade.

4. **JUSTIFICATIVA**

4.1. O projeto visa atender a demanda formalizada pelo Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD), por meio de sua Agenda Regulatória, aprovada pela Portaria nº 11, de 27 de janeiro de 2021, que, por sua vez, ocorre em atenção ao disposto nos arts. 33, 34 e 35 da LGPD.

4.2. O art. 33 da LGPD prevê quais os mecanismos autorizadores da transferência internacional de dados, dentre os quais está a transferência para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nessa Lei. Por sua vez, o art. 34 explica

que o nível de proteção de dados do país estrangeiro ou do organismo internacional será avaliado pela ANPD. O art. 35 da lei determina, ainda, que a definição do conteúdo de cláusulas-padrão contratuais, dentre outros, será realizada pela ANPD, nos seguintes termos:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência;
>
> b) cláusulas-padrão contratuais;
>
> c) normas corporativas globais;
>
> d) selos, certificados e códigos de conduta regularmente emitidos;
>
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
>
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> V - quando a autoridade nacional autorizar a transferência;
>
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
>
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
>
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
>
> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação) , no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional.
>
> Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração:
>
> I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
>
> II - a natureza dos dados;
>
> III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
>
> IV - a adoção de medidas de segurança previstas em regulamento;
>
> V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
>
> VI - outras circunstâncias específicas relativas à transferência.
>
> Art. 35. A definição do conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, a que se refere o inciso II do caput do art. 33 desta Lei, será realizada pela autoridade nacional.

§ 1º Para a verificação do disposto no caput deste artigo, deverão ser considerados os requisitos, as condições e as garantias mínimas para a transferência que observem os direitos, as garantias e os princípios desta Lei.

§ 2º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação da autoridade nacional, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento, quando necessário.

§ 3º A autoridade nacional poderá designar organismos de certificação para a realização do previsto no caput deste artigo, que permanecerão sob sua fiscalização nos termos definidos em regulamento.

§ 4º Os atos realizados por organismo de certificação poderão ser revistos pela autoridade nacional e, caso em desconformidade com esta Lei, submetidos a revisão ou anulados.

§ 5º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no caput deste artigo serão também analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos §§ 1º e 2º do art. 46 desta Lei.

4.3. Diante disso, é importante que a ANPD identifique o conteúdo adequado para as cláusulas-padrão contratuais, que possuem previsão normativa no âmbito do art. 33, II, b, bem como forneça diretrizes suplementares relativas aos demais mecanismos de transferências internacionais de dados pessoais, quando cabível, em especial os também constantes no inciso II do art. 33.

4.4. Também se demonstra profícuo o estabelecimento das diretrizes para regulamentação acerca do processo de concessão, por parte desta Autoridade, de grau de adequação a países ou organizações internacionais que possuam grau protetivo de proteção de dados pessoais equiparado às disposições constantes na LGPD.

4.5. Dessa forma, a área técnica pretende apresentar proposta de regulamento sobre transferência internacional de dados pessoais, a ser deliberada pelo Conselho Diretor, que estabeleça, nos termos da LGPD:

a) procedimento para concessão de grau de adequação a países ou organismos internacionais, nos termos do art. 33, I.

b) o conteúdo do mecanismo previsto no art. 33, II, b, *id est*, as cláusulas-padrão contratuais, nos termos do art. 35, *caput*.

c) a regulamentação necessária para utilização das cláusulas contratuais específicas e das normas corporativas globais, nos termos do art. 33, II, a, c e art. 35, *caput*, e §§1º , 2º e 5º .

4.6. A equipe prevê como metas da Agenda a elaboração do Relatório de Análise de Impacto Regulatório (AIR) e a realização de Consulta Pública até o 1º semestre de 2022 e, até o 2º semestre de 2022, a aprovação final da proposta.

5. **ESCOPO DO PROJETO**

5.1. O presente projeto tem por escopo a apresentação de proposta de norma sobre a transferência internacional de dados pessoais, considerando que é um tema de extrema relevância e reflete enorme protagonismo de atuação da ANPD com vistas a garantir a devida segurança jurídica para as relações interoperacionais que envolvem a legislação temática.

5.2. Como produto, será elaborada uma proposta de regulamento sobre transferência internacional de dados pessoais, envolvendo a normatização procedimental de ações e garantias jurídicas que devem vir a ser proporcionadas por eventuais controladores e processadores de dados pessoais em relações transfronteiriças.

6. **ALINHAMENTO ESTRATÉGICO**

6.1. O presente projeto está diretamente relacionado à execução do Planejamento Estratégico da ANPD (2363117), aprovado na Reunião Deliberativa nº 1, de 20 de janeiro de 2021. Sob a perspectiva de resultados, o projeto alinha-se ao objetivo de promover o fortalecimento da cultura de proteção de dados pessoais. Sob a perspectiva de processos, o projeto está aderente ao objetivo estratégico de estabelecer um ambiente normativo eficaz para a proteção de dados pessoais.

7. **RESTRIÇÕES**

7.1. Preliminarmente, não foram identificadas restrições a este projeto.

8. **PREMISSAS**

8.1. A ANPD tem competência para editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade.

8.2. A ANPD entende ser necessário, no que tange ao tratamento de dados pessoais e ao seu fluxo transfronteiriço, assegurar que o tratamento e processamento desses dados estão sendo feitos com observância às diretrizes da LGPD, ou seja, respeitando o direito de privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem e, ao mesmo tempo, fomentando a livre iniciativa e a livre concorrência, o desenvolvimento econômico e tecnológico. **Assim, devem ser adotados, preferencialmente, modelos menos burocráticos e mais flexíveis que possam viabilizar, de modo prático, rápido e eficaz, o fluxo transfronteiriço de dados.** A intenção é que os requisitos previstos na LGPD sejam cumpridos, vinculados à manutenção da proteção de dados já protegidos sob a lei nacional, como condicionante para que seja autorizado o seu fluxo internacional.

8.3. Além disso, importa aqui, ainda, elaborar uma regulamentação que seja harmônica e compatível, na medida do possível, com outras regulamentações estrangeiras. É importante ressaltar que o Capítulo V, específico às transferências internacionais de dados pessoais, guarda semelhança com o dispositivo correspondente do Regulamento Geral de Proteção de Dados europeu, aprovado pela Resolução 2016/679. Por essa razão, as premissas constantes no modelo europeu serão consideradas para análise do projeto de regulamentação de transferências internacionais de dados, a ele não se limitando, contudo. Também serão analisados outros modelos disponíveis, a exemplo do modelo neozelandês (*Office of the Privacy Commissioner),* do modelo da ASEAN (*ASEAN Digital Senior Officials´ Meeting*) e do modelo do Reino Unido (recém-saído da União Europeia), que está em fase de elaboração e passa, no presente momento, por consulta pública (*Information Commissioner´s Office*).

9. **PRINCIPAIS ENTREGAS DO PROJETO**

Principais Entregas	Data
Relatório de Análise de Impacto Regulatório (AIR)	1º Semestre de 2022
Realização de Consulta Pública	1º Semestre de 2022
Aprovação Final do Regulamento	2º Semestre de 2022

10. **EXCLUSÕES (NÃO ESCOPO)**

10.1. Este projeto não tem no escopo regulamentar matérias não vinculadas à transferência internacional de dados.

11. **RECURSOS PREVISTOS**

11.1. Sem prejuízo de outros que venham a ser mapeados quando das discussões relativas ao projeto, far-se-á uso:

a) do Sistema Eletrônico de Informações (SEI); e

b) dos recursos humanos indicados pelas áreas interessadas da ANPD.

12. **PARTES INTERESSADAS**

12.1. São partes interessadas a ANPD, os agentes de tratamento de dados (importadores e exportadores), os titulares de dados, as autoridades estrangeiras de proteção de dados pessoais.

13. **RISCOS PREVIAMENTE IDENTIFICADOS**

13.1. Identificam-se como principais eventos de risco para o cumprimento dos prazos do projeto:

a) Judicialização do tema; e

b) Concorrência com o andamento de demais projetos constantes na Agenda Regulatória.

14. **CONSIDERAÇÕES FINAIS**

14.1. Tendo em vista o exposto, não há considerações adicionais.

15. **APROVAÇÃO**

15.1. O presente Termo de Abertura de Projeto (TAP) segue assinado pela gerente do projeto e pelos integrantes da equipe, devendo ser encaminhado para as demais áreas da ANPD para indicação dos servidores que acompanharão o processo de regulamentação.

Sabrina Fernandes Maciel

Especialista em políticas públicas e servidora da ANPD

Ailana Linhares de Sousa Medeiros

Servidora da ANPD

Caroline Nazaré dos Santos Chucre Kappel

Servidora da ANPD

Mariana Talouki

Coordenadora-Geral de de Relações Institucionais e Internacionais

Isabela Maiolino

Coordenadora-Geral de Normatização

Documento assinado eletronicamente por **Mariana Almeida de Sousa Talouki, Coodenadora-Geral de Relações Institucionais e Internacionais**, em 10/11/2021, às 08:18, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Caroline Nazaré dos Santos Chucre Kappel, Assessor(a) Técnico(a)**, em 10/11/2021, às 08:31, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Ailana Linhares de Sousa Medeiros, Assessor(a) Técnico(a)**, em 10/11/2021, às 08:37, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Isabela Maiolino, Coordenadora-Geral de Normatização**, em 17/11/2021, às 15:21, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Sabrina Fernandes Maciel Favero, ANPD - Autoridade Nacional de Proteção de Dados**, em 17/11/2021, às 15:24, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted] A autenticidade do documento pode ser conferida informando o código verificador [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Memória de Reunião Nº 25/2022/CGN/ANPD/PR

Data: 01/04/2022
Horário: 14h30
Local: Online, via Microsoft Teams
Participantes: Juliana Muller, Fernando de Mattos Maciel Maciel, Davi Teofilo Nunes Oliveira, Isabela Maiolino e Sabrina Fernandes Maciel Favero
Pauta: Reunião prepatória para Tomada de Subsídios de Transferência Internacional de Dados

Memória

Os servidores da Coordenação-Geral de Normatização e da Coordenação-Geral de Relações Institucionais e Internacionais (CGRII) reuniram-se para alinhamento das próximas etapas da Tomada de Subsídios.

Encaminhamentos

Ficou acordado que será realizada Tomada de Subsídios (TS) sobre a norma de Transferência Internacional na plataforma participa mais Brasil. Em seguida, será realizada uma reunião com especialistas convidados.
Ficou alinhado que, para a próxima reunião (07/04), os servidores irão trabalhar em um documento com sugestões de perguntas para a Tomada de Subsídios e respectiva Nota Técnica. Espera-se que o documento seja apresentado para o Conselho Diretor em sua reunião do dia 11/04.
Com a aprovação do Conselho, as perguntas serão publicadas na plataforma mais Brasil entre os dias 15 e 18 de abril.
Cronograma de próximas reuniões
07/04 - 14h00 - Reunião pra fechar as perguntas e a nota da TS;
11/04 - a definir - Apresentação das perguntas para o CD;
15/04 - Publicação das perguntas na plataforma mais Brasil;
19/04 - 9h30 - Reunião para definição dos atores que vamos ouvir;
22/4 - 10h00 - Reunião para discutir o AIR;

Documento assinado eletronicamente por **Davi Teófilo Nunes de Oliveira**, **Assessor(a) Técnico(a)**, em 01/04/2022, às 16:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Sabrina Fernandes Maciel Favero**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 01/04/2022, às 16:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Fernando de Mattos Maciel**, **Coordenador(a)**, em 01/04/2022, às 16:12, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Isabela Maiolino**, **Coordenador(a)-Geral**, em 01/04/2022, às 18:13, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Juliana Muller Reis Jorge**, **Coordenador(a)-Geral**, em 01/04/2022, às 20:20, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA
PRESIDÊNCIA DA REPÚBLICA
Protocolo da Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Memória de Reunião Nº 26/2022/CGN/ANPD/PR

Data: 07/04/2022
Horário: 14h30
Local: Teams
Participante: Ailana Linhares, Fernando Maciel, Juliana Muller, Sabrina Fernandes, Virginia de Melo, Mariana Talouki e Davi Teofilo.
Pauta: Tomada de Subsídios para a norma de transferência internacional de dados

Memória

Na reunião foram discutidas possíveis questões a serem submetidas na Tomada de Subsídios da norma de Transferências Internacionais. Os servidores presentes alinharam entendimentos sobre o escopo das perguntas a serem disponibilizadas na plataforma Participa mais Brasil em observância às competências da ANPD para a regulamentação do tema. A discussão levou em consideração a pertinência das perguntas para esta etapa do processo regulatório e buscou alinhar as expectativas da iniciativa regulatória.

Encaminhamentos

As questões serão enviadas para avaliação da Coordenadora-Geral de Normatização, Isabela Maiolino, para posterior alinhamento com o Conselho Diretor da ANPD.

Davi Teofilo Nunes Oliveira

Assistente Técnico da Coordenação-Geral de Normatização.

Documento assinado eletronicamente por **Sabrina Fernandes Maciel Favero**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 04/05/2022, às 15:37, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Fernando de Mattos Maciel**, **Coordenador(a)**, em 04/05/2022, às 17:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Davi Teófilo Nunes de Oliveira**, **Assessor(a) Técnico(a)**, em 11/05/2022, às 10:35, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Juliana Muller Reis Jorge**, **Coordenador(a)-Geral**, em 11/05/2022, às 11:13, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Ailana Linhares de Sousa Medeiros**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 11/05/2022, às 14:46, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código verificador [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Esplanada dos Ministérios, Bloco C, 2º andar — Telefone:

CEP 70046-900 Brasília/DF - https://www.gov.br/planalto/pt-br

PRESIDÊNCIA DA REPÚBLICA
PRESIDÊNCIA DA REPÚBLICA
Protocolo da Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Memória de Reunião Nº 27/2022/CGN/ANPD/PR

Data: 19/04/2022
Horário: 09h30
Local: Online, via Microsoft Teams
Participantes: Juliana Muller, Ailana Linhares, Virgínia Trinks, Caroline Kappel, Davi Teofilo Nunes Oliveira, Isabela Maiolino e Sabrina Fernandes Maciel Favero.
Pauta: Tomada de Subsídios para a norma de Transferência Internacional de Dados

Memória

Os servidores da Coordenação-Geral de Normatização (CGN) e da Coordenação-Geral de Relações Institucionais e Internacionais (CGRII) reuniram-se para discussão final sobre as questões a serem submetidas na Tomada de Subsídios, bem como para definição de atores a serem consultados.

Encaminhamentos

O documento final acordado será encaminhado para avaliação do Conselho Diretor da ANPD.

SABRINA FERNANDES MACIEL FAVERO

Especialista em Políticas Públicas e Gestão Governamental

Documento assinado eletronicamente por **Isabela Maiolino**, **Coordenador(a)-Geral**, em 04/05/2022, às 15:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Sabrina Fernandes Maciel Favero**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 04/05/2022, às 15:37, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Davi Teófilo Nunes de Oliveira**, **Assessor(a) Técnico(a)**, em 11/05/2022, às 10:31, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Juliana Muller Reis Jorge**, **Coordenador(a)-Geral**, em 11/05/2022, às 11:13, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Ailana Linhares de Sousa Medeiros**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 11/05/2022, às 14:47, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Esplanada dos Ministérios, Bloco C, 2º andar — Telefone:

CEP 70046-900 Brasília/DF - https://www.gov.br/planalto/pt-br

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Memória de Reunião Nº 36/2022/CGN/ANPD/PR

Data: 11 e 12/05/2022
Horário: 14hs e 10h30, respectivamente
Local: Online, via Microsoft Teams
Participantes: Miriam Wimmer, Lucas Borges, Arthur Sabbat, Nairane Farias Rabelo Leitão, Joacil Rael, Equipe de Projeto: Rodrigo Santana, Juliana Muller, Virgínia Trinks, Caroline Kappel, Davi Teofilo Nunes Oliveira, Fernando Mattos Maciel e Sabrina Fernandes Maciel Favero.
Pauta: Tomada de Subsídios para a norma de Transferência Internacional de Dados Pessoais.

Memória

Os servidores da Coordenação-Geral de Normatização (CGN) e da Coordenação-Geral de Relações Institucionais e Internacionais (CGRII) reuniram-se com o Conselho Diretor, em ocasiões distintas em razão de incompatibilidade de agendas, para discussão final sobre as contribuições recebidas na consulta interna a respeito das questões a serem submetidas na Tomada de Subsídios.

Encaminhamentos

A CGRII comprometeu-se a fazer os ajustes finais no texto e circular o documento final para ciência dos diretores.
Nada mais havendo a tratar, as reuniões se deram por encerrada, das quais, para constar, eu, Sabrina F. Maciel Favero, lavrei a presente memória.

SABRINA FERNANDES MACIEL FAVERO

Especialista em Políticas Públicas e Gestão Governamental

Documento assinado eletronicamente por **Sabrina Fernandes Maciel Favero**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 13/05/2022, às 15:50, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código [redacted] no site:
https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Esplanada dos Ministérios, Bloco C, 2º andar — Telefone:

CEP 70046-900 Brasília/DF - https://www.gov.br/planalto/pt-br

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização
Coordenação-Geral de Relações Institucionais e Internacionais

Nota Técnica nº 20/2022/CGN/ANPD

Assunto: **Proposta de realização de Tomada de Subsídios para regulamentação de transferência internacional de dados pessoais, nos termos dos arts. 33 e 35 da LGPD da Lei nº 13.709, de 14 de agosto de 2018.**

1. INTRODUÇÃO

1.1. O item 9 da agenda regulatória bianual 2021-2022 da Autoridade Nacional de Proteção de Dados (ANPD), aprovada pela Portaria nº 11, de 27 de janeiro de 2021, trata da regulamentação da transferência internacional de dados pessoais, incluindo a avaliação de nível de proteção de dados de país estrangeiro ou de organismo internacional e a definição do conteúdo de cláusulas-padrão contratuais, dentre outros, nos termos dos artigos 33 a 35 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

1.2. O processo de regulamentação é norteado pelos fundamentos da disciplina da proteção de dados pessoais previstos no art. 2º da LGPD, bem como pelas diretrizes estabelecidas pela Portaria nº 16, de 8 de julho de 2021, que aprova o processo de regulamentação no âmbito da ANPD. O referido instrumento normativo estabelece os procedimentos para elaboração, revisão, implementação, monitoramento e avaliação da regulamentação da Autoridade, dentre as quais consta a etapa de Análise de Impacto Regulatório (AIR).

1.3. De acordo com o estabelecido no art. 14 da referida Portaria, a Análise de Impacto Regulatório (AIR) estabelece mecanismos de participação de especialistas e da sociedade por meio da tomada de subsídios, bem como coleta de dados e informações que a equipe de projeto considerar relevantes.

1.4. A tomada de subsídios consiste, portanto, em importante instrumento regulatório que visa obter elementos, informações e dados relevantes para o processo de regulamentação a partir da escuta dos diferentes *stakeholders* que, possivelmente, serão afetados pela publicação de ato normativo. Realizada ainda no curso da elaboração de proposta normativa, a AIR permite identificar e aprimorar os aspectos significativos à matéria em questão, delimitando os problemas a serem enfrentados e as possíveis alternativas regulatórias.

1.5. Nesse sentido, vale salientar que a tomada de subsídios ora proposta se alinha à recomendação constante do manual *Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório – AIR*[1] publicado pela Casa Civil da Presidência da República:

> ***A boa prática regulatória recomenda que a consulta e o diálogo com os atores interessados no problema regulatório devem começar o mais cedo possível, ainda nos estágios iniciais da AIR**. O objetivo é convidar os atores relevantes a contribuir para melhorar a qualidade da análise que orientará a decisão. Quando envolvidos após já tomada a decisão, a tendência é que estes atores só se debrucem sobre a minuta apresentada, questionando seus dispositivos sem considerar o processo de análise que culminou em sua proposição, mesmo que a AIR seja disponibilizada para consulta junto com o instrumento. [Grifos no original]*

1.6. Em conformidade com o disposto no inciso II, do art. 12, da Portaria nº 16/2021, a equipe de projeto poderá, no exercício de seu poder discricionário, elaborar proposta de Tomada de Subsídios com a finalidade de obter insumos para o processo de regulamentação. A Tomada de Subsídios proposta pode ser aberta ao público ou restrita a convidados, com a finalidade de obter insumos para o processo de regulamentação, por meio do encaminhamento de contribuições escritas ou reuniões técnicas.

1.7. Nessa etapa do processo, pretende-se avaliar a conveniência e a oportunidade da realização de tomada de subsídios para amparar a AIR.

1.8. É o relatório.

2. ANÁLISE

2.1. O Capítulo V da LGPD, que trata especificamente da Transferência Internacional de Dados, apresenta, em seu art. 33, as hipóteses legais que autorizam a transferência internacional de dados pessoais, *in verbis*:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência;
>
> b) cláusulas-padrão contratuais;
>
> c) normas corporativas globais;
>
> d) selos, certificados e códigos de conduta regularmente emitidos;
>
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
>
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> V - quando a autoridade nacional autorizar a transferência;
>
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
>
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
>
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.

2.2. Por sua vez, o art. 35 da LGPD dispõe que a ANPD definirá o conteúdo de cláusulas-padrão contratuais, bem como a verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, descritos no inciso II do caput do art. 33. Adicionalmente, o §1º do art. 35 estabelece que, para a verificação prevista no caput do art. 35, devem ser considerados os requisitos,

condições e garantias mínimas para a observância dos direitos, garantias e princípios da LGPD quando da transferência de dados pessoais para outra jurisdição.

2.3. Assim, é necessário que se discuta, neste momento, a regulamentação dos arts. 33 e 35 da LGPD, de forma que a proteção dos dados pessoais de titulares brasileiros não seja um impedimento à inserção do País na economia global, bem como a inovação e o desenvolvimento econômico não prejudiquem a proteção de um direito fundamental tão apreciado e em solidificação no território nacional.

2.4. Da mesma forma, é relevante considerar possíveis modelos internacionais vigentes que poderão nortear a regulamentação a ser editada pela ANPD, bem como a possibilidade de se estabelecer regramento diferenciado a partir dos modelos existentes.

2.5. Os mecanismos de transferência internacional de dados tornaram-se instrumentos chave para o desenvolvimento da economia digital e, também, para a garantia da efetiva proteção dos dados pessoais ao cruzarem fronteiras. A implementação de várias regulações em proteção de dados ao redor do globo revela a preocupação geral com os fluxos transfronteiriços de dados. Contudo a grande diversidade de modelos de proteção de dados traz consigo a necessidade de um esforço de convergência e interoperabilidade entre esses diferentes sistemas a fim de que tais fluxos sejam permitidos.

2.6. Nesse sentido, as cláusulas-padrão contratuais (CPC) têm sido o mecanismo de transferência internacional de dados mais utilizado mundialmente, funcionando inclusive como ferramenta de convergência entre diferentes sistemas. Isso porque esse mecanismo permite compatibilizar, via instrumento contratual, as regras de proteção de dados de diferentes jurisdições, em especial aquelas do país que exporta os dados pessoais. Ademais, as CPCs podem ser consideradas um instrumento de prateleira e de menor custo de implementação em comparação aos demais. Dessa forma, elas acabam sendo a opção para pequenas e médias empresas.

2.7. Outras opções de mecanismos de transferência internacional de dados não conseguem atender a necessidade urgente de regularizar, de maneira ubíqua, os fluxos transfronteiriços. Por exemplo, as decisões de adequação possuem um processo relativamente moroso além de atenderem apenas às localizações geográficas analisadas na avaliação da adequação. Selos e certificados ainda não foram regulamentados pela Autoridade, dado que a definição dos padrões técnicos mínimos de segurança é tema bastante complexo e está sendo estudado pela ANPD para que sejam aplicados na regulamentação. Códigos de conduta regularmente emitidos, a seu turno, possuem um estreito espectro de utilização. Portanto, dada a urgência dos atores em verem regulamentado algum mecanismo que possibilite a transferência internacional de dados em consonância com a Lei, é natural que as cláusulas-padrão contratuais sejam o primeiro mecanismo a ser normatizado pela ANPD.

2.8. Ademais, há de se considerar que a escolha dos mecanismos que devem ser regulamentados e o momento mais oportuno para sua realização é uma decisão que possui aspectos de mérito, mas também elementos estratégicos. Se a disponibilização de instrumentos para as transferências internacionais é premente, escolher regulamentar de uma só vez todos os mecanismos previstos no art. 33 da LGPD implicaria uma maior demora em se expedir o regulamento. Por outro lado, é racional considerar em conjunto mecanismos que possuam critérios de análise essencialmente semelhantes, uma vez que essa abordagem otimiza os esforços da ANPD ao mesmo tempo em que organiza os regulamentos de acordo com uma mesma lógica.

2.9. Assim, dado que há urgência em se regulamentar o tema, que iniciar pelas cláusulas-padrão contratuais é a opção que disponibiliza à sociedade o mecanismo de maior alcance, e que a regulamentação de cláusulas contratuais específicas e de normas corporativas globais segue requisitos fundamentalmente similares aos das CPCs, a ANPD optou por incluir nesse primeiro bloco de regulamentação esses três instrumentos, o que denominou de “instrumentos contratuais”.

2.10. Nesse contexto, a equipe de projeto considera oportuna e conveniente a realização de Tomada de Subsídios para o presente projeto de regulamentação com o objetivo de receber contribuições dos diferentes agentes econômicos, titulares de dados pessoais e dos demais afetados pelo

problema regulatório relativo à transferência internacional de dados.

2.11. Para tanto, as contribuições à tomada de subsídios devem ocorrer em forma de respostas às questões sobre:

a) a) o conteúdo das cláusulas-padrão contratuais, previstas no art. 33, II, b, e

b) b) a regulamentação necessária para utilização das cláusulas contratuais específicas e das normas corporativas globais, nos termos do art. 33, II, a, c e art. 35, *caput*, e §§1º, 2º e 5º.

c) As informações colhidas com a Tomada de Subsídios serão aplicadas pela ANPD na elaboração de AIR sobre o tema.

2.12. Assegurados os direitos dos titulares de dados, o livre fluxo de dados é algo extremamente desejável ao desenvolvimento da economia digital. A LGPD permite que isso ocorra após proferida uma decisão de adequação. O grau de proteção adequado à LGPD envolve a análise de todos os aspectos arrolados no art. 34 para que se entenda que a estrutura de proteção de dados estrangeira é compatível com essa lei, o que carece de regulamentação pela ANPD e demandará um tempo substantivo de implementação.

2.13. Por adotar regime de exceção para as transferências internacionais de dados pessoais, a LGPD exige que, na ausência de uma decisão de adequação, sejam necessárias salvaguardas adicionais, como as previstas no inciso II do art. 33: cláusulas contratuais específicas; cláusulas-padrão contratuais; normas corporativas globais; ou selos, certificados e códigos de conduta regularmente emitidos. O problema que se pretende resolver com o regulamento objeto desta tomada de subsídios é disponibilizar meios eficazes e rápidos capazes de permitir as transferências internacionais de maneira adequada, na ausência de decisão de adequação abrangendo o país destino da transferência.

2.14. Dada a complexidade do tema das transferências internacionais e a diversidade de opções adotadas para lidar com ele, a equipe de projetos avaliou que seria fundamental consultar as partes interessadas e a sociedade de maneira ampla. Sabe-se que a maioria dos processos de regulamentação do tema ao redor do mundo se utilizaram de consultas semelhantes, de forma que essa etapa se inspira nas boas práticas regulatórias internacionais.

2.15. Assim, a equipe de projeto elaborou os questionamentos (SEI nº 3370435) com o fito de auxiliar a ANPD na elaboração de AIR. Em todas as perguntas, para possibilitar a adequada compreensão da ANPD sobre a resposta, solicitam-se as devidas justificativas, com dados e informações que as suportem.

3. **ANEXOS**

3.1. Aviso da Tomada de Subsídio nº 2/2022 (SEI nº 3368496);

3.2. Perguntas da tomada de subsídios nº 2/2022 (SEI nº 3370435)

4. **REFERÊNCIAS**

[1] Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório – AIR / Subchefia de Análise e Acompanhamento de Políticas Governamentais [et al.]. Brasília: Presidência da República, 2018.

5. **CONCLUSÃO**

5.1. Diante do exposto, a equipe de projeto, em conformidade com os arts. 12, inciso II, 18 e 19 da Portaria nº 16/2021, considera conveniente e oportuna a realização de tomada de subsídios, do tipo aberta ao público, a ser efetivada por meio de encaminhamento de contribuições escritas pela

Plataforma Participa + Brasil, com prazo de contribuição de 30 (trinta) dias, a contar da publicação do aviso da tomada de subsídios no Diário Oficial da União. Ressalta-se que a Tomada de Subsídios não representa o posicionamento final da ANPD.

5.2. À consideração superior.

Brasília, 17 de maio de 2022.

DAVI TEÓFILO NUNES OLIVEIRA
Assistente Técnico

SABRINA FERNANDES MACIEL FAVERO
Especialista em Políticas Públicas e Gestão Governamental

FERNANDO DE MATTOS MACIEL
Coordenador de Normatização

CAROLINE NAZARÉ DOS SANTOS CHUCRE KAPPEL
Coordenadora de Relações Institucionais

De acordo. Encaminhe-se o Aviso para assinatura do Diretor Presidente da ANPD e, posteriormente, para Secretaria Geral para providências referentes à publicação no Diário Oficial da União.

Brasília, 17 de maio de 2022.

RODRIGO SANTANA DOS SANTOS
Coordenador-Geral de Normatização, substituto

JULIANA MULLER REIS JORGE
Coordenadora-Geral de Relações Institucionais e Internacionais

Documento assinado eletronicamente por **Sabrina Fernandes Maciel Favero**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 17/05/2022, às 11:43, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Fernando de Mattos Maciel**, **Coordenador(a)**, em 17/05/2022, às 11:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)-Geral substituto(a)**, em 17/05/2022, às 11:45, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Davi Teófilo Nunes de Oliveira**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 17/05/2022, às 11:49, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Caroline Nazaré dos Santos Chucre Kappel**, **Assessor(a) Técnico(a)**, em 17/05/2022, às 14:22, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

Documento assinado eletronicamente por **Juliana Muller Reis Jorge**, **Coordenador(a)-Geral**, em 17/05/2022, às 14:41, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted] A autenticidade do documento pode ser conferida informando o código [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Despacho DOU nº 3368496/2022-CGN/ANPD

PRESIDÊNCIA DA REPÚBLICA

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

AVISO DE TOMADA DE SUBSÍDIOS Nº 02/2022

O DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), nos termos do disposto nos arts. 14, I e 18 da Portaria nº 16, de 8 de julho de 2021, comunica que será realizada Tomada de Subsídios por meio da plataforma Participa Mais Brasil, conforme informações a seguir:

Objetivo: obter contribuições para subsidiar a elaboração de minuta de regulamento sobre transferências internacionais de dados pessoais, a partir da coleta de colaborações escritas da sociedade.

As sugestões deverão ser enviadas eletronicamente até o dia 17 de junho de 2022, exclusivamente por meio da plataforma Participa Mais Brasil pelo link: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional.

As perguntas da tomada de subsídios também estarão disponíveis no portal da ANPD (www.anpd.gov.br).

WALDEMAR GONÇALVES ORTUNHO JÚNIOR

DIRETOR-PRESIDENTE DA ANPD

Documento assinado eletronicamente por **Waldemar Gonçalves Ortunho Junior**, **Diretor-Presidente**, em 17/05/2022, às 15:52, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted] utenticidade do documento pode ser conferida informando o código verificador [redacted] site: ps://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Tomada de subsídios para regulamentação de transferência internacional de dados

Os mecanismos de transferência internacional de dados se tornaram instrumentos-chaves tanto para a efetiva proteção dos direitos dos titulares de dados quanto para o desenvolvimento da economia digital e do comércio internacional. Dada a urgente necessidade de regulamentação de tais mecanismos, a ANPD planeja expedir o regulamento referente ao tema em etapas. A primeira delas terá como escopo os instrumentos contratuais de transferências internacionais de dados pessoais, previstos no art. 33 inciso II, alíneas a, b e c, da LGPD, que são as cláusulas-padrão contratuais, as cláusulas contratuais específicas e as normas corporativas globais.

Para facilitar a compreensão das perguntas, considere-se "exportador" o agente de tratamento localizado no Brasil que transferirá os dados pessoais para um importador localizado em outro país e "importador", o agente de tratamento situado fora do território nacional que receberá esses dados do exportador.

A ANPD considera bem-vindas contribuições a quaisquer das perguntas a seguir, não sendo obrigatória a elaboração de respostas a todos os questionamentos abaixo elencados.

1) Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?

2) Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?

3) Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?

4) Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?

5) Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê?

    a. cláusulas-padrão contratuais;

    b. cláusulas contratuais específicas; e

    c. normas corporativas globais.

6) Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?

7) As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?

8) Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?

9) É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?

10) Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?

11) Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?

12) Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?

13) Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?

14) Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?

15) Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?

16) Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?

17) Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?

18) Quais as melhores alternativas para resolver as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?

19) Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?

20) Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

00261.000968/2021-06

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Gabinete do Diretor-Presidente

Brasília, 17 de maio de 2022.

À Coordenação-Geral de Administração - CGA.

Assunto: **Publicação no DOU.**

1. Solicito a publicação no Diário Oficial da União do Despacho relativo ao Aviso de Tomada de Subsídios nº 02/2022 (SEI nº 3368496).

MARIANA TALOUKI
Chefe de Gabinete

Documento assinado eletronicamente por **Mariana Almeida de Sousa Talouki**, **Chefe de Gabinete**, em 17/05/2022, às 16:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted] A autenticidade do documento pode ser conferida informando o código [redacted] site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Administração

Brasília, 17 de maio de 2022.

Ao Setor de Publicação de Atos Oficiais da Coordenação de Documentação - CODOC-PUBL

Assunto: **Publicação em DOU**

1. Encaminho para providências de publicação no DOU o Aviso de Tomada de Subsídios nº 02/2022 (SEI nº 3368496).

Atenciosamente,

VINICIUS CARVALHO REIS
Coordenador-Geral de Administração

Documento assinado eletronicamente por **Vinicius Carvalho Reis**, **Coordenador(a)-Geral**, em 17/05/2022, às 17:08, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código verificador [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 18/05/2022 | Edição: 93 | Seção: 3 | Página: 2

Órgão: Presidência da República/Autoridade Nacional de Proteção de Dados

AVISO DE TOMADA DE SUBSÍDIOS Nº 2/2022

O DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), nos termos do disposto nos arts. 14, I e 18 da Portaria nº 16, de 8 de julho de 2021, comunica que será realizada Tomada de Subsídios por meio da plataforma Participa Mais Brasil, conforme informações a seguir:

Objetivo: obter contribuições para subsidiar a elaboração de minuta de regulamento sobre transferências internacionais de dados pessoais, a partir da coleta de colaborações escritas da sociedade.

As sugestões deverão ser enviadas eletronicamente até o dia 17 de junho de 2022, exclusivamente por meio da plataforma Participa Mais Brasil pelo link: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional.

As perguntas da tomada de subsídios também estarão disponíveis no portal da ANPD (www.anpd.gov.br).

WALDEMAR GONÇALVES ORTUNHO JÚNIOR

Este conteúdo não substitui o publicado na versão certificada.

00261.000968/2021-06

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Secretaria-Geral

Brasília, 18 de maio de 2022.

Ao Gabinete do Diretor Presidente

Assunto: **Link de documento para publicação de matéria**

1. Encaminho *link* de publicação dos documentos acerca da Tomada de Subsídio nº 02 que trata da Regulamentação de Transferência Internacional de Dados com vistas à produção e publicação de matéria do site ANPD:

- Nota Técnica nº 20/2022/CGN/ANPD: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000968_2021_06-nota-tecnica.pdf
- Perguntas da Tomada de Subsídios: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000968_2021_06-perguntas.pdf
- Aviso de Tomada de Subsídio: https://www.in.gov.br/en/web/dou/-/aviso-de-tomada-de-subsidios-n-2/2022-400762386

Núbia Augusto de Sousa Rocha
Secretária-Geral

Documento assinado eletronicamente por **Nubia Augusto de Sousa Rocha**, **Secretária-Geral**, em 18/05/2022, às 10:00, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted] A autenticidade do documento pode ser conferida informando o código [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Publicações da ANPD

Publicado em 28/05/2021 10h25 Atualizado em 18/05/2022 08h32

Compartilhe:

A ANPD busca orientar os diversos agentes sobre o tema de proteção de dados pessoais. Para isso, criado o repositório de publicações, dentre eles guias e documentos técnicos.

O objetivo dessas publicações é registrar a memória institucional sobre os temas e servir de referência para titulares de dados pessoais, agentes de tratamento e sociedade em geral.

Publicações

Outras publicações

- Artigo "Meus dados vazaram, e agora?" - considerações e orientações da ANPD a respeito do assunto. Publicado em 10/02/2021.

Regulamentações da ANPD

- PORTARIA Nº 1, DE 8 DE MARÇO DE 2021 - estabelece o Regimento Interno da ANPD
- PORTARIA Nº 15, DE 2 DE JULHO DE 2021 - institui o Comitê de Governança da Autoridade Nacional de Proteção de Dados.
- PORTARIA Nº 16, DE 8 DE JULHO DE 2021 - aprova o processo de regulamentação no âmbito da ANPD
- RESOLUÇÃO CD/ANPD Nº 1, DE 28 DE OUTUBRO DE 2021 - Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.
- RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022 - Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte.

Notas Técnicas

- Nota Técnica nº 46/2022/CGF/ANPD- Manifestação técnica da Coordenação-Geral de Fiscalização acerca da divulgação dos microdados do Enem e de censos escolares pelo INEP à luz da Lei nº 13.709, de 14 de agosto de 2018 — Lei Geral de Proteção de Dados Pessoais (LGPD).

Relatório de Análise de Impacto Regulatório - AIR

- Relatório de Análise de Impacto Regulatório emitido no processo de proposição do Regulamento de Fiscalização da ANPD
- Relatório de Análise de Impacto Regulatório emitido no processo de proposição do Regulamento de Microempresas, empresas de pequeno porte, startups e pessoas físicas que tratam dados pessoais

Tomadas de Subsídios

- Tomada de Subsídios nº 02- Regulamentação de Transferência Internacional de Dados Pessoais

1. Nota Técnica nº 20/2022/CGN/ANPD
2. Lista de Perguntas da Tomada de Subsídio
3. Aviso de Tomada de Subsídio

Documentos institucionais

Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

- RESOLUÇÃO CNPD Nº 1, DE 6 DE MAIO DE 2022- estabelece o Regimento Interno do CNPD. Acesse aqui.

Compartilhe:

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Secretaria-Geral

Brasília, 18 de maio de 2022.

À Coordenação-Geral de Normatização

Assunto: **Publicação dos documentos referente à Tomada de Subsídios nº 02/2022**

1. Encaminho documento 3378066 contendo a publicação dos documentos relativos à Tomada de Subsídios nº 02/2022 na página "Documentos e Publicações" no site da ANPD.

Núbia Augusto de Sousa Rocha
Secretária-Geral

Documento assinado eletronicamente por **Nubia Augusto de Sousa Rocha**, **Secretária-Geral**, em 18/05/2022, às 17:05, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código [redacted] o site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

Tomada de subsídios sobre transferências internacionais de dados pessoais inicia nesta quarta-feira

Publicado em 18/05/2022 11h02 Atualizado em 18/05/2022 11h28

Nesta quarta-feira (18/05), a Autoridade Nacional de Proteção de Dados (ANPD) inicia a tomada de subsídios para coleta de colaborações da sociedade para a elaboração do regulamento sobre transferências internacionais de dados pessoais.

As colaborações deverão ser enviadas **exclusivamente** por meio da plataforma *Participa Mais Brasil*, na opção *Opine Aqui* até o dia **17 de junho de 2022** (sexta-feira).

As transferências internacionais de dados tornaram-se instrumentos chave para o desenvolvimento da economia digital. Nesse contexto, a regulamentação dos mecanismos que viabilizam tais transferências é importante não apenas para viabilizar a inserção competitiva de empresas brasileiras em cadeias globais de valor, como também para garantir a efetiva proteção dos titulares e de seus dados pessoais.

Tendo em vista a complexidade do tema, a tomada de subsídios é um importante instrumento regulatório que visa obter elementos para a elaboração de normativos.

Na tomada de subsídios são coletadas informações e dados relevantes para o processo de regulamentação a partir da escuta dos diferentes setores interessados que, possivelmente, serão afetados pela publicação do ato normativo.

A autoridade confia que a Tomada de Subsídios contribuirá de forma relevante para a elaboração da regulamentação sobre transferências internacionais de dados pessoais, cuja minuta será objeto de consulta e audiência pública em breve.

Read the text above in english *here*.

Confira as perguntas abaixo:

A ANPD considera bem-vindas contribuições a quaisquer das perguntas a seguir, não sendo obrigatória a elaboração de respostas a todos os questionamentos abaixo elencados:

1) Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?

2) Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?

3) Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?

4) Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?

5) Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê?

a. cláusulas-padrão contratuais;

b. cláusulas contratuais específicas; e

c. normas corporativas globais.

6) Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?

7) As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado? Anexo - Perguntas da Tomada de Subsídios (3370435) SEI 00261.000968/2021-06 / pg. 1

8) Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?

9) É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?

10) Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?

11) Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?

12) Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?

13) Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?

14) Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?

15) Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?

16) Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?

17) Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?

18) Quais as melhores alternativas para resolver as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?

19) Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?

20) Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

Com essa tomada de subsídios, a ANPD inicia o cumprimento do item 9 da agenda regulatória bianual 2021-2022 da Autoridade, aprovada pela Portaria nº 11, de 27 de janeiro de 2021, que trata da regulamentação da transferência internacional de dados pessoais.

Acesse a *Nota Técnica*.

Acesse o *Aviso de Tomada de Subsídios nº 02/2022*.

Acesse a lista de perguntas consolidadas em formato PDF.

CONTEÚDO RELACIONADO

Questions in English - TS.pdf

Compartilhe:

ENC: Tomada de subsídios 2/2022 - Regulamento sobre transferências internacionais de dados pessoais

ANPD - Relacoes Institucionais <relacoes.institucionais@anpd.gov.br>
Sex, 27/05/2022 15:14
Para: ANPD - Normatizacao <normatizacao@anpd.gov.br>

De: Andressa Lin Fidelis <alin@levysalomao.com.br>
Enviado: sexta-feira, 27 de maio de 2022 14:14
Para: ANPD - Relacoes Institucionais <relacoes.institucionais@anpd.gov.br>; ANPD - International <international@anpd.gov.br>
Cc: Mariana Tavares de Araujo [redacted]
Assunto: RES: Tomada de subsídios 2/2022 - Regulamento sobre transferências internacionais de dados pessoais

Prezados,

Em complemento à mensagem abaixo, gostaríamos de ressaltar que a solicitação de extensão de prazo seria para que o International Comments and Policy Committee, o qual lidera os temas de advocacia internacional relacionados a concorrência, defesa do consumidor e privacidade de dados da American Bar Association (ABA), a maior associação de advogados do mundo, apresentasse suas sugestões e contribuições. A ABA é uma entidade com membros de diversos países, o que torna o processo de coleta de contribuições complexo e um pouco lento.

A ABA tem muito interesse em contribuir para o regulamento em referência, razão pela qual solicita 2 semanas de extensão no prazo, para que possa apresentar sua contribuição até dia 1º de julho de 2022.

Atenciosamente,
Andressa.

LEVY & SALOMÃO
ADVOGADOS
www.levysalomao.com.br

Andressa Lin Fidelis
OAB-SP 305.270
Av. Brigadeiro Faria Lima, 2601
12º andar
01452-924 São Paulo SP Brasil
T +55 11 3555 5022

De: Andressa Lin Fidelis
Enviada em: sexta-feira, 27 de maio de 2022 11:02
Para: relacoes.institucionais@anpd.gov.br; international@anpd.gov.br
Cc: Mariana Tavares de Araujo [redacted]
Assunto: Tomada de subsídios 2/2022 - Regulamento sobre transferências internacionais de dados pessoais

Prezados Juliana e equipe,

Com relação à Tomada de Subsídios nº 2/2022 para a elaboração de minuta de regulamento sobre transferências internacionais de dados pessoais, cujo prazo para envio de colaborações se encerra dia 17.06.2022, gostaríamos de perguntar se seria possível solicitar uma extensão de prazo para submetermos nossa contribuição.

Em caso positivo, devemos enviar a solicitação para os endereços de e-mails aqui copiados ou para outro destinatário?

Muito obrigada,
Andressa.

LEVY & SALOMÃO
ADVOGADOS
www.levysalomao.com.br

Andressa Lin Fidelis
OAB-SP 305.270

Av. Brigadeiro Faria Lima, 2601
12º andar
01452-924 São Paulo SP Brasil
T +55 11 3555 5022

Carta n. 5/2022/DPBR

DataPrivacyBR Research

São Paulo, 25 de maio de 2022

À Presidência da Autoridade Nacional de Proteção de Dados Pessoais
Sr. Diretor Presidente Waldemar Gonçalves Ortunho Junior
presidencia@anpd.gov.br

C/C
Coordenação Geral de Relações Institucionais

Coordenação Geral de Normatização

Assunto: Pedido de prorrogação de prazo da Tomada de Subsídios n. 2/2022

Prezado Senhor Presidente,

Prezados membros do Conselho Diretor,

Prezados membros da Coordenação Geral de Normatização e Coordenação Geral de Relações Institucionais e Internacionais,

A partir da publicização da Tomada de Subsídios 2/2022, sobre transferências internacionais de dados pessoais, o Data Privacy Brasil tem se mobilizado para contribuir com a Autoridade, como tem feito em todas as tomadas de subsídios e consultas públicas. Como um espaço de articulação entre duas pessoas jurídicas, temos unido esforços entre a Escola **Data Privacy Brasil Ensino** e a **Associação Data Privacy Brasil de Pesquisa**, organização sem fins lucrativos, com o objetivo de contribuir com o aprimoramento das normas que pretendem dar concretude aos objetivos da Lei Geral de Proteção de Dados Pessoais (Lei 13.709/2018).

Entretanto, o prazo de 30 dias estabelecido pela Autoridade para recebimento de contribuições se mostra prejudicial a uma participação qualificada e significativa de toda a sociedade civil. As 20 perguntas trazidas pela tomada de subsídios exigem um trabalho de pesquisa de fôlego para que as contribuições sejam frutíferas à Autoridade.

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

DataPrivacyBR Research

Destacamos que, no período do prazo, importantes e significativos eventos nacionais e internacionais para a governança da internet e para a regulação de proteção de dados pessoais estarão acontecendo. Dentre eles a CPDP - Computers, Privacy and Data Protection conference, a RightsCon e o 12º Forum da Internet no Brasil. Este último, inclusive, com um painel intitulado "Diretrizes para transferência internacional de dados: contribuição multissetorial para a agenda da ANPD". Além disso, a participação nos eventos demanda uma intensa dedicação e comprometimento na carga de trabalho dos membros das organizações participantes e que buscam contribuir com a qualificação do debate público.

A partir do exposto, solicitamos que a Autoridade prorrogue por, pelo menos, mais 30 dias o prazo para envio de contribuições para a tomada de subsídios aberta. Com esse prazo adicional, espera-se que os debates e proposições levantadas nestes importantes fóruns possam ser assimiladas, absorvidas e incorporadas pela sociedade civil em suas contribuições.

Atenciosamente,

Rafael Zanatta
Diretor da Associação Data Privacy Brasil de Pesquisa

Endereço
Alameda Santos, 1293
3º Andar – Jardim Paulista
São Paulo – SP
CEP 01419-904

Contato
contato@dataprivacybr.org

dataprivacybr.org

ENC: Invite - ANPD Public Consultation on International Data Transfers

Mariana Almeida de Sousa Talouki <[redacted]
Ter, 14/06/2022 11:15

[redacted]

Cc: ANPD - Normatizacao <normatizacao@anpd.gov.br>;Miriam Wimmer
[redacted]

Pessoal,

Segue pedido de extensão de prazo.

Acho que vale a pena considerar, tendo em vista a grande ajuda que o CIPL pode dar.

Atenciosamente,

Logo da Autoridade Nacional de Proteção de Dados - ANPD
Mariana A. de S. Talouki
Chefe de Gabinete
Autoridade Nacional de Proteção de Dados - ANPD
Tel: +55 61 3411.4682

[redacted]

Enviado: terça-feira, 14 de junho de 2022 11:12
Para: ANPD - International <international@anpd.gov.br>; Mariana Almeida de Sousa Talouki
[redacted]
Assunto: FW: Invite - ANPD Public Consultation on International Data Transfers

Dear Miriam, Mariana and ANPD colleagues:

CIPL is currently preparing comments to the below referenced consultation on cross-border data transfers. The comments are due this Friday and we are doing our best to finalize them by that deadline in parallel to many other competing commitments this week and we also still need to have them translated into Portuguese. It would be very helpful if we could get an extension, maybe until the end of next week. Would that be possible?

Thank you very much for your consideration!

Kind regards,

Markus

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Markus B. Heyder
VP and Senior Policy Counselor
Centre for Information Policy Leadership
mheyder@huntonak.com

Hunton Andrews Kurth LLP
2200 Pennsylvania Avenue, NW
Washington, DC 20037
DIR: 202 419 2005
MOB: 202 368 0138
TEL: 202 955 1500
FAX: 202 778 2201
www.informationpolicycentre.com

This communication is confidential. If you are not an intended recipient, please advise by return email immediately and then delete this message, including all copies and backups.

From: ANPD - International <international@anpd.gov.br>
Sent: 26 May 2022 13:51
To: ANPD - International <international@anpd.gov.br>
Subject: Invite - ANPD Public Consultation on International Data Transfers

Caution: This email originated from outside of the firm.

Dear Sir or madam,

International data transfer mechanisms have become a key instrument both for the adequate protection of data subjects' rights and for the development of the digital economy and international trade.

In Brazil, ANPD holds the mandate to issue such regulation according to our General Data Protection Law (LGPD).

The regulation process occurs in stages and one of our first steps is the Call for contributions. The aim is to obtain elements for the elaboration of regulations by listening to the different interested sectors that might be affected by the publication of the normative act.

With this call for contribution, the ANPD begins compliance with item 9 of the Authority's 2021 regulatory agenda 2021-2022.

In this context we would like to invite you to provide contibutions through the *Opine Aqui* option at the *Participa Mais Brasil* platform (https://www.gov.br/participamaisbrasil/consult) until Friday, June 17th, 2022.

Participa + Brasil - Página Inicial

Bem Vindos

www.gov.br

Finally ANPD is available in case there are any questions via the **normatizacao@anpd.gov.br** email address.

Kind regards,

Coordenação-Geral de Relações Institucionais e Internacionais - CGRII
Autoridade Nacional de Proteção de Dados - ANPD
Tel: +55 61 34114679

00261.000968/2021-06

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Brasília, 14 de junho de 2022.

À Secretaria-Geral da Autoridade Nacional de Proteção de Dados

Assunto: **Prorrogação de prazo de tomada de subsídios**

1. Trata-se ao pedido de dilação de prazo para recebimento de contribuições no âmbito da tomada de subsídios sobre a norma de transferência internacional de dados feito pela Associação Data Privacy Brasil de Pesquisa (SEI nº 3408465), pelo escritório Levy & Salomão Advogados (SEI nº 3405450) e pelo CIPL - Centre for Information Policy Leadership (SEI nº 3436135).

2. A Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados (LGPD), e o Decreto 10.474, de 26 de agosto de 2020, determinam que os regulamentos e normas editados pela ANPD devem ser precedidos de consulta pública e Análise de Impacto Regulatório. Já o Regimento Interno da ANPD estabelece, em seu art. 6º, § 5º, que, na fixação dos prazos para a apresentação de críticas e sugestões às consultas públicas, a ANPD deverá considerar, entre outros, a complexidade, a relevância e o interesse público da matéria em análise.

3. Assim, considerando que o pedido de prorrogação mencionado encontra amparo na legislação, visto que a temática relativa à transferência internacional de dados possui alta relevância e significativa complexidade, podendo, portanto, ensejar prazo majorado no período de tomada de subsídios para análise mais pormenorizada do tema, esta Coordenação-Geral de Normatização defere os pedidos formulados e prorroga o período de tomada de subsídios por mais 13 dias, até o dia 30 de junho de 2022.

4. Assim, encaminha-se o presente processo à Secretaria-Geral da ANPD para publicação no boletim interno caso necessário.

ISABELA MAIOLINO
Coordenadora-Geral de Normatização

Documento assinado eletronicamente por **Isabela Maiolino**, **Coordenador(a)-Geral**, em 14/06/2022, às 17:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código verificador [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

AVISO DE TOMADA DE SUBSÍDIOS Nº 02/2022

PRORROGAÇÃO DE PRAZO

O DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), nos termos do disposto nos arts. 14, I e 18 da Portaria nº 16, de 8 de julho de 2021, comunica a prorrogação do prazo para apresentação de sugestões no âmbito da Tomada de Subsídios nº 02/2022.

As sugestões deverão ser enviadas eletronicamente até o dia 30 de junho de 2022, exclusivamente por meio da plataforma Participa Mais Brasil pelo link: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional.

As perguntas da tomada de subsídios também estarão disponíveis no portal da ANPD (www.anpd.gov.br).

WALDEMAR GONÇALVES ORTUNHO JÚNIOR

DIRETOR-PRESIDENTE DA ANPD

Documento assinado eletronicamente por **Waldemar Gonçalves Ortunho Junior**, **Diretor-Presidente**, em 14/06/2022, às 18:06, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código verificador [redacted] no site:
https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

PRESIDÊNCIA DA REPÚBLICA
Autoridade Nacional de Proteção de Dados
Secretaria-Geral

Brasília, 14 de junho de 2022.

Ao Protocolo-Central

Assunto: **Encaminhamento de publicação ao Diário Oficial da União**

1. Solicita-se publicação do documento SEI 3437000 na seção 3 do Diário Oficial da União de 15/06/2022.

Atenciosamente,

Renata de Castro Ferreira dos Santos

Assessora Técnica

Documento assinado eletronicamente por **Renata de Castro Ferreira dos Santos**, **Assessor(a) Técnico(a)**, em 14/06/2022, às 18:12, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020. .

[redacted]

A autenticidade do documento pode ser conferida informando o código verificador [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 15/06/2022 | Edição: 113 | Seção: 3 | Página: 2

Órgão: Presidência da República/Autoridade Nacional de Proteção de Dados

AVISO

TOMADA DE SUBSÍDIOS Nº 2/2022

PRORROGAÇÃO DE PRAZO

O DIRETOR-PRESIDENTE DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), nos termos do disposto nos arts. 14, I e 18 da Portaria nº 16, de 8 de julho de 2021, comunica a prorrogação do prazo para apresentação de sugestões no âmbito da Tomada de Subsídios nº 02/2022.

As sugestões deverão ser enviadas eletronicamente até o dia 30 de junho de 2022, exclusivamente por meio da plataforma Participa Mais Brasil pelo link: https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional.

As perguntas da tomada de subsídios também estarão disponíveis no portal da ANPD (www.anpd.gov.br).

WALDEMAR GONÇALVES ORTUNHO JÚNIOR
Diretor-Presidente da ANPD

Este conteúdo não substitui o publicado na versão certificada.

Contribuições CNT - Tomada de Subsídios sobre Transferência Internacional
Bruno Lustosa Rodrigues <brunorodrigues@cnt.org.br>
Seg, 20/06/2022 08:24
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Cc:

- João Guilherme Vogado Abrahao <guilhermeabrahao@cnt.org.br>

1 anexos (855 KB)
Contribuições CNT - Regulamento sobre transferências internacionais de dados pessoais.pdf;
Boa noite,

Segue anexo arquivo com contribuições da Confederação Nacional de Transporte – CNT para a Tomada de Subsídios sobre Transferência Internacional. A contribuição foi feita no site do https://www.gov.br/participamaisbrasil/tomada-de-subsidios-transferencia-internacional. Enviamos o arquivo para garantir a participação.

Atenciosamente,

BRUNO LUSTOSA RODRIGUES
Assessor
Diretoria de Relações Institucionais

(61) 2196-5826
brunorodrigues@cnt.org.br
SAUS Quadra 1 - Bloco J - Ed. Clésio Andrade – Brasília/DF - CEP: 70.070-944

1) Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?

O maior obstáculo para as empresas que transferem dados do Brasil para outros países, assim como na relação inversa, é a falta de regulação das salvaguardas previstas no art. 33 da LGPD, as quais devem ser observadas pelos agentes de tratamento quando da realização de transferência internacional.

Deste modo, apenas os seguintes mecanismos do art. 33 é que, em tese, poderiam ser utilizados imediatamente, sem depender dessa regulação complementar:

(i) para proteção da vida ou da incolumidade física do titular ou de terceiros (art. 33, IV);
(ii) decorrentes do consentimento específico e em destaque do titular (art. 33, VIII)e;
(iii) para o cumprimento de obrigação legal ou regulatória pelo controlador; execução de contrato ou tratativas preliminares; e exercício regular de direitos em processo judicial, administrativo ou arbitral (arts. 33, IX cc. art. 7º, II, V e VI).

Na prática, essas hipóteses não se enquadram na maioria das transferências de dados internacionais, que ocorrem, via de regra, entre empresas do mesmo grupo para viabilizar a prestação de um determinado serviço ou execução de uma determinada atividade, ou em razão da gestão centralizada, ou pelo fato de contratarem serviços de nuvem para armazenar as informações da companhia, e cujo servidor esteja localizado no exterior.

Nesse contexto, as empresas se veem obrigadas a utilizarem cláusulas contratuais que buscam garantir os mesmos direitos e garantias aos titulares que tiveram seus dados tratados no Brasil, mesmo quando esses dados são exportados.

Neste contexto, para o agente situado no Brasil não haverá critérios objetivos e parâmetros a serem considerados que facilitem a negociação dessas cláusulas contratuais, o que aumenta a assunção de risco no caso concreto.

Por outro lado, quando o agente localizado no Brasil recebe um instrumento jurídico elaborado com base em parâmetros provenientes de outro país (por exemplo, países da União Europeia), não tem segurança acerca do que deve aceitar ou não para estabelecer uma aplicação harmônica do disposto no cenário internacional com aquilo que é admitido pela LGPD.

Esse cenário aumenta a insegurança das partes na condução de seus negócios, considerando a ausência de parâmetros a serem observados na relação com seus parceiros, além do risco de descumprimento à LGPD nos termos do seu art. 44 da LGPD.

2) Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?

A melhor maneira de garantir a interoperabilidade dos instrumentos contratuais previstos na LGPD (art. 33, II) com os instrumentos contatuais das demais jurisdições, e inclusive promover segurança jurídica no Brasil, seria utilizar o já estabelecido especialmente no cenário europeu para construir e estruturar os parâmetros dos mecanismos de transferência internacional no Brasil, de maneira a possibilitar uma *"harmonização"* do que se estabelecerá no Brasil com o que se utiliza no cenário internacional.
Considerando que a ANPD tem participado de forma ativa em fóruns internacionais de debates, como a Análise de Recomendações da OCDE, Comitê Consultivo da Convenção 108, bem como vem adotando medidas formais de associação (GPA, GPEN e rede ibero-americana) em um esforço de articulação e diálogo com autoridades de outros países e órgãos públicos, a exemplo

da assinatura de Memorando de Entendimento com a Agência Espanhola de Proteção de Dados, em 2021[1], sem prejuízo de parcerias bilaterais com países como EUA, Reino Unido e Alemanha[2].

Logo, em linha com o trabalho que vem sendo realizado por esta Autoridade, faz sentido que os mecanismos de transferência internacional devem ser compatíveis com os mecanismos e salvaguardas do GDPR. Esta medida, inclusive, possibilitará que futuramente seja possível que o Brasil seja abarcado no rol de países com nível de proteção adequado, conforme entendimento da Comissão Europeia[3]. Tal circunstância trará às empresas brasileiras a possibilidade de realização de transferências de dados que envolvam países da União Europeia, sem que seja necessária a adoção de salvaguardas adicionais, na medida em que seria considerada uma transferência capaz de assegurar aos titulares e aos seus dados pessoais o mesmo nível de proteção obtido no tratamento realizado na União Europeia.

Neste sentido, acordos de cooperação técnica e memorandos de entendimento firmados pela ANPD com outros países e autoridades permitirão a adoção de mecanismos de cooperação internacional que facilitem a aplicação das legislações nacionais correspondentes na matéria de proteção de dados pessoais, voltados para o conhecimento e intercâmbio das melhores práticas e experiências, em relação a conflitos de jurisdição com países terceiros.

3) Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?

No cenário europeu, na ausência de adequação do país terceiro que recepcionará os dados pessoais (Artigo 45(3), GDPR), ou seja, caso o país não proporcione grau de proteção de dados pessoais adequado, o membro da União Europeia deverá recorrer a um dos outros mecanismos de salvaguarda previstos na lei para a realização de transferência internacional. A LGPD adota racional semelhante ao estabelecer as salvaguardas apropriadas para a transferência internacional de dados, de modo que a adoção de instrumentos contratuais é uma das possibilidades previstas no art. 33, II da lei.

Neste contexto, entendemos que a escolha do instrumento mais efetivo dependerá da relação firmada entre as partes, bem como da complexidade das operações de tratamento a serem realizadas.

Dentre tais instrumentos, e considerando a prática proveniente do cenário europeu, merecem destaque aqueles previstos nas alíneas "a", "b" e "c" do art. 33, II da LGPD, quais sejam:

a) Normas corporativas globais: no âmbito europeu, as *Binding Corporate Rules*, equivalentes às normas corporativas globais previstas na lei brasileira (art. 33, II, c, LGPD), são regras com caráter vinculante que se aplicam a empresas de um mesmo grupo, para garantir que as transferências internacionais de dados pessoais realizadas na modalidade intragrupo estejam em conformidade com o GDPR.

---

[1] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-assina-memorando-de-entendimento-com-a-agencia-espanhola-de-protecao-de-dados. Acesso em 24/05/2022.

[2] Disponível em: https://www.gov.br/anpd/pt-br/semana-da-protecao-de-dados-2022/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais. Acesso em 24/02/2022.

[3] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,Uruguay%20as%20providing%20adequate%20protection. Acesso em 24/02/2022.

Na prática, sua aplicação pode ser considerada dificultosa, considerando que o grupo empresarial que desejar implementar tal instrumento, deverá submetê-lo a um processo de aprovação da autoridade competente da União Europeia (Article 63, GDPR)[4], de maneira que por envolver filiais situadas em diversos países, é possível que seja necessário obter aprovação de diversas autoridades competentes, o que torna o processo mais moroso e oneroso. Por outro lado, uma vez implementadas, costumam ser mais fáceis de ser mantidas, considerando a completude de informações contidas em seu bojo. Ainda, permitem um nível de flexibilidade maior em relação aos demais mecanismos de transferência, na medida em que a autoridade não precisa aprovar *"non-material updates"*.

b) Cláusulas-padrão contratuais: as SCCs (*Standard Contractual Clauses*) prevista no GDPR, equivalentes às cláusulas-padrão contratuais previstas na LGPD (art. 33, II, b), podem ser utilizadas como estratégia para transferências internacionais intergrupo, ou seja, entre empresas distintas e cujo país terceiro, receptor dos dados, não ofereça níveis de proteção considerados adequados. O 0 previamente pela Autoridade, não é necessário que as empresas despendam tempo excessivo com negociações, visto tratar-se de um modelo fechado, mais seguro e simples.

   Ainda, de acordo com o *IAPP-EY Annual Provacy Governance Report 2019*[5], as SCCs costumam ser particularmente importantes para pequenas e médias empresas que podem não ter recursos suficientes para negociar contratos individualmente com cada parceiro comercial. A mesma pesquisa afirma que no cenário europeu, dentre os mecanismos de transferência internacional, 88% dos stakeholders afirmam utilizar as cláusulas contratuais padrão como salvaguarda principal, sendo estas, portanto, as mais utilizadas pelas empresas no âmbito da GDPR, e para as quais a ANPD pode dedicar particular importância no cenário brasileiro.

   Ainda considerando aspectos provenientes do cenário internacional, impende salientar que embora as SCCs sejam amplamente utilizadas por empresas menores e em casos de compartilhamento bilateral de dados, seu uso por grandes multinacionais pode ser impraticável a depender do contexto e frequência da transferência internacional de dados realizada, tendo em vista que: *(i)* as SCCs podem não ser adequadas para situações em que haja uma rede complexa de atividades de tratamento; (ii) empresas maiores com muitas afiliadas no exterior poderão ter que implementar centenas de SCCs para abranger todas as atividades de transferência internacional realizadas, o que pode ser extremamente custoso; (iii) alguns Estados-Membro da União Europeia exigem formalidades adicionais, como preenchimento e aprovação das SCCs pela autoridade supervisora, tornando o processo moroso e oneroso.[6]

c) Cláusulas Contratuais específicas: em situações que não sejam viáveis normas corporativas globais ou das cláusulas-padrão contratuais, o uso de cláusulas contratuais específicas pode se apresentar como uma salvaguarda eficaz, tendo em vista que são ajustáveis a qualquer tipo de relação e capazes de abranger qualquer nível de complexidade das transferências internacionais. Trata-se, portanto, de um subterfúgio

[4] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. Acesso em 24/05/2022.

[5] Disponível em: https://iapp.org/resources/article/privacy-governance-report/ . Acesso em 24/05/2022.

[6] Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 24/05/2022.

menos oneroso e mais flexível, que pode ser implementado por todas as empresas, independentemente de seu porte.

4) Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?

Os principais benefícios da transferência internacional são os seguintes:

(i) a possibilidade de as partes armazenarem dados internacionalmente (*data centers* situados fora do Brasil), o que repercutirá nos custos do negócio;

(ii) viabilização de transações de exportação/importação, com o estabelecimento de fluxos de dados entre países, instrumento chave para o desenvolvimento da economia digital e da inovação;

(iii) possibilidade de mais serviços oferecidos ao consumidor, com acesso a um número maior de bens a um custo mais baixo, estimulando, assim, a livre concorrência;

(iv) possibilidade de que pequenas empresas também tenham acesso a informações e serviços provenientes do cenário internacional, e possam se manter competitivas no mercado, reduzindo, por exemplo, a necessidade de altos investimentos com infraestrutura digital local.

Os principais impactos relacionados à transferência internacional são os seguintes:

(i) criação de facilitadores à economia, ou, entraves e custos operacionais de modo a inviabilizar modelos de negócio e barrar o desenvolvimento econômico e a inovação dos agentes de tratamento;

(ii) incentivar ou desestimular o fluxo de dados pessoais;

Assim, como alternativa para endereçamento em instrumentos contratuais, a ANPD deve considerar:

(i) adotar parâmetros de fácil aplicação, considerando o porte das empresas e o fluxo de dados que pretendem transferir internacionalmente, de modo que haja harmonia com o contexto internacional, já bem mais maduro em relação a esta temática;

(ii) regular as salvaguardas de modo a possibilitar que estejam em harmonia com o cenário internacional, sobretudo com o cenário europeu, é relevante, ainda, considerando que grande parte do mercado e de *players* internacionais já vêm se estruturando ou já estão estruturados de modo a atender as especificidades da legislação estrangeira, em razão dos seus modelos de negócio e relações estabelecidas com agentes internacionais;

(iii) utilizar paramentos objetivos na regulação do art. 33 da LGPD.

(iv) publicar e contemplar em guia específico orientações, ainda que iniciais, acerca dos mecanismos elencados no art. 33 da LGPD, e os respectivos parâmetros a serem considerados no contexto de utilização de cada instrumento jurídico, inclusive os

papéis dos agentes envolvidos na transferência, e seu nível de autonomia no tratamento e dados pessoais[7];

(v) medidas de segurança que sejam consideradas razoáveis (art. 34, IV, LGPD), bem como critérios a serem observados em relação à transferência internacional, considerando o porte da empresa, a natureza dos dados e as categorias dos titulares envolvidos;

(vi) ANPD deve firmar acordos diplomáticos no âmbito internacional com outras autoridades reguladoras, de modo a viabilizar que sejam admitidos no exterior os instrumentos elaborados pelo Brasil e validados pela Autoridade brasileira.

5) Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê?

a. cláusulas-padrão contratuais: as cláusulas-padrão contratuais, por serem instrumentos jurídicos mais utilizados pelas empresas no cenário europeu e por serem de fácil utilização, merecem destaque no cenário brasileiro, pela ANPD. Isto principalmente para evitar entraves jurídicos e divergências em sua aplicação, já que grande parte de empresas multinacionais já se baseiam nas regras adotadas internacionalmente.

Logo, sugerimos que a ANPD edite um modelo de cláusulas-padrão para transferência internacional de dados pensado para as situações em que já exista em contrato firmado entre as partes a previsão de aplicação das cláusulas-tipo da Comissão Europeia, ou seja, um rol de disposições complementares − mas não conflitantes − com as europeias.

Nesta linha, sugerimos que na elaboração das cláusulas-padrão brasileiras, haja observância dos critérios estabelecidos no art. 46, II, c, do GDPR, além de documentos já disponibilizados pelo EDPB, inclusive um Q&A, acerca da aplicação e utilização desses mecanismos de transferência[8]. Sugerimos, ainda, a definição de parâmetros de utilização que não sejam excessivamente burocráticos e acabem tornando o uso do documento inviável para empresas globais. Recomendamos, também, que a estruturação das cláusulas-padrão se dê de forma clara e concisa para que empresas de pequeno porte possam utilizar sem tantos entraves, e para que não tenham dificuldades de compreensão.

Cumpre ressaltar que, devido sua natureza, as cláusulas-padrão contratuais, ao menos no cenário europeu e conforme recomendações da Comissão Europeia[9], não podem vincular as autoridades públicas de países terceiros, uma vez que estas não são parte signatária do contrato. Consequentemente, os exportadores de dados podem ter de agregar às garantias constantes das referidas cláusulas-padrão medidas complementares para assegurar o cumprimento do nível de proteção exigido pela legislação da União Europeia quando o dado pessoal for tratado por um determinado país terceiro, circunstância que também pode tornar-se necessária no Brasil.

[7] Disponível em: https://gdpr.eu/what-is-data-processing-agreement/. Acesso em 25/05/2022.

[8] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en . Acesso em 26/06/2022.

[9] Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE

Quanto à estrutura a ser utilizada, a Comissão Europeia concebeu as SCCs para serem instrumentos dinâmicos e adaptáveis compostos por: cláusulas fixas, que se destinam a permanecer inalteradas independentemente das partes a elas submetidas; módulos, adaptáveis ao agente de tratamento (controlador ou operador) que figurará como exportador ou importador; e cláusulas e anexos em branco ("livres"), que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados, entre outras). É nesse sentido que recomendamos que a ANPD siga na elaboração do referido documento, de modo a serem dinâmicos e adaptáveis conforme a necessidade das partes envolvidas na transferência internacional.

É importante mencionar ainda que, em razão de muitas empresas já utilizarem DPAs para regerem uma relação controlador-operador, caso elas também utilizem SCCs, em caso de divergência, os termos das SCCs prevalecerão sobre os do DPA ou sobre qualquer outro instrumento que discipline o tratamento de dados entre as partes[10]. Nesta linha, sugerimos que esta Autoridade Nacional oriente os agentes de tratamento de dados sobre as medidas a serem adotadas em caso de haver divergências entre um contrato inicialmente firmado e as disposições das cláusulas-padrão contratuais.

Ainda, vale mencionar que o EDPB[11] apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas contratuais padrão, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção dos dados pessoais transferidos. É recomendável que esta ANPD também oriente os agentes de tratamento em relação a tais medidas suplementares, o que os auxiliará na implementação de salvaguardas efetivas para garantir a proteção dos dados sob transferência internacional, bem como para garantir sua confidencialidade, disponibilidade e integridade.

Por fim, em linha com a resposta 19, sugere-se que seja incluída uma disposição nas cláusulas contratais padrão quanto à necessidade de o importador promover ao exportador comunicação prévia caso tome conhecimento da necessidade de divulgação de dados pessoais que sejam objeto da transferência internacional para autoridades públicas estrangeiras.

b. cláusulas contratuais específicas;

Ao consultar a legislação europeia sobre a aprovação de cláusulas contratuais específicas, observa-se que os artigos 46 (3) (a), e 46 (4) do GDPR sujeitam o documento a autorização pela autoridade supervisora competente para, posteriormente, submetê-lo ao mecanismo de consistência pelo EDPB.

No entanto, tratando-se de cláusulas contratuais para situações de transferências específicas e não recorrentes, elas deverão descrever de modo claro a relação entre os propósitos do tratamento e a transferência internacional de dados pessoais de forma a facilitar e simplificar a utilização pelo agente. Nesta linha, deve indicar a salvaguarda da LGPD que consubstancia a operação (arts. 33 a 36, da LGPD), especificando a sua finalidade, discriminando as

[10] Cláusula 5ª - COMMISSION IMPLEMENTING DECISION (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[11] Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE.

responsabilidades dos agentes de tratamento e o fluxo de dados, além também de indicar como serão garantidos os direitos e liberdades dos titulares de dados[12].

Em linha com o aplicado no cenário europeu, em caso de qualquer alteração às circunstâncias da transferência internacional, precisará haver a comunicação à Autoridade para sua reavaliação. Contudo, esses fatores podem gerar entraves aos processos de transferência internacional de dados, ao menos enquanto não esclarecido como será realizado.

Especificamente em relação às cláusulas específicas, já que utilizadas para cenários determinados, sugerimos a adoção de critérios que permitam um nível maior de flexibilidade em relação aos demais mecanismos de transferência, adotando, por exemplo, a linha das BCRs, cujas atualizações *"non-material"* não precisariam ser aprovadas pela Autoridade ou mesmo aspectos que, se alterados e caso não conflitem com premissas bases definidas pela Autoridade, dispensariam também referida aprovação.

Em relação à estrutura e conteúdo, um caminho possível seria verificar as antigas SCCs adotadas em 2001 e 2010 e atualmente substituídas, já que eram instrumentos contratuais elaborados para resolver situações específicas, como transferências C2C (entre controladores, no caso das SCCs de 2001) e as transferências C2P (de controladores para operadores, no caso das SCCs de 2010). As novas SCCs adotadas pela Comissão Europeia para transferências de dados pessoais para fora do Espaço Econômico Europeu levam em consideração abordagem diversa e mais abrangente do que as versões anteriores.

Ainda, vale frisar que o EDPB apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas contratuais padrão, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção. É recomendável que esta Autoridade, portanto, também oriente os agentes de tratamento em relação a tais medidas suplementares, o que os auxiliará na implementação de salvaguardas efetivas para garantir a proteção dos dados sob transferência internacional, bem como para garantir sua confidencialidade, disponibilidade e integridade.

Por fim, em linha com a resposta 19, sugere-se que seja incluído como um critério para aprovação de cláusulas contratuais específicas a necessidade de o importador promover ao exportador a comunicação caso tome conhecimento da necessidade de divulgação de dados pessoais que sejam objeto da transferência internacional para autoridades públicas estrangeiras.

c. normas corporativas globais.

Os critérios para elaboração de normas corporativas globais devem levar em conta os critérios para transferência internacional provenientes do cenário internacional, considerando que várias empresas situadas no Brasil têm sede fora do país e já vem adotando critérios da própria Comissão Europeia e GDPR.

Assim, sugerimos a utilização de parâmetros estabelecidos no art. 47 do GDPR, especialmente os relacionados ao conteúdo das normas corporativas globais, contendo em seu bojo aspectos como (i) a estrutura e os contatos do grupo empresarial ou do grupo de empresas envolvidas numa atividade econômica conjunta e de cada uma das entidades que o compõe; (ii) as transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão; (iii) o seu caráter juridicamente vinculativo;

[12] Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/transferencia_internacional.pdf . Acesso em 26/05/2022.

(iv) evidências que demonstrem o compromisso da organização empresarial em observar os princípios previstos no art. 6º da LGPD, sobretudo o princípio da transparência; (v) documentos que evidenciem que os Encarregados de todas as empresas do grupo que aderirem às normas estão alinhados em relação às salvaguardas que deverão ser implementadas para garantir proteção aos dados pessoais submetidos a transferência internacional; (vi) outros documentos que demonstrem a estrutura de governança da organização e seu nível de conformidade.

Além disso, recomenda-se a esta Autoridade que (i) determine para quais contextos serão admitidas normas corporativas globais (a exemplo da União Europeia, há dois tipos de BCRs, as de controlador e as de operador); e (ii) como se dará o processo de submissão do documento e consequente aprovação por esta Autoridade das normas corporativas globais, se assim o entender, seguindo a linha do adotado no contexto europeu e de maneira a estabelecer o máximo possível de diretrizes para que este processo se torne mais simplificado e até mesmo menos moroso para os agentes.

De toda forma, o material disponibilizado no site da Comissão Europeia e as diretrizes do WP29 fornecem estrutura sugerida para um conjunto de BCRs, a fim de auxiliar empresas na elaboração das suas próprias regras e poderá vos servir de auxílio neste processo.[13]

No mais, para empresas cuja sede é fora do Brasil e que já tenham normas corporativas globais implementadas considerando os parâmetros europeus, espera-se que o papel desta Autoridade seja o de validar o documento para ser implementado no âmbito do Brasil, de modo que a organização não tenha que produzir um segundo documento com a mesma função. Assim, sugerimos a esta Autoridade também o endereçamento deste ponto.

Vale ressaltar que, até o momento, a lista publicada pela EDPB[14] indica que, desde 2018, 30 (trinta) normas corporativas globais foram aprovadas pelas autoridades supervisoras sob o GDPR, para as quais o EDPB emitiu sua respectiva opinião/decisão vinculante. Tais instrumentos também podem servir como base para esta Autoridade .

Ainda, vale frisar que o EDPB[15] apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas contratuais padrão, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção. É recomendável que esta Autoridade também oriente os agentes de tratamento em relação a tais medidas suplementares, o que os auxiliará na implementação de salvaguardas efetivas para garantir a proteção dos dados sob transferência internacional, bem como para garantir sua confidencialidade, disponibilidade e integridade.

Por fim, em linha com a resposta 19, sugere-se que seja incluído como um critério para aprovação de normas corporativas globais a necessidade de o importador promover ao

---

[13] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#:~:text=Approval%20of%20binding%20corporate%20rules,-Companies%20must%20submit&text=The%20authority%20will%20approve%20the,more%20than%20one%20Member%20State. Acesso em 24/05/2022.

[14] Disponível em: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en. Acesso em 24/05/2022.

[15] Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE.

exportador a comunicação caso tome conhecimento da necessidade da divulgação de dados pessoais para autoridades públicas estrangeiras.

6) Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?

A inclusão de países no rol daqueles com nível de proteção de dados considerado adequado, no contexto europeu (art. 45, GDPR), tem como intuito possibilitar um fluxo livre de dados pessoais entre a União Europeia e países terceiros, sem que seja necessário adotar salvaguardas complementares ou autorização adicional. Este racional é adotado pelo fato deste processo de avaliação pela Comissão Europeia ser mais demorado e realizado com base em critérios robustos e específicos, como o conteúdo das normas aplicáveis nos respectivos países, e a forma como é assegurada a sua aplicação efetiva pelo país[16].

Neste sentido, entendemos que os elementos previstos no art. 34 da LGPD, destinados à avaliação do nível de proteção de dados de países estrangeiros, devem ser utilizados nos instrumentos contratuais de forma macro, se limitando àqueles critérios que não impactem na fácil e objetiva aplicabilidade do instrumento contratual em questão.

Assim, entendemos que nos instrumentos contratuais devem ser considerados, pela ANPD, a natureza dos dados que serão transferidos (art. 34, II, LGPD), as medidas de segurança que serão adotadas (art. 34, IV, LGPD), além de outros fatores específicos inerentes à transferência (art. 34, VI, LGPD) que possam demandar a elevação do nível de proteção para que sejam resguardadas a confidencialidade, disponibilidade e integridade dos dados sob transferência.

Por fim, em linha com o art. 34, I da LGPD, é recomendável que esta Autoridade oriente os agentes de tratamento a fim de que os exportadores adotem medidas que visem garantir que os importadores os informem previamente caso o país destinatário dos dados pessoais apresente normas que possam submeter a riscos os dados pessoais transferidos, o que inclui divulgações indevidas e/ou divulgações a autoridades/órgãos públicos[17].

7) As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?

Entendemos que, embora seja necessário um conteúdo pré-definido para que as empresas possam utilizar as cláusulas-padrão contratuais de maneira segura, objetiva e facilitada, é importante que seu conteúdo não seja rígido, mas modular, a fim de que o documento possa se amoldar às especificidades do contexto da transferência, de modo que possam ser mencionadas informações relevantes como os tipos de dados que serão transferidos, e de modo que o

[16] Disponível em: https://ec.europa.eu/newsroom/article29/items/614108. Acesso em 24/05/2022.

[17] Recital 19 - Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

documento seja adaptável considerando os agentes de tratamento envolvidos na operação, sobretudo o tipo de agente que ocupará o papel de exportador, e o tipo de agente que figurará como importador.

Foi neste sentido, inclusive, que a Comissão Europeia implementou as SCCs, de forma que (i) o agente de tratamento que transferir os dados para o país terceiro é livre para incluir as SCCs em um contrato mais amplo, ou mesmo para adicionar outras cláusulas ou salvaguardas adicionais, desde que não conflitem com as já aprovadas pela Comissão[18]; (ii) as SCCs combinam cláusulas gerais com pontos de modulação e pontos "livres", para serem ajustados e complementados a depender dos diferentes cenários de transferência e da complexidade da cadeia de tratamento. Assim, em adição às cláusulas-padrão gerais, devem os agentes selecionar o módulo aplicado à determinada situação. É possível, ainda, que agentes adicionais que venham a fazer parte da cadeia de atividades de tratamento, se valham das disposições das SCCs[19], o que poderá permitir que se concentre em um único instrumento as normas a serem seguidas e observadas por toda a cadeia de agentes envolvidos na transferência internacional.

Nesse sentido, a Comissão Europeia concebeu as SCCs para serem instrumentos dinâmicos e adaptáveis compostos por: cláusulas fixas, que se destinam a permanecer inalteradas independentemente das partes a elas submetidas; módulos, adaptáveis a depender do agente de tratamento (controlador ou operador) que figurará como exportador ou importador; e cláusulas e anexos em branco, que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados, entre outras).

Deste modo, recomendamos que esta Autoridade siga na elaboração das cláusulas-padrão contratuais conforme modelo adotado pela Comissão europeia, incluindo tanto disposições fixas, quanto disposições modulares e anexos para preenchimento pelas partes.

8) Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?

O formato mais adequado seria aquele que permitisse que o agente de tratamento escolhesse o clausulado de forma a abranger as especificidades da sua atividade de tratamento com determinado parceiro, mas que ao mesmo tempo desse ao agente uma segurança jurídica de que de fato foi adotada a cláusula mais pertinente para aquela relação. Neste sentido, trazer leques e subdivisões excessivas poderia até mesmo dificultar a escolha das cláusulas pelo agente e tornar complexo um mecanismo de transferência que deveria, a princípio, ser de fácil utilização.

[18] Recital 3 - Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[19] Recital 10 - Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Recorrendo à experiência internacional, a Comissão Europeia, ao adotar SCCs, optou pela modelagem das cláusulas[20], de modo que o documento é composto por (i) cláusulas fixas, que permanecem inalteradas independentemente das partes a elas submetidas; (ii) módulos adaptáveis a depender do agente de tratamento (controlador ou operador) que figurará como exportador ou importador; e (iii) cláusulas e anexos em branco, que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados envolvidos, entre outras).

A simplificação do modo como poderá se dar a modulação poderá evitar, inclusive, que o agente utilize as cláusulas de forma errônea, considerando o cenário fático.

Por outro lado, a ICO, no *International Data Transfer Agreement,*[21]disponibiliza ao agente de tratamento uma árvore de decisões, além de *checkboxes* para preenchimento, de forma um pouco mais fechada e direcionada. O formato adotado pelo ICO, por ter adaptações mais limitadas, pode ser capaz de evitar que as partes adicionem informações equivocadas no documento e o tornem inaplicável ou não aderente ao caso concreto.

Em todo caso, independentemente do critério a ser adotado pela ANPD, sugerimos um documento que seja autoexplicativo e contemple o que a autoridade espera (ao menos nos campos de livre preenchimento) em cada cenário relativo às transferências internacionais.

9) É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?

É sobremaneira necessário adotar módulos diferenciados, considerando o agente que figurará como exportador e o agente que figurará como importador. Em linha com a resposta dada para a questão 7 e considerando que as obrigações atribuídas pela LGPD a cada agente de tratamento e suas responsabilidades são diferentes, bem como considerando o nível de autonomia que possuem para o tratamento de dados pessoais, entendemos ser importante que haja regras específicas para cada agente na transferência internacional de dados.

Nessa linha, de modo a buscar a harmonização com o cenário internacional, recomendamos que sejam adotados os requisitos já observados pela Comissão Europeia no documento *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*[22], bem como em seus anexos relacionados.

Em suma, houve a adoção pela Comissão Europeia de conjunto de cláusulas de controladores/operadores situados na União Europeia (ou sujeitos ao GDPR) para controladores/operadores situados fora da União Europeia (ou não sujeitos ao GDPR), com ajustes modulares capazes de permitir que tanto o controlador quanto o operador assumam papéis de exportador e importador.

---

[20] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en . Acesso em 24/05/2022.

[21] Disponível em: idta.docx (live.com). Acesso em 25/05/2022.

[22] Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. Acesso em 25/05/2022.

De maneira geral e exemplificativa, nas transferências de dados de um operador para outro operador, o nível de exigências destinado ao importador deverá ser maior no que tange (i) as medidas de controle da atuação do importador (limitações relacionadas à transferências/compartilhamento de dados, por exemplo), (ii) deveres de cooperação e de notificação do agente exportador em situações que envolvam incidentes de segurança, (iii) deveres de cooperação e de notificação do agente exportador em situações que envolvam a necessidade de responder a requisições de autoridades competentes e/ou requisições de titulares de dados. Isto porque neste caso, o exportador deverá ter condições de assegurar que se mantenha o nível de proteção aos dados pessoais transferidos e, ainda, deverá ter condições de cumprir eventuais regras impostas pelo controlador nas atividades de transferência de dados que irá realizar.

Ainda de maneira exemplificativa, em transferências realizadas entre controladores, embora seja relevante que medidas de cooperação sejam implementadas, pela definição do papel do controlador na LGPD, não é necessário que haja rigor excessivo e subordinação em relação às atividades de tratamento por ele realizadas, de modo que é relevante que o exportador assegure que tomará conhecimento das atividades realizadas no escopo do tratamento, a fim de que possa manter o controle sobre os dados transferidos, tendo em vista a possibilidade de se dar sua responsabilização solidária em casos nos quais houver tratamento inadequado ou ilícito de dados pessoais.

Ressalta-se ser possível também que agentes de tratamento adicionais façam parte da cadeia de atividades de tratamento e se valham das disposições das SCCs[23], circunstância que consideramos ser relevante e aplicável ao cenário brasileiro, tendo em vista que poderá permitir que se concentre em um único instrumento as normas a serem seguidas e observadas por toda a cadeia de agentes envolvidos na transferência internacional, possibilitando maior controle sobre a atividade.

10) Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?

Considerando o escopo diverso de aplicação de ambos os mecanismos, bem como a complexidade do fluxo de dados e quantidade de agentes de tratamento envolvidos a depender do contexto da transferência, entendemos que os requisitos de ambos os instrumentos também devem ser distintos. Isto porque as Normas Corporativas Globais (*Binding Corporate Rules*, no contexto europeu) costumam ser direcionadas a empresas multinacionais, com um fluxo maior de atividades de tratamento e mais agentes envolvidos na operação, ao passo que as cláusulas-padrão contratuais (*Standard Contractual Clauses*, no âmbito da União Europeia), são mais comumente utilizadas para relações com agentes em menor quantidade, e uma menor complexidade no fluxo das atividades de tratamento.

Em linha com a ideia de uma harmonização internacional, sugerimos que, no que couber no âmbito de aplicação da LGPD, sejam utilizados os requisitos e parâmetros já estabelecidos pela Comissão Europeia para aprovação de ambos os instrumentos.

Isto porque, em suma, as cláusulas-padrão contratuais necessitariam de uma construção e elaboração prévias pela Autoridade, de forma que, uma vez tornadas públicas, estariam "pré-aprovadas" para utilização dos agentes.

[23] Recital 10 - Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Seus requisitos de aplicabilidade devem englobar a adequada escolha de seus módulos específicos pelo agente exportador, caso este seja o formato escolhido pela ANPD, bem como deve ser exigido que o exportador e o importador avaliem previamente, se há leis ou normas do país terceiro que poderiam impactar em sua eficácia. É recomendável, ainda, que o exportador tenha a obrigação de avaliar se as referidas cláusulas-padrão não contradizem com cláusulas estabelecidas nos instrumentos contratuais específicos firmados entre as partes, ou em outros mecanismos complementares eventualmente adotados para viabilizar a transferência internacional.

As Normas Corporativas Globais, por outro lado, decorrerão de uma ação positiva do agente de tratamento, no sentido de submeter o documento, elaborado de forma mais personalizada para o seu negócio, ao processo de aprovação da Autoridade. No que tange as referidas normas, é recomendável que a Autoridade disponha sobre informações específicas que deverão constar no referido documento, tais como: (i) políticas e procedimentos da Organização que demonstrem seu compromisso com a observância dos princípios previstos no art. 6º da LGPD; (ii) documento que evidencie as medidas de transparência que utiliza, bem como a maneira pela qual possibilita que os titulares exerçam seus direitos, à luz da LGPD; (iii) documentos que evidenciem o caráter vinculante das normas dentro da Organização; (iv) documentos que evidenciem que os Encarregados de todas as empresas do grupo que aderirem às normas estão alinhados em relação às salvaguardas que deverão ser implementadas para garantir proteção aos dados pessoais submetidos a transferência internacional; (v) outros documentos que demonstrem a estrutura de governança da organização e seu nível de conformidade.

Por fim, é recomendável que as instruções relacionadas à composição e formato das normas corporativas globais sejam detalhadas a fim de possibilitar que as Organizações submetam a esta Autoridade, para aprovação, normas condizentes com o nível de robustez esperado, o que poderá tornar menos dificultoso o procedimento destinado à aprovação.

11) Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?

Sobre a definição de grupo econômico para fins de aplicação das normas corporativas, podem ser considerados os seguintes critérios:

(a) estrutura corporativa única[24] ou com influência significativa de ao menos uma empresa nas decisões de outra, como direção, controle ou administração[25];

[24] A LGPD também utiliza a nomenclatura "conglomerado" (art. 52, II), que se refere à junção de duas ou mais empresas, de diferentes segmentos, que trabalham em função de uma única estrutura corporativa.

[25] Conforme definição de "grupo econômico" disposta no art. 2º, §2º da CLT (Consolidação das Leis Trabalhistas).

(b) combinação de recursos ou esforços[26] para alcançar interesses em comum[27]; e
(c) adoção de mecanismo aplicável a todas as empresas do grupo envolvidas e aos funcionários, de natureza juridicamente vinculante[28].

Referidos critérios permitem que sejam abrangidos grupos de empresas multinacionais com subsidiárias e afiliadas, franquias, consórcios, joint ventures ou parcerias profissionais, para os quais o ICO[29] indica a aplicação das *binding corporate rules*.

[26] Características de "grupo de sociedades" conforme art. 265 da Lei nº 6.404/76 (Lei das Sociedades Anônimas).

[27] O EDPB engloba no conceito de "grupo" o conjunto de empresas envolvidas em uma atividade econômica conjunta. https://ec.europa.eu/info/files/working-document-approval-procedure-binding-corporate-rules-controllers-and-processors-wp263rev01_en

[28] O critério tem fundamento no art. 47 (1) (a) do GDPR, o qual prevê a necessidade de que as BCRs sejam juridicamente vinculativas e aplicáveis a todas as entidades do grupo envolvidas na transferência. Ademais, utiliza-se por base o artigo 34, V da LGPD. Como exemplo, citam-se: acordos intragrupo, compromissos unilaterais vinculantes, políticas internas com precisão de sanções disciplinares para colaboradores, entre outros instrumentos.

[29] https://ico.org.uk/for-organisations/binding-corporate-rules/

12) Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?

Primeiramente, recomenda-se que o nível de detalhamento seja coerente com as demais obrigações já impostas pela LGPD, seja para fins de atendimento aos princípios de transparência e livre acesso ao titular[30] e exercício de direito de acesso[31], seja para demonstração de conformidade pelo agente de tratamento, como por meio do registro das atividades[32]. Nesse último aspecto de responsabilização e prestação de contas, a sugestão também tem por base o art. 30 do GDPR[33], que apresenta detalhamento acerca das informações que devem constar no registro de atividades, bem como em orientações do EDPS[34]. Adicionalmente, poderão ser complementadas com dados específicos acerca do compartilhamento de dados pessoais, com base em recomendação do ICO[35].

Diante dessas considerações, sugere-se como informações mínimas:

- os tipos de dados pessoais;
- as categorias de titulares envolvidos
- finalidade específica do tratamento;
- período de retenção;
- identificação dos agentes de tratamento envolvidos;
- país em que está localizado o agente de tratamento;
- a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares; e
- medidas de segurança tecnológica e organizacional implementadas em relação ao compartilhamento e aos dados pessoais.

[30] Para tanto, considera-se o rol de informações dispostas no art. 9º da LGPD.

[31] Sob este aspecto, considera-se o disposto no art. 19, II da LGPD acerca das informações que deveriam constar da declaração completa de acesso.

[32] A obrigação de registro de atividades aplicável aos agentes de tratamento está prevista no art. 37 da LGPD, porém não indica quais são as informações que devem ser mapeadas. Considerando o objetivo a que se propõe o registro, entendemos que se aplicam as informações dos artigos 9º e 19, II, somados à base legal aplicável para a finalidade específica.

[33] No tocante ao art. 30 do GDPR, destaca-se ainda que o rol de informações apresenta peculiaridades entre o controlador e o operador, porém para fins de transferência internacional estas não alterarão a sugestão promovida.

[34] International transfers | European Data Protection Supervisor (europa.eu)

[35] https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf

13) Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?

A princípio, entende-se que o potencial risco seria a incompatibilidade entre procedimentos. Isso porque cada grupo econômico seguiria seu próprio conjunto de regras, ou até mesmo voltado para setores econômicos que não guardam relação entre si e sujeitos a regulamentações setoriais que impactem as operações internas.

Todavia, as normas corporativas seguem padrões com base na LGPD para sua aprovação, portanto o espaço para divergências pode ser minimizado.

Nesse sentido, um risco decorrente de eventuais incompatibilidades procedimentais seria a possibilidade de os meios de supervisão e fiscalização não serem implementados com a mesma eficácia entre os agentes de tratamento envolvidos.

Em um cenário para mitigar ambos os riscos, é possível considerar que as partes poderão acordar entre si um instrumento adicional, como uma cláusula contratual, demandar uma avaliação das normas corporativas da outra parte ou eleger um conjunto de normas a ser observado por ambas.

Por outro lado, embora normas corporativas globais não guardem qualquer relação de obrigatoriedade de que as regras sejam observadas para transferências externas ao grupo, suas disposições regulam temas semelhantes às cláusulas contratuais que seriam firmadas entre grupos distintos em seu lugar.

Com isso, o benefício notável seria a redução de burocracias no compartilhamento e a possibilidade de um fluxo de dados pessoais facilitado para empresas que já demostraram possuir procedimento internos eficientes.

Ademais, seria possível argumentar que esta poderia ser uma medida que incentivaria a elaboração de normas corporativas globais como meio de reduzir a exposição dos negócios a riscos, sendo benéfico para a imagem e reputação das empresas. Isso porque as operações com grupos que já obtiveram suas normas corporativas globais aprovadas poderiam ter maturidade necessária para resguardar os dados pessoais e seus titulares, uma vez que o cumprimento dos requisitos de atendimento às normas corporativas globais, idealmente já exigiria o desenvolvimento de um programa de governança em privacidade robusto.

Por fim, as normas corporativas globais poderiam constituir uma opção mais atrativa do que a adoção de cláusulas-padrão contratuais nesse cenário. Isso porque podem ser ajustadas para atender às necessidades do negócio e, uma vez implementadas e operacionais, são mais fáceis de serem mantidas e atualizadas, na medida em que esta Autoridade não precisaria, portanto, aprovar suas atualizações não materiais, o que pode economizar tempo e custos[36].

Para melhor visualização, apresentamos tabela comparativa abaixo:

Tabela da questão 13

[36] Opice Blum, Bruno e Vainzof Advogados. WHITE PAPER – Mecanismos de Transferência Internacional de Dados - Cláusulas-Padrão Contratuais e Regras Corporativas Vinculantes. Disponível em: https://opiceblum.com.br/wp-content/uploads/2022/02/white_paper_transferencia_internacional_de_dados_v.final_.pdf

Permissão de transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD	
Riscos	Benefícios
Incompatibilidade entre procedimentos	Minimização de divergências com base na LGPD
Possibilidade de os meios de supervisão e fiscalização não serem implementados com a mesma eficácia entre os agentes de tratamento envolvidos	Maior harmonia na forma de interpretação e aplicação da LGPD nos processos de supervisão e fiscalização pela ANPD
Pluralidade de legislações e regulamentações setoriais	Possibilidade de utilização de instrumento adicional, como uma cláusula contratual, para demandar uma avaliação das normas corporativas da outra parte ou eleger um conjunto de normas a ser observado por ambas
Maior burocracia para efetivar a transferência internacional	Redução de burocracias no compartilhamento e a possibilidade de um fluxo de dados pessoais facilitado para empresas que já demostraram possuir procedimento internos eficientes
Maior exposição da operação específica ao risco por ausência de procedimento externo	Menor exposição dos negócios ao risco, diante dos procedimentos internos robustos, potencializando o fluxo de dados e preservando a segurança
Maior tempo e custo para aprovação de atualizações nos instrumentos utilizados para fundamentar a transferência entre os agentes de tratamento	Normas corporativas globais são mais fáceis de serem mantidas e atualizadas, na medida em que a ANPD não precisaria aprovar alterações não materiais, economizando tempo e custos

14) Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?

Ao consultar a legislação europeia sobre a aprovação de cláusulas contratuais específicas, observa-se que os artigos 46 (3) (a) e 46 (4) do GDPR sujeita a autorização pela autoridade supervisora competente e, posteriormente, submetê-lo ao mecanismo de consistência pelo EDPB.

Como exemplo de fluxos para aprovação de normas corporativas globais, diversas autoridades europeias se valem de formulários a serem preenchidos pelos agentes de tratamento, a partir de um questionário de itens essenciais e da submissão do arquivo com as normas corporativas globais. Os critérios para aprovação de normas corporativas globais são os pontos de referência analisados em conjunto com os requisitos do art. 47 do GDPR.

Até o momento, a lista publicada pela EDPB[37] indica que, desde 2018, 30 normas corporativas globais foram aprovadas pelas autoridades supervisoras sob GDPR, para as quais o EDPB emitiu sua respectiva opinião/decisão vinculante.

Ainda, vale mencionar que o EDPB[38] apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas contratuais padrão, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção.

No contexto regulatório da ANPD, o ideal é que fosse publicado um procedimento específico, contemplando minimamente os seguintes pontos:

a) definição de procedimento para aprovação de contratos específicos e normas corporativas globais, incluindo minimamente: prazos, requisitos, e formalização da decisão;
b) se cabe recurso, bem como a indicação do seu respectivo prazo e autoridade julgadora; e
c) forma de publicação dos contratos e das normas corporativas globais aprovadas.

[37] https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en

[38] EDPB. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

15) Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?

Inicialmente, deve-se estabelecer o que serão consideradas "alterações na configuração original". Isso porque é natural que mudanças sejam realizadas a fim de otimizar o fluxo de informações e a continuidade das atividades.

Para tanto, sugerimos que as alterações nos seguintes aspectos da operação sejam considerados como "alterações na configuração **original"**: *(i)* nova finalidade, não prevista em contrato, *(ii)* envio para outros países não previstos originalmente no contrato, *(iii)* forma e duração do tratamento, *(iv)* controlador responsável, *(v)* compartilhamento com outros agentes ou terceiros *(i)* e alterações que representem risco aos direitos e liberdades dos titulares.

Partindo da premissa apresentada, todos os direitos dos titulares previstos na LGPD deverão ser garantidos, tais como: (a) direito de acessar os dados que tratados sobre agentes de tratamento nessa nova configuração; (b) direito de oposição ao novo tratamento, caso a nova configuração descumpra a LGPD; (c) direito de anonimização, bloqueio ou eliminação, caso o titular entenda que o novo tratamento seja excessivo, desnecessário ou em desconformidade com a LGPD; (d) direito de correção, caso os dados estejam incompletos, inexatos ou desatualizados para a nova configuração; (e) caso o tratamento tenha fundamento no consentimento, o direito de revogação a qualquer tempo; e (f) o direito de peticionar perante a ANPD caso a nova configuração implique em violação à lei.

Como referência, a Comissão[39] europeia esclarece acerca dos direitos de titulares em casos de transferências internacionais baseadas em cláusulas contratuais padrão, reforçando especialmente o direito de que os titulares sejam informados acerca do tratamento, bem como sobre o direito de obtenção de uma cópia das cláusulas conforme utilizadas, nos termos do art. 15 (3) do GDPR.

Quanto à comunicação aos titulares, além do direito abrangente de que os titulares sejam informados sobre operações de tratamento, as circunstâncias que tornariam a comunicação direta imprescindível seria apenas quando o tratamento seja fundamentado no consentimento e a alteração disser respeito à finalidade, forma e duração do tratamento, controlador responsável, com base no art. 8º, §6º da LGPD.

Referido artigo também faz menção às alterações referentes a "informações acerca do uso compartilhado", sugere-se que a interpretação seja feita de forma flexível, para não burocratizar eventual troca de agentes de tratamento e de países que não atraia risco aos titulares. Ademais, nesse aspecto, entende-se que aplicar-se-ia o direito de obter informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, o qual deve ser provocado ativamente pelo titular.

[39] https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf

16) Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?

Para resolução de conflitos entre agentes de tratamento, entendemos que o meio recomendável, a princípio, seria que os agentes possam realizar a autocomposição utilizando os próprios meios contratuais, bem como determinar acerca de recursos de arbitragem, conciliação ou processo judicial. Quanto a este último, deverão ser previstas em contrato a lei e jurisdição aplicáveis.

No que tange aos titulares, quando a transferência tiver por base um instrumento contratual, a ANPD poderá prever como orientação que os agentes de tratamento determinem no contrato responsabilidades acerca: *(i)* do fluxo de comunicação entre si para atendimento a requisições de titulares, *(ii)* da existência de meios facilitados para que o titular contate cada uma das partes e *(ii)* da existência de procedimentos internos para lidar com as requisições dentro de um prazo razoável.

Ainda, quanto à definição de lei aplicável, mencionada anteriormente, a ANPD poderá orientar que os agentes de tratamento considerem como aplicável a lei que tutela de forma mais rígida os direitos e garantias dos titulares de dados.

Ademais, dentro do papel de conscientização que compete à ANPD, entendemos que é relevante a indicação aos agentes de tratamento e titulares, por meio de guias e orientações, acerca dos meios alternativos de resolução dos conflitos sobre privacidade, para que possam optar livremente, tais como mediação e conciliação.

No tocante às alternativas para atuação da ANPD frente às questões internacionais para resolução de conflitos, a melhor alternativa poderia ser a promoção de ações de cooperação com autoridades internacionais de natureza semelhante à ANPD, ação cuja competência resta evidenciada no art. 55-J, IX da ANPD e que já tem sido colocada em prática.

Ademais, há uma lista[40] extensa e não exaustiva de *frameworks* de cooperação internacional sobre proteção de dados pessoais existentes, aos quais a ANPD poderá integrar.

Os contratos multilaterais possuem seu benefício na medida em que garantem uma maior padronização na aplicação de determinados entendimentos e regras na comunidade internacional. Isso é particularmente relevante na medida em que, ao se falar de privacidade, a transnacionalidade costuma ser o padrão das empresas.

Um contrato multilateral vai permitir o a padronização e comunicação regulatória e, consequentemente, desburocratizar o processo de transferência internacional de dados. Por outro lado, pelo fato dos contratos multilaterais envolverem muitos países de jurisdições completamente diferentes, observa-se uma grande dificuldade em traçar diretrizes específicas e próprias para os temas. Nesse sentido, os contratos multilaterais, para atingir um número significativo de países, acabará tendo de ser extremamente genérico.

[40] A lista publicada pelo EDPB pode ser encontrada em: International Cooperation & Cooperation with Other Authorities | European Data Protection Board (europa.eu). No tocante aos *frameworks*, aplicáveis à ANPD, destacam-se: Organisation for Economic Cooperation and Development (OECD); Global Privacy Assembly (GPA) – global conference (successor of the ICDPPC); Global Privacy Enforcement Network (GPEN) – network of privacy enforcement authorities; Common Thread Network (CTN); Ibero-American data protection network (RIPD)

Os contratos bilaterais, por sua vez, possuem seu benefício na medida em que diversas regras mais específicas poderão ser traçadas, uma vez que envolve um número bem menor de jurisdições. Ele seria uma saída para contratos firmados com países junto aos quais ocorre uma quantidade muito significativa e determinante de dados. Contudo, uma tendência com relação a este tipo de contrato é a priorização de fluxos com países mais desenvolvidos do aspecto de proteção de dados pessoais e privacidade, criando-se barreiras para trocas com uma gama mais abrangente e diversificada de países.

Nesse contexto, portanto, cabe a esta Autoridade sugerir a elaboração de contratos multilaterais ou bilaterais entre países fornecendo o conteúdo que deve estar presente.

Independentemente do instrumento escolhido, a resolução de conflitos no âmbito internacional poderá ser promovida especialmente a partir de padrões e princípios para as autoridades envolvidas, sem que isso represente uma decisão de adequação.

Isso porque uma decisão de adequação deve ser guiada por critérios formais considerando o estado da lei, a autonomia da autoridade supervisora, entre outros elementos essenciais.

17) Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?

Sugerimos que a ANPD elabore para auxiliar os agentes de tratamento na gestão e documentação pertinente às transferências internacionais, como a disponibilização de materiais opcionais para os agentes de tratamento, por exemplo:

(a) guias para utilização das salvaguardas do art. 33 da LGPD;
(b) orientações[41] para análise de riscos de transferência internacional com indicação de medidas de segurança e conformidade suplementares e aplicáveis ao contexto de transferências internacionais[42];
(c) modelos de planilhas para registro das operações que envolvam transferência internacional;
(e) estudos acerca da probabilidade de respeito aos direitos e garantias de titulares nos países (com base em diretrizes de recursos humanos, adesão a acordos internacionais e no estado das leis, por exemplo[43]);
(f) checklist de análise de conformidade de terceiro (importador).

[41] https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf

[42] EDPB. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

[43] There are many public sources which set out the human rights record for countries. For example, the Foreign, Commonwealth & Development Office (FCDO) produce regular Human Rights and Democracy Reports.

18) Quais as melhores alternativas para resolver as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?

Entendemos que o cenário de responsabilização não deva se desviar das responsabilidades que já cabem aos agentes de tratamento a partir de sua atuação fática quanto à atividade desempenhada, ou seja, a depender se figuram como controladores - inclusive com as particularidades de controladores independentes e conjuntos -, operadores ou suboperadores. Para tanto, uma vez verificado que houve transferências posteriores a jurisdições não conhecidas ou até mesmo a outros importadores, o regime de responsabilidade deve seguir o disposto tanto nos artigos 42 a 45 da LGPD, quanto nas orientações já formuladas pela ANPD em seu Guia[44].

Quando houver mudança de jurisdição nas cadeias consecutivas de compartilhamento, estaremos diante de uma nova configuração de exportador-importador, de modo que o novo exportador também assumirá responsabilidade pela observância das regras dispostas nos artigos 33 a 36 e regulamentações futuras. Com isso, o exportador inicial será responsável pela primeira transferência, e os exportadores seguintes se responsabilizarão pelas respectivas transferências. Este cenário não exclui eventual responsabilidade solidária entre todos os agentes de tratamento envolvidos, na medida em que cada um deverá cumprir com as regras impostas pela LGPD individualmente na operação de tratamento em questão.

Esta Autoridade poderá considerar ainda a possibilidade de inclusão de anexos nacionais nas cláusulas contratuais padrão ou nas normas corporativas globais, que têm como principal objetivo a inclusão de eventuais particularidades contidas em lei nacional, conforme proposto em consulta pública pelo ICO[45].

Já no que tange aos compartilhamentos na mesma jurisdição, entendemos que o importador inicial deve assegurar que terceiros porventura envolvidos se submetam às mesmas proteções resguardadas e exigidas pelo exportador inicial, bem como que tais terceiros sejam documentados no registro de atividades mantido pelo importador.

Independentemente do cenário (dentro ou fora da mesma jurisdição), deve haver espaço para que os agentes de tratamento determinem entre si os limites à continuidade da cadeia de compartilhamento, na medida em que o exportador inicial poderá permitir, limitar ou proibir transferências, quando o importador inicial figurar como operador ou suboperador, bem como realizar eventual averiguação do cumprimento destas delimitações, visando maior proteção aos titulares envolvidos na operação.

[44] Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf (www.gov.br)

[45] ICO consults on how organisations can continue to protect people's personal data when it's transferred outside of the UK | ICO

19) Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?

Sugerimos que sejam adicionadas as seguintes medidas atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras:

a) comunicação prévia acerca do compartilhamento: como meio de cooperação entre os agentes de tratamento, a comunicação acerca do pedido de divulgação, nos casos em que a lei aplicável não impuser proibições ou restrições nesse sentido.

   Nesse tema, considerando a legislação europeia, o EDPB e o EDPS[46] reforçam que, em caso de pedidos de acesso dos tribunais e outras autoridades públicas, os importadores devem promover a comunicação antes de responder ao pedido. Tal recomendação, inclusive, é abarcada nas *Standard Contractual Clauses*, e, também sugerimos que seja contemplada nas cláusulas-padrão contratuais art. 33, II, b".

   Considerando que a divulgação de dados para autoridades públicas estrangeiras também foi tema relevante no recente contexto das transferências referentes ao *Privacy Shield Framework*[47], revogado pela CJEU[48], destaca-se a abordagem adotada incluía sugestões de posturas voluntárias que poderiam ser adotadas como reforço de transparência, com a "emissão voluntária de relatórios periódicos de transparência sobre o número de pedidos de informações pessoais que recebem das autoridades públicas por razões de aplicação da lei ou de segurança nacional";

b) declaração sobre o regime legal: no mais, conforme avaliação de riscos proposta pelo ICO[49], pode-se indicar, a título de recomendação, que o exportador avalie junto ao importador, ou que obtenha uma declaração deste último sobre o regime legal do país de destino e a probabilidade de acesso de autoridades públicas aos dados pessoais (incluindo vigilância), bem como se existem limitações que podem ser impostas a este acesso.

[46] https://edps.europa.eu/sites/edp/files/publication/edpb_edps_jointopinion_202102_art46sccs_en_1.pdf

[47] Privacy shield framework: Access Requests by Public Authorities: https://www.privacyshield.gov/article?id=16-Access-Requests-by-Public-Authorities

[48] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield is invalid. judgment.pdf (noyb.eu)

[49] https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf

20) Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

Os mecanismos adequados a tal título são aqueles utilizados para fins de transparência, por meio dos quais os agentes de tratamento elencam as informações relevantes aos titulares de forma clara, adequada e ostensiva, nos termos do art. 9º da LGPD.

A título exemplificativo, cita-se o Aviso de Privacidade, cuja disponibilização pode ser feita por meio de canais acessíveis aos titulares, seja nos meios físicos ou digitais, bem como pode ser um instrumento abrangente ou específico para determinada transferência internacional. Ademais, é um documento pelo qual é possível assegurar o acesso gratuito e facilitado.

Quanto à forma de apresentação de informações, para maior efetividade, o agente de tratamento poderá optar pelo meio mais adequado à sua realidade e aos meios de interação com o titular, desde que promova ativamente a exposição de informações.

Sobre o tema, a doutrina europeia[50] provê recomendações para garantia de transparência, aplicáveis para o contexto de transferências internacionais, às quais dizem respeito: a disposição das informações em camadas, utilização de ferramentas como *pop-ups, dashboards*, avisos de privacidade específicos *(just-in-time), QR codes*, entre outros. Vale ressaltar que tais recomendações não possuem caráter vinculante, mas se apresentam como orientações aos agentes de tratamento.

Quanto à implementação do mecanismo eleito para conferir transferência, ainda que o agente de tratamento deva se atentar aos requisitos do art. 9º da LGPD, não recomendamos a exigência de elementos adicionais obrigatórios para o contexto de transferência internacional, sob pena de que o titular seja impactado com um documento denso ou complexo em demasia, afastando o objetivo pretendido com o princípio da transparência.

[50] Guidelines on Transparency under Regulation 2016/679 (wp260rev.01) https://ec.europa.eu/newsroom/article29/items/622227

Contribuição ABEAR - ANPD na Tomada de Subsídios sobre Transferência Internacional,
Patricia Perez <patricia@snea.com.br>
Sex, 17/06/2022 14:34
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Cc:

- Antonio Augusto do Poço Pereira <augusto.pereira@abear.com.br>

Prezados Senhores, boa tarde!

Encaminhamos em anexo, documento com informações complementares aos questionamentos formulados pela ANPD na Tomada de Subsídios sobre Transferência Internacional, enviada pela plataforma *Participa Mais Brasil*., através do CPF Nº 011.833.137-05 – Patricia Carneiro Rodrigues Perez.

Tal contribuição foi elaborada pela ABEAR – Associação Brasileira das Empresas Aéreas e suas associadas.

Qualquer dúvida, estamos à disposição.

Att.;

Patricia C. R. Perez I Assistente Diretoria
SNEA - Sindicato Nacional das Empresas Aeroviárias
Tel: + 55 (11) 3892 3919 / [redacted]
Av. Ibirapuera, 2332 - Conjunto 22 - Torre Ibirapuera I - Moema - SP - CEP: 04028-002
patricia@snea.com.br I **www.snea.com.br**

Contribuições do Setor Aéreo enviadas à ANPD, via ABEAR, face à tomada de subsídios sobre transferências internacionais de dados pessoais

1) Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?

O maior obstáculo para as empresas que transferem dados do Brasil para outros países, assim como na relação inversa, é a falta de regulação das salvaguardas previstas no art. 33 da LGPD, as quais devem ser observadas pelos agentes de tratamento quando da realização de transferência internacional.

Deste modo, apenas os seguintes mecanismos do art. 33 é que, em tese, poderiam ser utilizados imediatamente, sem depender dessa regulação complementar:

(i) para proteção da vida ou da incolumidade física do titular ou de terceiro (art. 33, IV);
(ii) decorrentes do consentimento específico e em destaque do titular (art. 33, VIII) e
(iii) para o cumprimento de obrigação legal ou regulatória pelo controlador; execução de contrato ou tratativas preliminares; e exercício regular de direitos em processo judicial, administrativo ou arbitral (arts. 33, IX cc. art. 7º, II, V e VI).

Na prática, essas hipóteses não se enquadram na maioria das transferências de dados internacionais, que ocorrem, via de regra, entre empresas do mesmo grupo para viabilizar a prestação de um determinado serviço ou execução de uma determinada atividade, ou em razão da gestão centralizada, ou pelo fato de contratarem serviços de nuvem para armazenar as informações da companhia, e cujo servidor esteja localizado no exterior.

Nesse contexto, as empresas se veem obrigadas a utilizarem cláusulas contratuais que buscam garantir os mesmos direitos e garantias aos titulares que tiveram seus dados tratados no Brasil, mesmo quando esses dados são exportados.

Assim, para o agente situado no Brasil não haverá critérios objetivos e parâmetros a serem considerados que facilitem a negociação dessas cláusulas contratuais, o que aumenta a assunção de risco no caso concreto.

Por outro lado, quando o agente localizado no Brasil recebe um instrumento jurídico elaborado com base em parâmetros provenientes de outro país (por exemplo, países da União Europeia), não tem segurança acerca do que deve aceitar ou não para estabelecer uma aplicação harmônica do disposto no cenário internacional com aquilo que é admitido pela LGPD.

Esse cenário aumenta a insegurança das partes na condução de seus negócios, considerando a ausência de parâmetros a serem observados na relação com seus parceiros, além do risco de descumprimento à LGPD, nos termos do art. 44 da LGPD.

Por fim, somado aos aspectos aqui expostos, vale destacar ainda, o quesito regulatório, de maneira que setores regulados tendem a enfrentar óbices em seus processos e na compatibilização de suas regras internas com as inúmeras especificidades regulatórias a serem observadas. Nesse sentido, é recomendável que a ANPD esteja alinhada com outras agências reguladoras a fim de endereçar suas regras de forma harmônica com outras legislações

às quais as empresas estejam submetidas, a fim de que não haja dificuldades práticas para aplicação daquilo que for definido pela Autoridade.

2) Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?

A melhor maneira de garantir a interoperabilidade dos instrumentos contratuais previstos na LGPD (art. 33, II) com os instrumentos contatuais das demais jurisdições, e, inclusive, promover segurança jurídica no Brasil, seria utilizar o já estabelecido especialmente no cenário europeu para construir e estruturar os parâmetros dos mecanismos de transferência internacional no Brasil, de maneira a possibilitar uma "*harmonização*" do que se estabelecerá no Brasil com o que se utiliza no cenário internacional.

Neste sentido, observa-se que a ANPD tem participado de forma ativa em fóruns internacionais de debates, como a Análise de Recomendações da OCDE, Comitê Consultivo da Convenção 108, bem como vem adotando medidas formais de associação (GPA, GPEN e rede ibero-americana) em um esforço de articulação e diálogo com autoridades de outros países e órgãos públicos, a exemplo da assinatura de Memorando de Entendimento com a Agência Espanhola de Proteção de Dados, em 2021[1], sem prejuízo de parcerias bilaterais com países como EUA, Reino Unido e Alemanha[2].

Logo, em linha com o trabalho que vem sendo realizado por esta Autoridade, faz sentido que os mecanismos de transferência internacional devam ser compatíveis com os mecanismos e salvaguardas do GDPR. Esta medida, inclusive, possibilitará que futuramente seja possível que o Brasil seja abarcado no rol de países com nível de proteção adequado, conforme entendimento da Comissão Europeia[3]. Tal circunstância trará às empresas brasileiras a possibilidade de realização de transferências de dados que envolvam países da União Europeia, sem que seja necessária a adoção de salvaguardas adicionais, na medida em que seria considerada uma transferência capaz de assegurar aos titulares e aos seus dados pessoais o mesmo nível de proteção obtido no tratamento realizado na União Europeia.

Portanto, acordos de cooperação técnica e memorandos de entendimento firmados pela ANPD com outros países e autoridades permitirão a adoção de mecanismos de cooperação internacional que facilitem a aplicação das legislações nacionais correspondentes na matéria de proteção de dados pessoais, voltados para o conhecimento e intercâmbio das melhores práticas e experiências, em relação a conflitos de jurisdição com países terceiros.

Inclusive, sob um aspecto regulatório, a parceria e cooperação pela Autoridade com outros órgãos reguladores e entidades poderá facilitar a aplicação da legislação de

[1] Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-assina-memorando-de-entendimento-com-a-agencia-espanhola-de-protecao-de-dados. Acesso em 27/05/2022.

[2] Disponível em: https://www.gov.br/anpd/pt-br/semana-da-protecao-de-dados-2022/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais. Acesso em 24/02/2022.

[3] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en#:~:text=The%20European%20Commission%20has%20so,Uruguay%20as%20providing%20adequate%20protection. Acesso em 24/02/2022.

proteção de dados pelos agentes, na medida em que as regras da ANPD estejam em harmonia com as regras relacionadas às práticas setoriais, diminuindo, dessa forma, a possibilidade de eventuais conflitos normativos.

3) Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?

No cenário europeu, na ausência de adequação do país terceiro que recepcionará os dados pessoais (Artigo 45(3), GDPR), ou seja, caso o país não proporcione grau de proteção de dados pessoais adequado, o membro da União Europeia deverá recorrer a um dos outros mecanismos de salvaguarda previstos na lei para a realização de transferência internacional. A LGPD adota racional semelhante ao estabelecer as salvaguardas apropriadas para a transferência internacional de dados, de modo que a adoção de instrumentos contratuais é uma das possibilidades previstas no art. 33, II da lei.

Neste contexto, entendemos que a escolha do instrumento mais efetivo dependerá da relação firmada entre as partes, bem como da complexidade das operações de tratamento a serem realizadas.

Dentre tais instrumentos, e considerando a prática proveniente do cenário europeu, merecem destaque aqueles previstos nas alíneas "a", "b" e "c" do art. 33, II da LGPD, quais sejam:

Normas corporativas globais: no âmbito europeu, as *Binding Corporate Rules*, equivalentes às normas corporativas globais previstas na lei brasileira (art. 33, II, c, LGPD), são regras com caráter vinculante que se aplicam a empresas de um mesmo grupo, para garantir que as transferências internacionais de dados pessoais realizadas na modalidade intragrupo estejam em conformidade com o GDPR.

Na prática, sua aplicação pode ser considerada dificultosa, considerando que o grupo empresarial que desejar implementar tal instrumento, deverá submetê-lo a um processo de aprovação da autoridade competente da União Europeia (*Article* 63, GDPR)[4], de maneira que por envolver filiais situadas em diversos países, é possível que seja necessário obter aprovação de diversas autoridades competentes, o que torna o processo mais moroso e oneroso. Por outro lado, uma vez implementadas, costumam ser mais fáceis de ser mantidas, considerando a completude de informações contidas em seu bojo. Ainda, permitem um nível de flexibilidade maior em relação aos demais mecanismos de transferência, na medida em que a autoridade não precisa aprovar *"non-material updates"*.

Cláusulas-padrão contratuais: as SCCs (*Standard Contractual Clauses*) previstas no GDPR, equivalentes às cláusulas-padrão contratuais previstas na LGPD (art. 33, II, b), podem ser utilizadas como estratégia para transferências internacionais intergrupo, ou seja, entre empresas distintas e cujo país terceiro, receptor dos dados, não ofereça níveis de proteção considerados adequados. Por ser um modelo pré-aprovado e avaliado previamente pela Autoridade, não é necessário que as empresas despendam tempo excessivo com negociações, visto tratar-se de um modelo fechado, mais seguro e simples.

Ainda, de acordo com o *IAPP-EY Annual Provacy Governance Report 2019*[5], as SCCs costumam ser particularmente importantes para pequenas e médias empresas que

[4] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en. Acesso em 27/05/2022.

[5] Disponível em: https://iapp.org/resources/article/privacy-governance-report/ . Acesso em 27/05/2022.

podem não ter recursos suficientes para negociar contratos individualmente com cada parceiro comercial. A mesma pesquisa afirma que no cenário europeu, dentre os mecanismos de transferência internacional, 88% dos stakeholders afirmam utilizar as cláusulas-padrão contratuais como salvaguarda principal, sendo estas, portanto, as mais utilizadas pelas empresas no âmbito da GDPR, e para as quais a ANPD pode dedicar particular importância no cenário brasileiro.

Ainda considerando aspectos provenientes do cenário internacional, impende salientar que embora as SCCs sejam amplamente utilizadas por empresas menores e em casos de compartilhamento bilateral de dados, seu uso por grandes multinacionais pode ser impraticável a depender do contexto e frequência da transferência internacional de dados realizada, tendo em vista que: (i) as SCCs podem não ser adequadas para situações em que haja uma rede complexa de atividades de tratamento; (ii) empresas maiores com muitas afiliadas no exterior poderão ter que implementar centenas de SCCs para abranger todas as atividades de transferência internacional realizadas, o que pode ser extremamente custoso; (iii) alguns Estados-Membros da União Europeia exigem formalidades adicionais, como preenchimento e aprovação das SCCs pela autoridade supervisora, tornando o processo moroso e oneroso.[6]

Cláusulas contratuais específicas: em situações que não sejam viáveis normas corporativas globais ou cláusulas-padrão contratuais, o uso de cláusulas contratuais específicas pode se apresentar como uma salvaguarda eficaz, tendo em vista que são ajustáveis a qualquer tipo de relação e capazes de abranger qualquer nível de complexidade das transferências internacionais. Trata-se, portanto, de um subterfúgio menos oneroso e mais flexível, que pode ser implementado por todas as empresas, independentemente de seu porte.

4) Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?

Os principais benefícios da transferência internacional são os seguintes:

(i) a possibilidade de as partes armazenarem dados internacionalmente (*data centers* situados fora do Brasil), o que repercutirá nos custos do negócio;
(ii) viabilização de transações de exportação/importação, com o estabelecimento de fluxos de dados entre países, instrumento chave para o desenvolvimento da economia digital e da inovação;
(iii) possibilidade de mais serviços oferecidos ao consumidor, com acesso a um número maior de bens a um custo mais baixo, estimulando, assim, a livre concorrência;
(iv) possibilidade de que pequenas empresas também tenham acesso a informações e serviços provenientes do cenário internacional, e possam se manter competitivas no mercado, reduzindo, por exemplo, a necessidade de altos investimentos com infraestrutura digital local.

Os principais impactos relacionados à transferência internacional são os seguintes:

[6] Disponível em: https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf. Acesso em: 27/05/2022.

(i) criação de facilitadores à economia, ou, entraves e custos operacionais de modo a inviabilizar modelos de negócio e barrar o desenvolvimento econômico e a inovação dos agentes de tratamento;

(ii) incentivar ou desestimular o fluxo de dados pessoais;

Assim, como alternativa para endereçamento em instrumentos contratuais, a ANPD deve considerar:

(i) adotar parâmetros de fácil aplicação, considerando o porte das empresas e o fluxo de dados que pretendem transferir internacionalmente, de modo que haja harmonia com o contexto internacional, já bem mais maduro em relação a esta temática;

(ii) regular as salvaguardas de modo a possibilitar que estejam em harmonia com o cenário internacional, sobretudo com o cenário europeu, é relevante, ainda, considerando que grande parte do mercado e de *players* internacionais já vem se estruturando ou já estão estruturados de modo a atender as especificidades da legislação estrangeira, em razão dos seus modelos de negócio e relações estabelecidas com agentes internacionais;

(iii) utilizar parâmetros objetivos na regulação do art. 33 da LGPD;

(iv) publicar e contemplar em guia específico orientações, ainda que iniciais, acerca dos mecanismos elencados no art. 33 da LGPD, e os respectivos parâmetros a serem considerados no contexto de utilização de cada instrumento jurídico, bem como considerando os papéis dos agentes envolvidos na transferência e seu nível de autonomia no tratamento e dados pessoais [7];

(v) prever medidas de segurança que sejam consideradas razoáveis (art. 34, IV, LGPD), bem como critérios a serem observados em relação à transferência internacional, considerando o porte da empresa, a natureza dos dados e as categorias dos titulares envolvidos;

(vi) firmar acordos diplomáticos no âmbito internacional com outras autoridades reguladoras, de modo a viabilizar que sejam admitidos no exterior os instrumentos elaborados pelo Brasil e validados pela Autoridade brasileira, bem como promover uma atuação conjunta com outros órgãos reguladores, avaliando suas respectivas especificidades e normas, a fim de que as regulamentações provenientes da ANPD não destoem do regulamentado em normas setoriais.

Em linha com o disposto acima, cumpre fazer menção ao importante e recente acordo firmado entre a Comissão Europeia e os Estados Unidos, que culminou na adoção do *Trans-Atlantic Data Privacy Framework*, que visa viabilizar fluxos de dados transatlânticos, abordando as preocupações levantadas pelo Tribunal de Justiça da União Europeia no Schrems II decisão de julho de 2020 que invalidou o *Privacy Shield*.

A intenção, a partir deste *framework,* é possibilitar que as partes assumam compromissos e adotem salvaguardas (por exemplo, cláusulas-padrão contratuais) que possibilitem e facilitem o fluxo de dados entre a União Europeia e os Estados Unidos. O referido framework e as negociações estabelecidas entre Estados Unidos e

[7] Disponível em: https://gdpr.eu/what-is-data-processing-agreement/. Acesso em 25/05/2022.

União Europeia podem ser utilizados como base pela ANPD, que poderá vislumbrar a realização de parcerias bilaterais com os EUA[8] e até mesmo com a Comissão Europeia, o que poderia ser um ponto de partida para que o Brasil seja enquadrado no rol de países considerados adequados para as respectivas transferências de dados pessoais.

5) Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê?

a. cláusulas-padrão contratuais

As cláusulas-padrão contratuais, por serem instrumentos jurídicos mais utilizados pelas empresas no cenário europeu e por serem de fácil utilização, merecem destaque no cenário brasileiro, pela ANPD. Isto principalmente para evitar entraves jurídicos e divergências em sua aplicação, já que grande parte de empresas multinacionais já se baseiam nas regras adotadas internacionalmente.

Logo, sugerimos que a ANPD edite um modelo de cláusulas-padrão para transferência internacional de dados pensado para as situações em que já exista em contrato firmado entre as partes a previsão de aplicação das cláusulas-tipo da Comissão Europeia, ou seja, um rol de disposições complementares – mas não conflitantes – com as europeias.

Nesta linha, sugerimos que na elaboração das cláusulas-padrão brasileiras, haja observância dos critérios estabelecidos no art. 46, II, c, do GDPR, além de documentos já disponibilizados pelo EDPB, inclusive um Q&A, acerca da aplicação e utilização desses mecanismos de transferência[9]. Sugerimos, ainda, a definição de parâmetros de utilização que não sejam excessivamente burocráticos e acabem tornando o uso do documento inviável para empresas globais. Recomendamos, também, que a estruturação das cláusulas-padrão se dê de forma clara e concisa para que empresas de pequeno porte possam utilizar sem tantos entraves, e para que não tenham dificuldades de compreensão.

Cumpre ressaltar que devido à sua natureza, as cláusulas-padrão contratuais, ao menos no cenário europeu e conforme recomendações da Comissão Europeia[10], não podem vincular as autoridades públicas de países terceiros, uma vez que estas não são parte signatária do contrato. Consequentemente, os exportadores de dados podem ter de agregar às garantias constantes das referidas cláusulas-padrão medidas complementares para assegurar o cumprimento do nível de proteção exigido pela legislação da União Europeia quando o dado pessoal for tratado por um

[8] Disponível em: https://www.gov.br/anpd/pt-br/semana-da-protecao-de-dados-2022/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais/participacao-da-anpd-no-cenario-internacional-e-a-regulamentacao-de-transferencias-internacionais-de-dados-pessoais. Acesso em 27/05/2022.

[9] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en . Acesso em 26/06/2022.

[10] Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_pt. Acesso em 27/05/2022. Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE

determinado país terceiro, circunstância que também pode tornar-se necessária no Brasil.

Quanto à estrutura a ser utilizada, a Comissão Europeia concebeu as SCCs para serem instrumentos dinâmicos e adaptáveis compostos por: cláusulas fixas, que se destinam a permanecer inalteradas independentemente das partes a elas submetidas; módulos, adaptáveis ao agente de tratamento (controlador ou operador) que figurará como exportador ou importador; e cláusulas e anexos em branco ("livres"), que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados, entre outras). É nesse sentido que recomendamos que a ANPD siga na elaboração do referido documento, de modo a serem dinâmicos e adaptáveis conforme a necessidade das partes envolvidas na transferência internacional.

É importante mencionar, ainda, que em razão de muitas empresas já utilizarem DPAs para regerem uma relação controlador-operador, caso elas também utilizem SCCs, em caso de divergência, os termos das SCCs prevalecerão sobre os do DPA ou sobre qualquer outro instrumento que discipline o tratamento de dados entre as partes[11]. Nesta linha, sugerimos que esta Autoridade oriente os agentes de tratamento de dados sobre as medidas a serem adotadas em caso de haver divergências entre um contrato inicialmente firmado e as disposições das cláusulas-padrão contratuais.

Ainda, vale mencionar que o EDPB[12] apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas-padrão contratuais, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção dos dados pessoais transferidos. É recomendável que esta Autoridade também oriente os agentes de tratamento em relação a tais medidas suplementares, o que os auxiliará na implementação de salvaguardas efetivas para garantir a proteção dos dados sob transferência internacional, bem como para garantir sua confidencialidade, disponibilidade e integridade.

Por fim, em linha com a resposta 19, sugere-se que seja incluída uma disposição nas cláusulas contratais padrão quanto à necessidade de o importador promover ao exportador comunicação prévia caso tome conhecimento da necessidade de divulgação de dados pessoais que sejam objeto da transferência internacional para autoridades públicas estrangeiras.

b. cláusulas contratuais específicas;

Ao consultar a legislação europeia sobre a aprovação de cláusulas contratuais específicas, observa-se que os artigos 46 (3) (a), e 46 (4) do GDPR sujeitam o

[11] Disponível em: https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32021D0914. Acesso em 25/05/2022. Cláusula 5ª - COMMISSION IMPLEMENTING DECISION (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[12] Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_pt. Acesso em 27/05/2022. Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE.

documento a autorização pela autoridade supervisora competente para, posteriormente, submetê-lo ao mecanismo de consistência pelo EDPB.

No entanto, tratando-se de cláusulas contratuais para situações de transferências específicas e não recorrentes, elas deverão descrever de modo claro a relação entre os propósitos do tratamento e a transferência internacional de dados pessoais de forma a facilitar e simplificar a utilização pelo agente. Nesta linha, deve indicar a salvaguarda da LGPD que consubstancia a operação (artigos 33 a 36, da LGPD), especificando a sua finalidade, discriminando as responsabilidades dos agentes de tratamento e o fluxo de dados, além também de indicar como serão garantidos os direitos e liberdades dos titulares de dados[13].

Em linha com o aplicado no cenário europeu, em caso de qualquer alteração às circunstâncias da transferência internacional, precisará haver a comunicação à Autoridade para sua reavaliação. Contudo, esses fatores podem gerar entraves aos processos de transferência internacional de dados, ao menos enquanto não esclarecido como será realizado.

Especificamente em relação às cláusulas específicas, já que utilizadas para cenários determinados, sugerimos a adoção de critérios que permitam um nível maior de flexibilidade em relação aos demais mecanismos de transferência, adotando, por exemplo, a linha das BCRs, cujas atualizações *"non-material"* não precisariam ser aprovadas pela Autoridade ou mesmo aspectos que, se alterados e caso não conflitem com premissas bases definidas pela Autoridade, dispensariam também referida aprovação.

Em relação à estrutura e conteúdo, um caminho possível seria verificar as antigas SCCs adotadas em 2001 e 2010 e atualmente substituídas, já que eram instrumentos contratuais elaborados para resolver situações específicas, como transferências C2C (entre controladores, no caso das SCCs de 2001) e as transferências C2P (de controladores para operadores, no caso das SCCs de 2010). As novas SCCs adotadas pela Comissão Europeia para transferências de dados pessoais para fora do Espaço Econômico Europeu levam em consideração abordagem diversa e mais abrangente do que as versões anteriores.

Ainda, vale frisar que o EDPB apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas-padrão contratuais, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção. É recomendável que esta Autoridade, portanto, também oriente os agentes de tratamento em relação a tais medidas suplementares, o que os auxiliará na implementação de salvaguardas efetivas para garantir a proteção dos dados sob transferência internacional, bem como para garantir sua confidencialidade, disponibilidade e integridade.

Por fim, em linha com a resposta 19, sugere-se que seja incluído como um critério para aprovação de cláusulas contratuais específicas a necessidade de o importador promover ao exportador a comunicação caso tome conhecimento da necessidade de divulgação de dados pessoais que sejam objeto da transferência internacional para autoridades públicas estrangeiras. Somada a essas medidas, a ANPD poderá endereçar o tema por meio de cooperação internacional com países nos quais houver

[13] Disponível em: https://portal.fgv.br/sites/portal.fgv.br/files/transferencia_internacional.pdf . Acesso em 27/05/2022.

um risco maior relacionado ao acesso de dados e vigilância por autoridades públicas estrangeiras.

c. normas corporativas globais.

Os critérios para elaboração de normas corporativas globais devem levar em conta os critérios para transferência internacional provenientes do cenário internacional, considerando que várias empresas situadas no Brasil têm sede fora do país e já vem adotando critérios da própria Comissão Europeia e GDPR.

Assim, sugerimos a utilização de parâmetros estabelecidos no art. 47 do GDPR, especialmente os relacionados ao conteúdo das normas corporativas globais, contendo em seu bojo aspectos como (i) a estrutura e os contatos do grupo empresarial ou do grupo de empresas envolvidas numa atividade econômica conjunta e de cada uma das entidades que o compõe; (ii) as transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão; (iii) o seu caráter juridicamente vinculativo; (iv) evidências que demonstrem o compromisso da organização empresarial em observar os princípios previstos no art. 6º da LGPD, sobretudo o princípio da transparência; (v) documentos que evidenciem que os Encarregados de todas as empresas do grupo que aderirem às normas estão alinhados em relação às salvaguardas que deverão ser implementadas para garantir proteção aos dados pessoais submetidos a transferência internacional; (vi) outros documentos que demonstrem a estrutura de governança da organização e seu nível de conformidade.

Além disso, recomenda-se a esta Autoridade que (i) determine para quais contextos serão admitidas normas corporativas globais (a exemplo da União Europeia, há dois tipos de BCRs, as de controlador e as de operador); e (ii) como se dará o processo de submissão do documento e consequente aprovação pela Autoridade das normas corporativas globais, se assim entender a ANPD, e seguindo a linha do adotado no contexto europeu e, de maneira a estabelecer o máximo possível de diretrizes para que este processo se torne mais simplificado e até mesmo menos moroso para os agentes.

De toda forma, o material disponibilizado no site da Comissão Europeia e as diretrizes do WP29 fornecem estrutura sugerida para um conjunto de BCRs, a fim de auxiliar empresas na elaboração das suas próprias regras e poderá vos servir de apoio à ANPD neste processo.[14]

No mais, para empresas cuja sede é fora do Brasil e que já tenham normas corporativas globais implementadas considerando os parâmetros europeus, espera-se que o papel desta Autoridade seja o de validar o documento para ser implementado no âmbito do Brasil, de modo que a organização não tenha que produzir um segundo documento com a mesma função. Assim, sugerimos a esta Autoridade também o endereçamento deste ponto.

Vale ressaltar que até o momento, a lista publicada pela EDPB[15] indica que desde 2018, 30 (trinta) normas corporativas globais foram aprovadas pelas autoridades

[14] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en#:~:text=Approval%20of%20binding%20corporate%20rules,-Companies%20must%20submit&text=The%20authority%20will%20approve%20the,more%20than%20one%20Member%20State. Acesso em 27/05/2022.

[15] Disponível em: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en. Acesso em 27/05/2022.

supervisoras sob o GDPR, para as quais o EDPB emitiu sua respectiva opinião/decisão vinculante. Tais instrumentos também podem servir como base para esta Autoridade.

Ainda, vale frisar que o EDPB[16] apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas-padrão contratuais, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção. É recomendável que esta Autoridade também oriente os agentes de tratamento em relação a tais medidas suplementares, o que os auxiliará na implementação de salvaguardas efetivas para garantir a proteção dos dados sob transferência internacional, bem como para garantir sua confidencialidade, disponibilidade e integridade.

Por fim, em linha com a resposta 19, sugere-se que seja incluído como um critério para aprovação de normas corporativas globais a necessidade de o importador promover ao exportador a comunicação caso tome conhecimento da necessidade da divulgação de dados pessoais para autoridades públicas estrangeiras.

6) Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?

A inclusão de países no rol daqueles com nível de proteção de dados considerado adequado, no contexto europeu (art. 45, GDPR), tem como intuito possibilitar um fluxo livre de dados pessoais entre a União Europeia e países terceiros, sem que seja necessário adotar salvaguardas complementares ou autorização adicional. Este racional é adotado pelo fato deste processo de avaliação, pela Comissão Europeia, ser mais demorado e realizado com base em critérios robustos e específicos, como o conteúdo das normas aplicáveis nos respectivos países, e a forma como é assegurada a sua aplicação efetiva pelo país[17].

Neste sentido, entendemos que os elementos previstos no art. 34 da LGPD, destinados à avaliação do nível de proteção de dados de países estrangeiros, devem ser utilizados nos instrumentos contratuais de forma macro, se limitando àqueles critérios que não impactem na fácil e objetiva aplicabilidade do instrumento contratual em questão.

Assim, entendemos que nos instrumentos contratuais devem ser considerados, pela ANPD, a natureza dos dados que serão transferidos (art. 34, II, LGPD), as medidas de segurança que serão adotadas (art. 34, IV, LGPD), além de outros fatores específicos inerentes à transferência (art. 34, VI, LGPD) que possam demandar a elevação do nível de proteção para que sejam resguardadas a confidencialidade, disponibilidade e integridade dos dados sob transferência.

Por fim, em linha com o art. 34, I da LGPD, é recomendável que esta Autoridade oriente os agentes de tratamento a fim de que os exportadores adotem medidas que visem garantir que os importadores os informem previamente caso o país

[16] Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_pt. Acesso em 27/05/2022. Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE.

[17] Disponível em: https://ec.europa.eu/newsroom/article29/items/614108. Acesso em 27/05/2022.

destinatário dos dados pessoais apresente normas que possam submeter a riscos os dados pessoais transferidos, o que inclui divulgações indevidas e/ou divulgações a autoridades/órgãos públicos[18].

7) As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?

Entendemos que, embora seja necessário um conteúdo pré-definido para que as empresas possam utilizar as cláusulas-padrão contratuais de maneira segura, objetiva e facilitada, é importante que seu conteúdo não seja rígido, mas modular, a fim de que o documento possa se amoldar às especificidades do contexto da transferência, de modo que possam ser mencionadas informações relevantes como os tipos de dados que serão transferidos, e de modo que o documento seja adaptável considerando os agentes de tratamento envolvidos na operação, sobretudo o tipo de agente que ocupará o papel de exportador, e o tipo de agente que figurará como importador.

Foi neste sentido, inclusive, que a Comissão Europeia implementou as SCCs, de forma que (i) o agente de tratamento que transferir os dados para o país terceiro é livre para incluir as SCCs em um contrato mais amplo, ou mesmo para adicionar outras cláusulas ou salvaguardas adicionais, desde que não conflitem com as já aprovadas pela Comissão[19]; (ii) as SCCs combinam cláusulas gerais com pontos de modulação e pontos "livres", para serem ajustados e complementados a depender dos diferentes cenários de transferência e da complexidade da cadeia de tratamento. Assim, em adição às cláusulas-padrão gerais, devem os agentes selecionar o módulo aplicado à determinada situação.

Vale mencionar, inclusive, que no sentido de uma flexibilização das cláusulas, a Comissão Europeia, ao emitir a decisão de implementação das SCCs em junho de 2021, adotou as chamadas *docking clauses*, que permitem que um importador ou exportador, a partir da autorização das partes originalmente constantes no instrumento jurídico, adentre às condições estabelecidas nas SCCs, desde que assinando um Anexo específico.[20]

Nesse sentido, a Comissão Europeia concebeu as SCCs para serem instrumentos dinâmicos e adaptáveis compostos por: cláusulas fixas, que se destinam a permanecer inalteradas independentemente das partes a elas submetidas; módulos, adaptáveis a depender do agente de tratamento (controlador ou operador) que

[18] Disponível em: https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32021D0914. Acesso em 25/05/2022. Recital 19 - Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[19] Disponível em: https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32021D0914. Acesso em 25/05/2022. Recital 3 - Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

[20] Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en . Acesso em 06/05/2022.

figurará como exportador ou importador; e cláusulas e anexos em branco, que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados, entre outras).

Deste modo, recomendamos que esta Autoridade siga na elaboração das cláusulas-padrão contratuais conforme modelo adotado pela Comissão europeia, incluindo tanto disposições fixas, quanto disposições modulares e anexos para preenchimento livre pelas partes..

Nesta linha, com foco em um viés regulatório, é recomendável que a ANPD possibilite que o importador e/ou exportador inclua, em espaço em branco ou mesmo em anexo específico, as legislações e regulamentos setoriais que de alguma forma se aplicam àquela relação e que porventura possam impactar no fluxo de dados ou na transferência internacional especificamente.

8) Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?

O formato mais adequado seria aquele que permitisse que o agente de tratamento escolhesse o clausulado de forma a abranger as especificidades da sua atividade de tratamento com determinado parceiro, mas que ao mesmo tempo desse ao agente uma segurança jurídica de que de fato foi adotada a cláusula mais pertinente para aquela relação. Neste sentido, trazer leques e subdivisões excessivas poderia até mesmo dificultar a escolha das cláusulas pelo agente e tornar complexo um mecanismo de transferência que deveria, a princípio, ser de fácil utilização.

Recorrendo à experiência internacional, a Comissão Europeia, ao adotar SCCs, optou pela modelagem das cláusulas[21], de modo que o documento é composto por (i) cláusulas fixas, que permanecem inalteradas independentemente das partes a elas submetidas; (ii) módulos adaptáveis a depender do agente de tratamento (controlador ou operador) que figurará como exportador ou importador; e (iii) cláusulas e anexos em branco, que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados envolvidos, entre outras).

A simplificação do modo como poderá se dar a modulação poderá evitar, inclusive, que o agente utilize as cláusulas de forma errônea, considerando o cenário fático.

Por outro lado, o ICO, no *International Data Transfer Agreement,*[22]disponibiliza ao agente de tratamento uma árvore de decisões, além de *checkboxes* para preenchimento, de forma um pouco mais fechada e direcionada. O formato adotado pelo ICO, por ter adaptações mais limitadas, pode ser capaz de evitar que as partes adicionem informações equivocadas no documento e o tornem inaplicável ou não aderente ao caso concreto.

[21] Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en . Acesso em 27/05/2022.

[22] Disponível em: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fico.org.uk%2Fmedia%2Ffor-organisations%2Fdocuments%2F4019536%2Fidta.docx&wdOrigin=BROWSELINK. Acesso em 25/05/2022.

Em todo caso, independentemente do critério a ser adotado pela ANPD, sugerimos um documento que seja autoexplicativo e contemple o que a autoridade espera (ao menos nos campos de livre preenchimento) em cada cenário relativo às transferências internacionais.

9) É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?

É sobremaneira necessário adotar módulos diferenciados, considerando o agente que figurará como exportador, e o agente que figurará como importador. Em linha com a resposta dada para a questão 7 e considerando que as obrigações atribuídas pela LGPD a cada agente de tratamento e suas responsabilidades são diferentes, bem como considerando o nível de autonomia que possuem para o tratamento de dados pessoais, entendemos ser importante que haja regras específicas para cada agente na transferência internacional de dados.

Nessa linha, de modo a buscar a harmonização com o cenário internacional, recomendamos que sejam adotados os requisitos já observados pela Comissão Europeia no documento *Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council*[23], bem como em seus anexos relacionados.

Em suma, houve a adoção pela Comissão Europeia de conjunto de cláusulas de controladores/operadores situados na União Europeia (ou sujeitos ao GDPR) para controladores/operadores situados fora da União Europeia (ou não sujeitos ao GDPR), com ajustes modulares capazes de permitir que tanto o controlador quanto o operador assumam papéis de exportador e importador. Ainda, foi dada a possibilidade de que outros agentes possam se valer das SCCs[24] originalmente firmadas, aderindo às cláusulas estabelecidas, o que impactará, inclusive, em uma melhor distribuição das responsabilidades entre os agentes, e na concentração, em um mesmo documento, de todo o fluxo relacionado à cadeia de tratamento, possibilitando maior controle sobre a atividade. Entendemos que este é um caminho que pode ser endereçado pela ANPD na estruturação das cláusulas-padrão contratuais.

No mais, de maneira geral e exemplificativa, nas transferências de dados de um operador para outro operador, o nível de exigências destinado ao importador deverá ser maior no que tange (i) as medidas de controle da atuação do importador (limitações relacionadas à transferências/compartilhamento de dados, por exemplo), (ii) deveres de cooperação e de notificação do agente exportador em situações que envolvam incidentes de segurança, (iii) deveres de cooperação e de notificação do agente exportador em situações que envolvam a necessidade de responder a requisições de autoridades competentes e/ou requisições de titulares de dados. Isto porque neste caso, o exportador deverá ter condições de assegurar que se mantenha o nível de proteção aos dados pessoais transferidos e, ainda, deverá ter condições de cumprir eventuais regras impostas pelo controlador nas atividades de transferência de dados que irá realizar.

[23] Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. Acesso em 25/05/2022.

[24] Disponível em: https://eur-lex.europa.eu/legal-content/EN-PT/TXT/?from=EN&uri=CELEX%3A32021D0914. Acesso em 25/05/2022.

Ainda de maneira exemplificativa, em transferências realizadas entre controladores, embora seja relevante que medidas de cooperação sejam implementadas, pela definição do papel do controlador na LGPD, não é necessário que haja rigor excessivo e subordinação em relação às atividades de tratamento por ele realizadas, de modo que é relevante que o exportador assegure que tomará conhecimento das atividades realizadas no escopo do tratamento, a fim de que possa manter o controle sobre os dados transferidos, tendo em vista a possibilidade de se dar sua responsabilização solidária em casos nos quais houver tratamento inadequado ou ilícito de dados pessoais.

10) Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?

Considerando o escopo diverso de aplicação de ambos os mecanismos, bem como a complexidade do fluxo de dados e a quantidade de agentes de tratamento envolvidos a depender do contexto da transferência, entendemos que os requisitos de ambos os instrumentos também devem ser distintos. Isto porque as Normas Corporativas Globais (*Binding Corporate Rules*, no contexto europeu) costumam ser direcionadas a empresas multinacionais, com um fluxo maior de atividades de tratamento e mais agentes envolvidos na operação, ao passo que as cláusulas-padrão contratuais (*Standard Contractual Clauses*, no âmbito da União Europeia), são mais comumente utilizadas para relações com agentes em menor quantidade, e uma menor complexidade no fluxo das atividades de tratamento.

Em linha com a ideia de uma harmonização internacional, sugerimos que, no que couber no âmbito de aplicação da LGPD, sejam utilizados os requisitos e parâmetros já estabelecidos pela Comissão Europeia para aprovação de ambos os instrumentos.

Em suma, as cláusulas-padrão contratuais necessitariam de uma construção e elaboração prévias pela Autoridade, de forma que uma vez tornadas públicas, estariam "pré-aprovadas" para utilização dos agentes. Seus requisitos de aplicabilidade devem englobar a adequada escolha de seus módulos específicos pelo agente exportador, caso este seja o formato escolhido pela ANPD, bem como deve ser exigido que o exportador e o importador avaliem previamente, se há leis ou normas do país terceiro que poderiam impactar em sua eficácia.

É recomendável, ainda, que o exportador tenha a obrigação de avaliar se as referidas cláusulas-padrão não contradizem com cláusulas estabelecidas nos instrumentos contratuais específicos firmados entre as partes, ou em outros mecanismos complementares eventualmente adotados para viabilizar a transferência internacional.

As Normas Corporativas Globais, por outro lado, decorrerão de uma ação positiva do agente de tratamento, no sentido de submeter o documento, elaborado de forma mais personalizada para o seu negócio, ao processo de aprovação da Autoridade. No que tange as referidas normas, é recomendável que a Autoridade disponha sobre informações específicas que deverão constar no referido documento, tais como: (i) políticas e procedimentos da Organização que demonstrem seu compromisso com a observância dos princípios previstos no art. 6º da LGPD; (ii) documento que evidencie as medidas de transparência que utiliza, bem como a maneira pela qual possibilita que os titulares exerçam seus direitos, à luz da LGPD; (iii) documentos que evidenciem o caráter vinculante das normas dentro da Organização; (iv) documentos que evidenciem que os Encarregados de todas as empresas do grupo que aderirem

às normas estão alinhados em relação às salvaguardas que deverão ser implementadas para garantir proteção aos dados pessoais submetidos a transferência internacional; (v) outros documentos que demonstrem a estrutura de governança da organização e seu nível de conformidade.

Por fim, é recomendável que as instruções relacionadas à composição e formato das normas corporativas globais sejam detalhadas a fim de possibilitar que as Organizações submetam a esta Autoridade, para aprovação, normas condizentes com o nível de robustez esperado, o que poderá tornar menos dificultoso o procedimento destinado à aprovação.

11) Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?

Sobre a definição de grupo econômico para fins de aplicação das normas corporativas podem ser considerados os seguintes critérios:

(a) estrutura corporativa única[25] ou com influência significativa de ao menos uma empresa nas decisões de outra, como direção, controle ou administração[26];
(b) combinação de recursos ou esforços[27] para alcançar interesses em comum[28];
(c) adoção de mecanismo aplicável a todas as empresas do grupo envolvidas e aos funcionários, de natureza juridicamente vinculante[29].

Referidos critérios permitem que sejam abrangidos grupos de empresas multinacionais com subsidiárias e afiliadas, franquias, consórcios, joint ventures ou parcerias profissionais, para os quais o ICO[30] indica a aplicação das *binding corporate rules*.

[25] Para fundamentar o critério de estrutura corporativa única, temos por base a nomenclatura "conglomerado" utilizada no art. 52, II da LGPD, que se refere à junção de duas ou mais empresas, de diferentes segmentos, que trabalham em função de uma única estrutura corporativa.

[26] O critério de influência também deve ser considerado, considerando a definição de "grupo econômico" disposta no art. 2º, §2º da CLT (Consolidação das Leis Trabalhistas). Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/Del5452.htm. Acesso em: 27/05/2022.

[27] Como segundo critério, recorremos às características de "grupo de sociedades" conforme art. 265 da Lei nº 6.404/76 (Lei das Sociedades Anônimas). Disponível em: https://www.planalto.gov.br/ccivil_03/Leis/L6404consol.htm Acesso em: 27/05/2022.

[28] O EDPB engloba no conceito de "grupo" o conjunto de empresas envolvidas em uma atividade econômica conjunta. https://ec.europa.eu/info/files/working-document-approval-procedure-binding-corporate-rules-controllers-and-processors-wp263rev01_en

[29] O critério tem fundamento no art. 47 (1) (a) do GDPR, o qual prevê a necessidade de que as BCRs sejam juridicamente vinculativas e aplicáveis a todas as entidades do grupo envolvidas na transferência. Ademais, utiliza-se por base o artigo 34, V da LGPD. Como exemplo, citam-se: acordos intragrupo, compromissos unilaterais vinculantes, políticas internas com precisão de sanções disciplinares para colaboradores, entre outros instrumentos.

[30] Disponível em: https://ico.org.uk/for-organisations/binding-corporate-rules/ Acesso em: 27/05/2022.

12) Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?

Primeiramente, recomenda-se que o nível de detalhamento seja coerente com as demais obrigações já impostas pela LGPD, seja para fins de atendimento aos princípios de transparência e livre acesso ao titular[31] e exercício de direito de acesso[32], seja para demonstração de conformidade pelo agente de tratamento, como por meio do registro das atividades[33]. Nesse último aspecto de responsabilização e prestação de contas, a sugestão também tem por base o art. 30 do GDPR[34], que apresenta detalhamento acerca das informações que devem constar no registro de atividades, bem como em orientações do EDPS[35].

Adicionalmente, as informações mínimas exigidas poderão ser complementadas com dados específicos acerca do compartilhamento de dados pessoais, com base em recomendação do ICO[36].

Diante dessas considerações, sugere-se como informações mínimas:

- os tipos de dados pessoais;
- as categorias de titulares envolvidos
- a finalidade específica do tratamento;
- o período de retenção;
- a identificação dos agentes de tratamento envolvidos;
- o país em que está localizado o agente de tratamento;
- a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares; e
- as medidas de segurança tecnológica e organizacional implementadas em relação ao compartilhamento e aos dados pessoais.

Essas informações podem ser apresentadas pelos agentes de tratamento por meio de preenchimento de anexos/formulários estruturados previamente pela ANPD nas cláusulas-padrão contratuais, bem como podem ser itens recomendados para inclusão nos demais mecanismos de transferência, notadamente aos instrumentos contratuais (acordo intragrupo, cláusulas contratuais específicas). Nesta hipótese, os agentes de tratamento poderão preencher diretamente o anexo/formulário, incluindo

[31] Para tanto, considera-se o rol de informações dispostas no art. 9º da LGPD.

[32] Sob este aspecto, considera-se o disposto no art. 19, II da LGPD acerca das informações que deveriam constar da declaração completa de acesso.

[33] A obrigação de registro de atividades aplicável aos agentes de tratamento está prevista no art. 37 da LGPD, porém não indica quais são as informações que devem ser mapeadas. Considerando o objetivo a que se propõe o registro, entendemos que se aplicam as informações dos artigos 9º e 19, II da LGPD, somados à base legal aplicável para a finalidade específica.

[34] No tocante ao art. 30 do GDPR, destaca-se ainda que o rol de informações apresenta peculiaridades entre o controlador e o operador, porém para fins de transferência internacional estas não alterarão a sugestão promovida.

[35] Disponível em: https://edps.europa.eu/data-protection/data-protection/reference-library/international-transfers_en Acesso em: 27/05/2022.

[36] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf Acesso em: 27/05/2022.

documentos que evidenciem as informações mínimas exigidas por esta Autoridade, ou indicar as referências de disposições nas quais as informações podem ser encontradas (por exemplo, numeração de disposições do instrumento contratual utilizado, bem como políticas e documentos do agente que sejam de conhecimento público e que estejam em locais facilmente acessíveis, como sua página da internet).

13) Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?

A princípio, entende-se que o potencial risco seria a incompatibilidade entre procedimentos. Isso porque cada grupo econômico seguiria seu próprio conjunto de regras, ou até mesmo voltado para setores econômicos que não guardam relação entre si e sujeitos a regulamentações setoriais que impactem as operações internas.

Todavia, as normas corporativas seguem padrões com base na LGPD para sua aprovação, portanto o espaço para divergências pode ser minimizado.

Nesse sentido, um risco decorrente de eventuais incompatibilidades procedimentais seria a possibilidade de os meios de supervisão e fiscalização não serem implementados com a mesma eficácia entre os agentes de tratamento envolvidos.

Para mitigar ambos os riscos, é possível considerar que as partes poderão acordar entre si um instrumento adicional, como uma cláusula contratual, demandar uma avaliação das normas corporativas da outra parte ou eleger um conjunto de normas a ser observado por ambas.

Por outro lado, embora normas corporativas globais não guardem qualquer relação de obrigatoriedade de que as regras sejam observadas para transferências externas ao grupo, suas disposições regulam temas semelhantes às cláusulas contratuais que seriam firmadas entre grupos distintos em seu lugar.

Com isso, o benefício notável seria a redução de burocracias no compartilhamento e a possibilidade de um fluxo de dados pessoais facilitado para empresas que já demostraram possuir procedimento internos eficientes.

Ademais, seria possível argumentar que esta poderia ser uma medida que incentivaria a elaboração de normas corporativas globais como meio de reduzir a exposição dos negócios a riscos, sendo benéfico para a imagem e reputação das empresas. Isso porque as operações com grupos que já obtiveram suas normas corporativas globais aprovadas poderiam ter maturidade necessária para resguardar os dados pessoais e seus titulares, uma vez que o cumprimento dos requisitos de atendimento às normas corporativas globais, idealmente já exigiria o desenvolvimento de um programa de governança em privacidade robusto.

Por fim, as normas corporativas globais poderiam constituir uma opção mais atrativa do que a adoção de cláusulas-padrão contratuais nesse cenário. Isso porque podem ser ajustadas para atender às necessidades do negócio e, uma vez implementadas e operacionais, são mais fáceis de serem mantidas e atualizadas, na medida em que esta Autoridade não precisaria aprovar suas atualizações não materiais, o que pode economizar tempo e custos[37].

[37] Disponível em: https://opiceblum.com.br/wp-content/uploads/2022/02/white_paper_transferencia_internacional_de_dados_v.final_.pdf Acesso em: 27/05/2022.

Para melhor visualização, resumimos os pontos na tabela abaixo:

Tabela da questão 13

Permissão de transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD	
Riscos	**Benefícios**
Incompatibilidade entre procedimentos.	Minimização de divergências com base na LGPD.
Possibilidade de os meios de supervisão e fiscalização não serem implementados com a mesma eficácia entre os agentes de tratamento envolvidos.	Maior harmonia na forma de interpretação e aplicação da LGPD nos processos de supervisão e fiscalização pela ANPD.
Pluralidade de legislações e regulamentações setoriais.	Possibilidade de utilização de instrumento adicional, como uma cláusula contratual, para demandar uma avaliação das normas corporativas da outra parte ou eleger um conjunto de normas a ser observado por ambas.
Maior burocracia para efetivar a transferência internacional.	Redução de burocracias no compartilhamento, e a possibilidade de um fluxo de dados pessoais facilitado para empresas que já demostraram possuir procedimento internos eficientes.
Maior exposição dos negócios ao risco por ausência de procedimento externo.	Menor exposição dos negócios ao risco diante dos procedimentos internos robustos, potencializando o fluxo de dados e preservando a segurança.
Maior tempo e custo para aprovação de atualizações nos instrumentos utilizados para fundamentar a transferência entre os agentes de tratamento.	Normas corporativas globais são mais fáceis de serem mantidas e atualizadas, na medida em a ANPD não precisaria aprovar alterações não materiais, economizando tempo e custos.

14) Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?

Ao consultar a legislação europeia sobre a **aprovação de cláusulas contratuais específicas**, observa-se que os artigos 46 (3) (a) e 46 (4) do GDPR sujeitam tais instrumentos à autorização pela autoridade supervisora competente e, posterior submissão ao mecanismo de consistência pelo EDPB.

Como exemplo de **fluxos para aprovação de normas corporativas globais**, diversas autoridades europeias se valem de formulários a serem preenchidos pelos agentes de tratamento, a partir de um questionário de itens essenciais e da submissão do arquivo com as normas corporativas globais. Os critérios para aprovação de normas corporativas globais são os pontos de referência analisados em conjunto com os requisitos do art. 47 do GDPR.

Até o momento, a lista publicada pela EDPB[38] indica que, desde 2018, 30 (trinta) normas corporativas globais foram aprovadas pelas autoridades supervisoras sob GDPR, para as quais o EDPB emitiu sua respectiva opinião/decisão vinculante.

Ainda, vale mencionar que o EDPB[39] apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas-padrão contratuais, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção.

No contexto regulatório da ANPD, o ideal é que fosse publicado um procedimento específico, contemplando minimamente os seguintes pontos:

a) definição de procedimento para aprovação de contratos específicos e normas corporativas globais, incluindo minimamente: prazos, requisitos, e formalização da decisão;
b) se cabe recurso, bem como a indicação do seu respectivo prazo e autoridade julgadora; e
c) forma de publicação dos contratos e das normas corporativas globais aprovadas.

15) Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?

Inicialmente, deve-se estabelecer o que serão consideradas "alterações na configuração original". Isso porque é natural que mudanças sejam realizadas a fim de otimizar o fluxo de informações e a continuidade das atividades.

Para tanto, sugerimos que as alterações nos seguintes aspectos da operação sejam considerados como "**alterações na configuração original**": (i) nova finalidade, não prevista em contrato; (ii) envio para outros países não previstos originalmente no contrato; (iii) forma e duração do tratamento diversa do previsto em contrato; (iv) mudança do controlador responsável; (v) compartilhamento com outros agentes ou terceiros; e (vi) alterações que representem riscos aos direitos e liberdades dos titulares.

Vale ainda frisar que **todos os direitos dos titulares previstos na LGPD deverão ser garantidos pelos agentes de tratamento**. Considerando o contexto de "alterações na configuração original" da transferência, destacamos alguns direitos para os quais deverá ser dispensada especial atenção:

(a) direito de acessar os dados que tratados sobre agentes de tratamento nessa nova configuração;
(b) direito de oposição ao novo tratamento, caso a nova configuração descumpra a LGPD;

[38] Disponível em: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en Acesso em: 27/05/2022.

[39] Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf Acesso em: 27/05/2022.

(c) direito de anonimização, bloqueio ou eliminação, caso o titular entenda que o novo tratamento seja excessivo, desnecessário ou em desconformidade com a LGPD;
(d) direito de correção, caso os dados estejam incompletos, inexatos ou desatualizados para a nova configuração; e
(e) o direito de peticionar perante a ANPD caso a nova configuração implique em violação à lei.

Como referência, a Comissão[40] Europeia esclarece acerca dos direitos de titulares em casos de transferências internacionais baseadas em cláusulas-padrão contratuais, reforçando especialmente o direito de que os titulares sejam informados acerca do tratamento, bem como sobre o direito de obtenção de uma cópia das cláusulas conforme utilizadas, nos termos do art. 15 (3) do GDPR.

Quanto à necessidade de **comunicação aos titulares** sobre a nova configuração da transferência, além do direito abrangente de que os titulares sejam informados sobre operações de tratamento, as circunstâncias que tornariam a **comunicação direta imprescindível** seria apenas quando o tratamento seja fundamentado no consentimento e a alteração disser respeito à finalidade, forma e duração do tratamento, bem como controlador responsável, com base no art. 8º, §6º da LGPD.

Referido artigo também faz menção às alterações referentes a "informações acerca do uso compartilhado". Sugere-se que a interpretação seja feita de forma flexível para não burocratizar eventual troca de agentes de tratamento e de países que não atraia risco aos titulares. Ademais, nesse aspecto, entende-se que aplicar-se-ia o direito de obter informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, o qual deve ser provocado ativamente pelo titular.

16) Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?

Dividimos a questão em três pontos: (a) resolução de conflitos entre agentes de tratamento, envolvendo instrumentos contratuais; (b) resolução de conflitos entre agentes de tratamento e titulares, envolvendo instrumentos contratuais; e (c) medidas para auxílio da ANPD na resolução de conflitos internacional.

Primeiramente, para resolução de conflitos entre agentes de tratamento, entendemos que o meio viável seria a indicação em contrato pela utilização de recursos de arbitragem, conciliação ou processo judicial, elegendo previamente a lei e jurisdição aplicáveis. Ainda, quanto à definição de lei aplicável, a ANPD poderá orientar que os agentes de tratamento considerem como aplicável a lei que tutela de forma mais rígida os direitos e garantias dos titulares de dados.

No que tange à resolução de conflitos entre agentes de tratamento e titulares, quando a transferência tiver por base um instrumento contratual, a ANPD poderá prever como orientação que os agentes de tratamento **determinem, no contrato, responsabilidades acerca**: (i) do fluxo de comunicação entre as partes para atendimento a requisições de titulares; (ii) da existência de meios facilitados para

[40] Disponível em: https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf Acesso em: 27/05/2022.

que o titular contate cada uma das partes; e (iii) da existência de procedimentos internos para lidar com as requisições dentro de um prazo razoável.

Ademais, dentro do papel de conscientização que compete à ANPD, entendemos que é **relevante a indicação aos agentes de tratamento e titulares**, por meio de **guias e orientações, acerca dos meios alternativos de resolução dos conflitos sobre privacidade**, para que possam optar livremente, tais como **mediação e conciliação**.

Quanto ao último ponto, acerca das alternativas para atuação da ANPD frente às questões internacionais para resolução de conflitos, a melhor alternativa poderia ser a **promoção de ações de cooperação com autoridades internacionais de natureza semelhante à ANPD**, ação cuja competência resta evidenciada no art. 55-J, IX da ANPD e que já tem sido colocada em prática.

Ademais, há uma lista[41] extensa e não exaustiva de *frameworks* de cooperação internacional sobre proteção de dados pessoais existentes, os quais a ANPD poderá integrar.

Os **contratos multilaterais** possuem seu benefício na medida em que garantem uma **maior padronização** na aplicação de **determinados entendimentos e regras** na comunidade internacional. Isso é particularmente relevante na medida em que, ao se falar de privacidade, a transnacionalidade costuma ser o padrão das empresas. Um contrato multilateral vai permitir **a padronização e comunicação regulatória**, e consequentemente, **desburocratizar o processo de transferência internacional** de dados. Por outro lado, pelo fato de os contratos multilaterais envolverem muitos países de jurisdições completamente diferentes, observa-se uma grande dificuldade em traçar diretrizes específicas e próprias para os temas. Nesse sentido, os contratos multilaterais, para atingir um número significativo de países, acabará tendo de ser extremamente genérico.

Os **contratos bilaterais**, por sua vez, possuem seu **benefício na medida em que diversas regras mais específicas poderão ser traçadas**, uma vez que envolvem um número bem menor de jurisdições. Eles seriam uma saída para contratos firmados com países com os quais ocorre uma quantidade muito significativa e determinante de fluxo de dados. Contudo, uma tendência com relação aos contratos bilaterais é a **priorização de fluxos com países mais desenvolvidos no aspecto de proteção de dados pessoais e privacidade, criando-se barreiras para trocas com uma gama mais abrangente e diversificada de países**.

Nesse contexto, portanto, cabe a esta Autoridade sugerir a elaboração de contratos multilaterais ou bilaterais entre países, fornecendo o conteúdo que deve estar presente.

Independentemente do instrumento escolhido, a resolução de conflitos no âmbito internacional poderá ser promovida especialmente a partir de padrões e princípios para as autoridades envolvidas, sem que isso represente uma decisão de adequação.

[41] Disponível em: https://edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/international-cooperation-cooperation-other_en Acesso em: 27/05/2022. No tocante aos *frameworks*, aplicáveis à ANPD, destacam-se: Organisation for Economic Cooperation and Development (OECD); Global Privacy Assembly (GPA) – global conference (successor of the ICDPPC); Global Privacy Enforcement Network (GPEN) – network of privacy enforcement authorities; Common Thread Network (CTN); Ibero-American data protection network (RIPD).

Por exemplo, cita-se o caso do *framework* decorrente da declaração conjunta[42] entre Comissão europeia e os Estados Unidos, correspondente a princípios para abrigar transferências entre os países, como uma forma de comprometimento das partes envolvidas, para posteriormente servir como insumo de uma decisão de adequação futura pela Comissão.

Nesse sentido, observa-se que cooperações internacionais podem ser feitas para resguardar as transferências internacionais e eventuais resoluções de conflitos, de forma paralela à avaliação cautelosa, e em observância aos critérios formais para tomada de decisões acerca do nível de adequação dos países.

17) Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?

Sugerimos que a ANPD elabore ferramentas para auxiliar os agentes de tratamento na gestão e documentação pertinente às transferências internacionais, como a disponibilização de materiais opcionais para os agentes de tratamento, como:

(a) guias para utilização das salvaguardas do art. 33 da LGPD, indicando, quando possível e pertinente, especificidades em relação a determinado setor regulado;
(b) estudos acerca da probabilidade de respeito aos direitos e garantias de titulares nos países (com base em diretrizes de recursos humanos, adesão a acordos internacionais e no estado das leis, por exemplo[43]);
(c) orientações para análise de riscos de transferência internacional com indicação de medidas de segurança e conformidade suplementares e aplicáveis ao contexto de transferências internacionais[44];
(d) modelos de planilhas para registro das operações que envolvam transferência internacional;
(e) *checklist* de análise de conformidade de terceiro (importador).

Vale reforçar o caráter opcional, embora incentivado, das medidas "c" a "e" acima indicadas, a fim de que não se torne uma obrigação adicional. Entendemos que a imposição de tal obrigação aos agentes poderia onerá-los excessivamente, bem como obstaculizar suas atividades, considerando que tais agentes poderão se valer de outras medidas de segurança, registro, avaliação de impacto e diligência de terceiros, com base em obrigações já dispostas na LGPD, a exemplo do que preveem os artigos 46 e 50 da lei.

[42] Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 Acesso em 27/05/2022.

[43] Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf Acesso em: 27/05/2022.

[44] Disponível em: https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf Acesso em: 27/05/2022.

18) Quais as melhores alternativas para resolver as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?

Entendemos que o cenário de responsabilização não deva se desviar das responsabilidades que já cabem aos agentes de tratamento a partir de sua atuação fática quanto à atividade desempenhada, ou seja, a depender se figuram como controladores - inclusive com as particularidades de controladores independentes e conjuntos -, operadores ou suboperadores. Para tanto, uma vez verificado que houve transferências posteriores a jurisdições não conhecidas ou até mesmo a outros importadores, o regime de responsabilidade deve seguir o disposto tanto nos artigos 42 a 45 da LGPD, quanto nas orientações já formuladas pela ANPD em seu Guia[45].

Quando houver mudança de jurisdição nas cadeias consecutivas de compartilhamento, estaremos diante de uma nova configuração de exportador-importador, de modo que o novo exportador também assumirá responsabilidade pela observância das regras dispostas nos artigos 33 a 36 e regulamentações futuras, ou ainda por regras próprias da legislação aplicável de sua jurisdição, o que poderia afetar a adoção de mecanismos da LGPD pelo novo exportador.

Este cenário não exclui eventual responsabilidade solidária entre todos os agentes de tratamento envolvidos, na medida em que cada um deverá cumprir com as regras impostas pela LGPD individualmente na operação de tratamento em questão.

Como meio de direcionar essa preocupação sem adicionar ao exportador original responsabilidades adicionais pelas transferências consecutivas, a alternativa encontrada pela Comissão Europeia foi a inclusão de "*docking clauses*"[46] opcionais nas *Standard Contractual Clauses*. Por meio desta cláusula, é possível que uma parte que não estava envolvida originalmente na relação, adira ao mesmo conjunto de obrigações e direitos, viabilizando a atribuição de responsabilidade entre os contratantes, sempre a partir do período de ingresso da terceira parte à relação.

Por exemplo, quando um controlador-exportador firmar cláusulas-padrão contratuais com um operador-importador, e houver a necessidade de compartilhamento posterior com um suboperador, se houver a inclusão de uma *"docking clause"* este último poderá aderir ao mesmo instrumento firmado pelo controlador-exportador.

A ANPD poderá considerar, ainda, a possibilidade de inclusão de anexos nacionais, nas cláusulas-padrão contratuais ou nas normas corporativas globais, que têm como principal objetivo inclusão de eventuais particularidades contidas em lei nacional, conforme proposto em consulta pública pelo ICO[47]

Já no que tange aos compartilhamentos na mesma jurisdição, entendemos que o importador inicial deve assegurar que terceiros porventura envolvidos se submetam às mesmas proteções resguardadas e exigidas pelo exportador inicial, bem como que

[45] Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/Segunda_Versao_do_Guia_de_Agentes_de_Tratamento_retificada.pdf Acesso em: 27/05/2022.

[46] Disponível em: https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en Acesso em: 27/05/2022

[47] Disponível em: https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk/ Acesso em: 27/05/2022.

os terceiros envolvidos serão documentados no registro de atividades mantido pelo importador. No mesmo sentido, as "*docking clauses*" opcionais indicadas pela Comissão Europeia também serviriam de exemplo aplicável para solucionar as questões de responsabilidade nesta relação.

Independentemente do cenário (dentro ou fora da mesma jurisdição), deve haver espaço para que os agentes de tratamento determinem entre si os limites à continuidade da cadeia de compartilhamento, na medida em que o exportador inicial poderá permitir, limitar ou proibir transferências, quando o importador inicial figurar como operador ou suboperador, bem como realizar eventual averiguação do cumprimento destas delimitações, visando maior proteção aos titulares envolvidos na operação.

19) Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?

Sugerimos que sejam adicionadas as seguintes medidas atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras:

a) **Comunicação prévia acerca do compartilhamento**: como meio de cooperação entre os agentes de tratamento, sugerimos a comunicação acerca do pedido de divulgação, nos casos em que a lei aplicável não impuser proibições nesse sentido.

   Considerando a legislação europeia, o EDPB e o EDPS[48] reforçam que em caso de pedidos de acesso dos tribunais e outras autoridades públicas, os importadores devem promover a comunicação antes de responder ao pedido. Tal recomendação, inclusive, é abarcada nas *Standard Contractual Clauses*, e, também sugerimos que seja contemplada nas cláusulas-padrão contratuais previstas no art. 33, II, b da LGPD".

b) **declaração sobre o regime legal**: conforme avaliação de riscos proposta pelo ICO[49], pode-se indicar a título de recomendação que o exportador avalie junto ao importador, ou que obtenha uma declaração deste último, acerca do regime legal do país de destino e a probabilidade de acesso de autoridades públicas aos dados pessoais (incluindo vigilância), bem como se existem limitações que podem ser impostas a este acesso.

   Vale a pena, ainda, considerar que acordos de cooperações técnica com autoridades reguladoras setoriais poderão gerar insumos valiosos acerca de como os pedidos de autoridades públicas estrangeiras são regulados internacionalmente, os quais poderão ser observados pelos agentes de tratamento a título de avaliação de riscos relativos à transferência internacional pretendida.

[48] Disponível em: https://edps.europa.eu/sites/edp/files/publication/edpb_edps_jointopinion_202102_art46sccs_en_1.pdf Acesso em: 27/05/2022.

[49] Disponível em: https://ico.org.uk/media/about-the-ico/consultations/2620397/intl-transfer-risk-assessment-tool-20210804.pdf Acesso em: 27/05/2022.

Compreende-se que esta Autoridade Nacional tem adotado a abordagem sugerida, diante dos acordos já firmados[50], de modo que sua expansão para demais setores como o de telecomunicações, financeiro e de saúde, por exemplo, são medidas que certamente trarão benefícios para a regulamentação do tema no Brasil.

A divulgação de dados para autoridades públicas estrangeiras também foi tema relevante no recente contexto das transferências referentes ao *Privacy Shield Framework*[51], revogado pela CJEU[52], destaca-se a abordagem adotada incluía sugestões de posturas voluntárias que poderiam ser adotadas como reforço de transparência, com a "emissão voluntária de relatórios periódicos de transparência sobre o número de pedidos de informações pessoais que recebem das autoridades públicas por razões de aplicação da lei ou de segurança nacional".

Ainda, a recente declaração conjunta[53] entre Comissão Europeia e os Estados Unidos possui o objetivo de restituir e aprimorar os princípios para abrigar transferências, dentre os quais estão incluídas regras e salvaguardas vinculativas para limitar o acesso aos dados por autoridades nos Estados Unidos ao que é necessário e proporcional para proteger a segurança nacional.

Assim tais medidas tratadas diretamente entre autoridades competentes podem criar um arcabouço de cooperação internacional e comprometimento para que agentes de tratamento possam compartilhar os dados pessoais em um ambiente mais seguro.

20) Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

Os mecanismos adequados são aqueles utilizados para fins de transparência, por meio dos quais os agentes de tratamento elencam as informações relevantes aos titulares de forma clara, adequada e ostensiva, nos termos do art. 9º da LGPD.

A título exemplificativo, cita-se o Aviso de Privacidade, cuja disponibilização pode ser feita por meio de canais acessíveis aos titulares, seja nos meios físicos ou digitais, bem como pode ser um instrumento abrangente ou específico para determinada transferência internacional. Ademais, é um documento pelo qual é possível assegurar o acesso gratuito e facilitado.

---

[50] Citam-se os Acordos de Cooperação Técnica firmados pela ANPD com CADE, Senacon, TSE e NIC.br. Disponíveis, respectivamente, em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-cade-assinam-acordo-de-cooperacao-tecnica; https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-senacon-assinam-acordo-de-cooperacao-tecnica; https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-tse-assinam-acordo-de-cooperacao-tecnica ; https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-e-nic-br-assinam-acordo-de-cooperacao; Acesso em: 27/05/2022.

[51] Disponível em: https://www.privacyshield.gov/article?id=16-Access-Requests-by-Public-Authorities Acesso em: 27/05/2022.

[52] Disponível em: https://noyb.eu/files/CJEU/judgment.pdf Acesso em: 27/05/2022.

[53] Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087 Acesso em 27/05/2022.

Quanto à forma de apresentação de informações, para maior efetividade, o agente de tratamento poderá optar pelo meio mais adequado à sua realidade e aos meios de interação com o titular, desde que promova ativamente a exposição de informações.

Sobre o tema, a doutrina europeia[54] provê recomendações para garantia de transparência, aplicáveis para o contexto de transferências internacionais, às quais dizem respeito: a disposição das informações em camadas, utilização de ferramentas como *pop-ups, dashboards*, avisos de privacidade específicos *(just-in-time), QR codes*, entre outros. Vale ressaltar que tais recomendações não possuem caráter vinculante, mas se apresentam como orientações aos agentes de tratamento.

Quanto à implementação do mecanismo eleito para conferir transferência, ainda que o agente de tratamento deva se atentar os requisitos do art. 9º da LGPD, não recomendamos a exigência de elementos adicionais obrigatórios para o contexto de transferência internacional, sob pena de que o titular seja impactado com um documento denso ou complexo em demasia, afastando o objetivo pretendido com o princípio da transparência.

[54] Disponível em: https://ec.europa.eu/newsroom/article29/items/622227 Acesso em: 27/05/2022.

Contribuição ADP Brasil - tomada de subsídios - transferências internacionais
Marcel Leonardi [redacted]
Qua, 29/06/2022 17:57
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

1 anexos (458 KB)
ADP – ANPD Questões Tomada de Subsídios - Transferência Internacional de Dados.pdf;
Caros membros da Coordenação-Geral de Normatização da ANPD,

Segue, em anexo, material de nossa cliente ADP Brasil relativo à tomada de subsídios sobre transferências internacionais de dados pessoais, com enfoque nas normas corporativas globais.

Essa contribuição complementa as respostas apresentadas na plataforma "Participa Mais" por este subscritor.

Agradecemos a gentileza de confirmar o recebimento desta mensagem e do anexo. Obrigado.

Marcel Leonardi
[redacted]
Rua Dr. Rafael de Barros | 209
Conj. 71 | Paraíso | CEP 04003-041
leonardi.adv.br

Always Designing for People®

TOMADA DE SUBSÍDIOS
Transferência Internacional de Dados e as Normas Corporativas Globais

Copyright © 2022 ADP, Inc. ADP Confidential.

1. TRANSFERÊNCIA INTERNACIONAL DE DADOS PESSOAIS E AS NORMAS CORPORATIVAS GLOBAIS

1.1. INTRODUÇÃO

1. A Autoridade Nacional de Proteção de Dados (ANPD) abriu, de 18/05/22 a 17/06/22, a tomada de subsídios para coleta de colaborações da sociedade para a elaboração do regulamento sobre transferências internacionais de dados pessoais. O objetivo da Autoridade é viabilizar a inserção competitiva de empresas brasileiras em cadeias globais de valor, garantindo, ao mesmo tempo, a efetiva proteção dos titulares e de seus dados pessoais. Para isso, disponibilizou diversas perguntas sobre o tema, a fim de orientar as contribuições dos interessados.

2. A ADP Inc. é uma empresa americana multinacional, com filial no Brasil (**ADP Brasil**) e atuação em mais de 140 países, que fornece serviços e softwares para soluções de Gestão de Capital Humano (HCM) hospedadas na nuvem que unem RH, Folha de Pagamento, Gestão de Talentos, Gestão de Ponto, impostos e benefícios, relatórios etc.

3. Os princípios de privacidade do titular e proteção dos dados estão incorporados no nosso modelo de negócios da empresa, em todas as etapas dos processos, à medida que projetamos e desenvolvemos novas tecnologias para nossos clientes parceiros. Tanto é assim que **a ADP Inc. está entre um grupo de elite de empresas mundiais que obteve a aprovação dos reguladores europeus para implementar as normas corporativas globais europeias**[1], chamadas de BCRs, como operador e controlador de dados.

4. Dessa forma, a **ADP Brasil vem**, em respeito à ANPD, por meio dessa contribuição, tendo em vista sua expertise e compromisso com os mais altos padrões de proteção de dados pessoais, **oferecer os seguintes subsídios sobre transferência internacional, em especial, no que se refere às normas corporativas globais**.

[1] Disponível em : <https://edpb.europa.eu/system/files/2021-03/edpb_information_20210126_pre-gdpr_bcrs_overview.pdf>.

Copyright © 2022 ADP, Inc. ADP Confidential.

1.2. IMPORTANTE: AUSÊNCIA DE HIERARQUIA ENTRE OS MECANISMOS DE TRANSFERÊNCIA INTERNACIONAL

5. Antes de adentrarmos nas normas corporativas globais, carece esclarecer que, na LGPD, **não existe relação hierárquica entre os mecanismos de transferência**. Aquele escolhido dependerá da finalidade e do contexto da transferência e da natureza dos dados pessoais, sendo necessário avaliar cuidadosamente o caso concreto para definir qual o mecanismo de transferência mais apropriado.

6. Com a tomada de subsídios sobre transferências internacionais de dados pessoais, lançada pela ANPD, é importante ressaltar essa ausência hierárquica entre os mecanismos: **entendemos que todos eles são igualmente importantes, e que a regulamentação proposta pela ANPD não deve priorizar nenhum deles em detrimento dos outros**.

1.3. NORMAS CORPORATIVAS GLOBAIS: CONCEITOS GERAIS

7. A LGPD prevê diversos mecanismos de transferência internacional de dados, como, por exemplo, o reconhecimento, pela ANPD, de que determinado país ou organismo internacional proporciona grau de proteção de dados pessoais adequado. Além disso, também prevê que essa transferência será permitida nos casos em que o controlador comprovar o cumprimento da legislação por meio de:

- cláusulas contratuais específicas para determinada transferência;
- cláusulas-padrão contratuais;
- **normas corporativas globais**; e
- selos, certificados e códigos de conduta regularmente emitidos.

8. As normas corporativas globais são regras de política interna, juridicamente vinculantes e aplicáveis à transferência de dados dentro de empresas que pertençam a um mesmo grupo econômico. Elas permitem que os dados sejam transferidos internacionalmente dentro do grupo, ainda que determinado país onde a empresa esteja presente não apresente regulamentação considerada suficiente para proteção dos dados transferidos.

Copyright © 2022 ADP, Inc. ADP Confidential.

Ou seja, as normas corporativas globais garantem que todas as transferências de dados dentro desse grupo econômico estarão em conformidade com a legislação de proteção de dados.

9. Elas são similares às *Binding Corporate Rules* (ou BCRs) do direito europeu. Nos termos do Regulamento Geral sobre Proteção de Dados ("GDPR"), uma das empresas do grupo submete sua política interna de proteção de dados pessoais para avaliação. A análise é feita pela autoridade nacional competente, conforme a localização da empresa.

10. Em geral, as BCRs devem conter os princípios de proteção de dados pessoais, como transparência, qualidade e segurança, os meios que garantem a efetividade da política interna do grupo (auditoria, treinamento etc.) e mecanismos que comprovem que a política seja, de fato, vinculante para as empresas do grupo.

11. No caso da ADP Inc. por exemplo, o fato de a empresa ter as BCRs reconhecidas na Europa permite que o grupo econômico transfira dados para os Estados Unidos sem sofrer sanções dos organismos de controle europeus. Isso ocorre, pois, as normas corporativas globais foram aprovadas pela Comissão Europeia e deverão ser aplicadas independentemente do país em que a empresa se encontre.

12. Sobre o tema, a LGPD menciona que, nas normas corporativas globais, o controlador deve oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados pessoais. Além disso, prevê a obrigação de comunicar à autoridade quaisquer alterações substanciais feitas nas normas, podendo ser necessária nova aprovação.

Copyright © 2022 ADP, Inc. ADP Confidential.

1.4. TOMADA DE SUBSÍDIOS DA ANPD E QUESTÕES ESPECÍFICAS SOBRE AS NORMAS CORPORATIVAS GLOBAIS

13. Na tomada de subsídios, a ANPD propôs as seguintes perguntas sobre o mecanismo:

> ***5)*** *Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê?*
> *a. cláusulas-padrão contratuais;*
> *b. cláusulas contratuais específicas; e*
> *c.* ***normas corporativas globais****.*
>
> ***10)*** *Há requisitos que precisam ser diferentes para* ***Normas Corporativas Globais*** *em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?*
>
> ***11)*** *Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das* ***normas corporativas globais****?*
>
> ***13)*** *Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas* ***normas corporativas globais*** *tenham sido aprovadas pela ANPD?*
>
> ***14)*** *Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de* ***normas corporativas globais*** *que poderiam servir de exemplo para a ANPD?*

14. Tendo em mente esses questionamentos e a influência do GDPR sob Lei Geral de Proteção de Dados (LGPD), iremos analisar o cenário europeu e quais orientações ele nos dá acerca da regulamentação das normas corporativas globais.

Copyright © 2022 ADP, Inc. ADP Confidential.

2. EXPERIÊNCIA POSITIVA EUROPEIA E OS BENEFÍCIOS DAS NORMASCORPORATIVAS GLOBAIS

2.1. FUNCIONAMENTO DAS *BCRs* NO DIREITO EUROPEU

15. Como mencionamos anteriormente, as normas corporativas globais, previstas pela LGPD, são similares às *Binding Corporate Rules* do direito europeu, e, assim como em relação às clausulas gerais contratuais europeias ("SCCs"), a União Europeia possui ampla experiência na aprovação dessas regras.

16. As BCRs permitem um nível a mais de governança e um maior controle sobre as práticas de proteção de dados pessoais, visto que essa não precisará ser analisada em cada contrato ou transferência dentro do mesmo grupo econômico.

17. De acordo com a autoridade de proteção de dados do Reino Unido ("ICO"), as BCRs são aplicáveis a grupos de empresas multinacionais, ou um grupo de empresas que exerçam uma atividade económica conjunta, como franquias, *joint ventures* ou parcerias profissionais.[2]

18. Em relação à parte operacional, nos termos do GDPR, uma das empresas do grupo submete sua política interna de proteção de dados pessoais para avaliação. A análise é feita pela autoridade nacional competente de determinado país-membro, conforme a localização da empresa e, posteriormente, validadas pela Comissão Europeia para que possam valer em todo território europeu.

19. Em geral, as BCRs devem conter os princípios de proteção de dados pessoais, como transparência, qualidade e segurança, os meios que garantem a efetividade da política

[2] Cf. https://ico.org.uk/for-organisations/binding-corporate-rules/

Copyright © 2022 ADP, Inc. ADP Confidential.

interna do grupo (auditoria, treinamento etc.) e mecanismos que comprovem que a política seja, de fato, vinculante para as empresas do grupo.

20. Caso o grupo tenha suas BCRs aprovadas, todas as transferências internacionais de dados pessoais intragrupo passam a estar em conformidade com o GDPR, não sendo necessário obter nova autorização da autoridade para realizá-las.

2.2. CRITÉRIOS PARA AVALIAÇÃO DAS *BCRs*

21. A Comissão Europeia indica que os seguintes elementos devem ser avaliados quando da aprovação ou rejeição de BCRs pela autoridade de proteção de dados:[3]

Critério	Explicação
Direito de petição	BCRs devem prever que o titular dos dados pessoais possa peticionar contra o agente do tratamento ou seu grupo empresarial perante a autoridade de proteção de dados de seu país.
Transparência	Grupo empresarial deve garantir transparência aos titulares dos dados compartilhados — informando, inclusive, sobre a circulação destes dados nas afiliadas. Direitos dos titulares devem ser garantidos e informados aos titulares.
Escopo de aplicação	BCRs devem especificar o escopo da transferência de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, os titulares afetados e a identificação do(s) país(es) terceiro(s). Além disso, os canais de contato devem se facilmente acessíveis aos titulares de dados.
Princípios de proteção de dados	BCR analisada deve conter princípios para o tratamento de dados pessoais que reflitam os princípios presentes no GDPR (e.g. finalidade, transparência, adequação, não-discriminação, etc).

[3] Working Document setting up a table with the elements and principles to be found in Binding Corporate Rules, elaborado pelo Working Party Article 29 e incorporados posteriormente pela EDPB. Cf. https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

Copyright © 2022 ADP, Inc. ADP Confidential.

Accountability	Todas as filiais que recebem dados pessoais e atuam como controladoras dos dados devem ser capazes de demonstrar o cumprimento das BCRs.
Solicitações de acesso por autoridades do país importador	BCRs devem conter provisões sobre solicitações de acesso a dados pessoais recebidas de autoridades governamentais de países terceiros, incluindo obrigações de notificação a titulares dos dados pessoais.

22. Assim como em relação às decisões de adequação, **os critérios da Comissão Europeia podem servir de base para o desenvolvimento dos critérios da ANPD** — reforçando, novamente, a importância da participação multissetorial na regulamentação do mecanismo.

23. Uma recomendação adicional, fundamental no cenário brasileiro, seria associar a aprovação de BCRs às decisões de adequação de determinado país (art. 33, I) proferidas pela ANPD. Entendemos que **a ANPD deve reconhecer a aprovação (ou facilitar a aprovação rápida) de BCRs que já tenham sido aprovadas por autoridades de proteção de dados de países que receberem decisão de adequação[4] da ANPD**. Isto garantiria mais dinamicidade na utilização do mecanismo e evitaria sobrecarregar a própria ANPD.

24. Por exemplo, caso a ANPD viesse a reconhecer o bloco de países da União Europeia como devidamente adequado, isso significaria que as BCRs aprovadas pela Comissão Europeia teriam trâmite acelerado na análise pela Autoridade.

2.3. BENEFÍCIOS DA IMPLEMENTAÇÃO DAS NORMAS CORPORATIVAS GLOBAIS

25. Conforme abordado anteriormente, as normas corporativas globais garantem uma série de regras acerca da transferência de dados de clientes, colaboradores e terceiros, independente de onde esses dados serão tratados. Um grupo econômico, ao optar por adotar as normas globais no lugar de outro mecanismo, terá diversos benefícios para seu

[4] Trata-se de outro mecanismo de transferência internacional de dados previsto na LGPD. Nos termos do Art.33, I "*a transferência internacional de dados pessoais somente é permitida (...) para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei*".

Copyright © 2022 ADP, Inc. ADP Confidential.

negócio, dentre eles:

- **Padrão único global**: As normas corporativas globais são legalmente vinculantes após serem aprovadas, ou seja, as empresas que integram o grupo econômico não possuem discricionariedade sobre sua aplicação. Isso faz com que haja um maior controle, por parte das autoridades de proteção de dados, acerca da transferência internacional.

- **Adaptabilidade**: em um modelo de negócios de um grupo econômico que atue em diversos países, com os mais variados modelos regulatórios, a adoção de normas corporativas globais permite uma maior adaptabilidade às diversas dinâmicas e processos entre as diversas empresas. A utilização das cláusula-gerais contratuais poderia gerar mais gastos para empresa e uma maior burocracia, bem como maior complexidade aos processos internos do grupo.

- **Alto padrão de *compliance***: As normas corporativas globais também representam um alto padrão de *compliance* global, diminuindo os riscos de incidentes de segurança nas transferências internacionais do grupo Econômico.

- **Celeridade**: Caso a ANPD opte por validar todas as BCRs aprovadas por países com mesmo nível de adequação, a autoridade será menos sobrecarregada com demandas de avaliação de BCRs.

Copyright © 2022 ADP, Inc. ADP Confidential.

3. CONSIDERAÇÕES FINAIS

3.1. CONCLUSÕES GERAIS

26. Tendo em vista sua atuação global com foco na privacidade e na proteção dos dados, bem como sua experiência relativa à aprovação de suas BCRs na União Europeia, **a ADP Brasil espera ter trazidos subsídios que contribuam com a regulamentação das normas corporativas globais pela ANPD**.

27. Entendemos que os critérios da Comissão Europeia podem servir de base para o desenvolvimento dos critérios da ANPD — reforçando, novamente, a importância da participação multissetorial na regulamentação do mecanismo.

28. Ao lado disto, recomendamos fortemente que a ANPD deve reconhecer a aprovação (ou facilitar a aprovação rápida) de normas corporativas globais/BCRs que já tenham sido aprovadas por autoridades de proteção de dados de países que receberem decisão de adequação da ANPD. Isto garantiria mais dinamicidade na utilização do mecanismo e evita sobrecarregar a própria ANPD.

29. Ressaltamos que o desenvolvimento e fortalecimento desse mecanismo de transferência internacional é necessário e fundamental para que as empresas que atuam no Brasil cumpram com a LGPD, sem inviabilizar sua atividade econômica.

30. A atuação da ANPD está presente na maior parte dos mecanismos de transferência internacional, seja elaborando modelos ou aprovando documentos recebidos dos controladores. Assim, a tomada de subsídios feita pela ANPD é extremamente necessária.

31. Por fim, vale ressaltar novamente que **não existe relação hierárquica entre os mecanismos de transferência**. Aquele escolhido dependerá da finalidade e do contexto da transferência e da natureza dos dados pessoais, sendo necessário avaliar cuidadosamente cada caso concreto para que se definir qual o mecanismo de transferência mais apropriado. Justamente por isto, entendemos que a ANPD não deve priorizar a regulamentação de um mecanismo de transferência em detrimento de outro.

Copyright © 2022 ADP, Inc. ADP Confidential.

32. Pela larga experiência que temos no uso de normas corporativas globais no contexto europeu, a ADP Brasil gostaria de reforçar os seguintes pontos:

- BCRs são um padrão internacionalmente reconhecido para proteção de dados pessoais e consistem em políticas desenvolvidas internamente por determinado grupo econômico.

- BCRs fornecem um conjunto consistente de regras internacionais sobre a transferência de dados pessoais de clientes, funcionários e terceiros, as quais serão aplicadas independente de onde esses dados forem tratados, que se tornam legalmente vinculantes assim que aprovadas pela autoridade de proteção de dados.

- As autoridades europeias consideram as BCRs como a melhor opção para proteger os direitos dos titulares, de acordo com os requisitos do GDPR.

- Atuando como operadora de dados pessoais com BCRs aprovadas, a ADP ajuda milhares de clientes e parceiros a atenderem aos mais altos padrões relacionados à proteção de dados, eliminando custos, documentação e burocracia associados à transferência internacional de dados, quando realizada por meio de outros mecanismos de transferência.

- Em outras palavras, por meio das BCRs da ADP, milhares de clientes e parceiros obtêm uma solução para transferência de dados de titulares europeus, atendendo às necessidades de negócios multinacionais. Além disso, as normas corporativas globais proporcionam maior clareza e consistência ao mecanismo de transferência, decorrentes da adoção de um único padrão global.

- Nossas BCRs estão incorporadas às políticas de compliance e processos internos da empresa, fornecendo um nível extra de proteção e governança aos dados tratados.

Copyright © 2022 ADP, Inc. ADP Confidential.

3.2. RESPOSTAS ESPECÍFICAS ÀS PERGUNTAS SOBRE NORMAS CORPORATIVAS GLOBAIS

Questão	Resposta
5) Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê? **a. cláusulas-padrão contratuais;** **b. cláusulas contratuais específicas; e** **c. normas corporativas globais.**	Critérios utilizados pela Comissão Europeia (Cf. seção 2.2).
10) Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?	A empresa deve comprovar que as políticas internas de proteção de dados resguardam todos os direitos previstos na LGPD e que contêm expressamente os princípios gerais previstos na lei. Ao lado disso, a avaliação das BCRs a partir dos critérios da seção 2.2 será suficiente.
11) Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?	Recomendamos que a definição de grupo econômico reflita aquela presente no Art. 4(19) do GDPR: um grupo composto pela empresa que exerce o controle e pelas empresas controladas.
13) Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?	Ao aprovar as normas corporativas globais, a ANPD reconhece que as políticas internas dos grupos econômicos são adequadas e suficientes para garantir os direitos dos titulares de dados, previstos na legislação nacional. Dessa forma, ao permitir a transferência de grupos distintos, mas ambos com as normas corporativas globais aprovadas, cria-se uma melhora no ambiente de negócios, facilitando a troca de informações e dados entre as empresas, ao mesmo tempo em que se resguardam os direitos dos titulares. Quanto ao risco, este pode ser considerado minimizado ao constatar-se que há uma preocupação mútua entre

Copyright © 2022 ADP, Inc. ADP Confidential.

	os grupos de que ambos estejam atuando em conformidade com a lei.
14) Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?	A Comissão Europeia de Proteção de Dados disponibiliza, em seu site, todas as normas corporativas globais aprovadas e as respectivas empresas, bem como as cláusulas-padrão contratuais. Tendo em vista a forte influência da legislação europeia sobre a brasileira, elas podem servir como exemplo para a ANPD.

Copyright © 2022 ADP, Inc. ADP Confidential.

CIPL Response to ANPD Request for Comments on the Regulation of International Data Transfers
Smith, Mark [redacted]
Qua, 29/06/2022 12:32
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Cc:

- [redacted]
- ANPD - International <international@anpd.gov.br>

Dear Commissioner,

Attached please find a PDF version of the comments submitted by the Centre for Information Policy Leadership (CIPL) on ANPD's Request for Comments on the Regulation of International Data Transfers.

We attempted to file our comments via the online portal on 29 June 2022, but we received the following message:

> This request has been blocked.
>
> In case of doubt, please send the code 12943736707981488822 in the subject of the message to the email address Bloco.de.aplicacoes@presidencia.gov.br .
>
> Requests not related to this blocking alert will not be handled through this channel.
>
> Technology Directorate of the Presidency of the Republic.
>
> [Go Back]

When we selected [Go Back] and attempted to resubmit our comments, we received the message: Sua opinião já foi registrada em 29/06/2022 (Your opinion has already been registered on 29/06/2022).

We ask that you please accept the attached PDF in case of an error with the portal.

Please let us know if you have any questions.

Kind regards,
Mark Smith

Centre for Information Policy Leadership
HUNTON ANDREWS KURTH

Mark E. Smith, CIPP/C/US, CIPM
Privacy & Data Policy Manager
Centre for Information Policy Leadership
[redacted]
p 202.419.2134
m 202.557.5147

Hunton Andrews Kurth LLP

2200 Pennsylvania Avenue, NW
Washington, DC 20037

HuntonAK.com

FINAL

CIPL Response to ANPD Request for Comments on the Regulation of International Data Transfers

Submitted 29 June 2022

International data transfer mechanisms have become a key instrument both for the adequate protection of data subjects' rights and for the development of the digital economy and international trade. Given the urgent need to regulate such mechanisms, ANPD plans to issue the regulation in stages. The first stage will have as scope the contractual instruments for international transfers of personal data, under article 33, II, (a), (b), and (c), of the LGPD, which are the standard contractual clauses, the specific contractual clauses, and the binding corporate rules.

To facilitate the understanding of the questions, consider "exporter" as the data processing agent[1] located in Brazil who will transfer the personal data to an importer situated in another jurisdiction, and "importer" as the processing agent located outside the Brazilian jurisdiction who will receive such data from the exporter.

ANPD welcomes contributions to any of the questions below. It is not mandatory to provide answers to all of the questions.

1) What are the current obstacles for companies to transfer data from Brazil to other countries? And from other countries to Brazil?

The Centre for Information Policy Leadership (CIPL)[2] welcomes the opportunity to comment on international data transfers and commends the ANPD on initiating the wide and inclusive consultation of key stakeholders on this critical topic.

Initially, CIPL notes that it would be helpful for ANPD to clarify the scope of what constitutes an international data transfer under Brazil's General Data Protection Law (LGPD) to which the various transfer mechanisms discussed below would apply. This would eliminate one preliminary obstacle to engaging in accountable data transfers. The European Data Protection Board (EDPB) addressed a similar issue in its Guidelines 05/2021, and we encourage ANPD to identify the criteria that would qualify a processing as an international transfer.

Specifically in response to the question, the principal obstacle for companies currently transferring personal data from Brazil is the lack of transfer mechanisms under LGPD arts. 33-36 duly regulated by ANPD.

If ANPD chooses to draft standard contractual clauses (SCCs) pursuant to LGPD art. 33(II)(a), CIPL encourages ANPD to develop simple, straightforward, high-level, outcome-based contractual clauses, ensuring that organizations have the flexibility to adapt provisions to their specific data processing

[1] *For the purposes of the Brazilian General Data Protection Law, the definition of processing agent refers to controllers or processors.*

[2] CIPL is a global privacy and data policy think tank in the law firm of Hunton Andrews Kurth LLP and is financially supported by the law firm and 89 member companies that are leaders in key sectors of the global economy. CIPL's mission is to engage in thought leadership and develop best practices that ensure both effective privacy protections and the responsible use of personal information in the modern information age. CIPL's work facilitates constructive engagement between business leaders, privacy and security professionals, regulators and policymakers around the world. For more information, please see CIPL's website at http://www.informationpolicycentre.com/. Nothing in this submission should be construed as representing the views of any individual CIPL member company or of the law firm of Hunton Andrews Kurth.

operations and transfer scenarios, including the flexibility to incorporate language already used in existing contractual instruments. Similar to the approaches taken by Australia, Hong Kong, New Zealand, and Singapore, ANPD could provide options for SMEs and startups with limited resources to create customizable clauses that would satisfy the LGPD's requirements. See, for example, the Model Contract Clauses Agreement Builder offered by New Zealand's Office of the Privacy Commissioner. For larger organizations with more robust resources, ANPD could list the type of protections and outcomes that need to be achieved and addressed in the contract under the LGPD and leave it to the parties to create the appropriate wording in their commercial contracts. Such a flexible approach to international data transfers would position ANPD as a global leader and could positively impact emerging privacy regulations in other countries as well.

ANPD could also take a further step by endorsing a high-level clause wherein the data recipient would simply guarantee compliance with the rights of the data subject and the obligations of the data protection regime under the LGPD. Such an outcome-based clause could be amended by the contracting parties with further specifications as needed under the circumstances.

Furthermore, ANPD could turn its focus to multilateral international certifications and mutual recognition measures, such as the Global Cross Border Privacy Rules (CBPR) system, discussed in response to Question 2.

Regardless of how ANPD decides to move forward, ANPD should provide a sufficient transition period for organizations to implement changes and satisfy the requirements of the new regulation. ANPD should also increase its outreach, engagement, and training with the impacted organizations to help drive understanding and compliance with the new rules. This is a new area of compliance for many Brazilian companies, and they will need some additional and specific direction through the process.

2) What is the best way to promote convergence and interoperability between contractual instruments for international data transfers with instruments from other jurisdictions? And how can ANPD act in this regard?

As explained in our answer to Question 1, CIPL encourages the development of simple, straightforward, high-level, outcome-based contractual clauses, ensuring that organizations have the flexibility to adapt provisions to their specific data processing operations and transfer scenarios, including the flexibility to incorporate language already used in existing contractual instruments. Outcome-based clauses ensure that the data recipient complies with the relevant data protection principles and obligations of the LGPD.

Also, ANPD should engage with the EU, UK, and other jurisdictions that have issued SCCs to explore ways to support mutual recognition of such instruments while ensuring (perhaps by way of an addendum, when needed) compliance with the LGPD's requirements.

CIPL notes that interoperability between contractual instruments is essential, both within Brazil and internationally, and should be enabled as much as possible. It ensures greater security and legal certainty for all existing and validated contractual instruments and helps organizations minimize administrative burdens and legal costs related to multiple sets of SCCs governing complex and multi-jurisdictional data flows.

In the same vein, ANPD should take into account privacy and data protection-related regulations already adopted by other regulators in Brazil (such as the Central Bank). We encourage ANPD to review such regulations and work with sectoral regulators to ensure consistency with the LGPD.

Moreover, ANPD should ensure that any contractual provisions relating to the international transfer of data are not so burdensome as to result in de facto data localization – a scenario where data may only be processed, accessed, and stored in Brazil. Such a framework would be highly onerous, harming both businesses and the Brazilian people.

CIPL further encourages ANPD to participate in the Global Cross Border Privacy Rules (CBPR) system in reliance on arts. 33(II)(d), 35 and 36 of the LGPD. The recently established Global CBPR Forum[3] is in the process of transitioning the current APEC CBPR into Global CBPR, which would enable non-APEC countries like Brazil to participate in the system. Participation in a global framework such as the CBPR has an added benefit of lessening the burden on resource-limited regulators like ANPD because front-line oversight and compliance are handled by third-party certification bodies, but ultimate enforceability would remain with ANPD and other global data protection authorities that participate in the system.

Similarly, we encourage ANPD to recognize the validity of certifications and other approval-based transfer mechanisms that organizations have received from other jurisdictions that offer the same level of protection as the LGPD, as they indicate that a robust regulatory review of processes and controls has taken place. This would enable organizations that already work with those transfer mechanisms to use them in Brazil as well, which would increase efficiency and reduce compliance costs.

3) What are the most effective and the most used instruments to enable international data transfers by large and small companies or organizations?

Based on CIPL's 2016 and 2017 surveys with Avepoint on GDPR readiness, standard contractual clauses were the most popular transfer mechanism used, with about half of all respondents (49.6%) relying on model clauses for international transfers. We believe the findings are still relevant today. While use of the now-defunct Privacy Shield (for US-EU transfers) was the second most popular transfer mechanism at the time (averaging at 32.6%), many organizations are still maintaining certification in hopes of a new agreement between the US and EU. Roughly one-in-five (21.6%) relied on BCRs. See Organisational Readiness for the European Union General Data Protection Regulation.

a) Most organizations today use private contracts—in particular, standard contractual clauses (SCCs)—to legitimize the transfer of personal information across borders from jurisdictions that impose transfer restrictions, as there are so few other choices. Whether such contracts are "effective," however, is a matter of debate. Experts from industry and civil society have often commented that the use of lengthy, detailed SCCs is unsustainable in the long run, given the enormous and growing number of cross-border transfers to vendors, processors, sub-processors, third-party business partners, other data controllers, etc., and the fact that data transfers are dynamic, involve changing data sets, and are part of evolving business models. Indeed, SCCs are at times cumbersome and unworkable, especially for multiple transfers between multiple parties in multiple jurisdictions. To the extent ANPD is developing a framework for data transfers based on contracts, ANPD should consider SCCs that are outcome-based, flexible, and modular. See also our response to Question 1.

[3] For additional information, see the Global Cross-Border Privacy Rules Declaration, https://www.commerce.gov/global-cross-border-privacy-rules-declaration.

b) Certification and codes of conduct schemes may be the most effective data transfer instruments, since they are consistent and public, thereby enhancing accountability while avoiding excessive contractual paperwork. Many organizations were hoping to use certifications after the GDPR came into force, but this mechanism has not yet gained traction. Still, some organizations have obtained certification with the APEC CBPR, and with the launch of the Global CBPR Forum, there is an expectation that CBPR certifications will increase. For additional information on the Global CBPR Forum, see our response to Question 2.

c) Multinational companies use Binding Corporate Rules (BCRs) to enable intra-group data transfers (to and from internal controllers and processors) and transfers of controllers' data across an external processors' global organization (BCR processor). These companies see BCRs as a form of certification or seal to confirm trusted and protected data flows within the international group of companies, as well as a way to demonstrate compliance with local laws based on a single data privacy compliance program across multiple countries. BCRs require a significant investment of time and resources and therefore are currently limited to large, international organizations. For our views on BCRs, see our response to Question 5c.

d) Many organizations use (or would like to use more broadly) specific legal bases for particular types of transfers, such as when necessary for the execution of a contract or for compliance with a legal obligation. As provided in the LGPD, ANPD should clarify how organizations may use stand-alone legal bases for data transfers, including for routine and repeated transfers. Providing these legal bases for transfers would ensure that businesses relying on cross-border data flows for their products and services will not be blocked from the Brazilian market, as could happen if their ability to transfer data were jeopardized.

4) What are the main benefits and impacts of international data transfers, and what are the best alternatives for addressing them in each of the contractual instruments for data transfers included in the LGPD and in international practice?

International data transfers drive today's global economy and growth. The ability to send (and receive) data from Brazil to other countries is critical to the success and security of Brazil's economy and society. The free flow of data allows organizations and individuals to access the best available technology and services at the best prices and safely engage in commerce, irrespective of where they are located. Today's digital economy and technologies demand that vast amounts of electronic data flow seamlessly across jurisdictions. The ability to use, share, and access information across borders enables research and development, fuels data-driven products and services, and promotes the exchange of ideas and information. It fosters innovation and competition by allowing new entrants access to data, which opens new markets and opportunities. It also benefits individuals, as it enables access to services and products across the globe and supports the growing reality of the Internet of Things.

International data transfers help organizations detect and prevent payment fraud and other crimes, and they also help them to conduct due diligence to comply with anti-money laundering (AML), counter-terrorist financing (CTF), anti-bribery and corruption (ABC), know-your-customer (KYC), and other rules. Data sharing across borders can also play a key role in countering discrimination and unconscious bias in development of AI technologies by providing access to larger, more representative and diverse data sets for the development of new artificial intelligence systems. Further, cross-border data flows can enhance data security and privacy protections. They ensure that companies of all sizes

can take advantage of decentralized data storage solutions and shared systems that are resilient to outages from malfunctions or natural disasters, as well as unauthorized access by third parties.

While the instruments for data transfers found in LGPD art. 33, II—namely, (a) specific contractual clauses for a given transfer, (b) standard contractual clauses, and (c) binding corporate rules (which are the three transfer mechanisms directly at issue in this consultation)—can all be useful to facilitate cross-border data flows in some contexts, they are not always well suited in their current forms for new technology trends (e.g., cloud platforms, artificial intelligence) and modern day data transfers that may include multiple parties, non-linear and fluid/dynamic data flows, and onward transfers between service providers and subcontractors.

To enable these data transfer mechanisms to achieve the outcome of facilitating and promoting free and trusted data flows, they should be made flexible and agile. For example, companies that have obtained approval for BCRs should be able to use them as a basis for transfers with another BCR-approved company, and not restricted to a single group of related entities for internal data transfers. This is a logical and progressive interpretation of BCRs, as both companies are deemed to have a high level of data protection within their groups for all data they process, including data received from other organizations. Equally, as mentioned above, contractual clauses must be flexible, modular, and outcome-based, to enable organizations of all sizes to use them with ease and without steep legal costs.

5) Which criteria and/or requirements should be considered in regulating each of the following international data transfer mechanisms and why?

a. standard contractual clauses;

Flexibility must be integrated in high-level, outcome-based clauses, ensuring that organizations have the ability to adapt provisions to their specific data processing operations and transfer scenarios, including the freedom to incorporate language already used in existing instruments. Outcome-based clauses ensure that the data recipient complies with the relevant data protection principles and obligations of the LGPD. A flexible instrument could provide a modular approach. It would also permit organizations to take risk factors into consideration, which would promote the efficient allocation of resources to implement additional safeguards to account for varying degrees of risk that might be associated with a particular transfer, keeping in mind that not all cross-border transfers are inherently risky.

b. specific contractual clauses; and

Initially, it would be helpful to clarify the distinction between standard contractual clauses and specific contractual clauses, which require prior authorization by ANPD before making a specific transfer. Because transfer-specific clauses with the attendant approval period could prolong negotiations and encumber commerce, CIPL encourages ANPD to streamline the process with a list of points to address or factors to be considered when drafting the clauses. ANPD could also develop a toolbox that provides guidance for organizations seeking the authorization of ANPD. But again, such clauses should afford a flexible, outcome-based approach.

c. binding corporate rules.

Binding corporate rules (BCRs) are currently data protection policies for the transfer of personal data within a group of undertakings or enterprises. Because BCRs require a significant investment of time and resources, BCRs are commonly an option only for large, international organizations. To facilitate

their wider use, BCRs need to be made scalable and configurable to the needs of organizations of all sizes and corporate structures. Moreover, their use should be explored beyond the confines of intra-corporate transfers (as discussed more fully below in response to Questions 10 and 11). Indeed, ANPD can play an important role in expanding the reach and accessibility of BCRs to small and medium enterprises (SMEs).

CIPL also encourages ANPD to consider the following suggestions pursuant to art. 33(II)(c), art. 35, and art. 36 of the LGPD:

- Endorse BCRs authorized by the EU, the UK, and other jurisdictions based on art. 35 of the LGPD. Upon accession to those BCRs, Brazilian entities within the corporate family would assume all the rights and obligations according to the existing BCRs. This can significantly facilitate compliance with applicable rules for companies active in the EU, the UK, and Brazil.
- Engage with regulators in the EU and UK (and other jurisdictions with BCRs) to support mutual recognition of BCRs developed by the ANPD.
- Recognize existing BCRs in force and approved in other jurisdictions that offer the same level of protection as the LGPD.
- Avoid creating new specific requirements just for Brazil so that BCRs approved by a company in another jurisdiction do not work in Brazil, or even worse, create conflicts between different sets of BCRs.
- Define clear and workable criteria for reviewing and approving BCRs, perhaps creating an expedited process for approval/adoption/recognition of BCRs already approved in other jurisdictions that offer the same level of protection as the LGPD.
- Create a proportionate, flexible, and interoperable approach to BCRs that enables the efficient movement of data across borders between different corporate groups, groups of undertakings, or enterprises engaged in a joint economic activity such as franchises, joint ventures, or professional partnerships.
- Develop a user-friendly and streamlined application framework and approval process.
- Consider accrediting third-party organizations to play a due diligence role in the BCR approval process to assist ANPD and help streamline its BCR approval operations.
- Create a toolbox, templates, and guidance inspired by the documents issued by the Article 29 Data Protection Working Party (WP263, WP264, WP265, WP256, WP257).

6) To what extent should the elements to be considered by ANPD in assessing the level of data protection of foreign countries or international bodies for adequacy purposes (article 34 of the LGPD) also be taken into account within the scope of the rules for contractual instruments?

ANPD should not conflate adequacy determinations with SCCs and other contractual instruments. Organizations are facing major difficulties following the decision of the Court of Justice of the European Union in *Schrems II*, which requires companies to conduct transfer impact assessments (or transfer risk assessments) to evaluate whether their envisioned transfer to the importing country is afforded an essentially equivalent standard of data protection to that of the EU, when taking into consideration available appropriate safeguards and potential supplemental measures. If Brazil were to follow a similar approach, it would impose a requirement on organizations that is not and should not be within their remit (i.e., to examine the data protection regime of every country to which they transfer personal information). Requiring individual organizations to comprehensively assess the privacy and data protection regimes of individual countries and to determine "transfer risks" on the basis of such assessments is unduly burdensome, ineffective, unreliable, inefficient, and oftentimes

impossible (especially for SMEs and start-ups with limited resources). Moreover, requiring organizations to conduct assessments would undermine the role of ANPD, as the LGPD is clear in art. 33(1) and art. 34 that adequacy assessments are within the remit of the ANPD. Organizations should simply be responsible for ensuring (through compliance with LGPD art. 33) that the company to which they transfer data remains accountable under Brazilian standards for the data it receives from Brazil.

Similarly, ANPD must be cognizant of the different roles that SCCs and adequacy determinations play in the global transfer arena. SCCs are typically used in instances where a country does not have an adequacy determination from the exporting country. As such, it would not make sense to include an assessment of country-level adequacy as part of the requirements for transfers via contractual instruments, as contracts are business-to-business tools, and do not address broader country-level adequacy issues. In CIPL's view, any assessment of a particular country's use of data for national security and intelligence purposes (and any related assessment of a country's means of redress for alleged violations thereof) is beyond the capabilities and competencies of most private organizations.

7) ***Should the standard contractual clauses be rigid and with predefined content, or should their regulation allow certain flexibility concerning the text of the clauses, specifying the desired results and allowing changes as long as they do not conflict with the standard text made available?***

As stated above, SCCs must be designed in a way that affords organizations appropriate flexibility to adapt them to their specific processing activities and transfer scenarios, including the freedom to incorporate language already used in existing instruments. Indeed, the rigidity associated with the EU standard contractual clauses has been a challenge for organizations for many years. CIPL (along with many other industry bodies, trade associations, and organizations) advocated for a more flexible approach during the EU Commission's update of the pre-GDPR SCCs. (See CIPL White Paper on Key Issues Relating to Standard Contractual Clauses for International Transfers and the Way Forward for New Standard Contractual Clauses under the GDPR). Thus, while the uniformity of standard clauses across industries has certain benefits, SCCs should nevertheless permit sufficient flexibility to account for differences in organizational structures or unique processing ecosystems.

ANPD should design clauses that are flexible from the start. For example, the clauses should not dictate the number of parties to the contract or the nature of the processing operations that can be covered, and organizations should be able to modify and adapt some of the language to ensure that the contractual clauses can work in practice for the transfer at hand.

8) ***What would be the most appropriate format for ANPD to make available models of standard contractual clauses for international data transfers? Are there any relevant tools that could be used to this end (e.g., decision tree, forms, checkboxes)? Are there any experiences on the theme that could serve as an example for ANPD?***

As mentioned above, CIPL encourages the development of outcome-based clauses, ensuring that organizations have the flexibility to adapt provisions to their specific data processing operations and transfer scenarios, including the flexibility to incorporate language already used in existing instruments. Outcome-based clauses ensure that the data recipient complies with the relevant data protection principles and obligations of the LGPD. These clauses can set out, for example, the outcomes and objectives to be achieved, such as data security during transmission and processing by the data importer, assistance with the data subject's rights by the data importer, a prohibition on

further processing for unrelated purposes by the data importer, etc. By specifying topics and outcomes, companies can be flexible in how they implement the actual requirements in their contracts. A flexible instrument could provide a modular approach. It would also permit organizations to take risk factors into consideration, which would promote the efficient allocation of resources to account for varying degrees of risk.

A decision tree to address desired outcomes would be helpful, as would a checklist to help determine which clauses would be applicable to a specific transfer. Given that international data transfers apply to a very broad spectrum of transfers, a modular approach that reflects requirements based on risk would be helpful. Moreover, a questionnaire, such as the Model Contract Clauses Agreement Builder offered by New Zealand's Office of the Privacy Commissioner, should be considered as an option for creating more customizable clauses. Whatever tools or resources ANPD creates should be viewed only as guides and should not be rigid or mandatory.

9) Is it necessary to have different rules depending on the type of processing agents (e.g., specific modules for controllers or processors) as data exporters or importers in international data transfers based on contractual clauses? If so, what would they be?

Because controllers and processors have different obligations, it is important for contractual clauses to be versatile or adaptable enough to reflect the actual roles and responsibilities of the parties. And the clauses must be able to be easily incorporated into any data processing agreements and related documents. Because a data recipient can sometimes act as both a controller and a processor, contractual clauses should never be one-size-fits-all; rather, they should be able to be applied flexibly depending on the context of the transfer.

In addition, controllers must ensure that their operators and sub-operators (processors and sub-processors) respect and protect the personal data entrusted to them, complying with all of the criteria and standards of the LGPD. In this regard, operators must comply with the controller's instructions and always ensure the security of personal data present in their systems. These requirements are already present in the LGPD – any contractual clauses regarding international transfers must ensure that these obligations do not end at the borders of Brazil. Such an approach is consistent with the LGPD's accountability standards, which apply regardless of where the data will be transferred.

10) Are there requirements that need to be different for Binding Corporate Rules from those usually required for Standard Contractual Clauses? If so, what would they be?

Yes. SCCs (as currently configured) impose on data importers obligations specific to their role as data importers and specific to the personal data at issue in the transfer. BCRs, by contrast, encompass a binding and enforceable code of conduct addressing all transfers of personal data within a group of undertakings or group of enterprises engaged in joint economic activity. BCRs include requirements relating to a comprehensive privacy program and compliance ecosystem, such as governance mechanisms, DPOs, policies and procedures, training and communication, and audits and assessments. Thus, BCRs are, in essence, an accountability mechanism, which supports compliance with local law, as well as enabling adequate protection for data transferred across borders. Because BCRs align closely with a company-level "adequacy" model, CIPL would encourage the use of BCRs beyond the context of intra-corporate transfers to enable transfers also between different corporate groups that have BCRs.

BCRs require a significant investment of time and resources and therefore are currently limited to large, international organizations. To enable SMEs to reap the benefits of BCRs without the attendant time and expense, ANPD may wish to consider an SME-friendly version of BCRs—provisionally called "Intra-Group Data Transfer Agreements"—as an alternative. These transfer agreements are a hybrid between contracts and BCRs and could potentially be an option for SMEs. They could also provide an opportunity for ANPD to work toward the adoption of norms that would not require as great an investment as do traditional BCRs, but would still provide "company-level" assurance for data transfers.

11) How should a corporate group be defined for the purpose of application of Binding Corporate Rules?

CIPL encourages ANPD to consider the factors mentioned by the Article 29 Data Protection Working Party in the EU (the predecessor of the European Data Protection Board (EDPB)) in the following guidance:

> [t]he notion of "corporate group" may vary from one country to another and may correspond to very different business realities: from closely-knit, highly hierarchically structured multinational companies to groups of loose conglomerates; from groups of companies sharing very similar economical activities and therefore processing operations to broad partnerships of companies with very different economical activities and different processing operations. Obviously, these differences in structure and activity impacts upon the applicability, design and scope of the binding corporate rules, and corporate groups must bear this in mind when submitting their proposals.[4]

However ANPD chooses to define "corporate group," it is important that the group complies with the BCRs.

Moreover, CIPL suggests that BCRs enable data transfers not only within corporate groups (however defined), but also between entities of different corporate groups that have BCRs, where the BCRs are based on the same underlying law or standard. That would significantly improve the usefulness of BCRs. Moreover, ANPD should consider options that would introduce more flexibility for SMEs, such as the Intra-Group Data Transfer Agreements discussed in response to Question 10.

12) What is the minimum information (level of detail) on personal data needed to allow proper compliance analysis by ANPD of the international transfers of data carried out by contractual instruments, in order to minimize negative impacts on business activities and preserve a high degree of protection for the data subject?

To refrain from imposing an excessive burden on contracting parties and to ensure agility in the preparation and negotiation of contractual instruments, the description of operations included in the relevant instruments must contain only the basic elements for the examination and understanding of the data flow. Thus, while international transfers should be assessed in the context of an overall accountability principle, data maps and data flows fluctuate over time and therefore should not be

[4] See: Article 29 Data Protection Working Party, Working Document: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, Draft Working Document on Binding Corporate Rules for International Data Transfers (on the basis of the discussions of the Sub (europa.eu).

used as a basis for demonstrating compliance. Companies should not be required to complete appendices or annexes as is done in the EU. See also our responses to Questions 4 and 5.

It should be noted that the LGPD, in art. 35, §2, grants the ANPD authority, on a case-by-case basis, to request additional information or carry out verification procedures when analyzing contractual instruments. This, we believe, is a clear indication from the legislature that ANPD, in the first instance, should draft practical contractual instruments, reserving the need to request additional information only for specific situations.

13) What are the risks and benefits of allowing transfers between different economic groups whose binding corporate rules have been approved by ANPD?

The benefits of allowing transfers between unaffiliated companies based on BCRs are significant, as it would dramatically increase the value and application of BCRs. If one BCR-approved organization is permitted to transfer data to and from another BCR-approved organization subject to the terms by which both organizations are already bound, both organizations would reap huge benefits from the assurance that each organization's comprehensive privacy program and compliance infrastructure already pass muster, and individuals would be able to share that assurance as well. In this scenario, BCRs would essentially function as a certification of appropriate privacy protections. CIPL foresees no risks from such an arrangement, rather, only benefits and incentives for more organizations to adopt a holistic and high level of protection envisaged by BCRs. We believe there will be a lot of interest in the market in this type of instrument. Evidence shows that companies are keen to be able to demonstrate that they are a trusted data steward and business partner no matter where they operate and where data comes from or goes to (both to consumers and in B2B relationships).

14) Are there any experiences with the verification and approval of specific contractual clauses and binding corporate rules that could serve as an example for ANPD?

In view of the experience in Europe, ANPD should be aware of the resourcing constraints resulting from the current model of adoption/refresh of BCRs. The adoption of BCRs in the EU is accurately perceived as a lengthy and burdensome process that requires a significant amount of resources and executive support. Many regulators are experiencing difficulties in resourcing BCR reviews and addressing back-logs of BCR applications, which should also be considered. ANPD should draw on this experience and consider a model whereby BCRs and similar instruments for international data transfers, like "intra group data transfer agreements," can be approved by third-party approval organizations without intensive involvement of the data protection authority. See also our response to Question 10. Such a system would still enable ANPD to hold organizations accountable for their BCR promise and "certification", as ANPD would be able to demand demonstration of compliance or investigate in case of a suspected breach by a company with BCRs.

Moreover, given that the approval of BCRs implies a considerable use of resources on the part of ANPD, we believe that a more accessible transfer mechanism could be participation in the Global CBPR. The use of accountability agents could enable more companies to accede to a solid transfer mechanism and lessen the resource pressure on ANPD. Furthermore, as mentioned in our response to Question 5c, ANPD should consider recognizing BCRs already approved by the EU, UK, and other countries.

As for specific contractual clauses, see our response to Question 5b.

15) What are the data subject's rights in case of changes in the original configuration of the transfer? In which situations is it essential to communicate directly with the data subjects or to enable some type of intervention by them?

Please refer to our response to Question 16. To the extent this question is asking about the role of data subject rights (DSRs) in the context of international data transfers, it is important to note that DSRs are not absolute and that transparency does not mandate control by individuals over the purpose of the transfer and the location of the data. Approval of data subjects should not be required, nor should they be allowed to intervene in contractual arrangements between the data exporter and importer or have a say on the decision of the mechanism used to transfer data, if the mechanism used is in compliance with the LGPD. Data subjects need to be informed and allowed intervention only if there is a change to a transfer that was done based on their consent. They should also be able to seek assistance with the original controller/data exporter in case of any data protection breaches resulting from a data transfer to another country.

16) What are the best alternatives for resolving conflicts between processing agents and/or between those agents and data subjects involving contractual instruments for international data transfers? Could bilateral, multilateral or international cooperation between data protection authorities assist in conflict resolution? If so, how?

Chapter IX of the LGPD describes the powers granted to ANPD. Among these powers, there is no mention of arbitration or mediation prerogatives. Therefore, it is important that ANPD remains within the scope of its mandate and avoids intervening in contractual disputes. The parties should be primarily responsible for solving any contractual disputes as well as any issues with the data subject.

However, we can foresee a situation where a cooperation between ANPD and the DPA of the importing country may be helpful and yield results, especially where the data exporter is not able to effectuate any change or solve the issue for the data subject and the problem or breach is on the part of the data importer. Of course, a data subject's first recourse is with the data exporter, but in the absence of an amicable resolution, a complaint to ANPD would be in order, and, if necessary, ANPD may need to reach out to the DPA of the importing country for clarification and potential resolution of outstanding issues. With respect to contractual instruments, conflicts around international data transfers should be solved with the means provided by the relevant contractual law.

The Global CBPR system effectively addresses violations of data privacy laws in the context of cross-border transfers, as it incorporates participation from data protection authorities in the Cross-border Privacy Enforcement Arrangement (CPEA). The CPEA provides mechanisms to promote effective cross-border cooperation between authorities in the enforcement of data protection law, including through referrals of matters and through parallel or joint investigations or enforcement actions. In addition, companies participating in the CBPR must use dispute settlement mechanisms provided to individuals by the accountability agents. These are effective and accessible tools to resolve conflicts.

In addition to the CBPR Forum, we encourage ANPD to promote interoperability between data protection and privacy regimes and facilitating international flows of personal data via the Ibero-American Data Protection Network and the Global Privacy Assembly.

17) What are the best alternatives to promote regulatory compliance (including concerning the importer) regarding international data transfers?

Please refer to our responses to Questions 3, 4, and 10. Additionally, we commend ANPD for providing this opportunity to comment on international data transfers, and we encourage ANPD to continue to dialogue with organizations and individuals as it develops guidance and clarifications regarding compliance with the LGPD.

18) What are the best alternatives to resolve practical issues related to the accountability of stakeholders who transfer data overseas, especially in cases where onward transfers to other jurisdictions occur or when data is processed by other data processing agents in the same jurisdiction?

Mandatory adoption of the same or substantially similar contractual clauses in all onward data transfers is likely the best alternative to resolve practical issues related to the accountability of stakeholders. In cases where onward transfers to other jurisdictions occur or when data is processed by other data processing agents in the same jurisdiction, the parties involved and especially the data importer should require that substantially similar protections are adopted for onward transfers.

19) What obligations should be assigned to the importer and exporter in case of access to data by foreign public authorities?

Practices with respect to government access should align with internationally recognized frameworks, and any issues should be resolved at the political level between governments through fora such as the OECD, which has developed a working group on trusted government access. Organizations should have policies and procedures in place to screen incoming requests and to respond in an appropriate manner. There should be no general notice requirements relating to appropriate and legitimate governmental access requests either to the ANPD or data subjects.

Requiring individual organizations to comprehensively assess the privacy and data protection regimes of individual countries, sectors, and industries and to determine "transfer risks" on the basis of such assessments is unduly burdensome, ineffective, unreliable, inefficient, and oftentimes impossible (especially for SMEs and start-ups with limited resources). In CIPL's view, any assessment of a particular country's use of data for national security and intelligence purposes (and any related assessment of a country's means of redress for alleged violations thereof) is beyond the capabilities and competencies of most private organizations. Indeed, as discussed in response to Question 6, under art. 34 of the LGPD, country adequacy determinations are within the remit of ANPD. What would be appropriate, however, is to require importing organizations to have internal procedures in place to respond to government access requests in a manner that ensures due process, data minimization, and proportionality.

When requesting data from U.S.-based providers, countries should utilize existing legal channels, such as requesting data production through the U.S. Mutual Legal Assistance Treaty (MLAT) process and through ratification of the Budapest Convention and the Second Additional Protocol to avoid conflicts of law. We also support new models for bilateral agreements between rights-respecting governments that improve cross-border access to digital evidence, like the CLOUD Act.

If a sovereign State requests disclosure of data that is under the control of an entity under the jurisdiction of another sovereign State, the MLAT process should be used to reconcile Brazilian

sovereignty with the sovereignty of the foreign State. The Brazilian Federal Constitution, in art. 4, items VII and IX, establishes a duty of cooperating with other governments for the progress of humanity, as well as the peaceful resolution of conflicts. Similarly, the Code of Civil Procedure has dedicated a specific chapter to the need for this kind of international cooperation. The LGPD also highlights international cooperation in art. 33, III and VI.

20) What are the most appropriate mechanisms to provide data subjects with clear and relevant information about the possible transfer of their personal data outside of Brazil as well as to ensure the adequate protection of data subjects' rights in international data transfers? How should these instruments be implemented?

The goal should be that all data is used and transferred within a compliant and accountable legal framework—such as SCCs, BCRs, or Global CBPR—so that individuals need not worry about whether their data is in Brazil or elsewhere because it will always be protected at the appropriate level. While individuals should be informed that their data will be subject to appropriate protections and safeguards regardless of where it travels, ANPD should not create strict requirements or mandate specific formats on how to convey such information. Instead, ANPD should develop guidelines that support transparency with flexibility.

ABIPAG: Contribuição Tomada de subsídios transferência internacional
Contato ABIPAG <contato@abipag.com.br>
Qui, 30/06/2022 18:38
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

À Autoridade Nacional de Proteção de Dados - ANPD.

Ref.: Contribuição ABIPAG - Tomada de subsídios transferência internacional.

Prezados, boa noite.

A Associação Brasileira de Instituições de Pagamento ("ABIPAG"), apresenta suas contribuições para a tomada de subsídios sobre a transferência internacional de dados pessoais, na forma do documento anexo.

A manifestação aborda aspectos intrínsecos ao mercado de pagamentos, relevando informações confidenciais que podem ser associadas ao segredo comercial e industrial.

Ademais, para se assegurar a plena liberdade de expressão e opinião da ABIPAG, a confidencialidade é necessária, já que são trazidos argumentos que podem causar retaliação de players importantes no mercado.

Por fim, cumpre destacar que foram protocoladas na plataforma Participa+Brasil as respostas às perguntas 1,3,4,5,7,9,10,11,12,13 e 14.

A ABIPAG agradece a oportunidade de contribuir com a tomada de subsídios em referência e se coloca à disposição para eventuais esclarecimentos.

Atenciosamente,

Nathália Menezes

Secretaria Executiva| Relações Institucionais - ABIPAG

Telefone: [redacted]

E-mails: ***contato@abipag.com.br*** **/** ***nathaliamenezes@abipag.com.br***

Brasscom | Contribuições à Tomada de Subsídios da ANPD sobre Transferência internacional de dados
Presidência | Brasscom <presidencia@brasscom.org.br>
Qui, 30/06/2022 19:00
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Cc: [redacted]

- Raissa Siqueira <raissa.siqueira@brasscom.org.br>;
- Sergio Sgobbi <sergio.sgobbi@brasscom.org.br>;
- Sergio Paulo Gallindo <sergiopaulo.gallindo@brasscom.org.br>;
- Sarah Martins <sarah.martins@brasscom.org.br>

Prezados, boa noite.

A **Brasscom**, Associação das Empresas de Tecnologia da Informação e Comunicação TIC e de Tecnologias Digitais, informa que foram submetidas as contribuições sobre Transferência Internacional de Dados pela **Plataforma Participa + Brasil**. Porém algumas **respostas excederam o limite** de caracteres da Plataforma. Por isso, ressaltamos que em algumas perguntas o **complemento da manifestação** enviaríamos por **e-mail.**

Dessa forma, segue **anexados** o inteiro teor da contribuição da Brasscom, juntamente com o comprovante da manifestação, a fim de comprovar que respeitamos o prazo.

Seguimos à disposição.

Cordialmente,

Presidência
Associação das Empresas de Tecnologia da Informação e Comunicação
e Tecnologias Digitais
E-mail: e-mail: presidencia@brasscom.org.br
Tel.: + 55 (61) 3536-9392 | [redacted]
Site: www.brasscom.org.br Redes Sociais: Clique aqui e siga-nos

COMENTÁRIOS DA BRASSCOM À TOMADA DE SUBSÍDIOS DA ANPD SOBRE TRANSFERÊNCIA INTERNACIONAL DE DADOS

Junho de 2022

As contribuições deverão ser realizadas exclusivamente na Plataforma Participa + Brasil

Prazo: 30/06/2022

1) Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?

Antes de tratarmos das questões apresentadas nessa tomada de subsídios, é preciso apresentarmos algumas considerações antecedentes essenciais que nortearam o desenvolvimento de nossas respostas e nossas sugestões sobre a atuação da ANPD no tema transferência internacional de dados pessoais.

Primeiramente, vale atentarmos para o objetivo e os fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD), como indicativos estruturantes do exercício das atribuições conferidas à Autoridade Nacional de Proteção de Dados (ANPD).

Assim, segundo previsto expressamente em seu artigo 1º, a LGPD tem por objetivo a proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade, sendo que a disciplina sobre os dados pessoais deve se fundar, conforme determinado no artigo 2º, em diversos interesses e direitos como o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Isso significa que, a ANPD, observando o princípio da legalidade que vincula a administração pública e considerando seu propósito de zelo aos dados pessoais, quando atuar na regulamentação do tema da transferência internacional de dados pessoais e na construção dos mecanismos que lhe competem, deve equilibrar todos esses fatores envolvidos e se atentar para a proporcionalidade na estruturação de suas medidas, o que trará, por consequência legitimidade às suas decisões.

Ademais, cabe à ANPD, ao tratar de tema tão complexo, se preocupar em conferir aos administrados segurança jurídica, clareza, motivação e previsibilidade de sua atuação, o que facilitará não apenas a observância da LGPD pelos agentes, com maior proteção aos titulares, mas também auxiliará na atividade fiscalizatória, evitando incertezas e eventuais excessos.

Nesse passo, um aspecto que precisa ser abordado pela ANPD se refere à definição do conceito de transferência internacional.

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu Capítulo V, trata do tema da transferência internacional de dados pessoais, mais especificamente, elenca os mecanismos que podem legalmente viabilizar a transmissão transfronteiriça de dados. A LGPD, embora mencione a ideia do que seja transferência internacional de dados pessoais e, numa interpretação sistemática, se compreenda que ela ocorre entre agentes de tratamento, isso não é claro na lei.

Isso porque os dispositivos da própria LGPD indicam que "tratamento internacional de dados" e "transferência internacional de dados" não são sinônimos. Com efeito, nos termos do art. 5, X, "tratamento" é o gênero que inclui toda forma de operação com dados pessoais, e "transferência" é apenas uma de suas espécies. Assim, nem todo o "tratamento de dados internacional" está no escopo do Capítulo V da LGPD.

Infelizmente, a definição trazida pela LGPD em seu art. 5, XV, para transferência internacional de dados pessoais é um conceito apenas tautológico, e que não responde a pergunta chave acerca do que seria uma "transferência". No entanto, ao analisar as demais hipóteses em que o termo é utilizado na lei, como nos arts. 13, §2º; 16, III; e 26, §1º, I, IV e V, é possível perceber que, em todos os casos, "transferência" faz alusão ao envio de dados de um agente de tratamento a outro. Da mesma forma, o art. 5º, XVI, da LGPD nos leva a essa interpretação ao incluir "transferência internacional de dados" como uma das hipóteses de "uso compartilhado de dados".

Logo, visando facilitar a identificação, diferenciar transferência internacional de mero trânsito de dados e prover segurança jurídica às relações, ressaltamos a importância da definição precisa do conceito de transferência internacional pela ANPD.

Nesse aspecto, o Guia do European Data Protection Board (EDPB)[1], que trata da interação entre o escopo territorial de aplicabilidade do General Data Protection Regulation (GDPR) e suas disposições sobre transferência internacional de dados, e apresenta três critérios cumulativos que qualificariam um tratamento de dados como uma transferência internacional e que poderiam ser aproveitados pela ANPD. Assim, exige o Guia que: (1) um controlador ou operador ("exportador") esteja sujeito ao GDPR para o tratamento em questão; (2) este controlador ou operador ("exportador") divulgue por transmissão ou de outra forma disponibiliza dados pessoais, sujeitos a este tratamento, a outro controlador, controlador conjunto ou operador ("importador"); (3) o importador, esteja em um país terceiro ou é uma organização internacional, independentemente deste importador estar ou não sujeito ao GDPR em relação ao tratamento dado de acordo com o Artigo 3º, do GDPR.

[1] EDPB Guidelines n. 05/2021

Partindo desse Guia do EDPB, conclusões importantes podem ser alcançadas, como a não identificação da transferência internacional de dados se o próprio titular de dados, situado em um país da União Europeia, decidir enviar diretamente seus dados a um agente de tratamento localizado em país terceiro, na medida em que não haverá agentes de tratamento nas duas pontas da transmissão de dados[2].

Tampouco será transferência internacional de dados se nos dois extremos da transferência estiver o mesmo agente de tratamento[3], ou se estivermos diante de um mero trânsito de dados por diversos países, inerente ao funcionamento global da Internet, mas onde não estão localizados os agentes exportador e importador.

Portanto, entendemos que os critérios apresentados pelo EDPB podem ser aproveitados pela ANPD para definição de transferência internacional e sua diferenciação com o mero trânsito de dados, o que por consequência, levará ou não à sujeição da operação de tratamento a um dos mecanismos elencados no artigo 33 da LGPD.

Isso porque, nas situações em que o tratamento de dados se afasta de uma transferência internacional, não significa que o agente de tratamento, subsumido ao artigo 3º da LGPD, possa deixar de seguir os preceitos da Lei e deixar de tomar as medidas de segurança necessárias para proteger o fluxo transfronteiriço dos dados pessoais, mas ao contrário. O que o esclarecimento do conceito visa é não onerar de forma desproporcional o agente de tratamento ou forçá-lo a adotar mecanismos de transferência quando essa adoção não gera um aumento de proteção ao titular por diversas razões, quais sejam, (i) porque a lei já está sendo atendida e seu objetivo sendo observado; (ii) porque a passagem de dados por vários países não significa o acesso a esses dados nessas diferentes jurisdições; (iii) porque, ou o próprio titular decidiu enviar seus dados (envio direto dos seus dados para terceiro), ou (iv) porque o trânsito de dados se dá dentro do mesmo agente de tratamento não configurando, essencialmente qualquer transferência (o dado transita dentro da mesma pessoa jurídica).

---

[2] Um exemplo dado pelo EDPB é o seguinte: "Maria, que mora na Itália, insere seus dados pessoais preenchendo um formulário em um site de roupas online para concluir seu pedido e receber o vestido que comprou online em sua residência em Roma. O site de roupas online é operado por uma empresa estabelecida em Singapura, sem presença na UE. Nesse caso, o titular dos dados (Maria) passa seus dados pessoais para a empresa de Singapura, mas isso não constitui uma transferência de dados pessoais, pois os dados não são transmitidos por um exportador (controlador ou operador), pois são transmitidos diretamente e em iniciativa própria do titular dos dados. Assim, o Capítulo V (do GDPR - "Transferência de dados pessoais para terceiros países ou organismos internacionais") não se aplica a este caso. No entanto, a empresa de Singapura precisará verificar se suas operações de processamento estão sujeitas ao GDPR de acordo com o Artigo 3(2)." (V. EDPB Guidelines n. 05/2021).

3 Outro exemplo do EDPB ilustra bem essa ideia, a saber: "George, funcionário da A, empresa sediada na Polônia, viaja para a Índia para uma reunião. Durante sua estada na Índia, George liga seu computador e acessa remotamente dados pessoais nos bancos de dados de sua empresa [na Polônia] para finalizar um memorando. Este acesso remoto de dados pessoais de um país terceiro, não se qualifica como transferência de dados pessoais, uma vez que George não é outro controlador, mas sim um funcionário e, portanto, parte integrante do controlador (empresa A). Portanto, a divulgação é realizada dentro do mesmo controlador (A). O tratamento, incluindo o acesso remoto e as atividades de tratamento realizadas por George após o acesso, são realizados pela empresa polonesa, ou seja, um controlador estabelecido na União sujeito ao artigo 3.º, n.º 1, do GDPR." (V. EDPB Guidelines n. 05/2021).

Nesse passo, reforçamos o princípio da proporcionalidade aplicado à Administração Pública, como um limite à sua discricionariedade, o qual preconiza que a autoridade administrativa deve sempre optar pela solução adequada, necessária, ou seja, escolher a medida justa nos limites do que é preciso, e deve ser proporcional em sentido estrito, no sentido de que as vantagens da solução encontrada para o alcance do interesse público almejado (proteção dos dados) superam as desvantagens na constrição de outros direitos (incluindo direitos individuais fundamentais diversos, como o da liberdade de expressão, informação, dentre outros expressamente envolvidos no tema em apreço).

Desta forma, sugerimos que a ANPD, esclareça o conceito de transferência internacional, o qual poderá exigir a presença cumulativa de todos os fatores abaixo listados, quais sejam:

1. Necessidade da presença de agentes de tratamento nas duas pontas (exportador e importador) da transferência internacional de dados;
2. Esses agentes de tratamento devem ser pessoas[4] diferentes;
3. O exportador deve estar sujeito à LGPD; e
4. O importador dos dados precisa estar em um país estrangeiro, ou em um organismo internacional não sujeito à LGPD.
5. Efetiva transferência de dados pessoais e não um mero fluxo transfronteiriço de dados.

Discorrido sobre esse aspecto de fundamental importância passamos para a abordagem dos obstáculos às transferências internacionais propriamente ditos.

Consideramos como principais obstáculos para transferência de dados do Brasil para outros países: a divergência de maturidade entre empresas sobre o tema e a falta de regulamentação dos mecanismos, previstos na LGPD, que permitem a transferência internacional de dados, incluindo os instrumentos contratuais, na medida em que dificultam os fluxos de dados e geram insegurança jurídica na relação entre organizações ante a incerteza sobre a forma de legitimar as transferências em conformidade com a Lei. Dessa dificuldade decorre a necessidade de os agentes adotarem mecanismos regulamentados em outras jurisdições mais restritivas que o Brasil para viabilizar as transferências e minimizar a possibilidade de impactos negativos no futuro. Para além disso, há uma grande dificuldade de se conhecer o nível de segurança do país de destino e, por conseguinte, monitorar/garantir que a proteção e a privacidade de dados necessária seja atendida. Ademais, o estabelecimento de obrigações a serem observadas nas transferências internacionais ulteriores também pode

4 Aqui não estamos nos referindo aos funcionários de pessoas jurídicas porquanto estes, conforme reconhecido pelo próprio Guia da ANPD sobre Agentes de Tratamento e Encarregado, não se qualificam como agentes de tratamento, mas sim a controladores e/ou operadores sejam eles pessoas físicas ou jurídicas, nos termos do artigo 5º incisos VI e VII da LGPD.

ser indicado como um dos empecilhos presentes nas transferências cujo exportador de dados está no Brasil.

Já no que diz respeito aos principais obstáculos para a transferência de dados de outros países para o Brasil podemos mencionar o cenário brasileiro ainda incipiente na proteção de dados pessoais, inclusive para garantir um nível adequado de proteção aos fluxos transfronteiriços de dados pessoais. Contudo, nesse particular, ressaltamos como extremamente positiva a transformação, com a Medida Provisória nº 1.124/2022, da natureza jurídica da ANPD em autarquia especial, com reforço expresso de suas autonomias técnica, decisória e patrimônio próprio, o que lhe confere mais independência e certamente contribuirá para uma possível decisão de adequação do Brasil pela Comissão Europeia.

Dentre outros obstáculos, porém, podemos citar a ausência de decisões de adequação de outras jurisdições que cobrem o Brasil, bem como a falta de acordos internacionais que facilitem o livre fluxo de dados, por meio de garantias mútuas, criando insegurança na transferência de dados, entre diferentes países.

Para além do âmbito da proteção de dados, um obstáculo relevante que dificulta a transferência de dados de outros países para o Brasil refere-se aos altos custos de implantação e manutenção de data centers no país. De acordo com a HEFICED, - organização britânica especializada em consultoria e fornecimento de soluções de nuvem - montar um data center no Brasil custa em média 61 milhões de dólares, 42% mais caro que nos EUA. O custo anual de manutenção é maior ainda, em média de 100 milhões de dólares, sendo o dobro do valor em comparação com os EUA[5]. Os altos custos resultam em serviços de nuvem localizados no Brasil mais caros. De acordo com o Leviathan Security Group, um cliente pagaria 60% menos usando servidores em nuvem fora do Brasil[6].

2) Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?

Acordos interoperáveis e multinacionais, ao invés de regulamentos dissonantes de país para país, garantirão que a Internet não se torne fragmentada, que as pessoas em todas as partes do mundo possam ter proteções adequadas para informações pessoais e permitirão que todos os países obtenham os ganhos da inovação digital. Esses acordos também estimulam a competitividade global de um país ao reduzir custos desnecessários de conformidades local e internacional e ensejam aumentos de produtividade.

Deste modo, a ANPD pode atuar nas seguintes frentes:

5 https://www.heficed.com/app/uploads/2021/03/IT-Infrastructure-in-Brazil.pdf
6 http://cloudsecurity.leviathansecurity.com/

a) Reconhecer que a proteção de dados e o seu livre fluxo podem andar de mãos dadas, implementados os instrumentos adequados para garantir a segurança, quando cabível, e trabalhar com outros países para promover a interoperabilidade entre diferentes sistemas de privacidade e estruturas globalmente reconhecidas, como GDPR, devendo estar sempre atenta à realidade brasileira e os ajustes contextuais que precisam ser feitos para evitar problemáticas já vividas com a implementação da rigorosa legislação europeia. Ademais, a adesão a acordos comerciais regionais e bilaterais, como o caso do Sistema de Regras de Privacidade Transfronteiriça da APEC (CBPR)[7], a Convenção para a Proteção de Indivíduos no que diz respeito ao Processamento Automático de Dados Pessoais ("Convenção 108"), do Conselho da Europa, as Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais ("Diretrizes de 1980"), da OCDE, e a Privacy Framework da Cooperação Econômica da Ásia-Pacífico de 2005/2015, são caminhos que podem ser igualmente explorados.

b) Esclarecer que nem todo fluxo de dados transfronteiriços configura uma transferência internacional de dados nos termos da LGPD, como antes dito, é imprescindível. Ou seja, cabe a ANPD pontuar que a transferência internacional ocorre entre agentes de tratamento localizados em países diferentes e sujeitos à legislação do país respectivo, ao passo que existem outros tipos de fluxos de dados transfronteiriços, como o dado em trânsito, que são da própria arquitetura da internet global e essencial para seu funcionamento, e que não caracterizam uma transferência internacional de dados pessoais. Portanto, a esse respeito, recomendamos considerar as diretrizes introduzidas pelo Conselho Europeu de Proteção de Dados (EDPB) como uma ferramenta útil para auxiliar a explicar esses meandros[8].

c) Auxiliar na interoperabilidade e convergência de mecanismos internacionais, cooperando com autoridades de proteção de dados de outros países para identificar as melhores práticas, e estabelecer um eixo convergente de interpretação sobre as disposições gerais sobre o assunto, por exemplo, por meio da elaboração de acordos de cooperação técnica, MoUs e parcerias bilaterais com outros países. Nesse ponto, salientamos a necessidade de consideração pela ANPD da novidade e complexidade do tema no cenário nacional para que haja permissão de uma adaptação paulatina a eventuais exigências que serão feitas

[7]https://www.apec.org/about-us/about-apec/fact-sheets/what-is-the-cross-border-privacy-rules-system#:~:text=The%20APEC%20Cross%2DBorder%20Privacy,2005%20and%20updated%20in%202015.

[8]https://edpb.europa.eu/system/files/2021-11/edpb_guidelinesinterplaychapterv_article3_adopted_en.pdf

aos agentes de tratamento evitando que sejam sobrecarregados com obrigações que não terão condições de imediatamente atender;

d) Emitir Guias Orientativos com diretrizes sobre transferência internacional de dados e as regulamentações em diferentes jurisdições sobre o assunto;
e) Definir os países que proporcionam grau de proteção de dados pessoais semelhante ao previsto na legislação brasileira;
f) Evitar promover um complexo regramento que provoque desnecessários entraves às organizações na realização de transferências internacionais, sendo ideais diretrizes gerais de definição de critérios e limites pautados em uma abordagem baseada no risco, conforme já consagrada como uma das bases fundamentais da via prática para o cumprimento das obrigações dispostas no GDPR e na própria LGPD.
g) Garantir que quaisquer condições que devam ser atendidas antes da transferência dos dados não sejam tão onerosas a ponto de resultarem no tratamento (acesso, uso, armazenamento, etc.) dos dados físicos apenas na jurisdição onde foram criados ("data localisation"). Qualquer estrutura ou orientação impossível ou extremamente onerosa de cumprir na prática prejudicará os cidadãos e as empresas brasileiras.
h) Considerar a adoção do modelo híbrido para as cláusulas-padrão contratuais, composto por cláusulas mandatórias e cláusulas flexíveis relacionadas às particularidades das relações negociais, inspirado no modelo desenvolvido pelo Office of the Privacy Commissioner da Nova Zelândia e no Reino Unido pelo Information Commissioner's Office (ICO), através do International Data Transfer Agreement (ITDA) e emitir um documento com comentários sobre os direitos que cada cláusula busca proteger. Importante destacar que sugerimos os modelos mencionados apenas como ideias, mas que devem ser melhorados pela ANPD, ou seja, não devem ser restritos ao exportador e importador, mas também viabilizados para contratos multilaterais, o que trará maior dinamismo para as transferências internacionais e fluidez para a economia de um modo geral.

3) Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?

Para essa questão cumpre-nos ressaltar que a estrutura do Regulamento Europeu de Proteção de Dados (GDPR) nem sempre condiz com a conformação do tema pelo nosso legislador, na LGPD. Exemplo disso no tocante à transferência internacional de dados se refere à hierarquia trazida no GDPR para os mecanismos legitimadores de transferência internacional,

conferindo maior importância à decisão de adequação, o que não acontece na LGPD que atribui a este fator peso equivalente aos demais mecanismos previstos no artigo 33 da Lei.

De todo modo, na experiência internacional, um dos instrumentos mais efetivos para legitimar a transferência de dados é o reconhecimento do "país com nível de proteção adequado", pois, assim, a transferência ocorre livremente, sem necessidade de autorização ou formalização. Ainda que efetivo, esse instrumento é bastante limitado (somente alguns países foram avaliados pela Comissão Europeia) em virtude dos critérios rigorosos para o reconhecimento, com necessidade de diversos ajustes, inclusive alterações no âmbito legislativo e regulatório dos países, a exemplo da Coreia do Sul e do Japão.

No entanto, existem dois instrumentos bastante utilizados, quais sejam as cláusulas-padrão contratuais e as normas corporativas globais[9], com uma preferência notável para o primeiro deles, haja vista sua maior amplitude de utilização ao não se limitar a grupos específicos, como ocorre com as normas corporativas globais.

No contexto europeu, falamos das Standard Contractual Clauses (SCC), definidas e publicadas pela Comissão Europeia[10]. De acordo com estudo da Digital Europe de 202011, cerca de 85% dos controladores respondentes utilizam as SCCs como mecanismo principal para a transferência dos dados.

Isso porque, após definição pela Autoridade de Proteção de Dados, basta a sua inclusão no texto do contrato ou do Data Processing Agreement (DPA) para que a transferência seja válida, sem necessidade de qualquer tipo de aprovação subsequente de autoridades de proteção de dados. Estas cláusulas são definidas e publicadas pela autoridade e, posteriormente, inseridas nos contratos que envolvem a transferência internacional de dados. A vantagem delas é justamente a simplicidade na execução e maior possibilidade de utilização porquanto podem ser inseridas em qualquer tipo de contrato.

Ademais, especialmente quanto às pequenas empresas que, em sua maioria, possuem limitados recursos financeiros, tecnológicos e pouca maturidade em proteção de dados, a opção das cláusulas-padrão contratuais como mecanismo permissivo para a transferência internacional dos dados também apresenta alta efetividade por conta da facilidade e da segurança jurídica que enseja.

Não obstante, outros instrumentos que, apesar de não sejam muito usados, têm potencial para serem consideravelmente efetivos seriam os selos e certificações na medida em que atribuem aos agentes de tratamento a responsabilidade de se autoavaliar e atender a requisitos mínimos de conformidade com a legislação de proteção de dados pessoais

9https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_key_points_and_messages__cipl-dcms_september_24_roudtable__9_nov_2020_.pdf
10 https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf
11https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf

respectiva. Tais requisitos são exigidos para a concessão do selo ou certificação, a qual fica condicionada à verificação e aprovação pelo organismo de certificação credenciado. Um exemplo relevante de certificações é o adotado pelo APEC CBPR acima mencionado.

Além disso, a ANPD também deve ter em mente as demais hipóteses habilitadoras de transferências internacionais nos termos da LGPD e que não dependem de regulamentação por parte da Autoridade (especialmente no art. 33, III a IX), inclusive alguns que são utilizados para empresas de todos os portes, como necessidade de prestação de serviços ou execução de contrato. No âmbito de incidência do GDPR, há limitações à invocação da base legal "execução de contrato", por exemplo, que não se encontram refletidos no regime próprio da LGPD. Pelo GDPR, controladores somente podem fundamentar a transferência internacional de dados em execução de contrato de forma eventual. Dita limitação não encontra respaldo na legislação brasileira e é totalmente autorizada nos termos do art. 33, IX.

4) Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?

Como principais benefícios relacionados às transferências internacionais podemos mencionar: (a) a melhoria da interação entre os diversos países, aumentando o nível de integração entre eles e promovendo a globalização; (b) o aumento da cooperação internacional para fins comerciais, a fim de integrar diferentes mercados e trazer benefícios econômicos para todas as partes envolvidas; (c) diversificação nos modelos de negócios, viabilizando serviços internacionalmente, por exemplo, de armazenamento em nuvem; (d) vantagens aos titulares que podem usufruir de diversos benefícios, facilidades, conexões, produtos e serviços que somente existem por conta do comércio digital transfronteiriço; (e) desenvolvimento da economia digital e tecnologia do país, com o aumento do uso de dados; (f) globalização das comunicações e dos serviços oferecidos para os titulares, a intensificação da economia global, o avanço tecnológico, a rápida disseminação de notícias, o compartilhamento de conhecimento e o aumento da competitividade; (g) incentivo à inovação; (h) redução de barreiras ao comércio internacional; (i) aumento da proteção de dados/cibersegurança de dados pessoais; (j) desenvolvimento de pesquisas conjuntas e auxílio mútuo na criação de novas tecnologias; (k) maior competitividade e redução dos custos de processamento de dados das empresas brasileiras.

De fato, as atividades globais de tratamento de dados são tecnicamente necessárias para o funcionamento da Internet, portanto, permitir fluxos de dados transfronteiriços contribui para os benefícios universais do acesso à Internet, incluindo a criação de empregos e oportunidades econômicas, possibilitando o acesso a serviços públicos essenciais, como

educação e informações de saúde, avançando em direitos humanos e justiça, e garantindo a transparência do governo e responsabilidade.

Já como impactos gerados pelas transferência internacional de dados destacamos: (a) necessidade de consistência entre os regulamentos em diferentes jurisdições no tocante a conjuntos semelhantes de obrigações e princípios; (b) insegurança jurídica pela dificuldade de conhecimento do cenário de cada país em relação às garantias relacionadas à proteção de dados pessoais; (c) criação de novas obrigações para os exportadores gerando, muitas vezes, altos custos de implementação, o que prejudica o acesso de pequenas empresas aos benefícios obtidos com a transferência de dados; Esses custos podem ser ainda maiores quando ocorrem mudanças substanciais nas regulamentações nacionais.

Sendo assim, como alternativas para o endereçamento desses impactos negativos sugerimos:

- A evolução contínua da regulamentação em proteção de dados seguindo a tendência mundial e acompanhando os rápidos avanços tecnológico e socioeconômico;
- A promoção de trabalhos conjuntos entre autoridades que tratam o tema, para alinhamento de recomendações globais, boas práticas e guias aplicáveis;
- Desenvolvimento dos selos e certificações como mecanismos viáveis para respaldar as transferências, em principalmente em empresas de processamento de dados o que simplificaria a seleção desses fornecedores;
- O desenvolvimento pela ANPD de um regime de transição para a adoção dos mecanismos previstos em lei para que as empresas que já transferem dados internacionalmente tenham prazo e meios razoáveis para se adaptar com o intuito de viabilizar o fluxo internacional de dados no Brasil e evitar a sobrecarga excessiva aos agentes de tratamento.

5) Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê?

a. cláusulas-padrão contratuais;

b. cláusulas contratuais específicas; e

c. normas corporativas globais.

O modelo de regulação mais moderno trazido pela LGPD se desenvolve a partir de uma abordagem baseada em risco, a qual, em linhas gerais, confere mais espaço para os agentes regulados se ajustarem aos preceitos legais, segundo avaliações próprias sobre suas

atividades. Ou seja, os agentes de tratamento, analisando os riscos ao titular que o tratamento de dados enseja, no caso as transferências internacionais, podem escolher e/ou adaptar os mecanismos disponíveis para se ajustarem ao previsto em lei.

Nessa linha de raciocínio e fazendo uma análise do GDPR, Raphaël Gellert[12] explica que a abordagem baseada em risco é parte do GDPR, mas não é expressamente definida nela e teria como característica o aumento de responsabilidade e discricionariedade dos regulados (nesse caso os controladores e operadores), isto é, os agentes de tratamento se tornam mais responsáveis pois podem recorrer a ferramentas de gestão de risco para (melhor) cumprir com a obrigação de proteção de dados. A base da abordagem baseada em risco do GDPR poderia ser encontrada no princípio do accountability, situado no artigo 24 do GDPR e também presente na legislação brasileira como princípio da responsabilização e prestação de contas.

Em pesquisa elaborada pelo Centre for Information Policy Leadership (CIPL)[13] que busca abordar o que tem sido feito pelas organizações em termos de adequação das transferências internacionais pós-Schrems II, o CIPL informa que: (i) de forma consistente com a abordagem baseada em risco do GDPR, as organizações avaliam o risco de transferir dados para fora da UE à luz de sua situação específica, bem como de acordo com a probabilidade e a gravidade dos riscos para os indivíduos; (ii) algumas organizações vêm avaliando as transferências de dados para fora da UE como parte de sua obrigação de responsabilidade sob o GDPR (e outros regimes legais) e já tinham medidas de mitigação antes do julgamento; (iii) algumas organizações veem mecanismos de responsabilização, como BCRs, códigos de conduta e certificações, como uma estrutura sólida para implementar possíveis medidas complementares, que foram exigidas pelo julgamento do Schrems II.

Assim, no que se refere à regulamentação e construção dos instrumentos contratuais viabilizadores das transferências internacionais segundo o previsto na LGPD e partindo do conceito apresentado sobre a abordagem baseada no risco, é fundamental que os mecanismos de transferência sejam minimamente harmonizados e sustentáveis, ao mesmo tempo em que é imperioso que a ANPD considere certa plasticidade na elaboração e no exame (quando posterior) dos instrumentos contratuais permitindo que a organização faça avaliações pautadas no tipo de dados transferidos, na configuração que pretende dar à transferência internacional e em sua experiência com as diversas leis aplicáveis.

Nesse sentido, deve-se conferir garantia para que as organizações levem em consideração suas circunstâncias peculiares, como as operações comerciais com as quais se envolve, o tipo de dados transferidos. Dito de outra forma, a premissa da gestão de risco deve orientar a regulamentação da ANPD com relação a transferência internacional de dados,

[12] *The role of the risk-based approach in the General data protection Regulation and in the European Commission's proposed Artificial Intelligence Act: Business as usual? Journal of Ethics and Legal Technologies – Volume 3(2) – November 2021.*

[13] *A Path Forward for International Data Transfers under the GDPR after the CJEU Schrems II Decision. September 2020.*

criando incentivos para que os agentes de tratamento realizem a avaliação de possíveis riscos, assim como a calibragem das salvaguardas eventualmente necessárias.

Portanto, incentivamos a ANPD integrar esta abordagem na versão final da minuta da regulamentação e construção dos mecanismos contratuais no que toca à transferência internacional, o que pode ser reforçado pela invocação do princípio da responsabilização e prestação de contas previsto no artigo 6º X da LGPD. Ressaltamos, ainda, a importância de submissão das minutas dos documentos elaborados pela ANPD à consulta pública antes de sua adoção oficial.

a. cláusulas-padrão contratuais;

A experiência internacional auxilia a ANPD a alcançar um ponto de equilíbrio na elaboração de cláusulas-padrão contratuais que, reiteramos, deve considerar uma abordagem baseada em risco, permitindo que a organização faça um reconhecimento pragmático das circunstâncias fáticas e do contexto individual das transferências de dados que precisam ser avaliadas com base nos riscos associados no terreno e na prática, sem se descurar das salvaguardas necessárias para a proteção dos dados pessoais.

Assim, os seguintes critérios e requisitos que nelas devem ser observados são:

- Disposições que especifiquem: (i) o exportador e o importador, (ii) as categorias de dados transferidos, (iii) a(s) finalidade(s) da transferência, (iv) a possibilidade de transferência ulterior dos dados e a vinculação às obrigações originárias, (v) as medidas de segurança aplicadas aos dados, (vi) o prazo de tratamento, e (vii) a garantia dos direitos dos titulares dos dados;
- Previsão de cláusulas tratando da possibilidade de descumprimento, responsabilidades e rescisão contratual, especialmente, mas não se limitando a: (i) obrigação do importador de informar ao exportador se, por qualquer motivo, não puder cumprir as cláusulas estipuladas; (ii) dever do exportador de suspender a transferência ao importador caso este não cumpra as cláusulas estipuladas; (iii) definição de responsabilidades em caso de descumprimento contratual e violação legal; e (iv) o direito de rescisão se o cumprimento não for restabelecido ou se houver violação substancial ou persistente do contrato pelo importador.

Nesse sentido, embora os modelos de cláusulas-padrão contratuais estejam prontos para uso, devem ser destacados quais são os requisitos e/ou princípios essenciais que devem estar presentes em todos os contratos.

b. cláusulas contratuais específicas; e

No tocante às cláusulas contratuais específicas, inicialmente é necessária sua conceituação pela ANPD de modo que sejam corretamente compreendidas e utilizadas. Os

mecanismos hoje existentes já são bastantes restritivos, logo é indispensável que se faça o melhor uso dos que estão disponíveis. Assim, ao analisá-las, a ANPD deve considerar critérios que garantam o cumprimento dos princípios elencados na LGPD partindo sempre da premissa, antes mencionada, da abordagem baseada em risco para seu desenvolvimento e adoção, pelo que tais cláusulas não devem ser tão detalhadas, sendo suficiente a especificação das categorias de dados transferidos e as finalidades da transferência específica a que se refere.

c. normas corporativas globais.

A regulamentação sobre as normas corporativas globais deve levar em consideração as especificidades que envolvam o relacionamento entre as empresas do mesmo grupo econômico, bem como aspectos gerais do tratamento de dados da empresa, como por exemplo as políticas de proteção de dados pessoais de seus integrantes. Como tais, as normas corporativas globais deverão conter disposições relativas:

I. à garantia dos princípios de proteção de dados pessoais;
II. ao exercício dos direitos dos titulares de dados;
III. às particularidades do tratamento de dados;
IV. ao seu caráter vinculante em relação a todos os membros do grupo econômico;
V. à estrutura organizacional dessas empresas;
VI. informações de contato de cada organização integrante e a definição de seu papel no tratamento internacional de dados.
VII. disposições sobre auditoria, como deve ser feita (interna ou externamente), quem deve arcar com seus custos, quem deve ser comunicado sobre o resultado, quais autoridades de dados devem ter acesso ao resultado14;
VIII. estabelecer procedimentos de comunicação e cooperação dos agentes com as autoridades de proteção de dados competentes, de forma a garantir que seja possível avaliar a eficácia das normas corporativas globais e efetuar os ajustes necessários, dada a sua necessidade de aprovação prévia pela autoridade supervisora.

[14] Sugestão extraída do GDPR e do Guia do 29WP (n. 256 rev.01) no seguinte sentido: As BCRs devem criar uma obrigação para o grupo de realizar auditorias de proteção de dados regularmente (por auditores credenciados internos ou externos) ou mediante solicitação específica do responsável/função de privacidade (ou qualquer outra função competente na organização) para garantir a verificação de conformidade com as BCRs; (...) O formulário de inscrição conterá uma descrição do sistema de auditoria. Por exemplo: qual entidade (departamento dentro do grupo) decide sobre o plano/programa de auditoria; qual entidade realizará a auditoria; hora da auditoria (regularmente ou mediante solicitação específica da função de Privacidade apropriada.); cobertura da auditoria (por exemplo, aplicativos, sistemas de TI, bancos de dados que processam dados pessoais ou transferências posteriores, decisões tomadas no que diz respeito ao requisito obrigatório sob as leis nacionais que entram em conflito com as BCRs, revisão dos termos contratuais usados para as transferências para fora do Grupo (para controladores ou processadores de dados), ações corretivas, ...); qual entidade receberá os resultados das auditorias etc.

6) Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?

A Brasscom entende que os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação, conforme art. 34 da LGPD[15] devem ser parcialmente levados em consideração no âmbito das regras para os instrumentos contratuais, ou seja, os elementos a serem examinados são apenas aqueles que coincidem com o exigido pelo artigo 33 inciso II da LGPD[16]. Afinal, os instrumentos contratuais de transferência internacional de dados são os aplicáveis às relações privadas, a fim de evitar entraves na transmissão dos dados, garantindo uma transferência segura e a proteção dos dados pessoais dos titulares dos dados.

Por outro lado, a avaliação da ANPD acerca do grau de adequação dos países e organizações estrangeiras tende a ser uma tarefa muito mais complexa e detalhada uma vez que observará, de maneira específica e profunda, aspectos intrínsecos do enraizamento da temática de proteção de dados sob todo o funcionamento econômico, social e político de uma nação, a natureza jurídica e o nível de independência da sua autoridade fiscalizadora, a aplicabilidade e a convergência dos princípios, diretrizes e definições estabelecidos na legislação local, inclusive setorial e perante as garantias e direitos aplicáveis aos titulares de dados.

Portanto, converter esses mecanismos em decisões de adequação privatizadas é contraproducente e não permite à organização a flexibilidade necessária para avaliar suas próprias atividades de tratamento.

Deste modo, à luz do previsto na LGPD pelo artigo 33, inciso II, os instrumentos contratuais devem prever a garantia de observância dos princípios gerais da LGPD, de alguns dos direitos pertinentes conferidos ao titular, a necessidade de adoção de medidas de segurança que tutelam adequadamente os dados pessoais, assim como aspectos referentes à responsabilidade dos agentes envolvidos (exportador e importador).

---

[15] *"Art. 34. O nível de proteção de dados do país estrangeiro ou do organismo internacional mencionado no inciso I do caput do art. 33 desta Lei será avaliado pela autoridade nacional, que levará em consideração: I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; II - a natureza dos dados; III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; IV - a adoção de medidas de segurança previstas em regulamento; V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI - outras circunstâncias específicas relativas à transferência."*

[16] *Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos: (...) II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência; b) cláusulas-padrão contratuais; c) normas corporativas globais; d) selos, certificados e códigos de conduta regularmente emitidos."*

Conforme mencionamos na pergunta anterior, os instrumentos contratuais devem levar em consideração questões operacionais e técnicas relacionadas à transferência internacional e sua elaboração deve seguir uma linha menos rigorosa trazendo contornos principais que precisam ser observados pelas organizações, mas deixando uma margem para escolha do agente de tratamento de como melhor estruturar sua transferência internacional de dados independentemente do nível de proteção de dados do país ou organismo estrangeiro no qual o importador está inserido.

Nesse sentido se posiciona a autoridade de dados do Reino Unido (ICO) ao afirmar que o objetivo deles, no tema transferência internacional de dados, é habilitar um sistema que mantenha altos padrões de proteção de dados e confiança e que permita uma implementação proporcional e baseada em risco do GDPR do Reino Unido[17].

7) As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?

Devemos considerar que o valor central das cláusulas-padrão contratuais (SCC´s) está na construção de um núcleo uniforme em toda a indústria. Assim, as cláusulas padrão deveriam possuir um conteúdo pré-definido, limitado ao básico necessário para que se atenda ao objetivo almejado pela LGPD. Por serem pré-estabelecidas pela ANPD, regularizam as transferências internacionais, facilitam sua incorporação aos contratos dos agentes de tratamento e, com isso, permitem a manutenção do fluxo internacional de dados sem a necessidade de sua verificação a posteriori e pontual pela autoridade de dados. Entretanto, cláusulas extremamente detalhadas que impõem obrigações exacerbadas aos agentes de tratamento podem se apresentar prejudiciais e impedir o alcance das vantagens mencionadas sem necessariamente aumentar a proteção dos dados pessoais.

Portanto o ideal é o equilíbrio, ou seja, estabelecer as cláusulas-padrão contratuais como um núcleo mínimo que não pode ser alterado e que diz respeito exatamente à observância dos princípios previstos na LGPD, ao mesmo tempo em que se admite a adaptabilidade de cláusulas que se refiram a particularidades dos agentes de tratamento e que não impliquem em redução das salvaguardas dos titulares. Como exemplo desse segundo bloco podemos mencionar cláusulas como as que se referem aos direitos de auditoria (quem é o responsável financeiro pela auditoria, quando a auditoria pode ocorrer, o aviso prévio necessário, os efeitos sobre o preço), limites contratuais de responsabilidade, detalhes sobre medidas de segurança a serem adotadas, consequências decorrentes de rescisão contratual, regras sobre eliminação dos

[17] Disponível em https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/ico-consultation-on-data-transferred-outside-of-the-uk/

dados, dentre outras, podem ser consideradas opcionais prestigiando, assim, a autonomia e a liberdade contratual, princípios norteadores do desenvolvimento das atividades econômicas.

Em suma, à vista da abordagem que defendemos baseada em risco, defendemos a versatilidade não das cláusulas-padrão quando representam o núcleo da proteção de dados pessoais em transferências internacionais, mas sim das cláusulas que definem a relação específica de cada tipo de negócio.

O entendimento europeu é que as Standard Contractual Clauses não poderiam ser "adaptadas" ou "modificadas" considerando o contexto de tratamento das empresas. De toda forma, tais poderiam ser "expandidas", a não ser que tais "expansões" não contradigam ou limitem o que já se encontra escrito e definido nas cláusulas-padrão.

Contudo, entendemos que é preciso evitar o rigor das SCC´s europeias e buscar um caminho mais proveitoso. Os modelos da Nova Zelândia e do Reino Unido se apresentam como alternativas interessantes, na medida em que permitem ao agente de tratamento moldar seu contrato, apresentando-o híbrido, ao ser composto por cláusulas rígidas, ou cláusulas-padrão ("General Terms"), que fixam os princípios norteadores para transferências internacionais, e "cláusulas" flexíveis que admitem adaptação de acordo com os diferentes modelos de negócio e finalidades para a transferência de dados pessoais[18]. Diferentemente das SCCs previstas pela Comissão Europeia em relação GDPR, as cláusulas neozelandesas, em particular, são mais curtas, genéricas e menos rigorosas, estabelecendo tão somente regras gerais para o tratamento dos dados pessoais divulgados, com base nos princípios do Privacy Act[19] e quaisquer cláusulas que conflitem com o núcleo imutável das cláusulas-padrão não terão validade jurídica. Porém, autoridade da Nova Zelândia ainda permite que as organizações estabeleçam termos específicos[20] para formar as suas próprias cláusulas tidas como adicionais, desde que as proteções básicas estabelecidas nos General Terms estejam presentes[21]. Ou seja, o conteúdo do contrato seria flexível, porém composto por cláusulas mínimas obrigatórias e imutáveis, atinentes à proteção de dados pessoais, e cláusulas maleáveis. Já o International Data Transfer Agreement ("IDTA") do Reino Unido, criado justamente para substituir as SCCs europeias, possui uma terminologia mais compreensível e apresenta uma estrutura mais simplificada que as SCC´s europeias.

Não obstante essas vantagens apresentadas, reiteramos nosso entendimento no sentido de que a ANPD deve se inspirar nesses modelos, buscando melhorá-los no que foi possível,

[18]https://privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/model-clause-agreement-builder/.

[19] https://www.legislation.govt.nz/act/public/2020/0031/latest/LMS23223.html

[20] O modelo neozelandês permite às partes introduzirem cláusulas especiais ("Special Terms") para personalizar o contrato de acordo com suas circunstâncias, por exemplo, a inclusão de uma cláusula que exija do importador certificações ISO/IEC, ou uma cláusula de auditoria. Contudo, as partes devem considerar se a adição de tais cláusulas prejudicaria as proteções no modelo padrão ("General Terms").

[21]https://privacy.org.nz/publications/statements-media-releases/new-principle-for-disclosing-personal-information-overseas/.

como, por exemplo, conferir mais amplitude e garantir sua aplicabilidade em contratos multilaterais e não apenas no contrato firmado entre o exportador e importador de dados, o que engessa, por demais, as relações negociais.

8) Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc.)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?

A ANPD, à semelhança de outras autoridades de proteção de dados, pode disponibilizar as cláusulas-padrão contratuais em seu site com uma breve contextualização quanto à necessidade de sua adoção, bem como exemplos de sua aplicação. Entretanto, o formato mais adequado para a ANPD apresentá-las dependerá de qual modelo a ANPD decidirá seguir. Como exemplos, sugerimos a implementação das seguintes ferramentas, caso a opção seja pelas experiências neozelandesa, britânica ou pela europeia:

- Nova Zelândia[22]:
  - Fornece um formulário gerador de cláusulas-padrão para auxiliar os interessados na elaboração de contratos, de acordo com o tipo de transferência e o tipo de tratamento realizado pelo importador. Há cláusulas obrigatórias com conteúdo que não pode ser alterado e cláusulas que podem ou não ser adotadas, segundo a conveniência das partes e especificidades do negócio.
  - Disponibiliza uma árvore de decisão para os interessados esclarecerem dúvidas e confirmarem a possibilidade de realização da transferência pretendida, bem como a necessidade de adoção de cláusulas-padrão contratuais no caso específico.
  - Fornece modelo de cláusulas-padrão contratuais comentadas, explicando a finalidade, as garantias trazidas por cada uma das cláusulas e as garantias mínimas que devem estar presentes nelas.

- Reino Unido[23]:
  - Apresenta uma estrutura de contrato composto por 4 partes, com a seguinte estrutura: (i) formulário para inserção e informações sobre o importador, exportador e sobre a transferência internacional em si; (ii) cláusulas de proteção extra opcionais; (iii) cláusulas comerciais; e (iv)

[22] https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/
[23]https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/

conjunto de cláusulas mandatórias, que devem estar presentes em todos os IDTA´s e por fim um glossário.

- União Europeia[24]:
  - Fornece cláusulas-padrão contratuais detalhadas, em todas as línguas dos Estados-Membros. Embora o português seja a única língua brasileira, a disponibilização de cláusulas em outros idiomas, principalmente o inglês, eliminaria a necessidade de tradução por cada agente, evitando traduções não harmoniosas e melhorando a comunicação entre as organizações importadoras de nacionalidades distintas.

A adoção de um modelo mais interativo, semelhante ao implementado pela Nova Zelândia, ou de um formato no qual há opções de escolha, como o do Reino Unido, beneficia os agentes de tratamento e os titulares dos dados, ao promover informações de fácil acesso e simples entendimento, o que também auxilia na regulação e controle das atividades por todos aqueles envolvidos.

A utilização de formulários, checkboxes e aplicação em casos práticos, comumente utilizados nos guias e orientações de autoridades europeias, por exemplo, poderia igualmente ser interessante para guiar os agentes de tratamento nacionais, que ainda não possuem uma maturidade adequada sobre um tema, a melhor entenderem a aplicação e a definição de quais cláusulas deveriam ser integradas nos negócios envolvendo dados pessoais com parceiros internacionais.

Ademais, a definição de uma estrutura de "árvore de decisão" também poderia ser útil, para indicar aos agentes, de forma específica e rápida, quais seriam as cláusulas e os módulos das SCCs a serem utilizados, mitigando a possibilidade de utilização de cláusulas não aplicáveis para o contexto específico da transferência que será executada.

9) É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?

Sugerimos que de fato sejam criados módulos específicos para controladores e operadores como exportadores e importadores de dados em transferências internacionais,

[24] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en

especialmente tendo em vista as atribuições legais distintas de cada agente de tratamento na cadeia da transferência de dados. A adoção de regras diferentes para cada situação facilita a compreensão da posição assumida pelos agentes de tratamento envolvidos nas transferências internacionais, aumenta as garantias aos titulares e auxilia as adequações a cada situação na prática. Assim, estabelecer diferentes obrigações de acordo com o papel do agente de tratamento torna o mecanismo mais efetivo, facilitando a realização das transferências de dados e a participação de diversos agentes.

Nesse sentido, a ANPD poderia adotar a abordagem Modular similar a UE[25], que possui 4 módulos de cláusulas aplicáveis a cada agente de tratamento dependendo se controlador ou operador:

- Controlador para controlador (C2C) - controlador BR para controlador INT;
- Controlador para operador (C2P) - controlador BR para operador INT;
- Operador para controlador (P2C) - operador BR para controlador INT;
- Operador para operador (P2P) - operador BR para operador INT (ou suboperador).

10) Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?

Entendemos que os requisitos devem ser distintos principalmente porque existem particularidades envolvendo o fluxo de informações dentro de um mesmo grupo (intragrupo), como, por exemplo, aquelas relacionadas à sua estrutura organizacional, códigos e políticas internas. Na prática, o mecanismo das normas corporativas globais se assemelha a uma estrutura comum de governança de dados, incorporando práticas de accountability na transferência internacional dos dados pessoais entre empresas do mesmo grupo, ao passo que nas cláusulas-padrão contratuais a verificação se limita ao âmbito das obrigações assumidas no contrato e que garantem um regime de proteção de dados pessoais.

Mais especificamente, e ao contrário das cláusulas-padrão, as normas corporativas globais devem indicar, como antes dito, (i) a estrutura do grupo econômico e os meios de contato para cada uma das empresas associadas; (ii) esclarecimentos sobre a relação dos membros do grupo e colaboradores com as normas corporativas globais; (iii) procedimentos que assegurem a possibilidade de verificação do cumprimento das normas, como auditorias e relatórios; (iv) aspectos relativos à responsabilidade e indenização por danos decorrentes da violação das normas corporativas globais por uma das empresas do grupo, incluindo a adoção das medidas necessárias para sanar os atos que requeiram reparação; (v) os tribunais e autoridades brasileiras competentes; (vi) ações de promoção da formação e qualificação dos colaboradores envolvidos no tratamento de dados; (vii) procedimentos de comunicação e

[25] https://www.gdprsummary.com/new-sccs-definitive-guide/ - Modular Approach

cooperação com a ANPD, em especial quanto a alterações nas normas corporativas globais e resultados quanto à eficácia das normas.

11) Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?

Considerando que o conceito de grupo econômico no Brasil depende de cada ramo do direito, cada qual possuindo sua própria definição, recomenda-se que a ANPD promova a definição e a harmonização da compreensão de "grupo econômico", por meio de ato administrativo. As leis existentes em nosso ordenamento jurídico e que trazem um conceito legal não devem ser aproveitadas na medida em que, aplicáveis a contexto diversos, exigem uma estruturação burocrática do grupo econômico, como ocorre com a Lei das S/As[26], ou, embora mais amplas e flexíveis como ocorre com a Consolidação das Leis do Trabalho (CLT)[27], não asseguram uma prática de gestão de dados similar entre as sociedades, níveis de segurança de informação comparáveis e processos de proteção de dados pessoais coordenados, todos elementos indispensáveis para uma implementação eficaz e segura das BCRs. Sendo assim, sugerimos os seguintes critérios cumulativos a serem considerados pela ANPD na definição de grupo econômico para a delimitação da aplicabilidade das BCRs:

a) relação de controle ou existência efetiva de controle societário comum;
b) semelhança de políticas e procedimentos adotados para fins de proteção de dados pessoais, em especial no que toca à observância dos princípios da LGPD; e
c) implementação de sistemas com certo grau de interoperabilidade entre as sociedades integrantes do grupo econômico.

Esse entendimento nos parece em conformidade com o que é estabelecido pela União Europeia, Reino Unido e Argentina, que trabalham com as variáveis: relação de controle e poder efetivo de influência sobre as sociedades integrantes do grupo econômico.

Por oportuno, ressaltamos como adequado que a ANPD expressamente limite a definição de grupo econômico que vier a adotar apenas para fins de aplicabilidade das normas corporativas globais, e não para a aplicação da legislação de proteção de dados no sentido lato.

Além disso, com o intuito de melhor aproveitar esse mecanismo de transferência internacional e na linha do que é admitido pelo GDPR em seu artigo 47 (2) (a) e expressamente admitido, por exemplo, pela autoridade de dados na Irlanda *(Data Protection Commission)*[28], a aplicabilidade das normas corporativas globais poderia ser estendida para situações que

[26] Artigo 243 e parágrafos da Lei nº 6.404/1976.
[27] Artigo 2º da CLT.
[28] Disponível em https://www.dataprotection.ie/en/organisations/international-transfers/transfers-personal-data-third-countries-or-international-organisations

extrapolam um grupo econômico e nas quais pode se identificar uma atividade econômica conjunta, como são os casos de parcerias, *joint ventures*, franquias.

No mesmo sentido da extensão da aplicabilidade das normas corporativas globais, a possibilidade de concessão da permissão pela ANPD para realização de transferências entre grupos econômicos cujas normas corporativas globais já tenham sido aprovadas pela ANPD igualmente é vista de forma extremamente positiva, dado que, o envio de dados entre ambos os grupos, igualmente garantiria um nível alto de proteção aos dados pessoais e aos titulares, sem impor maiores dificuldades para o fluxo internacional de dados. Isso porque os agentes que obtiveram aprovação das BCRs perante a ANPD, terão demonstrado a adequação do instrumento e o devido respeito aos requisitos estabelecidos pela autoridade, bem com à LGPD, de modo que autorizar a transferência internacional entre dois grupos que já possuem as normas corporativas globais próprias apenas ratifica aprovações já efetivadas pela ANPD.

Esse posicionamento vem sendo defendido pelo *Center for Information Policy Leadership* (CIPL) ao longo dos anos, com base nos seguintes fundamentos[29]:

I. a GDPR não prevê uma definição para "atividade econômica conjunta" e, portanto, a expressão poderia ser interpretada de forma ampla, podendo abranger dois grupos de empresas que estabelecem uma relação formal ou comercial e contratual relativa à prestação de um serviço, ao desenvolvimento de um produto ou a uma colaboração ou atividade conjunta que envolva algum compartilhamento de dados entre duas organizações;
II. independentemente do entendimento sobre o que seja "atividade econômica conjunta", a transferência extragrupo deveria ser possível dado que a aprovação das BCRs demonstraria que aqueles grupos teriam um alto nível de proteção de privacidade e um programa de privacidade abrangente; e
III. a decisão de aprovação de uma BCR seria similar a uma decisão de adequação, o que se demonstraria pela identidade dos princípios que devem estar contidos nas BCRs e garantidos por determinado país para obter uma decisão de adequação, sendo assim, a transferência entre dois grupos com BCRs aprovadas deveria ser possível sem o uso de qualquer mecanismo adicional.

Portanto, entendemos como legalmente possível tal aplicabilidade mais ampla das normas corporativas globais, o que sugerimos seja acatado e incentivado pela ANPD.

[29] Esse argumento foi sustentado em dois documentos distintos <http://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_white_paper_final_-_essential_legislative_approaches_for_enabling_cross-border_data_transfers.pdf> e <https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_comments_on_wp29_data_portability_guidelines_15_february_2017.pdf> .

12) Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?

Considerando nossa posição de que a construção dos mecanismos de transferência internacional de dados pessoais deve se pautar numa abordagem baseada em risco e visando não impor um ônus excessivo aos agentes, desencorajamos a ANPD a solicitar informações detalhadas para fins de análise da conformidade dos mecanismos adotados. Tais mecanismos devem ser minimamente verificados pela ANPD, cabendo aos agentes de tratamento, até mesmo em virtude do princípio da responsabilização e prestação de contas, realizar essa análise mais criteriosa.

Nessa linha de raciocínio, entendemos que o descritivo de operações a constar de referidos instrumentos deve conter somente os elementos básicos para o exame e entendimento do fluxo de dados pessoais. Ressalte-se que a LGPD, no artigo 35, §2º, previu a possibilidade de a ANPD, caso a caso, requerer informações suplementares ou realizar diligências de verificação ao analisar instrumentos contratuais, em clara indicação, por parte do legislador, da importância de se manter, em um primeiro momento, tais instrumentos contratuais concisos e práticos, reservando maior detalhamento apenas para algumas situações específicas. Logo, poderiam ser exigidas as seguintes informações:

I. Categorias de dados pessoais transferidos;
II. Finalidades da transferência internacional;
III. Alocação de obrigações e responsabilidades entre os agentes exportador e o importador dos dados;
IV. Medidas a serem tomadas em caso de incidente de segurança envolvendo dados;
V. Possibilidade ou não de transferência ulterior para suboperador e vinculação deste às obrigações contratuais originárias.

13) Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?

Como antes mencionado, permitir a transferência de dados entre diferentes grupos econômicos, que tiveram suas respectivas normas corporativas globais aprovadas, seria benéfico, pois facilitaria o processo de transferência transfronteiriça de dados entre empresas que já garantem o cumprimento da LGPD, uma vez que as empresas contratantes apresentam uma estrutura de governança de dados já validada pela ANPD, o que tranquiliza os envolvidos quanto ao nível de maturidade e segurança nos processos de tratamento de dados pessoais.

As normas corporativas globais podem ser adaptadas a cada organização e, uma vez implementadas, são relativamente fáceis de serem atualizadas. Isso reduziria custos para todas as partes envolvidas e estimularia maior interação entre os grupos de empresas, o desenvolvimento econômico e a inovação.

Todavia, é importante destacar que a elaboração das normas corporativas globais pelas empresas e posterior análise pela ANPD, levam em consideração: (i) a natureza dos dados transferidos internamente pelo grupo; (ii) sua(s) finalidade(s); e (ii) outras questões específicas de transferências que ocorram intragrupo, aspectos que possivelmente não seriam compatíveis no caso de transferências entre grupos econômicos distintos. Portanto, no caso de utilização de normas corporativas globais para transferências entre grupos distintos, seria importante admitir ou exigir eventuais ajustes em relação a pontos relevantes ou seja, esclarecimentos sobre a natureza dos dados, volumetria e finalidade da transferência em questão.

Quanto ao risco, este pode ser considerado minimizado dado que há uma preocupação mútua entre os grupos que já desenvolveram procedimentos e sistemas para tratarem dados pessoais em conformidade com a lei.

14) Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?

Há experiências de verificação e aprovação de normas corporativas globais na Europa, regulamentadas pelo GDPR que a ANPD pode observar.

Para as normas corporativas globais, o GDPR exige a sua submissão à aprovação da autoridade de dados competente e já existe uma extensa lista de empresas e grupos empresariais para os quais este mecanismo internacional de tratamento de dados foi aprovado. Deve-se levar em conta que a UE tem algumas particularidades, dada a possibilidade de envolvimento de várias autoridades nacionais de supervisão de diferentes Estados-Membros.

Na experiência europeia, o grupo interessado em ter suas normas corporativas globais aprovadas deve identificar uma autoridade fiscalizadora para atuar como líder e apresentar a proposta inicial juntamente com os documentos relevantes, como Políticas de Privacidade, diretrizes para funcionários, plano e programas de auditoria, programas de treinamento, evidências de recursos suficientes para suportar danos causados por membros do grupo localizados fora da União Europeia, procedimento para lidar com reclamações, lista de entidades do grupo relacionadas a BCRs, Política de Segurança da Informação, contratos padrão utilizados com operadores, entre outros[30].

[30] Binding Corporate Rules: The General Data Protection Regulation. PWC. https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf

No tocante às cláusulas contratuais específicas, não existe um procedimento unificado da União Europeia para sua verificação e aprovação. Qualquer empresa que queira adotá-las ao invés das SCCs deve submetê-las à validação da autoridade nacional de sua jurisdição e cada país tem seus procedimentos específicos[31] para aprovação.

Portanto, não há experiências suficientes capazes de criar uma interpretação padrão sobre o tema, e esse debate ainda é bastante incipiente em outras jurisdições. Existem divergências quanto ao alcance das cláusulas específicas para as transferências internacionais, nomeadamente quanto ao fato de não poderem ser restringidas às transferências efetuadas de forma regular, podendo ser aplicadas em substituição de cláusulas-padrão contratuais ou normas corporativas globais em certas situações.

A interpretação, com base no GDPR, é a de que as cláusulas contratuais específicas devem limitar-se a transferências pontuais, para fins específicos e envolver um número limitado de titulares de dados, nos termos do §1º do artigo 49 do GDPR. Essa compreensão poderia parcialmente ser aplicada à LGPD haja vista que o artigo 33 II "a" "*menciona cláusulas contratuais específicas para determinada transferência*", contudo a limitação do número de titulares afetados restringiria a utilidade desse mecanismo sem respaldo na LGPD. Como nossa legislação não apresenta maiores restrições para além daquela que exige "transferência determinada", entendemos que a ANPD poderia fazer um exercício de otimizar sua utilidade, por isso, encorajamos uma interpretação mais ampla desse instrumento específico.

15) Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?

Solicitamos à ANPD que, na consulta pública futura que submeterá o tema, seja mais clara sobre o significado da expressão "mudanças na configuração original de transferência".

Como uma primeira resposta, se o significado estiver atrelado à alteração da finalidade inicial da transferência internacional de dados em razão de uma nova configuração do processo da transferência, entendemos que o titular dos dados deve ser informado através da atualização da Política de Proteção de Dados Pessoais do exportador, devido ao princípio da transparência.

É importante observar que os titulares dos dados podem exercer seus direitos previstos no Art. 18, da LGPD, que inclui ser informado sobre o tratamento de seus dados pessoais a

[31] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data.
https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

qualquer momento. Ainda assim, instamos à ANPD que siga com os salutares esforços de reforçar a construção de uma cultura de proteção da privacidade e dos dados pessoais.

16) Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?

No tocante à resolução de conflitos entre agentes de tratamento, devemos prestigiar autonomia de vontade e liberdade contratual, princípios norteadores das relações jurídicas privadas. O ordenamento jurídico brasileiro disponibiliza diversos meios de solução de conflitos como a mediação, conciliação, arbitragem e o acesso ao Poder Judiciário através do direito fundamental de inafastabilidade da jurisdição[32]. Nessa ideia, o incentivo à solução alternativa de conflitos, previsto logo no artigo 3º e seus parágrafos do Código de Processo Civil de 2015, foi fortemente celebrado pelos operadores do direito [33] e se mostra muitas vezes mais eficaz na medida em que estimula a composição das partes, ao invés de sujeitá-las a uma decisão judicial imposta pelo Poder Judiciário.

Desta forma, as melhores alternativas são aquelas que, dentre as legalmente disponibilizadas, e cabem às partes escolherem a mais adequada e mais viável segundo suas particularidades. A LGPD não confere à ANPD atribuição para definir sobre o instrumento que obrigatoriamente seria adotado, porquanto esse aspecto foge ao escopo de regulamentação da ANPD no tema.

De todo modo, a ANPD poderia sugerir a adoção de certas cláusulas ao dar exemplos e alertar sobre a importância da definição desse assunto no contrato, assim como sobre a importância da cláusula de eleição de foro para dirimir eventuais controvérsias. Nesse passo, as SCC´s da União Europeia contêm cláusula específica que prevê a sujeição do importador à Agência Nacional de Proteção de Dados ou ao Poder Judiciário do país do exportador em caso de litígio.

Com relação aos conflitos entre agentes de tratamento e os titulares de dados, como estes não são partes dos contratos, poderão se valer da reclamação à ANPD, conforme expressamente previsto no §1º do artigo 18 da LGPD, ou do acesso ao Poder Judiciário ante a inafastabilidade da jurisdição como um direito fundamental.

Além dos mecanismos acima sugeridos que são voltados para o âmbito privado, a integração do Brasil em acordos bilaterais e multilaterais, bem como a promoção da

[32] V. artigo 5º XXXV da Constituição da República Federativa do Brasil.

[33] O artigo 3.º em seus parágrafos ressalta a arbitragem, conciliação e mediação como meios alternativos de resolução de conflitos. O §2.º prevê que, sempre que possível, o Estado promoverá a solução consensual dos conflitos.

cooperação internacional entre ANPD e as autoridades de proteção de dados estrangeiras, podem ser medidas profícuas e de grande valia na resolução de conflitos. Mais uma vez vale mencionar o Sistema de Regras de Privacidade Transfronteiriça da APEC (CBPR), implementado através do *APEC Privacy Framework*[34], o qual as empresas dos países membros da APEC podem implementar para demonstrar conformidade com as regras de proteção de dados internacionalmente reconhecidas. Mais especificamente, este sistema prevê a possibilidade de tratamento de reclamações de consumidores e titulares de dados de forma consensual, através de agentes responsáveis pela recepção e investigação de reclamações e pela resolução de litígios entre consumidores e empresas certificadas relativamente ao descumprimento dos requisitos previstos no programa.

Entende-se que a atuação da ANPD em acordos desse gênero, especialmente com previsão de solução extrajudicial de conflitos, pode ser uma alternativa viável e eficiente à judicialização, além de estimular a cooperação internacional e a harmonização entre os entendimentos e práticas das diferentes jurisdições.

17) Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?

A melhor alternativa para promover a conformidade no tocante aos instrumentos contratuais é a previsão de obrigações que determinem às partes:

a) a demonstração do cumprimento das cláusulas previstas no instrumento. Ou seja, o importador deve manter documentação adequada das atividades de tratamento realizadas sob sua responsabilidade para que possa ser demonstrada;
b) a disponibilização das informações acima mencionadas à ANPD quando especificamente solicitadas.

Em relação às normas corporativas globais, estas podem prever os procedimentos que serão adotados para garantir a conformidade intragrupo, o que pode ser realizado por meio de auditorias, relatórios e treinamento dos funcionários que tenham acesso direto ou indireto aos dados.

Paralelamente, como esta seria a primeira orientação sobre transferências internacionais de dados fornecida pela ANPD e considerando que a LGPD ainda é uma lei nova, cabe à ANPD exercer seu papel fundamental de educação e conscientização, através de definições de termos relevantes, de esclarecimento e suporte aos agentes de tratamento e aos titulares com a elaboração de Guias Orientativos, sugestões das melhores práticas na transferência internacional de dados.

[34] https://www.apec.org/docs/default-source/publications/2017/8/apec-privacy-framework-(2015)/217_ecsg_2015-apec-privacy-framework.pdf?sfvrsn=1fe93b6b_1

Além disso, acordos bilaterais e multilaterais entre países e organismos internacionais também podem ser considerados como potencializadores de conformidade com a legislação de proteção de dados.

Por fim, seja qual for o caminho adotado pela Autoridade, é fundamental que a regulamentação preveja prazo razoável para que os agentes de tratamento submetidos às regras para transferência internacional de dados adequem suas relações contratuais de acordo com os novos instrumentos editados pela ANPD. Sobre esse ponto, a título de referência, no Reino Unido, onde o nível de maturidade em proteção de dados é significativamente mais elevado se comparado ao Brasil, após editar seu novo modelo de cláusulas (IDTA), a ICO concedeu prazo de 2 (dois) anos para que agentes de tratamento submetidos à salvaguarda das cláusulas-padrão para transferência internacional de dados adequem seus contratos no contexto da legislação britânica de proteção de dados.

18) Quais as melhores alternativas para resolver as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?

A questão apresentada envolve basicamente duas problemáticas: a primeira delas diz respeito à transferência internacional de dados, inclusive as ulteriores, envolvendo diversas jurisdições; a segunda se refere à transferência internacional de dados para um importador que realiza transferências ulteriores dentro da sua jurisdição.

Nesse ponto, precisamos lembrar do conceito de transferência internacional antes mencionado, porquanto o mero trânsito de dados por diversos países não significa transferência internacional. Ou seja, os diferentes países por onde os dados passam não devem interferir nas leis às quais os dados estão sujeitos, a menos que esses dados sejam, de fato, transferidos entre pessoas jurídicas sediadas em diferentes jurisdições, que estão, portanto, sujeitas a leis diversas. A lei de proteção de dados deve ser aplicada de forma a evitar conflitos desnecessários, de modo a não se preocupar com o mero movimento físico de dados através das fronteiras, mas, ao invés disso, deve concentrar sua aplicação nas transferências efetivas de dados entre agentes de tratamento diferentes.

Sendo assim, com relação à primeira questão apresentada, é essencial o esforço dos países em buscar implementar suas leis visando a harmonização com as leis de outros países, inclusive aderindo às melhores práticas globais gerais, como aquelas que estão sendo desenvolvidas pelo grupo de trabalho da OCDE sobre acesso governamental confiável. Quando surgirem questões de conflito de leis, os governos devem procurar resolver a questão diplomaticamente, como solicitar a produção de dados por meio da Convenção de Haia e do Tratado de Assistência Jurídica Mútua (MLAT) ou MOUs entre as autoridades públicas

relevantes, bem como pela Convenção de Budapeste e o Segundo Protocolo Adicional, em vez de comprometer a capacidade de empresas específicas ou indústrias inteiras de operar nessas jurisdições, colocando-as no meio desses conflitos.

Não obstante, com relação à segunda problemática levantada, é importante esclarecer que (a) possibilidade ou não de transferências ulteriores para além do importador e (b) se essas transferências podem ou não ser feitas em apenas uma ou em diversas jurisdições é um aspecto a ser previsto contratualmente. O exportador pode decidir permiti-las ou não. Em decidindo autorizá-las, seria conveniente esclarecer as situações de responsabilização dos agentes de tratamento envolvidos na cadeia das transferências internacionais, com base no que está previsto na LGPD.

Nesse passo, tanto as SCC´s europeias como as da Rede Iberoamericana permitem essas transferências posteriores, desde que o terceiro esteja vinculado às obrigações do contrato originário que dispôs sobre transferência internacional de dados, ou seja, qualquer transferência ulterior está sujeita ao cumprimento, por parte dos agentes subsequentes, de todas as salvaguardas das cláusulas originárias, em particular aos princípios garantidos no GDPR. A inobservância das obrigações assumidas deverá ensejar responsabilidade para aquele que a descumpriu.

Isto posto, os instrumentos contratuais devem estabelecer em caso de admissão de transferências ulteriores, quais as condições elas podem ocorrer e, além disso, prever: (i) a observância dos princípios que garantem a proteção de dados pessoais; (ii) o regime de responsabilidade trazido pela LGPD; (iii) a possibilidade de direito de regresso, também já previsto em lei; (iv) definição da jurisdição para o exercício dos direitos pelo titular dos dados.

Deste modo, havendo um conflito envolvendo diversos Estados porque os agentes de tratamento envolvidos estão situados em países diferentes, normas de direito internacional serão aplicadas para a definição do país com jurisdição para solucionar a controvérsia, no entanto, as balizas contratuais serão válidas entre as partes e serão exigíveis se não contrariarem a lei cogente do país que decidirá o problema.

19) Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?

As obrigações de acesso aos dados por autoridades públicas devem ser globalmente harmonizadas para que as obrigações para importadores e exportadores sejam consistentes e interoperáveis com estruturas internacionalmente reconhecidas, como aquelas que estão sendo desenvolvidas pelo grupo de trabalho da OCDE sobre acesso governamental confiável. Por exemplo, ao solicitar dados de provedores baseados nos EUA, os países devem utilizar os canais legais existentes, como solicitar a produção de dados por meio do processo do Tratado de Assistência Jurídica Mútua dos EUA (MLAT) e pela ratificação da Convenção de Budapeste

e do Segundo Protocolo Adicional para evitar conflitos de lei. Também apoiamos novos modelos de acordos bilaterais entre direitos que respeitem governos que melhorem o acesso transfronteiriço a evidências digitais, como o CLOUD Act.

Nesse sentido, se um Estado soberano ordena a disponibilização de dados que estejam sob o controle de uma entidade sob jurisdição de outro Estado soberano, não há outra opção senão recorrer ao instituto jurídico da cooperação internacional, a fim de conciliar a sua soberania com a soberania de Estados estrangeiros. Esta é a resposta reivindicada pelo art. 4º, incisos VII e IV, da Constituição Federal brasileira, que privilegia o dever de cooperação entre os povos para o progresso da humanidade, bem como a solução pacífica de conflitos. Além disso, no mesmo sentido da norma constitucional, o Código de Processo Civil dedicou um capítulo específico à necessidade desse tipo de ação internacional cooperativa. A LGPD na mesma linha incentiva a cooperação internacional, no art. 33, III e VI. Portanto, não caberia à ANPD o desenvolvimento de obrigações às partes contratantes na medida em que o tema foge do escopo pertinente às relações jurídicas entre entes privados.

20) Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

No caso de um contrato entre o agente de tratamento e o titular dos dados, o referido contrato deve fornecer as informações necessárias sobre a transferência internacional dos dados em uma cláusula que assegure clareza e fácil compreensão. Desta forma, a informação relativa ao titular dos dados, a finalidade e duração da transferência, bem como os meios para exercer os direitos do titular dos dados, seriam facilmente acessíveis.

Na ausência de contrato com o titular dos dados, as informações sobre a transferência internacional de dados devem estar publicamente disponíveis e facilmente acessíveis. Por exemplo, através das Políticas de Privacidade disponibilizadas no site do agente de processamento.

Além disso, os agentes de tratamento devem disponibilizar um canal de comunicação direta, gratuito e de fácil acesso com os titulares dos dados, caso estes necessitem de esclarecimentos ou informações adicionais sobre a transferência internacional dos seus dados, ou mesmo para o exercício dos seus direitos.

Por fim, os mecanismos de transferência internacional previstos na LGPD devem respeitar os direitos dos titulares dos dados, estabelecendo meios para seu exercício. Portanto, além de estar em conformidade com as regras e princípios da LGPD, o exportador deve assegurar que o importador também estará em conformidade com a legislação, o que poderá ser feito por

meio de cláusulas contratuais e verificação dos relatórios de análise de risco da empresa importadora.

****

CrowdStrike feedback to Public Consultation: ANPD International Data Transfer
Haley Cook <haley.cook@crowdstrike.com>
Qua, 29/06/2022 17:31
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Hello,

Please find attached CrowdStrike's full response to the consultation, which compliments the comments already submitted online. Thank you.

Sincerely,

Haley Cook, CIPP/US
Associate Privacy Counsel
E: Haley.cook@crowdstrike.com
T: 518-791-3275

REQUEST FOR COMMENT RESPONSE

ANPD: International Transfers of Personal Data

June 30, 2022

I. INTRODUCTION

In response to the Brazilian Data Protection Authority's (ANPD) request for feedback on its development of regulations regarding international transfers of personal data, CrowdStrike offers the following views.

We approach these questions from the standpoint of a leading international, US-headquartered, cloud-native cybersecurity provider that defends globally distributed enterprises from globally distributed threats. CrowdStrike offers insights informed by multiple practice areas: cyber threat intelligence; proactive hunting, incident response and managed security services; and an AI-powered software-as-a-service cybersecurity platform and marketplace. Accordingly, this perspective is informed by CrowdStrike's role in protecting organizations from data breaches and a variety of other cyber threats.

II. COMMENTS

The ANPD has written a thoughtful set of questions regarding international data transfers. We understand that the ANPD is seeking answers to those questions, as well as other items the ANPD should take into consideration. In this regard, we do not have feedback on all of the ANPD's specific questions but, we do want to offer several points that may be of value in developing regulations on international data transfers. In particular, modern IT architecture and cybersecurity are dependent upon international data flows, and it is important to incentivize and empower organizations in Brazil to utilize state-of-the-art solutions.

A. International Data Transfers

i. Current Obstacles

We commend the ANPD for asking for feedback on any obstacles companies currently face when transferring data between Brazil and other countries. One of the lessons learned from the European Union is the difficulty of relying on a "white list approach," where a small number of countries are designated as providing parity in the data laws of another country. The difficulty with this approach is two-fold. First, instead of relying upon a single international standard, such approaches create competing standards for adequacy that may or may not take into account a holistic approach to data protection in another jurisdiction nor other risk-mitigation measures related to data flows. Second, current experience has demonstrated that approval processes can be burdensome for both the applicant country and the host data protection authority. Brazil's economy is dependent upon global data flows, and relying upon a white list approach can take years of administrative time, as it involves review and complex analysis of legal regimes that are often not static. The white list approach creates obstacles that can inhibit Brazilian companies, organizations and public sector bodies from engaging in cross border data flows and even accessing key technologies.

ii. Transfer Mechanisms

a. Contractual Agreements

CrowdStrike agrees that one way to adequately protect cross-border transfers of personal information is in the form of written agreements, specifically, contractual agreements. Each of these parties, controllers, processors, and subprocessors, are contractually bound to those with whom there is privity of contract, and the resulting legal protections create a "Chain of Contractual Accountability." Moreover, each party must abide by its own LGPD requirements in a "Chain of Independent Obligations." In other words, data subject rights remain protected by (i) enforceable contractual obligations between respective parties, and (ii) direct application of LGPD to any party processing personal data within the scope of LGPD.

Where both the Chain of Contractual Accountability and the Chain of Independent Obligations exist, the legal position of the data subject is adequately protected. For example, a controller that is party to a Data Processing Agreement with a processor will afford protections to its own data subjects because the processor is also obligated to obtain commitments from its own processors that process the

controllers' data. Acting in concert with these contractual protections, the parties' independent obligations under LGPD, including the requirements to establish a compliant LGPD program and deploy state-of-the-art and risk appropriate security safeguards in line with LGPD Art. 6 and Art. 46, act to further strengthen the protection of personal data and the legal rights of data subjects. Ultimately, existing, well-established concepts of privity of contract coupled with LGPD's direct application to global processing activities provide sufficient protections for data subjects.

b. Standard Contractual Clauses

Another transfer mechanism that the ANPD specifically asked for feedback on are Standard Contractual Clauses (SCC). Regarding SCCs, we have a few points. SCCs are reliable, easy to use and manageable. As the ANPD considers developing and implementing SCCs, we emphasize that SCCs should be written with flexibility in mind and should, as an international transfer mechanism, be multilingual. When parties have the flexibility to negotiate contractual terms, they may be customized to specific use cases and technological designs. Accordingly, SCCs written with narrow specifications and rigid obligations risk being impractical with the realities of the data flows they seek to protect.

B. Importance of cybersecurity

Supporting contractual agreements and SCCs can be done with a strong policy on cybersecurity. Cross-border data flows are necessary for cybersecurity. In fact, many of the most innovative technologies for protecting personal data against data breaches leverage endpoint telemetry data, cloud-native Software-as-a-Service (SaaS) delivery, 24/7 global threat hunting, and cross correlation of indicators of attack. Moreover, modern IT infrastructure in general often invariably involves cross-border data transfers.

We recommend considering the importance of cybersecurity as a supplemental measure to the written agreements by looking at threats, predominantly in terms of threat actors. Malware, malicious infrastructure, and adversary tactics, techniques, and procedures (TTPs) change over time, but often the groups behind malicious activities are more durable. This means that considering threat actor motivations

helps defenders understand everything from their incentives to the risks posed by failing to prevent them from breaching your environment. Threat actors generally fall into the categories of: criminal groups, which largely seek profit; nation state entities, which pursue a variety of geopolitical ends; and 'hacktivists,' which have ideological motives. When crafting guidance, governments must be concerned with each, particularly during a time of unprecedented attacks from specific nation states along with the general trend of increased e-crime.

Specific threats vary across these different types of actors, but a few are especially notable. Criminal groups increasingly target public sector entities with ransomware, which disrupts victim IT environments in order to extort funds. Nation state groups have also used ransomware-like tools and TTPs to cause disruptions for other ends. Additionally, nation states have been observed to hack and leak sensitive communications for political ends, or steal intellectual property or sensitive business information to strengthen domestic commercial actors. Across all types of threat groups, adversaries are leveraging TTPs that enable them to avoid using malware, which complicates detection and prevention for entities using unsophisticated or legacy security solutions.

Further, we advocate for speed based cybersecurity metrics such as the "1-10-60 Rule."[1] This concept holds that security teams should endeavor to reliably detect malicious events within one minute; investigate them within ten minutes; and isolate or remediate affected hosts or resources within one hour. Further, organizational leaders should measure each of these performance indicators over time, and continuously improve them until the goals are met. Organizations that can defend themselves at this velocity will be well-equipped to outpace the vast majority of threat actors,[2] and prevent minor security events from becoming costly, complex, and sometimes devastating incidents.

That being said, we believe today's economy depends more than ever before on cross-border data flows and data portability. This trend will continue, especially in light of the digital transformation accelerated by Covid-19 and the "work from

[1] A more in-depth explanation of this concept is available here: https://www.crowdstrike.com/resources/crowdcasts/the-1-10-60-minute-challenge-a-framework-for-stopping-breaches-faster/.
[2] *See* CrowdStrike's 2020 Global Threat Report: https://www.crowdstrike.com/resources/reports/2020-crowdstrike-global-threat-report/.

anywhere" movement. The importance of cross-border data flows is far-reaching, and affects individuals, entities, and society more broadly. Any restriction on cross-border data flow or data portability requirements could have adverse implications for Brazil's innovation, jobs, access to services, and effective cybersecurity. This means that it is critical to provide organizations with deference to make their own context-informed–and critically, risk-informed–decisions about cross-border data by adhering to core data protection principles related to the circumstances of specific transfers.

Data protection is best achieved where intentional transfers of personal data are permitted with practical safeguards, while unintentional transfers of personal data via data breaches are thwarted by protecting against ever-evolving cybersecurity threats with innovative technologies. As a leading cybersecurity provider, it is our view that perhaps the most significant threat to personal data comes from threat actors operating unlawfully. While responsible data controllers and processors adhere to robust compliance programs, cyber adversaries do not play by the rules

III. CONCLUSION

Cyber attacks from advanced nation-state actors, criminal groups, and hacktivists pose a substantial threat to the safety of personal and other sensitive data. Therefore, cybersecurity should play a critical role in and is thus critical when developing regulations on international transfers of personal data. As the ANPD develops its regulations on international data transfers, we recommend continued engagement with stakeholders. Finally, because the underlying technologies evolve faster than law and policy, we recommend and emphasize that any legislative updates and proposed rulemaking focus on principles rather than prescriptive requirements and include a mechanism for periodic revisions.

ABOUT CROWDSTRIKE

CrowdStrike® Inc. (Nasdaq: CRWD), a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloud-scale AI and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on

or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 3 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security.

With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.

There's only one thing to remember about CrowdStrike: We stop breaches. Learn more: https://www.crowdstrike.com/.

IV. CONTACT

We would welcome the opportunity to discuss these matters in more detail. Public policy inquiries should be made to:

Drew Bagley CIPP/E
VP & Counsel, Privacy and Cyber Policy Policy

Dr. Christoph Bausewein, CIPP/E
Director & Counsel, Data Protection &

Email: policy@crowdstrike.com

©2022 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are trademarks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

***

FEBRABAN | Contribuições à Tomada de Subsídios sobre a norma de Transferência Internacional | Erros/Bloqueios de Aplicações
Diretoria Jurídica <DiretoriaJuridica@febraban.org.br>
Qui, 30/06/2022 23:02
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Prezados, boa noite.

Conforme evidência abaixo e outra dezena de evidências anexas a este e-mail, desde as 21h, o site do **Participa + (ANPD)** encontra-se com bloqueios de aplicações que impedem a submissão adequada das contribuições à tomada de subsídios sobre a norma de transferência internacional por meio do site.

> Esta requisição foi bloqueada.
>
> Em caso de dúvida, por favor envie o código 12943736707981331143 no assunto da mensagem para o endereço eletrônico bloqueio.de.aplicacoes@presidencia.gov.br.
>
> Solicitações não relacionadas a este alerta de bloqueio não serão tratadas por meio deste canal.
>
> Diretoria de Tecnologia da Presidência da República.

Assim sendo, a **Federação Brasileira de Bancos (FEBRABAN)** solicita a esta D. Autarquia que excepcionalmente receba suas contribuições à referida tomada de subsídios por e-mail, considerando todas as diversas tentativas, sem sucesso, de envio das contribuições pelo site, por meio de mais de um perfil (CPF) cadastrado no **Participa + (ANPD)**.

Espera-se que estas contribuições possam ser aceitas pela ANPD e possam auxiliar nas discussões para a elaboração da norma aplicável à matéria.

Sendo o que nos cumpria para o momento, a FEBRABAN permanece à disposição da ANPD para quaisquer esclarecimentos necessários.

Atenciosamente,

Diretoria Jurídica

FEBRABAN | Federação Brasileira de Bancos
www.febraban.org.br
Só imprima se necessário. Evite desperdício.
Entre em nosso site na página de Sustentabilidade e confira nossas dicas para ações sustentáveis.

São Paulo, 30 de junho de 2022.

À
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)
Coordenação-Geral de Normatização
Brasília - DF
A/C: Exma. Sra. Isabela Maiolino (normatizacao@anpd.gov.br)

Ref.: Tomada de Subsídios sobre a norma de transferência internacional

Prezada Senhores,

A **FEDERAÇÃO BRASILEIRA DE BANCOS - FEBRABAN**, entidade representativa do setor bancário brasileiro com compromisso de fortalecer o sistema financeiro e suas relações com a sociedade e contribuir para o desenvolvimento econômico, social e sustentável do País, vem por meio desta apresentar suas contribuições à tomada de subsídios sobre transferência internacional, divulgada em maio pela ANPD.

Espera-se que estas contribuições possam auxiliar qualitativamente nas discussões da ANPD para elaboração da norma sobre a matéria.

Ficamos à disposição para esclarecimentos.

Atenciosamente,

FEDERAÇÃO BRASILEIRA DE BANCOS - FEBRABAN

FEBRABAN

QUESTIONÁRIO

Tomada de Subsídios sobre Transferência Internacional

1. **Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?**

Os principais obstáculos para transferência internacional de dados pessoais do Brasil para outros países são:

(i) Necessidade de harmonização e atendimento simultâneo entre a legislação e a regulação do país de destino com os preceitos da LGPD.

(ii) Inexistência de regulamentação pela ANPD dos mecanismos de transferência internacional previstos na LGPD, inclusive as decisões de adequação previstas no inciso I do art. 33.

(iii) Inviabilidade de realização de transferência internacional com base no consentimento do titular (art. 33, VIII), que não se mostra um mecanismo operacionalmente adequado na prática.

(iv) Complexidade na implantação e negociação dos mecanismos previstos na LGPD, entre as quais, as cláusulas-padrão contratuais.

(v) Práticas negociais que vedam a realização de transferência internacional de dados para certas regiões, devido a regras internas de parceiras comerciais (por exemplo, vedação à transferência para países com embargos comerciais).

(vi) Inexistência de posicionamento da ANPD quanto à aceitação de selos e certificações, impossibilitando adoção segura de tais mecanismos pelas empresas.

(vii) Necessidade de compatibilizar e considerar regras específicas que podem envolver determinada transferência; por exemplo, cibersegurança (Res. CMN n. 4893).

(viii) Mecanismos de transferência internacional que se mostram demasiadamente onerosos e complexos para sua implementação prática.

(ix) Falta de clareza sobre o que de fato representa uma transferência internacional de dados para fins de aplicação das restrições e hipóteses específicas previstas na LGPD,

destacando que não deve ser considerada transferência internacional, no mínimo, a hipótese em que o "importador" dos dados também já esteja sujeito à LGPD.

Os principais obstáculos para transferência internacional de dados pessoais de outros países para o Brasil são:

(i) Ausência de reconhecimento internacional do Brasil como país com grau de proteção de dados e privacidade adequado em relação a outros países.
(ii) Necessidade de atendimento a exigências internacionais mais rigorosas.
(iii) Ausência de previsibilidade e segurança compatível.

2. Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?

A convergência e interoperabilidade com mecanismos de jurisdições distintas deve ser pautada pela multiplicidade e flexibilidade de padrões, de modo a não inviabilizar o uso de instrumentos contratuais por haver uma falta de flexibilidade, adequação de seu teor e custos elevados.
Ainda que se tome por base instrumentos já construídos e que possam servir de padrão para fomentar situações de convergência e interoperabilidade, deve haver flexibilidade para adaptações e aprimoramentos constantes, eventuais alinhamentos conceituais e terminológicos com outras jurisdições, suas legislações e instrumentos, sempre respeitando a LGPD.
A harmonização com padrões de outras localidades não pode ser inviável ou adotar modelos muito restritivos, com a mera importação de padrões. Essa harmonização deve ser cuidadosa a ponto de refletir especificidades da experiência brasileira no tratamento e proteção de dados e o atual estágio dessa proteção e tratamento de dados pessoais no país.
Neste aspecto, a atuação da ANPD deve estar pautada por alinhamentos e adequações conceituais e interpretativas próprias quando da propositura de cláusulas-padrão.

Uma alternativa na atuação da ANPD pode ser a aceitação de selos e certificados globalmente reconhecidos ou ainda a participação da ANPD no fórum internacional de transferência internacional de dados, CBPR - *Global Cross-Border Privacy Rules System* (www.cbprs.org).

Por fim, de modo a facilitar o acesso, conhecimento e aplicação, todas as medidas adotadas pela ANPD referentes à transferência internacional de dados devem ser públicas e disponíveis na página da autoridade na rede mundial de computadores.

3. Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?

O mecanismo de transferência internacional mais efetivo é a decisão de adequação, tanto para transferências do Brasil para outro país, quanto para transferências de outros países para o Brasil. Nesse sentido, a ANPD deve desenvolver o necessário para reconhecer outras jurisdições como adequadas. Em relação a instrumentos contratuais, cláusulas-padrão estão entre as formas mais efetivas e utilizadas para legitimar uma transferência internacional de dados. Destaca-se a flexibilidade das cláusulas-padrão, que podem ser usadas em diversos cenários de transferência, bem como na possibilidade de incorporação em contrato, seja na forma de previsão expressa no instrumento, ou em anexo específico, ou ainda mediante simples referência, tal como se faz em menção a dispositivos legais.

Especificamente para agentes de tratamento de pequeno porte, que apresentam corpo técnico reduzido, poucos recursos e baixo poder de barganha negocial, a adoção de tais cláusulas-padrão pode ser benéfica e facilitar as transferências internacionais. Na experiência internacional, essa escolha vem se mostrando favorável.

As cláusulas corporativas globais também são instrumentos utilizados para embasar transferências internacionais entre empresas do mesmo grupo.

Sem prejuízo das maior efetividade de tais cláusulas-padrão ou de cláusulas corporativas globais, todas as demais hipóteses previstas na LGPD podem ser usadas para autorizar as transferências internacionais de dados, independentemente do porte do agente de tratamento, e são fundamentais para viabilizar transferências internacionais.

Por fim, é importante ressaltar que não há hierarquia entre as previsões contidas nos incisos do art. 33, pelo que não compete à ANPD estabelecer qualquer obrigatoriedade ou priorização de alguns instrumentos ou hipóteses em detrimento de outras. Deve ficar a critério dos agentes de tratamento a aplicação da previsão mais adequada ao caso concreto.

4. **Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?**

Em um mundo globalizado e cuja atuação dos agentes econômicos encontra-se fortemente vinculada ao uso da tecnologia e à economia digital, a transferência internacional de dados é fundamental para desenvolvimento social, econômico e tecnológico do país, trazendo benefícios (i) para as empresas, na realização de seus negócios; e (ii) para os próprios titulares de dados, na oferta de novos produtos e serviços viabilizados pelo fluxo dos dados.

A economia, inclusive a digital, depende da transferência internacional de dados para desenvolvimento de tecnologias como internet das coisas, economia de aplicativos, e-commerce, computação em nuvem, big data, serviços digitais e serviços de streaming, entre outros.

Certos das vantagens proporcionadas pela transferência internacional de dados, bem como da necessidade de sua realização, a regulamentação do tema não deve criar entraves e dificuldades para operações em curso e futuras, com imposição de regras de rígidas importadas de outras jurisdições, como o modelo vigente na União Europeia, tampouco ser o motivo para arbitragens e conflitos regulatórios.

É preciso conferir um prazo de adequação razoável aos agentes de tratamento e respeitar o legado de tratamentos já realizados de forma a não criar insegurança jurídica e efeitos adversos nos negócios realizados em nível internacional.

Qualquer imposição de padrões pela ANPD deve resguardar contratos já firmados e se aplicar ao futuro de forma a permitir a rediscussão e acomodação de práticas e tratamentos, sob pena e risco de inviabilidade de negócios e atividades e resoluções contratuais.

Além de definir quais países serão considerados adequados, a ANPD deveria buscar: (i) adequada regulamentação de cláusulas-padrão flexíveis e alinhadas à realidade brasileira, (ii) estruturação adequada para aprovação, se for efetivamente necessária, de normas corporativas globais e as cláusulas específicas em prazos curtos, tempestivos e razoáveis, e (iii) reconhecimento de selos e as certificações globais aceitáveis para esses processos de transferência internacional de dados.

Em qualquer caso, a ANPD deve evitar entraves já observáveis em outras jurisdições, com importação de modelos rígidos, sujeitos à aprovação prévia, morosa e bastante custosa de instrumentos para a transferência. O impacto regulatório de qualquer decisão nesse sentido será adverso e criará externalidades inaceitáveis para um país cujos agentes de tratamento dependem de parceiros e relações internacionais para os seus negócios.

5. **Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê? a) cláusulas-padrão contratuais; b) cláusulas contratuais específicas; e c) normas corporativas globais.**

Deve-se buscar um equilíbrio na adoção e indicação de critérios e requisitos dos mecanismos de transferência internacional para que a rigorosidade no seu tratamento, o excesso de exigências regulatórias e a onerosidade de adoção e implementação não sejam tais a ponto de desincentivar ou, até mesmo, inviabilizar a sua utilização pelos agentes de tratamento.

Quanto às **cláusulas-padrão contratuais**, a linguagem não pode ser única e rígida. A regulamentação deve permitir ajustes conforme cada caso, desde que sigam determinados princípios e conceitos já disciplinados na LGPD. Em qualquer caso, essas cláusulas devem ser orientadas à observância da LGPD, e sua utilização deve ter uma abrangência ampla, de modo a possibilitar a transferência a qualquer país.

A regulamentação pode prever, de forma sugestiva e orientativa, um padrão para indicar um ponto de partida de seu conteúdo, sem prejuízo da adequação ao caso concreto, e deixar a critério do agente a sua adoção literal ou seu ajuste, sempre em consonância com aqueles princípios, direitos e garantias já previstos aos titulares de dados pessoais na LGPD.

Na mesma linha, devem seguir as **cláusulas contratuais específicas**. Em qualquer caso, é necessário que a regulamentação traga critérios objetivos, requisitos mínimos e formas simplificadas de aprovação pela ANPD, se essa aprovação for essencial.

Cláusulas contratuais adequadas aos critérios objetivos e aos princípios, direitos e garantias direcionadores de sua elaboração poderiam ser consideradas válidas e eficazes, salvo se a área de fiscalização da ANPD avalie em contrário. De qualquer modo, o procedimento de aprovação deveria ser automático, sempre que comprovada a aderência a critérios ou fatores objetivos pré-determinados. Parece bastante oneroso e moroso para a ANPD e para todos os agentes econômicos demandar uma avaliação individual, caso a caso e setor a setor. Um procedimento de aprovação prévia pela ANPD exigiria uma estrutura mais robusta da agência e prontidão de análise e não poderia levar à suspensão ou efeitos adversos em negócios realizados internacionalmente, até sua aprovação, sob pena de prejudicar a atuação não só desses agentes, mas do país como um todo na economia internacional.

Quanto às **normas corporativas globais**, os critérios para a regulamentação devem estar pautados em uma abordagem baseada em riscos (*risk based approach*) e na prestação de contas (*accountability*), conforme princípios e diretrizes gerais previstos na LGPD, cabendo às empresas de um mesmo grupo econômico implantarem acompanhamento por controles internos, sem prejuízo da fiscalização da ANPD quanto ao conteúdo e à aderência a tais normas. Entendemos que, por se tratar de transferências entre empresas do mesmo grupo, é possível flexibilizar os requisitos a serem adotados nas normas corporativas globais e também sugerimos que a ANPD: (i) reconheça as normas corporativas globais já aprovadas em outras jurisdições, dispensando a necessidade de aprovação pela ANPD ou criando processo simplificado e acelerado de aprovação; e (ii) defina critérios viáveis para aprovação das normas corporativas globais, observando o contexto brasileiro.

6. **Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?**

   Os critérios de avaliação do nível de proteção de países estrangeiros, detalhados nos incisos do art. 34 da LGPD, devem ser avaliados de forma principiológica e genérica. Entretanto, o art. 34, da LGPD prevê a avaliação específica de aspectos legais e regulamentares de outros países, o que entendemos não ser totalmente aplicável no caso, uma vez que os instrumentos contratuais de transferência devem ser passíveis de utilização em qualquer país ou organismo internacional que não tenha uma decisão de adequação, nos termos do art. 33, I, da LGPD.
   Há de ser estudada a viabilidade padronização das cláusulas considerando, por exemplo, a caraterização do agente de tratamento, os tipos de dado sujeitos à transferência internacional, entre outros.

7. **As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?**

   As cláusulas-padrão devem se pautar em uma regulamentação flexível e de conteúdo adaptável a diferentes cenários, com sugestões não vinculantes de conteúdo, contanto que aderente a princípios e diretrizes da LGPD.
   A observância desses princípios e diretrizes da LGPD já têm o condão de levar aos resultados almejados, ainda que se parta de um diferente conteúdo, de flexibilidade quanto à sua atualização ou da facilidade de sua implementação, inclusive, por mera referência, anexo, aditivo ou no corpo dos contratos.
   Os textos eventualmente pré-determinados devem ser modelos ou exemplos com flexibilidade redacional e instrumental, contanto que se mantenham aderentes a princípios, direitos,

obrigações e responsabilidades contidos na essência das cláusulas-padrão. A flexibilidade em nada conflita com a exigência de aderência a princípios e finalidades; ao contrário, permite que um padrão de cláusula transversal a diversos agentes e setores seja adequadamente utilizado para os fins da proteção dos dados pessoais.

O uso das cláusulas-padrão deve considerar a atuação e o setor econômico envolvido, levando em conta especialmente os segmentos que já possuem regramento próprio à proteção dos dados em geral e à segurança cibernética, com impactos transfronteiriços.

É o caso do setor financeiro, por exemplo, cujas instituições estão sujeitas não só a LGPD, mas a uma exigente regulamentação de setor para a coleta, processamento e armazenamento de dados (caso da Resolução CMN n. 4.893, que dispõe *sobre os requisitos para a contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem*), incluindo requisitos a serem observados para contratação com prestadores de serviços estrangeiros. Aliás, essa regulamentação pode ser um bom exemplo do modo como a ANPD poderia prever essas cláusulas, pois indica aos agentes regulados os critérios e os conteúdos amplos das disposições contratuais, sem enrijecer, no entanto, exigindo uma redação específica.

8. **Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?**

Os modelos de cláusulas-padrão devem ser mantidos à disposição para consulta no website da ANPD, na rede mundial de computadores, acompanhados de orientações de uso, em linguagem didática e versão traduzida para outros idiomas. Podem ser complementados por um guia orientativo próprio, com exemplos práticos e cenários debatidos em consulta pública.

A disponibilização de ferramentas dinâmicas, de fácil consulta e constante atualização – checklists, formulários e questionários (Q&A), ou árvores de decisão - também é bem-vinda na medida em que facilite e incentive o uso destes mecanismos e modelos, sendo, no entanto, opcional. Essa opção traz mais segurança jurídica a contratos já celebrados, em andamento, e

permite a adoção paulatina de ajustes e adequações, sem onerar as partes ou impor novas negociações.

É importante que essas ferramentas não se tornem mais um formalismo ou procedimento apenas para aferir o cumprimento de orientações. A necessidade e o benefício de uso devem ser deixados à análise dos agentes econômicos para a substantiva proteção dos dados pessoais.

Sugerimos avaliar a experiência da Nova Zelândia, com cláusulas de um padrão mais curto, genérico e menos oneroso aos agentes de tratamento envolvidos na transferência internacional de dados.

9. **É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?**

É recomendável maior flexibilização ou dispensa, se for o caso, de aplicação de regras a depender do tipo de agentes de tratamentos e seus padrões de relacionamentos (exportador ou importador) no caso concreto. Cabe destacar que operadores e controladores já estão sujeitos a obrigações específicas pela LGPD conforme seja a posição do agente de tratamento, não havendo motivos para (i) a expansão das obrigações existentes; e (ii) a unificação dessas obrigações ao observar apenas a posição de importador ou exportador sem considerar que se trata de um controlador e ou operador.

10. **Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?**

Considerando o âmbito de aplicação das normas corporativas globais e das cláusulas-padrão contratuais, os requisitos para tais instrumentos devem ser diferentes.

Normas corporativas globais são previstas para aplicação de empresas de um mesmo grupo econômico e possuem normalmente um escopo mais restrito e vinculado ao interesse comum desse grupo, conforme seu setor de atuação, inclusive no tocante à proteção de dados. A

regulamentação deve seguir linha orientativa e mais flexível, inclusive, do que das cláusulas-padrão. Podem ser propostas diretrizes e formulários (*template*) de conteúdo mínimo, acompanhado da possibilidade de fiscalização *a posteriori*, com pedido de informações complementares, em linha com o parágrafo 2º do art. 35 da LGPD, adequados a garantir o atendimento à LGPD e a proteção aos titulares de dados pessoais. Outrossim, deve-se atentar para evitar conflitos e para absorver as normas corporativas já adotadas por grupos multinacionais, conforme análise de outras autoridades reguladoras estrangeiras. A adoção dessas normas já confere, de antemão, alguma padronização e conforto quanto ao cumprimento dos princípios e direitos pelos seus membros.

Ainda, a regulamentação das normas corporativas globais não deve requerer submissão e aprovação prévia da ANPD, sob pena de a ausência de tempestividade, o excesso de onerosidade e o procedimento burocrático tornarem-se um gargalo que desestimule a própria adoção desse instrumento.

Por fim, a regulamentação deve contemplar flexibilizações e dispensas de normas corporativas globais anteriormente aprovadas por países estrangeiros ou organismos internacionais que a ANPD repute ter um nível de proteção de dados pessoais adequado aos padrões e exigências da LGPD.

11. Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?

A definição do grupo econômico de fato ou de direito deve observar os mesmos critérios já existentes no ordenamento e prática jurídicos brasileiros, observada a prática internacional. Além da consideração, por exemplo, de grupos econômicos no direito empresarial, pode ser útil observar o entendimento de outras autoridades internacionais. No entendimento da autoridade do Reino Unido – ICO, por exemplo, ao regular as normas corporativas globais – BCR (*Binding Corporate Rules*), verifica-se o seguinte critério adicional: “grupos empresariais multinacionais, grupos de empresas ou um grupo de empresas que exerçam uma atividade econômica conjunta, como franquias, joint ventures ou parcerias profissionais”.

Ainda, um critério importante a se considerar para fins de aplicação das normas corporativas globais é que a submissão às normas corporativas globais depende de manifestação expressa e adesão formal ao seu conteúdo, não sendo aplicável de forma automática a todas as empresas do grupo econômico, cabendo ao grupo empresarial determinar as empresas que estariam sujeitas às normas corporativas globais. Além disso, o conceito de grupo empresarial deve ser aplicável para fins de transferência internacional, mas não necessariamente no caso de outras situações previstas na LGPD em que seja necessário considerar o grupo econômico.

12. Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?

A ANPD pode solicitar as seguintes informações para permitir a análise da conformidade de transferências internacionais:

(i) As categorias amplas de dados pessoais, objeto de transferência internacional.

(ii) O papel do agente de tratamento (controlador e operador) na transferência internacional (importador e exportador), caso a ANPD adote modelos de cláusulas padrão adaptáveis ao papel dos agentes.

13. Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?

Visto que a aprovação das normas corporativas globais não é procedimento simples, a possibilidade de aproveitamento das normas corporativas globais entre grupos, quando tais normas já foram aprovadas pela ANPD ou por outras autoridades, é medida benéfica e recomendada aos agentes de tratamento.

14. Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?

Em razão da complexidade deste instrumento, que exige aprovação prévia, caso a caso, pela autoridade de dados, o instrumento não é muito utilizado e não existem muitos exemplos a serem mencionados como referencial para a ANPD sobre a aprovação de cláusulas específicas. De todo modo, pode-se citar, por exemplo, a experiência asiática (Singapura) e da Nova Zelândia, cuja análise não exige uma aprovação prévia e burocrática de todos os instrumentos.

E há experiências que podem ser revistas para se evitar a reprodução dos entraves que estão criando aos agentes econômicos, caso, por exemplo, da atual, custosa, morosa e excessivamente burocrática experiência da Argentina e da União Europeia. No caso da ANPD, deve-se buscar um equilíbrio na verificação e aprovação prévia de cláusulas contratuais específicas e de normas corporativas globais. Os instrumentos não devem ser todos aprovados e devem ser consideradas hipóteses de flexibilização e dispensa, até porque a ANPD precisará obter uma estrutura suficiente e dedicada de funcionários para uma aprovação célere, pouco onerosa, pouco burocrática e eficiente nessas aprovações.

15. Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?

Os agentes de tratamento permanecem sujeitos à observância das mesmas garantias e direitos dos titulares, ainda que alterada a configuração original da transferência internacional dos dados. Assim sendo, a comunicação direta e imprescindível aos titulares dos dados parece desnecessária, visto que permanecem exigíveis (i) o atendimento ao princípio da transparência, inclusive mediante a previsão, nas Políticas e Avisos de Privacidade, da possibilidade de transferência internacional de dados e (ii) a disponibilização do acesso à informação a qualquer momento, mediante requisição.

16. **Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?**

Com relação à resolução de conflitos, as opções já existentes, como a arbitragem e o Poder Judiciário, já se mostram plenamente satisfatórias para atender conflitos entre agentes de tratamento e entre estes e titulares de dados.

No relacionamento entre agentes de tratamento, cumpre observar qual foi a opção negociada em contrato e invocar sua aplicação (câmara arbitral específica ou foro de eleição das partes). Quanto ao titular dos dados, as previsões contidas na LGPD, que permitem acionar diretamente, extrajudicialmente ou judicialmente, os agentes de tratamento e exercer seus direitos, inclusive recorrendo à própria ANPD, já se mostram adequados.

Assim sendo, não é necessário um procedimento adicional para tratar desses conflitos, mantendo apenas a aplicação dos mecanismos de resolução de conflitos já existentes, respeitando, ainda, competências territoriais e de jurisdição já estabelecidas pelas regras de Direito Internacional Público e Privado, soberanas sobre qualquer regulamentação. Sem prejuízo, acordos bilaterais, multilaterais ou acordos de cooperação entre autoridades de proteção de dados podem ser estudados e adicionados para complementação de procedimentos de caráter transnacional.

17. **Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?**

Entre as alternativas para promover a conformidade da transferência de dados com a regulamentação, pode-se propor uma previsão contratual que impute atendimento de requisitos ou critérios específicos, de acordo com os princípios e diretrizes da LGPD. Alternativamente, é possível adotar selos, certificados e códigos de conduta, de aceitação global, aderentes aos

padrões de proteção da LGPD. Ainda, guias orientativos, flexíveis ao caso concreto e ao setor de atuação. Por fim, pode-se eleger e indicar expressamente países com nível satisfatório de proteção de dados.

18. **Quais as melhores alternativas para resolver as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?**

A responsabilização dos agentes de tratamento nas transferências internacionais, inclusive em casos de subcontratações, deve ser aferida conforme legislação brasileira atualmente em vigor, sem prejuízo de eventual disciplina de distribuição e limitação própria da responsabilidade entre esses agentes exportadores e importadores, de acordo com específicas disposições contratuais, sem prejuízo dos direitos de titulares de dados.

19. **Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?**

O fornecimento de dados pessoais por determinação de autoridade pública estrangeira deve ser feito nos termos da legislação estrangeira que possa vigorar em relação ao importador ou exportador, sem prejuízo de comunicação ao outro agente sobre essa solicitação, conforme permitido e determinado pelas legislações aplicáveis e por eventual contrato ou outra hipótese legal que possa reger e fundamentar a transferência internacional.

20. Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

A Política ou Aviso de privacidade é o instrumento mais adequado para fornecer aos titulares de dados informações claras sobre os tratamentos de dados realizados pelo controlador, inclusive a transferência internacional de dados. Nesse sentido, não há necessidade de nenhuma complementação para assegurar mais proteção de direitos, contanto que a referida política adote uma linguagem clara e acessível aos titulares de dados e disponibilize canais de acesso adequados para que estes exerçam seus direitos e, entendendo necessário, mediante requisição, obtenham esclarecimentos sobre os tratamentos realizados, conforme previsto na LGPD.

O princípio de transparência é observado, nesse sentido, a partir do detalhamento possível e exemplificativo das modalidades de transferências internacionais, dispensadas medidas complementares.

Anexo | Tomada de Subsídios sobre Transferência Internacional
Frente Parlamentar do Setor de Serviços - FPS <contato@fpservicos.org.br>
Qui, 30/06/2022 19:31
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Prezados,

A Frente Parlamentar do Setor de Serviços, representante de setores como promotores de crédito e correspondentes bancários, telecobranças, medicina diagnóstica, consórcios recursos humanos e terceirização de mão de obra, marketing promocional e vigilância privada e transporte de valores, vem apresentar suas colaborações para a Tomada de Subsídios sobre Transferência Internacional de dados pessoais, buscando auxiliar na construção de um modelo regulatório que garanta nível adequado aos padrões internacionais de proteção de dados pessoais e, ao mesmo tempo, não dificulte o desenvolvimento econômico brasileiro.

Considerando o amplo escopo do tema, apresentamos proposta para um foco regulatório: **a utilização de instrumentos de Relatórios de Impactos de Transferências (conhecidas internacionalmente como Transfers Impact Assessments – TIA)**

Segue, em anexo, a íntegra das contribuições.

Atenciosamente,

Hélzio Mascarenhas
Secretário-Executivo
([redacted])
helziomascarenhas@frenteparlamentarservicos.com.br
www.fpservicos.org.br

SUBSÍDIOS Á REGULAMENTAÇÃO DE TRANSFERÊNCIAS INTERNACIONAIS DE DADOS PESSOAIS

Brasília, 30 de junho de 2022.

Aos senhores e senhoras Diretores(as) da Autoridade Nacional de Proteção de Dados do Brasil

A Frente Parlamentar do Setor de Serviços, representante de setores como promotores de crédito e correspondentes bancários, telecobranças, medicina diagnóstica, consórcios recursos humanos e terceirização de mão de obra, marketing promocional e vigilância privada e transporte de valores, vem apresentar suas colaborações para a Tomada de Subsídios sobre Transferência Internacional de dados pessoais, buscando auxiliar na construção de um modelo regulatório que garanta nível adequado aos padrões internacionais de proteção de dados pessoais e, ao mesmo tempo, não dificulte o desenvolvimento econômico brasileiro.

Considerando o amplo escopo do tema, será apresentada proposta para um foco regulatório: a utilização de instrumentos de Relatórios de Impactos de Transferências (conhecidas internacionalmente como *Transfers Impact Assessments – TIA)*.

Primeiramente, é necessário estabelecer o contexto prático em que as empresas brasileiras realizam transferências internacionais de dados pessoais, a fim de que a regulação não venha a impor obrigações que podem ser, na prática, quase impossíveis de serem alcançadas. Para isso, serão explorados um cenário simples e um cenário complexo.

O cenário simples são empresas que atuam em múltiplos países, possuindo servidores de armazenamento de dados pessoais em vários desses locais, ou, então, empresas que possuem poucos fornecedores de serviços para sistemas de gestão e

armazenamento e estão localizados em outros países. Esse cenário é simples no sentido de ser fácil identificação e controle sobre as transferências realizadas, sendo que o agente de tratamento consegue identificar riscos através de procedimentos internos. Nele, os agentes conseguem manter controle sobre os tipos de dados transferidos, os mecanismos

administrativos e técnicos envolvidos, além de contato direto com outros agentes de tratamento.

Por sua vez, o cenário complexo é a realidade de muitas empresas e, a depender das imposições regulatórias, pode gerar riscos legais e operacionais para elas. Esse cenário é baseado na complexidade das operações de empresas atuais, que muitas vezes utilizam inúmeros fornecedores de sistemas e serviços, e que por sua vez, esses fornecedores utilizam vários outros fornecedores seus, e assim sucessivamente. As transferências internacionais podem acontecer em vários pontos dessa cadeia, ou, então, em um ponto do tratamento que é de difícil conhecimento pelo Controlador responsável.

Contextualizando, pode-se tomar como exemplo empresas que realizam exames de diagnóstico de imagem e, em muitos casos, sequer são empresas de porte e estrutura considerável. Esses Controladores coletam dados pessoais sensíveis referentes à saúde (art. 5º, inciso II da LGPD) como atividade fim e são agentes importantes na prestação de serviços de saúde. Normalmente, na prestação do serviço, inúmeros fornecedores estão envolvidos no tratamento dessa categoria especial de dados: aqueles que mantém o funcionamento dos equipamentos utilizados na captura das imagens, aqueles que são responsáveis por sistemas de armazenamento dessas imagens, aqueles que fornecem sistemas de análises automatizadas das imagens e até mesmo os servidores de trocas de mensagens entre os profissionais da saúde. Ocorre que esses fornecedores podem estar localizados no Brasil, mas eles possuem fornecedores próprios para seus sistemas, e que podem demandar transferências internacionais, como fornecedores de espaço de armazenamento em nuvem. Ainda, esse é o cenário de agentes envolvidos nos tratamentos das categorias especiais, mas a mesma empresa também utiliza sistemas semelhantes para controles administrativos (financeiro, contábil, RH etc) que podem acabar realizando transferências internacionais.

Percebe-se, portanto, a complexidade da questão.

A regulação deve levar em conta a distribuição de obrigações pelas transferências nessa cadeia de tratamentos a fim de que não seja apenas do controlador, muitas vezes

mero consumidor de serviços de um grande fornecedor de sistemas que é caracterizado como operador.

Uma vez estabelecido um cenário fático, apresentamos a proposta de que a regulação faça referência à elaboração de Relatórios de Impacto de Transferências pelos agentes de tratamento envolvidos nessas cadeias de tratamento.

Esse instrumento de controle de riscos surgiu para retratar o processo pelo qual os agentes de tratamento verificaram o impacto sobre a privacidade na transferência de dados pessoais para países terceiros não considerados adequados pela Comissão Europeia, e passou a ser largamente utilizado por agentes de tratamentos sujeitos à Regulação Geral de Proteção de Dados da União Europeia após a decisão do Tribunal de Justiça da União Europeia (TJUE) no processo C-311/18, conhecido como Schrems II, em 2020. A Corte da União Europeia declarou o sistema de princípios Privacy Shield da Comissão Europeia inválido, sistema que era utilizado para a garantia de legitimidade das transferências de dados por empresas localizadas em países membros do bloco europeu e Estados Unidos da América[1].

A decisão, ao invalidar esse mecanismo principiológico de certificações para transferências internacionais, também ressaltou que a utilização de mecanismos de transferências como Cláusulas Contratuais Padrões (também presente na LGPD no art. 33, inciso II, alínea *b*) não garantem, por si só, a conformidade legal. Para atingir essa conformidade, análises específicas devem ser realizadas pelos agentes de tratamento, segundo o órgão jurisdicional[2].

A partir disso, o Comitê Europeu para Proteção de Dados (CEPD), adotou a Recomendações 01/2020, relativas "às medidas complementares aos instrumentos de

---

[1] Em comunicado do Parlamento Europeu sobre a decisão é descrito o contexto da invalidação e algumas das consequências práticas. Disponível em https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/652073/EPRS_ATA(2020)652073_EN.pdf . Acesso em 01 de junho de 2022

[2] A leitura das respostas às questões 7ª e 11ª do acórdão, itens 122-149, prevê a insuficiência desses instrumentos contratuais por si só, gerando obrigações para os agentes de tratamento envolvidos. Disponível em https://curia.europa.eu/juris/document/document.jsf?text=&docid=228677&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=12312155 . Acesso em 01 de junho de 2022

transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da EU"[3]. Ainda, por mais que em sua decisão o TJUE não tenha exigido que a análise de impacto fosse documentada por escrito, na recomendação citada, o CEPD prevê que em caso de solicitação pelas autoridades de supervisão e/ou judiciais competentes, o agente de tratamento deverá apresentar análise documentada sobre os impactos da transferência[4], a qual poderá ser utilizada para demonstrar que as partes dispensaram os melhores esforços para garantir uma transferência segura.

Nessas medidas, o CEPD elencou seis etapas que os agentes de tratamento envolvidos nas transferências internacionais devem percorrer para garantir a legitimidade do tratamento e a observância ao princípio da *accountability* (presente na LGPD no art. 6º, inciso X). Uma vez formalizados os resultados dessas etapas, o documento recebeu o nome comum de *Transfer Impact Assessment – TIA*.

As etapas são (CEPD, 2020, p. 10-28):

- primeira: conhecimento das transferências através de levantamento dos processos de tratamentos de dados pessoais que levam a outros países;.
- segunda: verificar o instrumento legal de transferência, como decisão de adequação ou cláusulas contratuais padrão (previstos no capítulo v da LGPD);
- terceira etapa: verificar o ambiente legal e regulatório do país destinatário para identificar riscos e medidas de proteção que são adotados;
- quarta etapa: identificar e adotar medidas complementares de proteção, a fim de garantir nível aproximado de segurança adotado na UE;
- quinta etapa: adotar formalmente as medidas identificadas através da elaboração de documentos e cumprimentos de requisitos legais e regulatórios adicionais; e
- sexta etapa: reavaliação periódica dos processos de transferências internacionais.

[3] Disponível em https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020measures-supplement-transfer_pt . Acesso em 01 de junho de 2022.

[4] ibidem, páginas 4 e 10. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-012020-measures-supplement-transfer. Acesso: em 05 de junho de 2022.

Dito isto, acreditamos que no Brasil, o estabelecimento de mecanismos de análise de impacto documentada, em conjunto a adoção de cláusulas contratuais que prevejam

que o agente de tratamento localizado em país terceiro garanta que a legislação e as práticas do país de destino aplicáveis ao tratamento dos dados pessoais não o impeçam de cumprir os direitos, as garantias e os princípios previstos pela Lei Geral de Proteção de Dados Pessoais, sejam medidas necessárias para garantir um nível adequado aos padrões internacionais de proteção de dados pessoais, sem atribuir obrigações desproporcionais aos controladores em posição de consumidores de serviços de operadores que sejam grandes fornecedores de sistemas.

Para garantir o cumprimento dessas medidas, sugerimos que as obrigações sejam impostas aos controladores e operadores, de modo a evitar atribuição de responsabilidades incompatíveis à realidade dos controladores, que muitas vezes não possuem condições de coletar de seus fornecedores informações suficientes para realizar uma adequada análise de impacto de transferência internacional, ou até mesmo de negociar cláusulas contratuais, seja pelo elevado número de suboperadores, seja por ausência de poder de negociação do controlador.

Hélzio Mascarenhas

Secretário Executivo da Frente Parlamentar do Setor de Serviços

Fabrício da Mota Alves

Coordenador do GT de Proteção de Dados e Tecnologia

Alisson Alexsandro Possa

Membro do GT de Proteção de Dados e Tecnologia

Bruna de Souza Nunes

Membro do GT de Proteção de Dados e Tecnologia

Tomada de Subsídios da ANPD sobre Transferência Internacional - Contribuição Google Brasil Internet Ltda.
Jaqueline Simas Claveland de Oliveira [redacted]
Qui, 30/06/2022 21:33
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Cc:

- [redacted]

Prezados, boa noite.

Na qualidade de advogados do Google Brasil Internet Ltda. ("Google"), encaminhamos, anexo, instrumento de mandato para representar o Google perante a ANPD, inclusive para a submissão de respostas à Tomada de Subsídios nº 02/2022 sobre Transferências Internacionais de Dados Pessoais por meio da plataforma Participa Mais Brasil.

Para facilitar a identificação, informamos que a submissão das respostas do Google na referida plataforma foi realizada na data de hoje, 30/06/2022, pela advogada Luiza Mendonça da Silva Belo Santos, OAB/DF n. 62.869 e [redacted]ora em cópia.

Por fim, também anexa, encontra-se carta do Google à ANPD com breve descritivo do seu posicionamento a respeito da regulamentação dos mecanismos contratuais de transferência internacional de dados, com o objetivo de sumarizar e complementar as respostas da empresa às perguntas propostas por essa Autoridade.

Solicitamos a gentileza de confirmar o recebimento desta mensagem e ficamos à disposição para qualquer esclarecimento necessário.

Cordialmente,

Thiago Luís Sombra - OAB/DF 28.393

Jaqueline Simas C de Oliveira - OAB/RJ 211.510

Isabela Fernandes Pereira - OAB/SP 424.503

Luiza Mendonça da Silva B Santos - OAB/DF 62.869

Jaqueline Simas Claveland de Oliveira

+55 21 3850 5180

[redacted]

MATTOS FILHO

Acesse nosso novo site e fique por dentro dos temas jurídicos que impactam seu negócio no portal Único.
Visit our new website and follow all the latest legal developments that impact your business on our new Único

news portal.

ALERTA - Esta mensagem e seus anexos foram enviadas por escritório de advocacia, são confidenciais ou legalmente protegidas e não podem ser usados ou divulgados por quem não seja seu destinatário.

NOTICE - This message and its attachments were sent by a law firm, are confidential or legally privileged and may not be used or disclosed by anyone who is not their intended recipient.

São Paulo, 30 de junho de 2022

À

Autoridade Nacional de Proteção de Dados ("ANPD")

Coordenação-Geral de Normatização e Coordenação-Geral de Relações Institucionais e Internacionais

Via e-mail: normatizacao@anpd.gov.br

Ref.: Tomada de Subsídios nº 02/2022 sobre transferências internacionais de dados pessoais e os mecanismos contratuais dispostos no art. 33, II, da LGPD

Em complemento às respostas submetidas por meio da plataforma Participa Mais Brasil, o Google apresenta um breve descritivo do seu posicionamento a respeito da regulamentação dos mecanismos contratuais de transferência internacional de dados dispostos no art. 33, II, da LGPD, quais sejam: **(i)** cláusulas-padrão contratuais, **(ii)** cláusulas contratuais específicas e **(iii)** normas corporativas globais.

Valores do Google

Nós desenvolvemos tecnologias de ponta para criar produtos e serviços que melhoram a vida das pessoas, proporcionam acessibilidade, aumentam a produtividade, fomentam a economia e tornam o ambiente *online* mais seguro. Nós mantemos os dados pessoais dos nossos usuários de forma segura, confidencial e sob o controle dos próprios usuários. Todos os dias cerca de 20 milhões de pessoas ao redor do mundo visitam o portal da Minha Conta do *Google* para configurar suas preferências de privacidade.

Além disso, apoiamos regulações de privacidade e proteção de dados robustas e protetivas, e buscamos continuamente aprimorar o fornecimento de informações contextualizadas e atualizadas sobre o tratamento de dados pessoais que realizamos para contribuir com a autodeterminação informativa dos usuários.

As respostas encaminhadas à Tomada de Subsídios nº 02/2022 da ANPD e o

posicionamento geral apresentado por meio do presente documento partem da experiência prática de desenvolver produtos e serviços para tornar a informação universalmente acessível, bem como da nossa experiência com a adequação a regras de privacidade e proteção de dados ao redor do mundo.

Livre fluxo de dados e economia global

A habilidade de transferir e acessar dados ao redor do mundo é imprescindível para todos os setores da economia e para organizações de todos os portes. Os fluxos de informações criam oportunidades para o desenvolvimento de produtos inovadores, disponibilização de serviços de computação em nuvem, fornecimento de serviços a preços reduzidos a consumidores e uso de recursos tecnológicos de ponta independentemente da localização do usuário. A circulação de informações facilita a conexão entre pessoas e interesses independentemente de onde estejam localizados. E, por tudo isso, acreditamos que o fluxo de dados pessoais para além das fronteiras nacionais deve ser encorajado e apoiado pelas legislações de proteção de dados

Além disso, fluxos transfronteiriços de dados incentivam investimentos em negócios de diversos países, ao mesmo tempo em que facilitam a entrada de novos agentes no mercado, o que converge exatamente com os fundamentos para a proteção de dados pessoais e para o uso e desenvolvimento da internet no Brasil, regidos, tanto pela LGPD, que prestigia o desenvolvimento econômico, tecnológico e a inovação, quanto pelo Marco Civil da Internet reconhece a escala mundial da rede, seu uso aberto e colaborativo, a livre iniciativa e a livre concorrência. Igualmente, iniciativas para regular operações que envolvam fluxos internacionais de dados devem considerar tal cenário e seus benefícios.

Interoperabilidade entre diferentes regimes de proteção de dados

Com o intuito de fomentar o livre fluxo de dados, acreditamos que devem ser implementadas soluções que viabilizem a interoperabilidade e a convergência entre os diferentes regimes de proteção de dados em escala global. A interoperabilidade de regimes normativos é um desafio para autoridades que regulamentam a proteção de dados em diversos países e para agentes de tratamento sujeitos a múltiplos regimes normativos concomitantemente. As autoridades de proteção de dados, incluindo a ANPD, possuem um papel central na promoção da convergência e interoperabilidade entre os regimes de proteção de dados e têm a possibilidade de criar mecanismos eficazes que **(i)** viabilizem a transferência internacional de dados pessoais no âmbito das respectivas legislações, **(ii)** assegurem a

convergência mútua entre diferentes regimes de privacidade e proteção de dados, e **(iii)** permitam que as organizações incorporem tais mecanismos facilmente nas práticas globais adotadas.

Com isso, a observância dos requisitos para transferências internacionais de dados é facilitada aos agentes de tratamento, sob a ótica de todas as legislações aplicáveis. Portanto, a partir da convergência e interoperabilidade de regimes, as organizações podem se valer de um conjunto único de regras para transferência internacional, alavancando e direcionando os investimentos aplicados em seus programas de conformidade na disseminação da cultura de proteção de dados, além do desenvolvimento de produtos e serviços que privilegiem as escolhas e preferências de seus usuários.

Soluções para as operações de transferências internacionais de dados pessoais

Nós acreditamos que não há uma solução única para todas as possíveis operações de transferências internacionais de dados pessoais (no termo em inglês, a chamada abordagem *one size fits all,* ou um único modelo para todos os casos). Os mecanismos para transferências de dados devem considerar **(i)** as particularidades de cada atividade de tratamento de dados, **(ii)** os regimes normativos e a legislação dos países de origem e destino, e **(iii)** as particularidades do modelo de negócios do exportador e do importador de dados.

Nesse sentido, entendemos que as obrigações de proteção de dados previstas nos instrumentos contratuais devem ser estabelecidas de acordo com **(i)** o papel desempenhado pelos agentes de tratamento envolvidos, **(ii)** o ecossistema setorial de tais agentes e **(iii)** o escopo e a natureza da transferência internacional realizada, obviamente, em consonância com os princípios gerais estabelecidos pela ANPD.

Nesse sentido, acreditamos que a flexibilidade na regulamentação de tais instrumentos é crucial, pois facilita a livre circulação de informações e preconiza o desenvolvimento econômico e tecnológico e a inovação.

Abordagem flexível na definição do conteúdo das cláusulas contratuais para evitar a imposição de conteúdo rígido e pré-definido aos instrumentos contratuais

Nós acreditamos que a regulamentação dos instrumentos contratuais para transferência internacional de dados, especialmente das cláusulas-padrão

contratuais, deve permitir certa flexibilidade em relação ao texto dos instrumentos, focando na especificação dos resultados pretendidos e permitindo eventuais alterações que sejam necessárias considerando os elementos fáticos de cada operação de transferência.

Nós acreditamos que o conteúdo das cláusulas contratuais deve permitir a negociação das partes, contando com eventual fiscalização posterior da ANPD, se necessário. Tal abordagem incentiva, de um lado, a livre circulação de informações e, de outro, a observância da LGPD, promovendo o fortalecimento da cultura global de proteção de dados, conferindo maior dinamicidade para os fluxos de dados e prestigiando os fundamentos dispostos no artigo 2º da LGPD, em especial o desenvolvimento econômico e tecnológico e a inovação.

Diante disso, acreditamos que a ANPD pode atuar em dois momentos: **(i)** na recomendação do conteúdo mínimo das disposições contratuais, que devem ser diferentes a depender do tipo de agentes de tratamento envolvidos e da finalidade e escopo da transferência internacional, desde que garantam, de forma geral, os princípios, os direitos do titular e o regime de proteção de dados previsto na LGPD; e **(ii)** na fiscalização posterior, se necessária, a partir da realização de procedimentos específicos.

Assim, a ANPD pode adotar abordagens distintas a depender do tipo de serviço prestado pelo agente de tratamento, propiciando maior dinamicidade para os fluxos de dados e prestigiando os próprios fundamentos da LGPD.

Adoção de cláusulas contratuais adaptadas ao escopo específico da transferência internacional de dados pessoais e à realidade setorial das partes envolvidas

Para prestigiar o desenvolvimento econômico e tecnológico e a inovação, propiciando maior dinamicidade para os fluxos de dados, acreditamos que é indispensável permitir que os agentes adotem as cláusulas contratuais que melhor se adequem à sua realidade de atuação e à finalidade e ao escopo da transferência internacional, adotando abordagens distintas a depender do tipo de serviço prestado pelo importador dos dados.

Para tanto, acreditamos que o estabelecimento de regras diferenciadas em relação ao conteúdo mínimo das cláusulas-padrão contratuais a depender do papel desempenhado pelos agentes de tratamento envolvidos na transferência internacional dos dados é essencial, incluindo obrigações gerais distintas para

controladores, operadores e sub-operadores, de acordo com a posição de cada um na operação, na condição de exportadores ou importadores de dados.

Promoção da conformidade com a regulamentação de transferências internacionais de dados pessoais

Entendemos que a adoção de medidas eficazes e capazes de comprovar o cumprimento integral da LGPD (nos moldes do princípio de prestação de contas) é o melhor caminho para promover a conformidade com a regulamentação de transferência internacional de dados.

Diante disso, acreditamos que os agentes devem ser responsabilizados pela conformidade à LGPD, mas que tal conformidade pode e deve ser demonstrada de diversas formas. Por isso, essa Autoridade deve definir requisitos e permitir certa flexibilidade em relação a **(i)** como tais requisitos serão adequadamente cumpridos na prática no âmbito das transferências internacionais; e **(ii)** como tal cumprimento poderá ser comprovado pelos agentes envolvidos na transferência internacional.

A imposição de obrigações específicas nos mecanismos contratuais que não estejam previstas na LGPD, a exemplo da realização de auditorias periódicas do exportador no importar, restringem diretamente o direito de agentes privados à liberdade contratual e ao princípio da autonomia das relações privadas, indo de encontro aos princípios constitucionais da livre iniciativa (art. 1º, IV) e da livre concorrência (art. 170, IV).

Portanto, é razoável que as obrigações de prestação de contas possam ser discutidas pelos agentes envolvidos na transferência internacional de dados de acordo com caso concreto e, eventualmente, incluídas no contrato, conforme aplicável e necessário.

Direitos dos titulares dos dados no âmbito de transferências internacionais de dados pessoais

Os exportadores e importadores que atuam como controladores de dados no âmbito da transferência internacional devem cumprir o princípio da transparência e assegurar que os titulares consigam exercer seus direitos previstos pela LGPD, conforme aplicável.

No âmbito das transferências internacionais, ressaltamos que comunicações direcionadas aos titulares podem ser recomendáveis caso ocorram mudanças

materiais e que impactem direta e significativamente os interesses dos titulares. Havendo necessidade de tal comunicação, o conteúdo, o meio e o formato da comunicação dependerá de uma análise prévia do controlador que considere aspectos específicos da relação que possui com o titular, incluindo a natureza da relação, expectativas do titular e meios adequados para seu envio.

As melhores práticas internacionais que podem servir de exemplo para a ANPD

Por fim, acreditamos que as seguintes experiências internacionais podem servir de exemplo para a Autoridade em relação às cláusulas-padrão contratuais: **(i)** Canadá, **(ii)** Nova Zelândia, **(iii)** Colômbia, e **(iv)** Uruguai. Os motivos que nos levam a crer que tais experiências podem auxiliar na construção da regulação dos mecanismos contratuais de transferências internacionais foram devidamente explorados nas respostas às provocações propostas por essa Autoridade.

Temos o firme compromisso de garantir a proteção de dados, a privacidade e a segurança de seus usuários em todos os seus produtos e serviços.

Sendo o que gostaríamos de apresentar no momento e agradecendo mais uma vez pela oportunidade de contribuir para os debates que levarão à regulação do tema, ficamos à disposição pelo e-mail juridicobrasil@google.com para dar continuidade ao debate com a ANPD sobre o assunto.

Cordialmente,

Equipe Google

Comentários do ITI em Resposta a Tomada de Subsídios sobre Transferência Internacional de Dados
Husani Durans de Jesus [redacted]
Qui, 30/06/2022 15:32
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Cc:

- [redacted]

Prezado(a) Senhor (a)

Meu nome é Husani Durans de Jesus e sou Gerente Sênior de Políticas Públicas para as Américas no Information Technology Industry Council (ITI). Em nome do ITI, porta-voz global do setor de tecnologia, gostaria de agradecer a oportunidade concedida pela a Autoridade Nacional de Proteção de Dados (ANPD) de apresentar contribuições para o projeto de regulamentação da transferência internacional de dados pessoais e aproveitar para enviar anexa nossa contribuição e informações complementares, adicional as respostas submetidas on-line.

Desde já, agradecemos a consideração e colocamo-nos à disposição para prestar quaisquer esclarecimentos.

Atenciosamente,
Husani

Husani Durans de Jesus (He/Ele/Él)
Senior Manager of Policy for the Americas
Information Technology Industry Council (ITI)
700 K Street NW, Suite 600
Washington, DC 20001
[redacted]
hdjesus@itic.org

Join the dialogue, follow ITI on Twitter & LinkedIn

ITI Promoting Innovation Worldwide

30 de junho de 2022

Resposta do ITI à tomada pela ANPD de subsídios iniciais para discutir o regulamento sobre transferências internacionais de dados

O Information Technology Industry Council (ITI) é a voz global, defensor e líder pensador para a indústria global de tecnologia da informação e comunicação. Fundado em 1916, o ITI é uma associação comercial internacional que promove políticas públicas e padrões da indústria, para o desenvolvimento mundial da concorrência e inovação. Nossos 80 membros incluem as empresas líderes em inovação do mundo, sediadas em todo o planeta e com cadeias de valor distribuídas ao redor do globo. Essas empresas são as maiores prestadoras de serviços de internet e comércio eletrônico, indústrias e fornecedores de equipamentos para redes sem fio e fixas, empresas de hardware e softwares para computadores, e empresas de tecnologia e eletrônicos para consumidores.

A privacidade e a confiança dos usuários são fundamentais para os negócios e operações globais dos nossos membros. O ITI endossa rígidas proteções para o fluxo transfronteiriço de dados e agradecemos a oportunidade de apresentar nossos subsídios à Autoridade Nacional de Proteção de Dados (ANPD) para a elaboração do regulamento sobre transferências internacionais de dados.

Encorajamos a ANPD a considerar como todos os participantes, incluindo autoridades públicas, autoridades com poder de polícia, grupos de consumidores, acadêmicos, órgãos de pesquisa e a indústria deveriam se unir para refletir sobre o papel desempenhado pelos fluxos de dados no alicerce de nossa vida moderna. Também elogiamos o reconhecimento da importância dos fluxos de dados transfronteiriços pela ANPD em diversas ocasiões, inclusive por meio do texto da presente tomada de subsídios. Gostaríamos de encorajar a ANPD a continuar apoiando esse objetivo, inclusive por meio da alavancagem de seu papel como líder global para combater as tendências de localização de dados. Apresentamos a seguir nossos comentários gerais sobre a facilitação das transferências internacionais de dados. Em seguida, apresentamos nossa opinião sobre algumas perguntas propostas pela ANPD. Estamos ansiosos para debater essas ideias e permanecemos à disposição de V.Sas. para continuarmos as discussões.

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

Recomendações Gerais

Com base em nossa experiência global foram desenvolvidos pelo ITI as recomendações e princípios a seguir.

Promover o alinhamento e interoperabilidade com abordagens internacionais predominantes. É crucial que qualquer regulamento sobre transferências internacionais de dados esteja alinhado com as abordagens internacionais predominantes. Assegurar a compatibilidade com as estruturas de proteção de dados e privacidade e os parceiros comerciais reduz a probabilidade de obstáculos à transferência de dados pessoais pelas empresas do Brasil a outras jurisdições e vice-versa.

Recomendamos que a ANPD apoie a interoperabilidade global com estruturas internacionais, incluindo:

1. Autorizando a utilização de instrumentos contratuais que as empresas já mantenham em vigor se tais contratos contemplarem proteções substantivas substancialmente similares àquelas exigidas pela Lei Geral de Proteção de Dados Pessoais (LGPD), incluindo as Cláusulas-Padrão Contratuais (CCPs) da UE e do Reino Unido e outros contratos *bespoke* baseado nos Artigos 33(II)(b) e 35 da LGPD.
2. Endossando ou considerando um rito sumário para a aprovação das Normas Corporativas Globais (NCGs) aprovadas por jurisdições cujas leis forem substancialmente análogas à LGPD, como atualmente é o caso da UE e do Reino Unido, baseado nos Artigos 33(II)(c) e 35 da LGPD.
3. Desenvolvendo ferramentas práticas, tais como requisitos harmonizados e diretrizes para aplicações possibilitando que as empresas adotem NCGs com um custo muito mais vantajoso e de maneira mais rápida, baseado nos Artigos 33(II)(c) e 35 da LGPD.
4. Participando do sistema de Regras Globais de Privacidade para Transferência Transfronteira (*Global Cross Border Privacy Rules* - CBPR) (que será modelado de acordo com o APEC CBPR) baseado nos Artigos 33(II)(d) e 35 da LGPD.
5. Considere priorizar decisões de adequação para que todos os países objeto de uma decisão de adequação da UE ou Reino Unido sejam considerados adequados para os fins dos Artigos 33(I) e 34 da LGPD, em consonância com a abordagem adotada em outras jurisdições, tais como na Argentina, Colômbia e Uruguai, e outras ao redor do mundo para decisões de adequação da UE. A decisão pode ser avaliada de acordo com diferentes padrões (por exemplo, "substancialmente semelhante", "comparável" ou "essencialmente equivalente").
6. Disponibilizando fundamentos legais para transferências rotineiras de dados, tais como necessidade para a prestação de serviços e necessidade para o cumprimento contratual, certificando-se que as empresas que se baseiem em fluxos internacionais

de dados para a entrega de seus produtos e serviços não sejam bloqueadas do mercado brasileiro.

Reconhecimento de instrumentos existentes de transferência internacional. A ANPD deve reconhecer os instrumentos existentes de transferência internacional que observem os requisitos impostos pelos Artigos 33 e 35 da LGPD, ao invés de introduzir um novo mecanismo de transferência feito sob medida apenas para as transferências no Brasil. Isso possibilitaria às organizações que já adotaram medidas para cumprir com as exigências de transferência internacional existentes, no âmbito de esquemas vinculantes prescritos, determinar quais ferramentas serão mais adequadas a cada situação, assegurando ao mesmo tempo salvaguardas apropriadas de proteção de dados. Essa abordagem apoiaria a interoperabilidade, reduzindo os custos de compliance uma vez que as empresas poderiam se basear em contratos existentes, entregando altos níveis de proteção e perfeitamente adequados para os fins da LGPD.

Expressamente reforçar o alinhamento dos instrumentos contratuais com a abordagem baseada em riscos da LGPD. O ITI e nossos membros sempre apoiaram a abordagem baseada em riscos da LGPD para a proteção de dados pessoais e continuamos a defender uma abordagem ágil em nosso engajamento pela proteção internacional de dados. Apoiamos os instrumentos contratuais e outros mecanismos de transferência descritos no Artigo 33 (ii) como meio de implementação dessa abordagem.

Qualquer regulamentação de transferências de dados pessoais deve ser feita de acordo com uma abordagem equilibrada e harmonizada. Considerando que os interesses em jogo nas transferências internacionais de dados não se limitam aos dados pessoais e que é necessária uma harmonização neste domínio, a ANDP deve considerar a contribuição de uma ampla gama de partes interessadas, incluindo os setores privado e público. Essa abordagem resultará em uma avaliação de impacto holístico das ações regulatórias que podem impedir ou suspender os fluxos de dados além da proteção de dados, com potencial impacto na bolsa de valores, antilavagem de dinheiro, saúde, segurança cibernética, inteligência nacional e crescimento econômico e equidade.

Permitir prazo suficiente para a transição. Caso a ANPD decida não autorizar o uso dos instrumentos contratuais que as empresas já mantenham em vigor para cumprir os requisitos substantivos da LGPD (reportamo-nos à recomendação acima) e, ao contrário, optar pela implementação de seu próprio conjunto de CCPs, a ANPD deve permitir prazo suficiente (no mínimo, dois anos) para a implementação pelas empresas de mecanismos de transferência internacional após a adoção de qualquer proposta pela Autoridade. Durante esse prazo, deverá ser permitido que as empresas continuem a utilizar os mecanismos de transferência internacional que já mantenham em vigor e que cumpram os princípios gerais da LGPD. Adicionalmente, recomendamos que os exportadores e importadores de dados estejam obrigados a aplicar os mecanismos de transferência para o Brasil atualizados somente para os

novos contratos firmados após a data de sua vigência, consequentemente possibilitando que os mecanismos de transferência que são compatíveis com os princípios gerais da LGPD permaneçam válidos durante o período de transição.

Respostas Específicas às Perguntas Apresentadas para a Tomada de Subsídios

Oferecemos a seguir considerações discretas sobre as perguntas apresentadas pela ANPD em sua tomada de subsídios.

1. **Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?**

Apesar de a LGPD estar atualmente em vigor, a regulamentação implementando os mecanismos para transferências internacionais de dados nos termos do Artigo 33 (ii) e 35 ainda não foi publicada, causando incerteza jurídica às empresas transferindo dados ao exterior. Com o intuito de gerar maior segurança no mercado brasileiro, a ANPD deve emitir orientação formal, esclarecendo que os mecanismos de melhores práticas internacionais que as empresas vêm utilizando há anos serão aceitos até a finalização da regulamentação e sua entrada em vigor, desde que tais mecanismos observem o grau de proteção exigido pela LGPD.

Outro desafio é a inexistência de decisões de adequação das demais jurisdições *vis-à-vis* o Brasil face à natureza em desenvolvimento do ambiente brasileiro de proteção de dados. Portanto, é fundamental que o Brasil concorde em aderir às estruturas de proteção de privacidade reconhecidas internacionalmente e celebre acordos com outros países para facilitar os fluxos de dados por meio de garantias mútuas, criando, assim, segurança jurídica a todos os envolvidos.

2. **Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?**

Para promover convergência e interoperabilidade entre os mecanismos existentes de transferências internacionais de dados, a ANPD deve adotar uma abordagem flexível e autorizar a utilização de instrumentos contratuais que as empresas já mantenham em vigor se os referidos contratos contemplem proteções substantivas suficientemente similares àquelas exigidas pela LGPD. A ANPD também deverá considerar a sua participação nos esquemas internacionais de certificação, tais como o sistema CBPR Global. Adicionalmente, a ANPD deve cooperar com as autoridades de proteção de dados de outros países para a identificação das melhores práticas e criação de um eixo convergente de interpretação acerca das disposições gerais sobre o objeto pretendido, como, por exemplo, a elaboração de acordos de cooperação técnica, memorandos de entendimento (MoUs) e parcerias bilaterais com outros governos, conforme recentemente

realizado entre a ANPD e a Agência de Proteção de Dados da Espanha. Além disso, também apoiamos o contínuo envolvimento pela ANPD com os envolvidos, certificando-se que qualquer pré-condição futura que teria sido atendida antes da transferência de dados do Brasil não seja intencionalmente onerosa de forma a causar mandatos de facto de localização de dados.

Ademais, as leis que regem as transferências internacionais de dados contratuais deveriam ser estritamente personalizadas para a sua aplicação exclusivamente a transferências legais entre os agentes de tratamento de dados, nas quais um deles está situado fora do Brasil, ao invés de qualquer movimentação de dados que ocorra na internet global, a qual é tecnicamente necessária para o funcionamento da internet. Tendo em vista como a internet global foi construída e tem evoluído, a movimentação de dados entre as fronteiras nacionais é parte de quase todas as comunicações ou atividades on-line, frequentemente incluindo aquelas que representam transferências de dados entre duas partes localizadas no mesmo país. Em outras palavras, os dados poderiam ser transferidos da parte A para a parte B, ambas localizadas no Brasil, mas com fluxo fora do Brasil em sua movimentação de A a B. As redes nas quais os dados trafegam são em geral agnósticas da "jornada" física dos dados e, ao contrário, otimizam o roteamento em tempo real para a redução da latência, aumentam a resiliência da rede e possibilitam conexões em tempo real.

Gostaríamos de enfatizar à ANPD que a existência de interoperabilidade entre instrumentos é essencial, tanto no território brasileiro quanto internacionalmente, e deve ser realizada na medida do possível, pois traz maior segurança e previsibilidade jurídica aos instrumentos existentes e validados. Nesse sentido, a ANPD deve considerar até que ponto sua regulamentação se alinha com outras regulamentações aplicáveis à privacidade e proteção de dados que estão sendo apresentadas por diferentes órgãos reguladores no país, como o Banco Central do Brasil.

Além do acima exposto, a ANPD deve:

(i) considerar a emissão de CCPs em linha com a Nova Zelândia e Cingapura, que são muito mais simples do que as CCPs da UE e, portanto, mais eficientes, simplificadas e menos susceptíveis de afetar negativamente os negócios ou obstruir o comércio internacional; e

(ii) buscar a participação nas Regras Globais de Privacidade para Transferência Transfronteira (CBPR), recentemente criado para tratar da interoperabilidade e auxiliar na padronização de abordagens regulatórias para proteção de dados e privacidade. Canadá, Singapura, Japão, Estados Unidos, República da Coréia, Taiwan e Filipinas fazem parte desta iniciativa.

3. **Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?**

Vários mecanismos contratuais são amplamente utilizados pelas empresas para legitimar as transferências de dados internacionalmente. Frequentemente, as empresas se baseiam em instrumentos contratuais tendo em vista que podem ser implementados sem a necessidade de requerimento de prévia aprovação de uma agência reguladora, como é o caso das Normas Corporativas Globais (NCGs). Por exemplo, estima-se que muitas das organizações na UE adotam CCPs para as transferências internacionais de dados. As empresas também empregam mecanismos como adequação, NCGs e certificações.

Adicionalmente, as bases legais para transferências rotineiras de dados devem sempre contemplar a necessidade para a prestação dos serviços e necessidade para o cumprimento contratual. A disponibilização dessas bases legais para as transferências asseguraria que as empresas, que se baseiam em fluxos de dados internacionais para a operação de seus produtos e serviços, não sejam bloqueadas do mercado brasileiro, como seria o caso se sua capacidade de transferir dados fosse prejudicada independentemente dessa necessidade. De fato, foi demonstrado que as restrições aos fluxos internacionais de dados prejudicam a segurança cibernética e privacidade de dados[1], introduzem significativas barreiras econômicas para as economias locais[2] e limitam os direitos a privacidade dos usuários da internet, sua liberdade de expressão e o acesso à informação [3].

4. **Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?**

As transferências internacionais de dados são essenciais para promover a produtividade, inovação e a pesquisa e desenvolvimento em múltiplos setores bem como para gerar comércio internacional, apoiar a cooperação internacional para a execução das leis e manter as pessoas socialmente conectadas. Possibilitar os fluxos internacionais de dados contribui para os benefícios de acesso à internet, incluindo facilitando a geração de postos de trabalho, permitindo

[1] Veja: Georgia Tech Scheller College of Business, The effects of Data Localization on Cybersecurity https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4030905

[2] Veja: Information Technology & Innovation Foundation (ITIF), How Barriers to Cross-Border Data Flows Are Spreading Globally, What They Cost, And How to Address Them. https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/

[3] Veja: Freedom House, User Privacy or Cyber Sovereignty? https://freedomhouse.org/report/special-report/2020/user-privacy-or-cyber-sovereignty

o acesso a serviços públicos essenciais e ampliando o acesso pelos consumidores a uma maior variedade de bens e serviços. Além disso, os fluxos internacionais de dados também beneficiam a segurança e privacidade de dados, assegurando que as empresas de todos os portes possam se beneficiar de soluções descentralizadas para armazenamento de dados e sistemas compartilhados, que são resilientes a interrupções por mau funcionamento ou desastres naturais e acesso não autorizado por terceiros.

Facilitar as transferências internacionais de dados e assegurar uma expressiva proteção à privacidade não são metas mutuamente excludentes ou antagonistas. Vários regimes existentes refletem a necessidade de preservar múltiplas abordagens para as transferências internacionais de dados, sem o enfraquecimento das salvaguardas de privacidade.

Uma ferramenta para abordar as transferências internacionais de dados é o "modelo de adequação", o qual envolve a designação do que seria essencialmente uma lista de países que oferecem graus "adequados" de proteção à privacidade. No entanto, a inclusão pela LGPD de diversos mecanismos alternativos para as transferências de dados nos termos do Artigo 33(II) indica que a LGPD considera uma abordagem de adequação por si só como insuficiente para lidar com as pressões e desafios de um mundo de dados onipresentes e interconectados. Ainda, o modelo de adequação apresenta desafios de recursos para as agências regulatórias, as quais devem avaliar com precisão e abrangência estruturas de privacidade em evolução e suas respectivas implementações em todas as economias (e verificar com regularidade a validade de cada avaliação).

Outros instrumentos que podem complementar e apoiar a fundação de um modelo mais robusto e com menor intensidade de recursos para as transferências de dados são aas cláusulas modelo, NCGs, certificações, selos independentes e estruturas multilaterais, tais como CBPRs, e as disposições de acordos comerciais bilaterais e multilaterais que garantam o livre fluxo de dados entre os países. Recomendamos que os regimes de privacidade oficialmente reconheçam e desenvolvam uma complementação ampla de ferramentas corregulatórias alternativas, o que reduziria os custos administrativos, de execução e compliance oriundos dos esforços para a adesão a um patchwork internacional de regulamentações sobre proteção de dados.

5. **Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê? a. cláusulas-padrão contratuais; b. cláusulas contratuais específicas; e c. normas corporativas globais.**

   a. **<u>Cláusulas-Padrão Contratuais:</u>**

Uma abordagem flexível e baseada em riscos é a chave para um mecanismo de transferência harmônico e sustentável.

O ITI recomenda que a ANPD considere uma abordagem flexível, com instrumentos contratuais como base para as transferências internacionais de dados. A ANPD deve fixar os requisitos específicos para as cláusulas contratuais e estabelecer que todos os contratos que observem esses requisitos são suficientes para reger as transferências de dados. Nesse sentido, encorajamos a ANPD a autorizar o uso dos instrumentos contratuais que as empresas já mantenham em vigor se tais contratos contemplarem proteções substantivas suficientemente similares àquelas exigidas pela LGPD, incluindo as Cláusulas-Padrão Contratuais (CCPs) da UE e do Reino Unido e outros contratos *bespoke*, com fundamento nos Artigos 33(II)(b) e 35 da LGPD.

Caso a ANPD decida criar suas próprias CCPs, o ITI recomenda que:

- As CCPs deverão incluir uma abordagem baseada em riscos para as transferências internacionais de dados entre pessoas jurídicas independentes considerando as diferentes jurisdições e permitindo que as organizações conduzam suas avaliações de acordo com o tipo de dados transferidos e sua experiência com as leis aplicáveis. A abordagem baseada em riscos é importante para impedir expectativas enganosas às organizações por fatores estranhos ao seu controle.
- As CCPs devem adotar o reconhecimento pragmático das circunstâncias fáticas e o contexto individual das transferências de dados que precisam ser avaliados de acordo com os riscos associados no local e na prática. Essa é a chave para garantir que as organizações possam levar em consideração suas circunstâncias únicas, suas operações comerciais e o tipo de dados nas transferências internacionais de dados.
- Encorajamos a ANPD a manter e integrar essa abordagem na versão final, o que poderá ser assistido com a inclusão de referências diretas ao princípio de responsabilização no Artigo 6, X.
- As CCPs devem focar em garantias contratuais que podem ser providenciados pelas partes através de medidas legais, técnicas e organizacionais e não ser introduzido como um meio de conflito de leis que são melhor solucionados através de acordos políticos.

Esclarecimento sobre a definição de transferências

- A ANPD deve esclarecer que mecanismos para justificar as transferências internacionais de dados, incluindo eventuais CCPs, somente são necessários se os dados forem transferidos do Brasil a outro país entre agentes de tratamento/processamento de dados. É importante esclarecer que uma transferência internacional de dados não é aplicável se os dados estiverem trafegando entre o titular dos dados e o controlador dos dados, mesmo se o titular dos dados estiver no Brasil e o controlador dos dados estiver localizado fora do Brasil. Serão aplicáveis outros aspectos da LGPD, tais como os requisitos quanto

às justificativas legais para o tratamento e direitos dos titulares dos dados, mas deve ser esclarecido que as disposições da LGPD sobre transferências internacionais de dados não são aplicáveis se somente estiverem envolvidos os controladores de dados e os titulares de dados.

- Os dispositivos deverão estar especificamente relacionados (i) ao exportador e importador, (ii) às categorias dos dados transferidos, (iii) à finalidade da transferência, (iv) à possibilidade de transferência posterior dos dados, (v) às medidas de segurança aplicadas aos dados, (vi) ao prazo do tratamento, e (vii) à garantia dos direitos dos titulares dos dados.
- As CCPs não deverão limitar o uso de outros mecanismos das transferências internacionais para as chamadas "transferências ulteriores", mas se referir ao conjunto completo de opções disponíveis nos termos da legislação brasileira.

Mais uma vez, o ITI reitera que a ANPD deve autorizar a utilização de instrumentos contratuais que as empresas já mantenham em vigor se tais contratos contemplarem proteções substantivas substancialmente similares àquelas exigidas pela LGPD, incluindo as Cláusulas-Padrão Contratuais (CCPs) da UE e Reino Unido e outros contratos *bespoke*.

Caso a ANPD considere necessário, a ANPD poderia considerar a criação de um aditivo modelo que poderia ser adicionado a outros instrumentos contratuais, tais como as CCPs UE, para garantir que as obrigações da LGPD sejam observadas. Os mencionados aditivos complementariam os respectivos contratos já em vigor. No entanto, se os mecanismos contratuais existentes já oferecerem o mesmo grau de proteção substantiva prescrito pela LGPD, esses aditivos não precisariam ser utilizados.

Finalmente, caso essa sugestão não for adotada, apoiamos a criação de CCPs que sejam comuns com as CCPs UE, conforme desenvolvidas em outros países, incluindo cláusulas com aplicação na esfera nacional ou territorial (e.g., Nova Zelândia , Sérvia, Argentina, Centro Financeiro Internacional de Dubai e Mercado Global de Abu Dhabi (ADGM)) e sob a estrutura de organizações regionais (e.g., cláusulas adotadas pela Rede Ibero-americana de Proteção de Dados e Associação das Nações do Sudeste Asiático).

b. <u>Cláusulas Contratuais Específicas:</u>

Seria útil esclarecer que as CCPs e outros instrumentos contratuais, acerca dos quais seu uso não exige aprovação prévia pela ANPD, não se confundem com as cláusulas contratuais específicas que exigem prévia autorização pela ANPD antes da realização de uma transferência específica. É também importante deixar claro que o uso dessas cláusulas contratuais não será mandatório e as empresas poderão livremente se basear em qualquer outro mecanismo estabelecido no Artigo 33 da LGPD, uma vez que não há hierarquia entre esses mecanismos.

O Artigo 35 da LGPD outorga poderes à ANPD para adotar cláusulas contratuais específicas para uma transferência específica de dados pessoais. Cabe à ANPD verificar se o contrato regendo a operação específica cumpre os requisitos da LGPD. Como consequência da aprovação, a organização somente poderá efetuar a transferência específica que tiver sido autorizada pela ANPD.

Apoiamos a criação pela ANPD de um modelo pré-aprovado de cláusulas contratuais específicas incorporando elementos essenciais, como, por exemplo, a descrição da transferência e o desenvolvimento de um *toolbox* para orientar as organizações no requerimento de autorização da ANPD.[4] A sua redação poderia ser adaptada dependendo das circunstâncias específicas da transferência a ser autorizada pela ANPD. Outra opção é uma lista de considerações que deverão ser consideradas na redação das cláusulas contratuais específicas pelas organizações.

Ademais, em sua análise, a ANPD deverá estar atenta à necessidade de assegurar o mesmo grau de proteção conferido pelos demais instrumentos contratuais.

c. <u>Normas Corporativas Globais (NCGs):</u>

Com o intuito de apoiar a interoperabilidade, solicitamos que a ANPD considere o reconhecimento das aprovações de empresas que possam ter sido obtidas de outras jurisdições com estruturas similares de proteção de dados, como na União Europeia sob a GDPR.

É ainda importante regulamentar as disposições que estabelecem procedimentos para a comunicação e cooperação com as autoridades competentes de proteção de dados, para garantir a avaliação da eficácia desses regulamentos e a realização de qualquer ajuste necessário, tendo em vista a necessidade de aprovação prévia.

Como mencionado acima, cláusulas contratuais específicas e NCGs enfrentarão as mesmas questões encontradas pela autoridade europeia. Os prazos para aprovação são superiores a 3 anos, forçando as empresas a usar as CCPs para não atrapalhar os negócios ou não ter nenhum mecanismo em vigor enquanto a aprovação não for concedida. Além disso, os requisitos de auditoria podem ser atendidos por um auditor independente ou por uma certificação de conformidade de dados.Em nossa opinião, há algumas sugestões para orientar a ANPD na regulamentação das NCGs no Brasil com fundamento nos Artigos 33(II)(c) e 35 da LGPD:

- Endossar as NCGs para Controladores (NCG-C) e as NCGs para Operadores (NCG-P) existentes e autorizadas da UE e Reino Unido com fundamento no Artigo 35 da LGPD. Com a adesão às NCGs, os membros brasileiros do grupo assumiriam todos os direitos e

[4] Consulte: Article 29 Data Protection Working Party, *Working document 01/2014 on Draft Ad hoc contractual clauses "EU data processor to non-EU sub-processor"*, CLÁUSULAS CONTRATUAIS AD HOC (europa.eu)

obrigações em conformidade com as NCGs, o que significativamente facilitaria o cumprimento dos regulamentos aplicáveis pelas empresas com atuação na UE, no Reino Unido e no Brasil. Alternativamente, a ANPD poderia acelerar a consideração das NCGs que já tenham sido aprovadas por outras jurisdições com leis similares à LGPD, como no Reino Unido e na União Europeia.

- Criar uma abordagem proporcional, flexível e interoperável para as NCGs possibilitando uma movimentação eficiente de dados internacionalmente entre grupos econômicos, grupos empresariais ou empresas envolvidas em atividades econômicas em conjunto, tais como franquias, associações ou parcerias profissionais.
- Negociar com as EDPB EU e ICO do Reino Unido o reconhecimento mútuo das NCGs para assegurar que qualquer esquema desenvolvimento para as empresas brasileiras obtenha os benefícios dos dados transferidos da e para a UE e Reino Unido.

d. <u>Esquemas de Certificação</u>

Gostaríamos de incentivar a ANPD a reconhecer a validade das aprovações e certificações recebidas de outras jurisdições que oferecem o mesmo nível de proteção que a LGPD, pois novamente afirmam que ocorreu uma revisão regulatória robusta de processos e controles, como na APEC CBPR.

Em geral, apoiamos a participação do Brasil no sistema de Regras Globais de Privacidade para Transferência Transfronteira que será modelado com base no APEC CBPR e a criação de agentes de responsabilização por meio dos Artigos 33(II)(d) e 35(§3) da LGPD. Esse sistema recentemente anunciado pretende operar com um sistema voluntário e baseado em responsabilização, facilitando os fluxos internacionalmente de dados "com respeito à privacidade". O sistema CBPR exige que as empresas participantes implementem políticas e práticas de privacidade de dados compatíveis com a Estrutura de Privacidade APEC, como, exemplificativamente, quanto à responsabilização, notificação, opção, limitação à coleta, integridade de informações pessoais, utilização das informações pessoais e evitando prejuízos. O novo sistema muito provavelmente se baseará nos mesmos princípios. Acreditamos que assim que esses princípios de certificação global tenham sido acordados, esse sistema poderia ser um mecanismo adicional útil a ser utilizado pelas organizações com o intuito de observar os requisitos da LGPD no âmbito do princípio da responsabilização (Artigo 6, X). Por conseguinte, recomendamos que a ANPD continue as discussões sobre a criação desse mecanismo e considere a sua adoção.

Gostaríamos de enfatizar que a participação no CBPR está em integral consonância com o regime da LGPD, não sendo incompatível com a adequação dos demais regimes, como, por exemplo, o GDPR, conforme demonstrado com a participação da Coreia e do Japão no sistema CBPR e com o fato de que os regimes de proteção de dados dos dois países terem obtido sua adequação nos termos do GDPR.

6. **Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?**

As empresas que utilizam instrumentos contratuais para a transferência de dados não devem estar obrigadas a avaliar o grau de proteção de dados conferido pelo país de destino (país no qual o importador de dados está localizado). Os instrumentos contratuais e as determinações de adequação são dois mecanismos distintos. Cumpre notar que a LGPD nos termos do Artigo 33(ii) não estabelece uma hierarquia entre os vários mecanismos que podem ser adotados para justificar as transferências de dados e articula que todos os seus mecanismos podem ser utilizados de modo independente.

Finalmente, cumpre destacar que as organizações, particularmente as empresas de pequeno e médio porte, não estão equipadas para a condução desse tipo de avaliação complexa das leis regulamentos de um país estrangeiro, conforme exige a determinação de adequação. Portanto, o escopo dos instrumentos contratuais não deve levar em conta as considerações de adequação.

7. **As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?**

Como anteriormente observado, recomendamos que a ANPD adote uma abordagem flexível para a utilização de instrumentos contratuais justificando as transferências internacionais de dados. O ITI encoraja a autorização pela ANPD de instrumentos contratuais que as empresas já mantenham em vigor se os referidos contratos contemplarem proteções substantivas suficientemente similares àquelas exigidas pela LGPD, incluindo as Cláusulas-Padrão Contratuais (CCPs) da UE e do Reino Unido e outros contratos *bespoke*.

Caso a ANPD decida criar suas próprias CCPs, a ANPD deverá seguir a mesma flexibilidade, particularmente considerando os graus distintos dos riscos envolvidos em cada situação. De fato, CCPs rígidas poderiam prejudicar as transferências internacionais de dados, criando barreiras comerciais e limitando a inovação, segurança cibernética e produção científica no país. Consequentemente, a flexibilidade é necessária para levar em conta as diferenças nas estruturas organizacionais ou ecossistemas únicos de processamento.

8. **Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que**

poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?

A ANPD deverá atingir o equilíbrio certo entre cláusulas fechadas e abertas. Deverá ser permitido que as partes negociem livremente os aspectos comerciais dos seus contratos, incluindo o detalhamento sobre os seus direitos de auditoria (e.g., qual parte seria financeiramente responsável pela auditoria, quando a auditoria pode ser conduzida, necessidade de prévia notificação, efeitos sobre o preço etc.), grau de cooperação quanto ao exercício dos direitos de proteção de dados, definição dos serviços e níveis de serviço, quaisquer limitações à responsabilização etc.

A UE disponibiliza seu modelo de CCPs no website do Departamento responsável pela regulamentação das questões envolvendo dados pessoais, com um breve contexto sobre a necessidade de adoção das cláusulas e sua aplicação. A Nova Zelândia também disponibiliza informações sobre o modelo contratual que pode ser adotado pelas empresas, permitindo também que as empresas utilizem outros contratos que proporcionem o mesmo grau de proteção. Sugerimos a adoção pela ANPD de uma abordagem semelhante.
As ferramentas abaixo foram implementadas na Nova Zelândia e na UE, e a ANPD poderia considerar a adoção de abordagens similares:

- Nova Zelândia
    - Disponibiliza um gerador de modelo de cláusula para assistir as partes interessadas na redação dos contratos, de acordo com o tipo de transferência e o tipo de tratamento realizado pelo importador.
    - Disponibiliza uma árvore de decisões às partes interessadas para responder perguntas e confirmar a possibilidade de realização da transferência pretendida e ainda a necessidade de adoção de determinadas cláusulas contratuais no caso específico.
    - Disponibiliza um modelo comentado de contrato, explicando a finalidade, as salvaguardas conferias por cada uma das cláusulas e as garantias mínimas que devem estar presentes.

- União Europeia
    - Disponibiliza CCPs em todos os idiomas dos Estados Membros. Embora o português seja a única língua oficial brasileira, a disponibilidade de cláusulas em outros idiomas, especialmente em inglês, eliminaria a necessidade de sua tradução por cada agente, evitando traduções não harmoniosas, reduzindo a

possibilidade de litígios e aprimorando a comunicação entre as diversas nacionalidades importadoras.

A adoção de um modelo mais interativo, como o modelo proposto pela Nova Zelândia, é benéfica aos agentes de tratamento e aos titulares dos dados, promovendo informações de fácil acesso e simples compreensão, o que ajuda na regulamentação e controle das atividades por todos os envolvidos.

9. É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?

Caso a ANPD adote as CCPs, é importante levar em conta os tipos distintos de transferências, tais como Controlador para Controlador (C2C), Controlador para Operador (C2P), Operador para Controlador (P2C), e Operador para Operador (P2P) e proporcionar flexibilidade para levar em conta esses tipos distintos de transferências de dados. A adoção de regulamentações distintas para cada situação amplia as salvaguardas e ajuda na sua adequação a cada situação prática. Portanto, a adoção de determinações distintas de acordo com o papel desempenhado pelo agente de tratamento possibilita e facilita maior número de transferências.

Exemplificativamente, a UE recentemente adotou uma abordagem modular[5] às suas CCPs, que possui quatro módulos de cláusulas aplicáveis a cada agente de tratamento: C2C, C2P, P2C e P2P.

10. Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?

As CCPs devem abordar os quatros cenários distintos de transferências (C2C, C2P, P2C e P2P) enquanto as NCGs devem ter por foco duas situações de transferência (grupo empresarial, na qualidade de controlador, ou grupo empresarial, na qualidade de operador). Os quatro cenários de transferência descritos acima nas CCPs detalham a complexidade da aplicabilidade nos cenários de transferência, os quais não são relevantes para a aplicação das NCGs, que trazem complexidade adicional nas transferências de dados. É importante notar que as NCGs não deverão seguir um grupo pré-estabelecido de cláusulas.

Ainda, ao contrário das cláusulas-padrão, as NCGs deverão indicar (i) a estrutura do grupo econômico e os meios de contato de todas as empresas que participam do grupo; (ii) esclarecimentos sobre a relação dos membros e dos funcionários do grupo com as NCGs; (iii) os

[5] https://www.gdprsummary.com/new-sccs-definitive-guide/ -Abordagem Modular

procedimentos para garantir a possiblidade de verificação do cumprimento dos regulamentos; (iv) os aspectos sobre responsabilização e indenização por danos resultantes do descumprimento das NCGs por uma das empresas do grupo, inclusive a adoção das medidas necessárias para sanar os atos que exijam reparação; (v) medidas promovendo treinamento e qualificação dos funcionários envolvidos no tratamento dos dados; e (vi) os procedimentos para comunicação e cooperação com a ANPD, particularmente sobre as alterações das NCGs e resultados quanto à eficácia dos regulamentos[6].

Consideramos que as NCGs, permitidas pelo Artigo 33 (II) (C) da LGPD, são um mecanismo importante que pode ser alavancado para possibilitar a troca de dados pessoais entre membros de um grupo econômico ou um grupo empresarial envolvidos em atividades econômicas conjuntamente em virtude de suas complexas estruturas arquitetônicas mundialmente, realizando um grande volume de transferências internacionais de dados.

11. Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?

Consideramos que a definição de "grupo econômico ou empresarial" deverá ser suficientemente extensa evitando limitações e condições à troca de dados pessoais entre os membros de um grupo econômico ou um grupo empresarial envolvidos em conjunto em atividades econômicas, como é o caso das franquias ou associações. Em ambos os casos, deverá observar a lei das sociedades por ações brasileira. O foco não será a estrutura empresarial, mas a aplicabilidade de um programa comum de proteção de dados baseado em sólidos controles e implementação.

12. Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?

Devem ser exigidas pela ANPD as seguintes informações:

- Categorias dos titulares dos dados cujos dados pessoais forem transferidos (e.g., usuários, clientes etc.).
- Categorias dos dados pessoais transferidos.
- Finalidade da transferência.
- Critérios adotados para a determinação do prazo de armazenamento dos dados (e.g., duração do contrato).

[6] Por exemplo o Artigo 47 - GDPR

13. Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD?

Permitir as transferências de dados entre grupos econômicos distintos cujas NCGs tenham sido aprovadas pelas ANPD certamente seria uma iniciativa benvinda. De fato, ajudaria a conectar a legislação brasileira com os sistemas globais emergentes para os fluxos internacionais de dados, o que reduziria custos para todas as partes envolvidas bem como encorajaria maior interação entre os grupos, promovendo desenvolvimento econômico e inovação.

Em acréscimo às NCGs, poderia ser considerada pela ANPD a alavancagem da opção de certificações, permitindo que uma NCG automaticamente gerasse uma certificação para a transferência de dados com outras empresas certificadas, bem como ajustes ocasionais quanto aos aspectos relevantes, tais como a natureza dos dados, volume e finalidades da transferência. Tendo isso em mente, gostaríamos de destacar os benefícios a seguir de permitir transferências entre grupos econômicos distintos baseadas nas NCGs:

- **Escopo da aplicação:**
    - Aplicação em todo o grupo econômico, independentemente do local de constituição dos membros, nacionalidade dos titulares dos dados cujos dados pessoais estejam sendo tratados ou qualquer outro critério ou consideração.
    - Resposta às necessidades de tratamento de dados, baseada em contextos jurídicos e culturais, filosofias comerciais e práticas distintas.
    - Redução da necessidade de salvaguardas apropriadas para cada transferência ou conjunto de transferências, tendo em vista que as NCGs regulamentam transferências intragrupo (por exemplo, com a adoção de NCGs para todo o grupo, os membros do grupo não estão obrigados a assinar quantas CCPs quanto o número de transferências).
    - Inclusão de um Acordo de Nível de Serviços, a ser assinado por todos os membros.
    - Garantia de que as medidas técnicas e organizacionais apropriadas tenham sido implementadas para os dados transferidos e tratados nos membros do grupo, incluindo transferências ulteriores, introduzindo as medidas necessárias para assegurar que os sistemas existentes observem os requisitos das NCGs.

- **Responsabilização:**
    - Garantia do robusto cumprimento da LGPD, conforme exigido pelo princípio da responsabilização (Artigo 6, X).
    - Criação de um sistema mais direto e mais eficiente que facilitará a implementação pelos funcionários e sua compreensão pelas pessoas.

- Implicação de que os membros do grupo econômico e todos os funcionários do grupo estarão obrigados a cumprir as políticas e normas internas, conforme exigido no âmbito do princípio da responsabilização.
- Adaptação na abordagem pragmática de que as organizações multinacionais buscam quanto às questões de compliance.
- Implantação de um programa comum de proteção de dados baseado em sólidos controles e implementação.

- **Direitos dos indivíduos:**

  - Exequibilidade jurídica pelas pessoas cobertas pelo escopo das NCGs.
  - Claro dever de cooperação com os membros do grupo, de forma que as pessoas cobertas pelo escopo das NCGs possam se beneficiar dos mecanismos alternativos para a solução de litígios.
  - Fácil acesso às NCGs pelos indivíduos.
  - Existência de um processo para o tratamento das reclamações para as NCGs.
  - Criação de um ponto de contato específico para as pessoas cobertas pelo escopo das NCGs.

- **Execução:**

  - Exequibilidade jurídica dos regulamentos corporativos pelas Autoridades de Proteção de Dados
  - Existência de um programa de auditoria contemplando as NCGs.
  - Existência de medidas disciplinares na hipótese de inobservância das NCGs.
  - Dever de cooperação com as Autoridades de Proteção de Dados.

14. Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?

A adoção das CCPs ou dos instrumentos contratuais individuais das empresas não deve exigir sua prévia aprovação pela ANPD. No que diz respeito às NCGs, as empresas cujas NCGs tiverem sido aprovadas em outras jurisdições similares, como, por exemplo, a UE, devem se beneficiar de um procedimento sumário para a sua aprovação pela ANPD. Esse sistema já foi implementado no Reino Unido.

Na UE e no Reino Unido, as NCGs têm sido adotadas há muitos anos. Apesar de as NCGs já estarem em uso nos termos da Diretiva 95/46, o GDPR codificou e formalizou seu papel como uma ferramenta para as transferências de dados. Na América Latina, países como a Argentina e Colômbia desenvolveram seus processos de aprovação para as NCG com base no GDPR, e as

diretrizes adotadas pelo Artigo 29 do Data Protection Working Party (Hoje: O Conselho de Proteção de Dados Europeu).

Como recomendado pelo Relatório Bienal da Comissão Europeia sobre a Implementação do GDPR, é crucial que a ANPD desenvolva ferramentas práticas, tais como requisitos harmonizados e diretrizes de aplicação, para a avaliação e eventual aprovação das NCGs e para possibilitar que mais empresas adotem as NCGs com menor custo e de maneira mais rápida. No contexto europeu, um grupo econômico interessado na aprovação de suas NCGs deverá identificar à autoridade fiscalizadora um líder e apresentar uma proposta inicial em conjunto com a documentação relevante, tais como políticas de privacidade, diretrizes para os funcionários, programas de auditoria, comprovação de recursos suficientes para arcar os danos causados pelos membros do grupo que não estejam localizados na UE, entre outros.[7]

A adoção das NCGs exige um programa de proteção de dados com grau de maturidade que não seria acessível a todas as empresas cujas transferências de dados sejam necessárias. Ademais, a aprovação das NCGs implica em um uso considerável de recursos por parte da ANPD. Acreditamos que poderia existir um mecanismo de transferência mais acessível com a participação no CBPR. O uso de agentes de responsabilização permitiria que mais empresas aderissem a um sólido mecanismo de transferência, reduzindo a pressão por recursos na ANPD. No que diz respeito às cláusulas contratuais específicas, não há procedimento unificado na UE para sua verificação e aprovação. Qualquer empresa que queira adotar cláusulas específicas, além das CCPs, deverá submetê-las à autoridade nacional de sua jurisdição para sua a revisão e cada país possui seus próprios procedimentos.[8] Não há experiência suficiente que possa criar uma interpretação padrão sobre o assunto e o debate ainda é muito incipiente nas demais jurisdições. A interpretação mais aceita é de que as cláusulas contratuais específicas devem estar restritas a transferências ocasionais, para finalidades específicas e envolvendo um número limitado de titulares de dados, em consonância com o Artigo 49 (1) do GDPR.

É importante notar que, o processo de aprovação da NCG na UE leva vários anos por conta da capacidade limitadas das autoridades supervisoras, desencorajando empresas de se candidatarem. Este longo processo também pode afetar a disposição das empresas em dedicar recursos significativos durante um longo período para revisar seus processos internos. Este cenário poderia facilmente se repetir no contexto da necessidade de aprovação de cláusulas contratuais específicas. Uma abordagem contratual flexível é comprovadamente o mecanismo mais eficiente.

---

[7] Normas Corporativas Globais: Regulamento Geral de Proteção de Dados. PWC. https://www.pwc.com/m1/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf

[8] Recomendações 01/2020 sobre as medidas complementando as ferramentas de transferência para assegurar o cumprimento da proteção dos dados pessoais na União Europeia. https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf

15. **Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?**

A aprovação dos titulares dos dados não deve ser obrigatória nem deverá ser permitida a sua intervenção em instrumentos contratuais entre o exportador dos dados e o importador ou sua manifestação sobre à decisão do mecanismo utilizado para a transferência de dados, caso o mecanismo utilizado esteja em conformidade com a LGPD. Qualquer outra configuração seria impraticável e dificultaria o fluxo de dados no Brasil. Os titulares dos dados precisam ser informados e deve ser permitida sua intervenção **somente** no caso de uma mudança na transferência que tenha sido realizada **com base no seu consentimento**.

16. **Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?**

Deve ser autorizada pelos agentes de tratamento a adoção de mediação para a resolução de conflitos. A LGPD já proporciona aos titulares de dados mecanismos para a execução de seus direitos, incluindo seu contato direto com os controladores dos dados.

Em termos de resolução de conflitos, o CBPR Global cria um excelente esquema, na medida em que incorpora a participação pelas autoridades de proteção de dados no Acordo Internacional para a Proteção da Privacidade (*Cross-border Privacy Enforcement Arrangement*), o qual prevê mecanismos para promover uma eficaz cooperação internacional entre as autoridades na execução das leis de proteção de dados, inclusive por meio de submissão das matérias e por meio de investigações ou medidas executórias paralelas ou em conjunto. Ademais, as empresas participando no CBPR participam de um mecanismo para resolução de litígios disponibilizado pelos agentes de Responsabilização. Existem poderosas ferramentas para a resolução dos conflitos.

17. **Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?**

A ANPD deve emitir um guia prático explicando como os mecanismos de transferência devem ser implementados de acordo com a LGPD e a regulamentação da ANPD. Essas informações poderiam ser prestadas no website da ANPD, em suas mídias sociais etc. Por exemplo, o ICO do Reino Unido disponibiliza campanhas educativas e guias em seu website. A ANPD também

deveria continuar trabalhando em conjunto com todos os envolvidos durante o desenvolvimento das suas regulamentações.

18. **Quais as melhores alternativas para resolver as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?**

[N/A]

19. **Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?**

A obrigação apropriada seria que o importador dos dados notificasse o exportador dos dados sempre que possível ao receber uma notificação de divulgação de informações pessoais. No entanto, esses requisitos deveriam reconhecer que essa notificação nem sempre é permitida em algumas jurisdições. Ademais, a legislação local poderá limitar as informações que o importador possa compartilhar com o exportador dos dados, de forma que as obrigações de notificação não devem contemplar uma relação rígida de informações a serem compartilhadas. Consideramos que essa questão é uma questão que deveria ser resolvida na esfera pública uma vez que as empresas estão obrigadas a cumprir as leis dos países nos que atuam. Acreditamos que o esse tópico poderia ser desenvolvido por meio das discussões em desenvolvimento em alguns fóruns internacionais relevantes, como a OCDE.

As obrigações de acesso a dados por autoridades deveriam ser harmonizadas globalmente, de forma que as obrigações aos importadores e exportadores sejam compatíveis e interoperáveis com as estruturas internacionalmente reconhecidas, tais como aquelas em desenvolvimento no grupo de trabalho da OCDE sobre o acesso de dados do setor privado disponibilizado aos governos.

Nesse sentido, se um Estado soberano ordenar a disponibilização de dados que estejam sob o controle de uma pessoa jurídica sob a jurisdição de outro Estado soberano, não há outra opção além de recorrer ao instituto jurídico de cooperação internacional, visando a reconciliação da soberania brasileira com a soberania dos Estados estrangeiros. Essa conduta está presente no Art. 4, incisos VII e IV, da Constituição Federal do Brasil, que estabelece dever de cooperação entre os povos para o progresso da humanidade e ainda de solução pacífica dos conflitos. No mesmo sentido do dispositivo constitucional, o Código de Processo Civil também dedicou um capítulo específico à necessidade desse tipo de cooperação internacional. A LGPD também destaca a cooperação internacional no Art. 33, III e VI.

20. Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

A ANPD não deveria criar requisitos rígidos ou formatos específicos obrigatórios a serem observados. Ao contrário, deveria ser desenvolvido pela ANPD uma orientação promovendo a flexibilidade, interoperabilidade e segurança. A título exemplificativo, as empresas deveriam estar autorizadas a compartilhar as informações necessárias com os titulares dos dados em seus websites, Termos de Serviço e Política de Dados e outros canais internacionais, como já pode estar ocorrendo. Conforme a Pergunta 17, um guia prático para a indústria poderá ser útil, particularmente para as pequenas e médias empresas.

Tomada de Subsídios n° 2/2022, sobre Transferências Internacionais de Dados
Christian Perrone <c.perrone@itsrio.org>
Qui, 30/06/2022 14:37
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Prezados membros da ANPD,

Na qualidade de Coordenador de Direito e GovTech do Instituto de Tecnologia e Sociedade do Rio (ITS-Rio) e participante da Tomada de Subsídios n° 2/2022, sobre Transferências Internacionais de Dados, envio o arquivo em anexo contendo as respostas complementadas pela relação de *hyperlinks* existentes, tão somente para indicar as referências mencionadas nas respostas, já devidamente formalizadas na Plataforma Participa Mais Brasil.

Agradeço a oportunidade, parabenizando todos desde já pela iniciativa.

Cordialmente,

Christian Perrone
Head de Direito e GovTech
Head Rights and Technology and GovTech

Instituto de Tecnologia e Sociedade do Rio de Janeiro
Institute for Technology and Society (ITS Rio)

Consulta Pública - Transferências Internacionais de Dados

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2 /2022

NOME DA INSTITUIÇÃO: Instituto de Tecnologia e Sociedade (ITS Rio)

O **Instituto de Tecnologia e Sociedade do Rio de Janeiro** vem, pela presente, apresentar a seguinte contribuição para a Tomada de Subsídios da Autoridade Nacional de Proteção de Dados (ANPD) acerca de regulamentação da Lei nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais, sobre transferências internacionais de dados pessoais.

Ementa: Proposta de realização de Tomada de Subsídios para regulamentação das transferências internacionais de dados pessoais, nos termos dos artigos 33 a 35 da Lei nº 13.709, de 14 de agosto de 2018.

Autoria: Autoridade Nacional de Proteção de Dados (ANPD)

TÓPICO/QUESTÃO	CONTRIBUIÇÃO/INSTITUIÇÃO
1) Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?	Os obstáculos giram em torno de: (i) desconhecimento dos mecanismos legais necessários para realizar transferências internacionais, inclusive com relação a incertezas de quais processos disponíveis devem ser seguidos, de modo que a adoção de guias de orientação e regulamentação específica poderia suprimir as lacunas existentes; (ii) altos custos para implementação de mecanismos aptos a autorizar as transferências internacionais em situações em que não há uma decisão de adequação, devendo existir um mecanismo mais simples, acessível e de amplo conhecimento por agentes de tratamento e titulares de dados;

	(iii) falta de conexões internacionais do Brasil com decisões de adequação exigidas por países que impõem em um primeiro plano a contemplação de tal medida para viabilizar o fluxo transfronteiriço de dados pessoais, como se observa da Argentina e do Uruguai em relação à União Europeia e; (iv) falta adesão do Brasil também em tratados e acordos multilaterais internacionalmente relevantes à construção de uma adequada interoperabilidade ao fluxo transfronteiriço de dados, a exemplo das Diretrizes da Organização para a Cooperação e Desenvolvimento Econômico (OCDE) para a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais e da Convenção 108+ do Conselho da Europa para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais. Como se destaca do Relatório "Transferência de dados entre Brasil, União Europeia e Reino Unido: Análise do Processo de Adequação", produzido pelo ITS-Rio, estes obstáculos inviabilizam a mera circulação de dados via computação de nuvem, com servidores instalados em outros países. Ainda, perde-se oportunidades em se proceder à assunção de compromisso firmada em acordos bilaterais com parceiros estratégicos ao Brasil, o que poderia ser um meio eficaz para ajustar eventuais desconformidades entre as legislações de forma recíproca.
2) Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?	Em vistas ao melhor fluxo de dados, aponta-se à perspectiva de construir parâmetros mínimos à proteção de dados pessoais a ser observada pelas empresas, prevendo de forma clara e objetiva os limites da responsabilização dos agentes de tratamento da cadeia de tratamento de dados, assegurando os direitos, liberdades e garantias dos titulares de dados. Assim, os pressupostos para a edificação da convergência e interoperabilidade devem levar em consideração: (i) a necessidade de convivência harmônica entre diferentes ordenamentos jurídicos por meio da adoção de mecanismos de proteção; (ii) o alcance da proteção em meio ao fluxo transfronteiriço sem necessariamente exigir uma equivalência nos

	mecanismos específicos de proteção de dados. Tem-se como consequência a busca por um grau de flexibilidade para se permitir a convivência paralela entre modelos distintos de proteção de dados em nível internacional. A ANPD deve apontar de forma clara quais elementos são primordiais à proteção de dados diante de situações transfronteiriças e quais são acessórios. Externamente, a cooperação internacional com outras Autoridades de Proteção de Dados é fundamental, assim como a publicização ampla, clara e acessível dos posicionamentos adotados, de modo que as respectivas Autoridades estrangeiras também estabeleçam as diferentes discussões da regulação transfronteiriça de dados frente ao Brasil. Seria igualmente interessante monitorar continuamente os diferentes foros de discussões da regulação transfronteiriça de dados, posicionando-se de forma notória as propostas de discussões, inclusive submetendo ideais que conversem com as diferentes jurisdições. Ainda, torna-se importante ter atenção às discussões travadas em tratados de livre comércio, pois, na atualidade, estes instrumentos estão firmando entendimentos do nível de proteção ou abordando a proteção de dados entre países.
3) Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?	Há que se entender que a Lei Geral de Proteção de Dados Pessoais (LGPD) optou por um modelo híbrido, em que há um mecanismo de transferências “mais livres” para países considerados adequados e outro para aqueles que não participam dessa estrutura legal. Logo, o histórico da União Europeia serve de indicativo dos desafios desse modelo. A proposta de “mecanismos de adequação” tende a ser melhor e menos custosa para toda a cadeia de tratamento de dados. Pequenas e médias empresas podem saber quais países podem transferir dados de maneira segura e com poucos custos adicionais de *compliance*. Serve como o mecanismo em que mais agentes podem

	participar e competir. Nesse sentido, a ANPD deve considerar de maneira ampla as possibilidades de decisão de adequação, sempre e quando se respeitem os parâmetros de proteção de dados. A abordagem europeia de "equivalência de proteção", por mais que promova um grau mais alto de salvaguardas e garantias, mostrou-se limitante quanto ao número de países que participam desse arranjo. Levando em consideração a estrutura do país, pode ser importante considerar um mecanismo mais flexível de decisões. Uma sugestão pode se dar a partir de decisões mais ágeis para países próximos, como membros do Mercosul. Nesse sentido, o mecanismo de listas previsto pela Colômbia (ou mesmo os "*white lists*" da União Europeia) também pode ser um caminho. Fora desse contexto, as cláusulas-padrão contratuais (CPCs) são de longe os mecanismos mais utilizados. Ainda que em alguns casos possa ser questionada a sua efetividade, deve ser compreendido que a teia estruturante do comércio internacional, e de fato a maior parte das transações que se direcionam a fluxos transfronteiriços de dados, baseia-se em arranjos contratuais. Nesse sentido, é importante que este instrumento seja de fácil uso e com o mínimo necessário de exigências e demais burocracias. Quanto maiores as existências de burocracias, maiores são os custos e, consequentemente, mais micro e pequenas empresas podem ficar excluídas dos fluxos, tendendo à concentração dos fluxos somente em empresas maiores, por terem mais capacidades para absorver custos. Igualmente importa notar que as redes negociais podem ser bastante complexas, logo, é significativo que exista possibilidade de estruturação das CPCs para refletirem essa complexidade, tendo em vista que este modelo parece ser mais apropriado às pequenas e médias empresas, levando em consideração o potencial de flexibilidade prática de adequação às diversas formas de organizações empresariais. Por outro lado, as normas corporativas globais (NCGs) parecem ser mais adequadas às grandes corporações e

	conglomerados econômicos. Curioso observar que, no contexto europeu, mesmo diante da complexidade do mecanismo e da necessidade de adequação a múltiplos sistemas, ainda existem poucas organizações que utilizem esses sistemas. No entanto, já é notável um salto significativo no seu uso desde a maior flexibilização do mecanismo de chancela pela União Europeia, com a entrada em vigor do Regulamento Geral de Proteção de Dados Pessoais (RGPD). O que tende a indicar uma demanda que pode vir a chegar ao país.
4) Quais são os principais benefícios e impactos relacionados ao tema das transferências internacionais de dados pessoais e quais são as melhores alternativas para o seu endereçamento em cada um dos instrumentos contratuais de transferências de dados presentes na LGPD e na prática internacional?	Dentre os benefícios, destacam-se o desenvolvimento socioeconômico em sentido amplo, com aperfeiçoamento do comércio e circulação de bens e serviços, fomento da inovação e promoção de tecnologias movidas à Internet das Coisas, Inteligências Artificiais e implementação do 5G à realidade nacional, projetando um ecossistema mais competitivo e eficiente. Nesse sentido, reconhece-se que na base da economia global está a circulação de dados. Um exemplo encontra-se que em países em desenvolvimento como o Brasil, onde cerca de 59% e 68% de ganhos no PIB em sistemas movidos à Internet das Coisas são diretamente atribuíveis ao fluxo transfronteiriço de dados pessoais, conforme se verifica de levantamento "Cross-Border Data Flows", de 2021, do *Global System for Mobile Communications*. A existência de mecanismos apropriados para a circulação transfronteiriça de dados faz com que se estimule um padrão mais alto de proteção para os direitos dos titulares, promovendo-se o *compliance* em toda a cadeia produtiva de importação e exportação de dados. O uso de instrumentos meramente complexos, no entanto, pode ter um efeito contrário. Isso porque, pode fazer com que partes da cadeia não efetivamente participem, devido a custos burocráticos ou por falta de oportunidade. Ou ainda, venham a participar sem estar de acordo com os mecanismos, diminuindo potencialmente o nível de proteção, o que pode ser ainda mais deletério, limitando também a legitimidade na atuação da Autoridade de Proteção de Dados.

	Quanto aos impactos, as melhores soluções em instrumentos contratuais para transferências inserem-se especialmente na perspectiva de permitir o maior fluxo e circulação transfronteiriça de dados, atuando de forma fiscalizatória ao se constatar violações à proteção de dados no caso concreto. Há que se ter em mente também que mecanismos regulatórios muito rígidos e rigorosos podem impactar de maneira negativa na viabilidade do fluxo transfronteiriço de dados, freando potenciais ganhos econômicos relacionados ao comércio internacional e à livre circulação de bens e serviços. Uma ilustração resta presente nas empresas estadunidenses que enfrentam atualmente dificuldades ao oferecerem serviços na União Europeia, devido às restrições de não adequação após o julgamento do caso Schrems II, da Corte de Justiça da União Europeia. A exemplo do que se verificou da atuação repressiva por parte de Autoridades de Proteção de Dados europeias, que suspenderam os fluxos de dados para os EUA, como a CNPD (Portugal) que suspendeu o envio de dados para uma empresa de serviços na nuvem dos EUA, e as Autoridades CNIL (França) e DSB (Áustria) que indicaram que serviços de análise de dados dos EUA também não poderiam ser utilizado, como no caso da suspensão das atividades do Google Analytics, por exemplo.
5) Que critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos de transferência internacional de dados pessoais e por quê? a. cláusulas-padrão contratuais;	Os critérios devem ser: a) cláusulas-padrão contratuais (CPCs): há a necessidade de estipulação de regras claras e flexíveis que sejam compatíveis com as diferentes responsabilidades e atribuições de Controladores e Operadores, projetando um espaço de uma maior variação às diferentes realidades empresariais, isto é, desde pequenas e médias empresas a grandes corporações. Sob este alcance, a ANPD pode considerar estruturá-las sob uma abordagem com marco comum de cláusulas, conteúdo mínimo essencial e uniforme, e uma ulterior gama de cláusulas com disposições que se adequem aos diferentes agentes e situações presentes nos fluxos transnacionais de dados; b) cláusulas contratuais específicas (CCEs): há que se

b. cláusulas contratuais específicas; e c. normas corporativas globais.	notar que a abordagem frente a esses mecanismos deve levar em consideração que a "especificidade" buscada pode se referir a certas peculiaridades existentes em determinados setores (eg. saúde, financeiro etc.). Portanto, a abordagem da ANPD deve comportar a possibilidade dessas adaptações também. c) normas corporativas globais (NCGs): uma abordagem mais teleológica e flexível, focada mais no "espírito" e nos princípios das normas de proteção de dados pode ser o caminho para uma maior adesão a esse mecanismo. As diferentes instituições que podem se interessar a propor esses mecanismos tendem a harmonizar normas de múltiplas jurisdições, o que na prática pode levar a escolhas difíceis sobre os caminhos a serem usados para a proteção e segurança de dados. Eventual exigência de um padrão muito rígido para a aprovação destas NCGs pode ter como resultado inibir a atuação de empresas no país ou ainda aumentar os custos de funcionamento.
6) Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países ou organismos estrangeiros para fins de adequação (art. 34 da LGPD) devem ser também levados em conta no âmbito das regras para os instrumentos contratuais?	O objetivo dos mecanismos que permitem os fluxos internacionais de dados pessoais é que esse fluxo possa ocorrer de maneira responsável salvaguardando os direitos dos titulares. A lógica seria de que a "bolha de proteção" que envolve dados pessoais no país de exportação também deva existir no país de importação. O mecanismo de decisões de adequação presente na LGPD estabelece critérios de avaliação que permitem verificar se, independente de outros instrumentos (usualmente negociais), o nível de proteção no segundo país (de importação) está de acordo com um padrão predisposto mínimo. Em outras palavras, a decisão de adequação indica uma "presunção" de proteção, que leva em consideração o *compliance* dos agentes de tratamento participantes, além de estruturas que busquem garantir esse *compliance* ou fiscalização e garantias (também individuais) em caso de não-*compliance*. Nesse sentido, os instrumentos negociais devem realizar uma função similar, isto é, devem criar obrigações que busquem também gerar um padrão de proteção adequado e o *compliance* com esse padrão. Igualmente também devem prever mecanismos de fiscalização e de lidar com situações de não-*compliance*.

	Portanto, o “espírito” dos critérios deve ser traduzido para a realidade negociar dos instrumentos contratuais. No entanto, é importante notar que isso **não significa que os agentes devam fazer uma análise da situação do ordenamento jurídico do outro país**, nem das circunstâncias socioeconômicas do outro país. Isso somente se refere à relação de adequação, porque ela é geral pensada sobre uma base de presunção. O que o agente exportador de dados deve ter que verificar são as relações específicas que envolvem a transação concreta entre ele e o agente importador. As CPCs e outros instrumentos negociais devem garantir que ambos importadores e exportadores de dados estejam de acordo e assegurem um padrão efetivo de proteção de dados. A visão europeia que aparece no julgamento da CJEU Schrems II, de que deve haver uma “mini avaliação de adequação”, foi densamente criticada por impactar de maneira negativa nas relações negociais e impor custos que não se relacionam com relações negociais. Como apontou Christopher Kuner em seu blog à época da decisão, em 2020, em que o precedente exigiria que os controladores se tornassem “especialistas” em extraterritorialidade de leis de dados, o que seria impraticável com a realidade privada. A título ilustrativo, no precedente europeu conhecido como Schrems II, que levou à invalidação do acordo Privacy Shield, entre União Europeia e Estados Unidos, insere-se a perspectiva de aparente confluência entre a análise daquilo que é levado em consideração para formalizar uma decisão de adequação e para a utilização de outros mecanismos como as CPCs. O contexto do país de importação e a capacidade da instituição importadora de cumprir com as garantias e salvaguardas são elementos relevantes do ponto de vista do sistema europeu. Mas isso denota consequências de aumento dos custos e complexidade de exportação de dados. Tendo em vista que a LGPD não estabelece essa necessária conexão entre a decisão de adequação e a utilização de outros mecanismos, é viável que a abordagem seja distinta e que a utilização de outros mecanismos, como as CPCs, siga princípios de risco e de responsabilização do exportador, adotando a lógica dos mecanismos

	transferência internacional do modelo canadense.
7) As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?	Deve-se admitir que há uma tensão entre CPCs que facilitem as partes, pois dependem de pouca negociação e tenham alto grau de previsibilidade, e CPCs que permitam às partes uma maior compatibilidade das obrigações às necessidades das relações negociais e às suas posições na cadeia transfronteiriça de tratamento de dados. Nesse sentido, internacionalmente se percebe uma tendência a alguma flexibilidade, como a exemplo de novos modelos de CPCs tanto pela União Europeia, de junho de 2021, que expressamente notam a necessidade de maior "flexibilidade", e pelo Reino Unido, 2022, que adaptam à nova realidade pós-Brexit, trazendo um maior número de modelos e uma maior modularidade respectivamente. Outros sistemas como os de Singapura ou da Nova Zelândia trazem maior flexibilidade e possibilidade de escolha. Singapura tem sido muito ativa nesse âmbito e aparentemente bastante bem-sucedida. Ao todo, Singapura tem 15 acordos de livre comércio firmados, que incluem a livre circulação em paralelo à proteção de dados pessoais, além de ter um sistema bastante aberto. A Nova Zelândia parece propor um modelo extremamente interessante que visa estabelecer um equilíbrio entre os dois interesses empresariais com grande potencial de tensão: rigidez para menor necessidade de custos de negociação e flexibilidade para abrir espaço para maior compatibilização das obrigações. Nisso, as CPCs da Nova Zelândia estão propostas com base em uma lógica de uma porção rígida, e outra pontual flexível, dentro de uma série de opções presentes na regulamentação. Nesse sentido, tendo em vista a realidade transnacional e o nível de cultura de proteção de dados nacional, entende-se que CPCs devem atentar-se em serem, em certa medida, potencialmente flexíveis de modo a se adequarem às vicissitudes fáticas da realidade empresarial, permitindo-se a adequação eficaz da proteção de dados pessoais em meio ao necessário

	fluxo transfronteiriço das informações. A especificação de resultados desejados deve ser modulada à perspectiva da adequada proteção dos dados pessoais, em observância à base principiológica, fundamental e dos direitos dos titulares de dados. No entanto, essa flexibilidade deve existir dentro de um sistema simples e acessível em que haja uma base comum e as opções sejam estruturadas para minimizar discussões negociais e aumento de custos. A existência de potenciais modelos diferentes deve ser considerada, pois pode ser benéfica para o ecossistema e permitir a participação de diferentes categorias de organizações. Embora a perspectiva de CPCs mais rígidas sejam interessantes do ponto de vista objetivo para fins de cumprimento das regras, por parte da ANPD, eventual delimitação muito criteriosa poderia levar a uma falta de adesão por parte das empresas às regras impostas. Nesse momento inicial, deve-se priorizar o alcance gradual e adaptável das CPCs.
8) Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?	O formato deve ser projetado sob a perspectiva de ser acessível e simples. Nesse caso, pode ser benéfico que haja uma multiplicidade de formatos, sempre que haja um formato global somado a um guia orientativo. Este último traz os pressupostos de validade e padrões mínimos de conduta elementares à perspectiva de atuação e cuidados a serem adotados pelos atores ao transferirem as informações pessoais. Isso porque, eventual rigidez dos modelos contratuais poderia levar ao engessamento do fluxo transfronteiriço de dados, o que, em um momento inicial de regulamentação, poderia ser prejudicial a inserção do Brasil no panorama internacional regulamentário. Destaca-se que eventual elevação dos patamares contratuais levaria a autorização por outros meios ou ainda o descumprimento às regras dispostas por serem inatingíveis. A experiência do modelo canadense é interessante sob este aspecto, na medida em que a Autoridade Nacional de Proteção de Dados (OPC) traz parâmetros mínimos sobre a perspectiva de proteção de dados pessoais, tais

	como: uso dos dados para as finalidades inicialmente fundamentadas; mitigação dos riscos em vistas à integridade e confidencialidade dos dados e; transparência no uso das informações pessoais com avisos claros aos titulares de dados do envio transfronteiriço de dados. Ainda o modelo neozelandês é relevante como exemplo à construção de CPCs mais flexíveis, A Autoridade Nacional de Proteção de Dados (OPC) disponibiliza questionários em seu site oficial, em que, ao final de respondido, o sistema gera de forma automática, o melhor modelo contratual a ser adotado pela empresa. Esta forma de *checklist* online é vantajosa, na medida em que se reduz custos com a implementação de consultorias técnicas especializadas, permitindo que as mais diversas entidades privadas possam se adequar ao fluxo transfronteiriço de dados de forma ágil, adequada e simplificada.
9) É necessário ter regras diferenciadas a depender do tipo dos agentes de tratamento (módulos específicos para os casos de controladores ou operadores) como exportadores e importadores de dados nas transferências internacionais realizadas por cláusulas contratuais? Quais?	A estrutura da LGPD propõe obrigações diferentes para controladores e operadores, o que leva a se pressupor que as CPCs devem espelhar essa distinção. A estrutura dos fluxos internacionais de dados e das cadeias de tratamento podem ser bastante variáveis e complexas, nesse sentido, seria interessante analisar a possibilidade de existirem pelo menos quatro categorias de cláusulas, haja vista as relações entre agentes de tratamento, isto é: Controlador-Controlador; Controlador-Operador; Operador-Operador e; Operador-Controlador. A escolha por um modelo como o neozelandês, com algum grau de flexibilidade, pode permitir que dentro dessa flexibilidade essas circunstâncias de obrigações diferentes dependendo da posição do agente possam ser acomodadas. Sob a experiência europeia, ilustrativamente, identifica-se que a utilização de modelos rígidos de CPCs pode dar azo a complexidades na adequação às circunstâncias fáticas e complexas ao tratamento de dados que incluem as transferências internacionais. Logo, alguma flexibilidade pode ser significativa para a acomodação de circunstâncias e especificidades dos fluxos transfronteiriços de tratamento de dados.

10) Há requisitos que precisam ser diferentes para Normas Corporativas Globais em relação aos usualmente exigidos para cláusulas-padrão contratuais? Quais?	Há um pressuposto importante quando se trata de NCGs, que é o fato de que elas devem se adequar a uma multiplicidade de ordenamentos jurídicos. Nesse sentido, a adequação deve ser a nível teleológico, devem ser os objetivos, os fundamentos, os princípios e os direitos dos titulares que devem guiar a avaliação de sua adequação ou não ao sistema nacional. Faz-se, portanto, necessário que exista alguma flexibilidade quanto à sua regulamentação e aprovação. A possível rigidez de CPCs pode ser contrária à lógica de NCGs. Nesse sentido, os requisitos mínimos diferenciadores giram em torno da adaptabilidade necessária às NCGs em permitir que grupos econômicos, organizações internacionais e instituições globais (inclusive da sociedade civil) implementarem as NCGs, tenham um espaço de compatibilidade, de modo a acompanhar as mudanças no dia a dia empresarial. Assim, dois outros pontos são relevantes: i) justamente por sua complexidade e multiplicidade de jurisdições, as NCGs devem ser avaliadas com uma visão de um horizonte temporal largo, pois suas modificações podem ser extremamente difíceis, nesse sentido não deve ser um requisito per se, mas deve ser uma abordagem que permita essa flexibilidade no tempo e; ii) por se tratar de situação global, um cuidado deve existir com os mecanismos de fiscalização e busca de conformidade e para fazer valer os direitos dos titulares.
11) Que critérios deveriam ser considerados na definição de grupo econômico ou empresarial que estaria habilitado para fins de aplicação das normas corporativas globais?	Um elemento prévio deve ser destacado. Ainda que se trate de NCGs, nada na lei leva a excluir que instituições organizadas em nível internacional que não sejam empresas não possam fazer uso desses mecanismos. Fundações e organizações da sociedade civil podem muitas vezes atuar globalmente ou em múltiplas jurisdições. Nesse sentido, em qualquer regulamentação da ANPD, pode ser importante não restringir a que somente empresas possam fazer uso do mecanismo. Dentre os critérios, destacam-se ao menos a localização de uma unidade do grupo seja no Brasil; indicação de comprometimento quanto às responsabilidades definidas na LGPD; indicação da localização da

	empresa com melhores perspectivas para lidar e cumprir com as NCGs; indicação do local onde ocorrem a maior parte das decisões relativas ao tratamento de dados e respectivas finalidades; comprometimento com a jurisdição brasileira com relação a eventuais acionamentos por parte de autoridades administrativas e judiciais. Vale destacar ainda que não existem óbices legais claros para que se restrinja a utilização de NCGs a grandes grupos necessariamente. Portanto, outras organizações como organizações internacionais ou organizações da sociedade civil que possuam diversas sedes e circulem dados entre estas podem eventualmente se beneficiar e em muitos casos de tais NCGs.
12) Quais informações mínimas (nível de detalhamento) sobre os dados pessoais devem ser exigidas para permitir a análise da conformidade pela ANPD das transferências internacionais de dados realizadas por instrumentos contratuais, que minimizem impactos negativos às atividades do grupo empresarial e preservem elevado grau de proteção ao titular de dados?	A lei parece ser silente sobre quais informações devem ser exigidas nesses casos. No entanto, tendo em vista as obrigações dos diferentes agentes e a necessidade de análise do tipo de tratamento e de seu risco, destacam-se três elementos cruciais: i) a natureza dos dados; ii) indicativos de volume; e iii) indicativos de risco do tratamento. Igualmente, alguns documentos jurídicos de conformidade parecem ser relevantes ou até necessários, próprios de serem solicitados pela ANPD, nos termos dos arts. 37 e 38, LGPD, como o Registro das Operações de Tratamento.
13) Quais os riscos e benefícios de se permitir transferências entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas	Dentre os riscos, têm-se eventuais descumprimentos fáticos dentro da complexa rede empresarial, a partir de eventuais exigências consideradas como um padrão muito alto de implementação. A própria natureza global das NCGs atrai complexidades na fiscalização e gerenciamento de *compliance*. Adicionalmente, a multiplicidade de jurisdições

pela ANPD?	envolvidas tende a ser um desafio e portanto um risco fazer valer os direitos dos titulares. Isso tende a ser um aspecto exponencial frente às diferentes personalidades jurídicas presentes e as suas proteções específicas em cada país. Com relação aos benefícios, destaca-se o maior controle sobre como as regras devem ser operadas na prática pelo grupo econômico, delineando contornos mais claros aos propósitos objetivados pela ANPD. Igualmente, estão os benefícios de *compliance* mais global em que a cadeia inteira de uma empresa estará sujeita a um padrão apropriado de proteção de dados. Isso sem mencionar a diminuição de custos e a uniformização da compreensão e das expectativas de titulares.
14) Existem experiências sobre a verificação e aprovação de cláusulas contratuais específicas e de normas corporativas globais que poderiam servir de exemplo para a ANPD?	A experiência europeia serve como um indicativo da complexidade de se lidar com a questão. Durante a validade da Diretiva 95/46/EC, somente 134 NCGs foram aprovadas; depois da aprovação do RGPD houve um aumento significativo de pedidos de aprovação e pelo menos 30 até o momento foram aprovadas. No entanto, ainda parece ser um procedimento burocrático e complexo, particularmente pelas características do arranjo institucional europeu de proteção de dados. Por outro lado, ainda sob a experiência europeia, identifica-se que o Grupo de Trabalho do Artigo 29.º (GT29) regulamenta de forma detalhada o art. 47, RGPD, sobre NCGs. Destaca-se elementos como: (i) o direito de titulares de dados apresentarem reclamações perante a Autoridade competente de seu domicílio; transparência com relação aos direitos e garantias dos titulares de dados; (ii) especificação com o escopo de atuação, delimitando a estrutura e os contatos do grupo de empresas ou grupo de empresas que exerçam uma atividade econômica conjunta e de cada um dos seus membros; (iii) responsabilidade dos agentes que atuam como Controladores e; (iv) comprometimento de que eventual legislação de um país terceiro ao qual a empresa esteja sujeita venha a

	ter efeito adverso às garantias das NCGs seja relatado à Autoridade competente. Já na Nova Zelândia, propõe-se um modelo padrão às CPCs. Dessa forma, há um modelo pré-formatado e rígido que deve ser adotado a toda e qualquer operação via as CPCs, mas que permitem de forma complementar cláusulas mais flexíveis, capazes de se adaptar à realidade de cada empresa, a exemplo de certificações, auditorias e inspeções, aptas a se moldarem de forma especializada. Portanto, de modo a afastar eventuais dificuldades em torno da complexidade da sistemática de aprovação de modelos contratuais por parte de Autoridades, sugere-se à ANPD a adoção de um procedimento mais expedito e simplificado, de forma a facilitar a aprovação de especificidades.
15) Quais são os direitos do titular no caso de alterações na configuração original da transferência? Em quais situações seria imprescindível a comunicação direta aos titulares ou algum tipo de intervenção destes?	Dentre os direitos, há principalmente o direito de acesso em conjunto com o princípio da transparência. Isso pressupõe uma relação de boa-fé e troca de informações suficientes para que o/a titular possa exercer a sua autodeterminação informativa. A lei não delimita as situações específicas de comunicação do titular, para além das que tratam de segurança da informação. No entanto, há que se pressupor que numa relação baseada na boa-fé e nos deveres de transparência e lealdade, em casos de mudança significativa na estrutura de equilíbrio de riscos de tratamento ou de impactos aos direitos dos titulares, deveria haver uma comunicação. Exemplos poderiam ser os usos para realização de perfis, uso de Inteligências Artificiais (IAs) ou outros mecanismos para inferências e que novos desenvolvimentos impactam as expectativas de uso dos dados, e.g. inovações tecnológicas na ferramenta. Ou ainda, mudanças na legislação de um determinado país onde os dados foram exportados e que poderiam impactar o exercício de direitos pelo titular. Nesses casos, o titular de dados deveria ter mecanismos fáceis para poder ser informado e poder agir (e.g. pedir suspensão ou requerer nos casos em

	que cabe a exclusão).
16) Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?	Tendo em vista a natureza transnacional destes conflitos, entre as melhores alternativas para a sua resolução pacífica resta a orientação por mecanismos consensuais, como conciliação, mediação e arbitragem no tocante a conflitos entre agentes de tratamento. Isto posto por serem mais adequados à situação concreta. Há diversos casos em que estão previstos esses mecanismos. Com relação a conflitos com titulares de dados, sugere-se a criação de um departamento interno à ANPD para que avalie e decida eventuais conflitos, de modo a assegurar maior isonomia aos direitos dos titulares de dados. Documentos internacionais juridicamente vinculantes podem auxiliar, especialmente no tocante a regras da Comissão das Nações Unidas para o Direito Comercial Internacional (UNCITRAL), como a Lei Modelo sobre Arbitragem Comercial Internacional, atendendo os pressupostos à composição de conflitos transfronteiriços. Para mais informação, temos o relatório "Lei Geral de Proteção de Dados Pessoais e Resolução de Conflitos: experiências internacionais e perspectivas para o Brasil", elaborado pelo ITS-Rio.
17) Quais as melhores alternativas para promover a conformidade com a regulamentação (inclusive em relação ao importador) referente às transferências internacionais de dados?	No que tange às melhores alternativas, destacam-se a existência de mecanismos de adequação internos à LGPD, especialmente, com relação a nomeação de um Encarregado, utilização de mecanismos técnicos e administrativos aptos a protegerem os dados pessoais, verificação periódica de documentos jurídicos ao compliance de dados, como o Registro das Operações de Tratamento e o Relatório de Impacto à Proteção de Dados.
18) Quais as melhores alternativas para resolver as questões práticas relacionadas à	Quanto às alternativas, destacam-se a formalização de contratações adequadas às subcontratações para o tratamento de dados, com especificação clara da separação de responsabilidades atribuídas a cada

responsabilização dos atores que transferem dados internacionalmente, em especial nos casos em que ocorrem transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador?	agente de tratamento; demonstrações periódicas da utilização de medidas eficazes à proteção de dados, em atenção ao princípio da responsabilização e prestação de contas; manutenção de todos os meios de prova relacionadas ao exercício de controle dos titulares de dados com as operações de tratamento, especialmente quando a coleta de dados é realizada diretamente pelo titular de dados, como consentimento, anuência contratual e registro das opções *opt-in* e *opt-out*; demonstração de realização de documentos regulatórios, como o Relatório de Impacto à Proteção de Dados e Avaliação dos Riscos do Legítimo Interesse.
19) Quais obrigações devem ser atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras?	Identifica-se a necessidade de uma definição ampla na regulação desta matéria, uma vez que a adoção de eventual abordagem que imponha restrições significativas, possa trazer impactos profundos no funcionamento legítimo do sistema de transferência internacional. O caso Schrems II da CJEU novamente é ilustrativo. A imposição de sanções e obrigações para exportadores de dados pessoais para os EUA direcionaram a complexidades tanto para exportadores quanto para importadores de dados pessoais. Indica-se que haja uma abordagem principiológica em que ambos os agentes tenham obrigações, principalmente de devida diligência, boa-fé, transparência, e precaução (de um ponto de vista de análise de riscos potenciais). Igualmente é importante que se tenha por base a possibilidade de verificação dos propósitos e finalidades por detrás de pedidos de acesso; de atendimento ao princípio da minimização de dados, ao disponibilizar tão somente os dados solicitados; demonstração clara de que as regras relativas à LGPD devem ser cumpridas diante de dados relativos a cidadãos brasileiros ou coletados em território brasileiro.
20) Quais os mecanismos mais adequados para fornecer aos titulares a	Com relação aos mecanismos, destaca-se a comunicação clara e ostensiva aos titulares de dados da existência de transferências internacionais de dados; a disponibilização de políticas de privacidade e

informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?	documentos jurídicos que esclareçam a forma de tratamento em meio ao fluxo transfronteiriço; a disponibilização quanto ao exercício dos direitos dos titulares de dados e; ainda a definição clara e objetiva da responsabilização por parte dos agentes de tratamento ao exportar e importar dados pessoais, em conformidade com a base principiológica e fundamental à LGPD.

Contribuições | Transferência Internacional de Dados
Loren Spindola (CELA) <loren.spindola@microsoft.com>
Qui, 30/06/2022 15:32
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Cc:

- Elias Abdala Neto (CELA) <elias.abdala@microsoft.com>;
- Alessandra Del Debbio (CELA) <aledd@microsoft.com>;
- Izabella Cesar Ribeiro (Pinhao E Koiffman Advogados) <v-izabellace@microsoft.com>

Prezados Senhores,

Temos o prazer de encaminhar as contribuições da Microsoft Brasil à tomada de subsídios sobre transferência internacional de dados.

Estamos à disposição para aprofundar os pontos abordados, caso julguem necessário.

Atenciosamente,

Loren Spíndola
Brazil Public Policy Lead
[redacted]
loren.spindola@microsoft.com

Microsoft

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

São Paulo, 30 de junho de 2022.

À
Agência Nacional de Proteção de Dados

Assunto: Colaboração à Tomada de Subsídios sobre Transferência Internacional de Dados.

Prezados Senhores,

Agradecemos a oportunidade de colaborar com tomada de subsídios sobre transferência internacional de dados pessoais pela Autoridade Nacional de Proteção de Dados - ANPD.

A missão da Microsoft é capacitar cada pessoa e cada organização no planeta para alcançar mais. Entendemos que a tecnologia desempenha um papel fundamental no aumento da produtividade no setor privado, aumentando a eficiência do governo e dos serviços públicos e melhorando a vida de todos os membros da sociedade. A Microsoft fornece produtos e serviços relacionados a praticamente a todo o ecossistema digital, incluindo software, hardware e serviços de computação em nuvem, que se estendem a muitos outros campos, como inteligência artificial, análise de dados, infraestrutura etc.

A presença da Microsoft no Brasil se estende por mais de 30 anos. Em 2020, lançamos a iniciativa Microsoft Mais Brasil, um plano de impacto que visa promover e contribuir para o crescimento do país, oportunidades de emprego e sustentabilidade. Diante da crescente demanda por serviços de computação em nuvem, a Microsoft vem expandindo seus datacenters e infraestrutura em nuvem no Brasil, bem como suas operações no país. Enquanto isso, o Brasil vem trabalhando em diferentes políticas para fortalecer sua economia por meio da transformação digital.

Vivemos em um mundo onde os fluxos de dados transnacionais se tornaram indispensáveis e os fluxos de dados internacionais são a regra, e não a exceção. São a pedra angular não só do comércio internacional, mas também da economia nacional e do desenvolvimento do país. Organizações e indivíduos obtêm grandes benefícios da movimentação de dados através das fronteiras, combinada com tecnologias e serviços que podem armazenar dados em diferentes partes do globo. Os fluxos de dados são particularmente relevantes para pequenas e médias empresas no Brasil (incluindo startups), que podem querer expandir seus negócios para outros países da região ou em outras partes do mundo, bem como atrair investimentos e novos serviços no Brasil, incluindo serviços de processamento de dados para empresas localizadas em outras jurisdições.

Ao mesmo tempo, a proteção de dados também é fundamental para o sucesso de qualquer transformação digital e, em última análise, para o desenvolvimento de uma

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

economia digital vibrante. No próximo ano, estima-se que mais de 75% da população mundial estará coberta por leis de privacidade modernas, e espera-se que essa porcentagem só cresça [1]. Como parte de nosso longo apoio a uma legislação de privacidade robusta, abrangente e interoperável, continuamos a trabalhar de forma construtiva com reguladores e legisladores em todo o mundo para promover proteção de dados e regulamentação de privacidade[2].

Acreditamos que regulamentação e inovação podem andar de mãos dadas. De fato, uma das lições que devemos tirar da pandemia é que precisamos reformular a forma como falamos sobre dados e regulamentação. Nos últimos anos, vimos muitos exemplos vívidos do valor de nossa infraestrutura de dados e seu extraordinário potencial para ajudar a humanidade por meio de avanços necessários em saúde e pesquisa[3]. Portanto, ao elaborar leis nacionais de privacidade robustas, abrangentes e interoperáveis, a questão que a sociedade civil, empresas, acadêmicos e governos deveriam fazer não é *se* podemos usar dados, mas sim *como* podemos permitir o uso responsável de dados para criar um mundo melhor e proteger os direitos humanos fundamentais.

Além desta seção introdutória e levando em consideração nossa experiência em regulamentação de proteção de dados em todo o mundo, temos o prazer de compartilhar nossas contribuições para as perguntas específicas abaixo. Para concisão e maior clareza, combinamos as respostas a perguntas relacionadas a um assunto central semelhante.

Por oportuno, gostaríamos de parabenizar a ANPD pelo relevante trabalho na regulamentação de proteção de dados, bem como nos colocar à disposição para continuar contribuindo com a discussão sobre a melhor forma de viabilizar uma infraestrutura de dados mais imersiva e inovadora, ao mesmo tempo em que promove a confiança do consumidor por meio de marcos legais que aumentem a privacidade e a proteção de dados.

Respeitosamente,

---

[1] https://www.zdnet.com/article/gartner-predicts-privacy-law-changes-consolidation-of-cybersecurityservices-and-ransomware-laws-for-next-4-years/

[2] https://blogs.microsoft.com/on-the-issues/2021/12/06/protecting-data-infrastructure-privacy/

[3] https://news.microsoft.com/on-the-issues/2021/06/30/open-data-health-care-ai-covid-19/

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

Alessandra Del Debbio
Vice-Presidente Jurídica e de Assuntos Corporativos

PERGUNTAS E RESPOSTAS

1.Quais são os obstáculos atuais para as empresas transferirem dados do Brasil para outros países? E de outros países para o Brasil?

Atualmente, as entidades que desejam transferir dados de ou para o Brasil enfrentam uma incerteza regulatória significativa porque a LGPD exige a implementação pela ANPD de vários mecanismos internacionais de transferência de dados - no entanto, não está claro quais obrigações para transferências de dados existem hoje (ou seja, antes da implementação da tais mecanismos). Além disso, algumas jurisdições mantêm regras que impedem a transferência de dados sem o cumprimento das condições especificadas por lei.

Mais amplamente, a falta de interoperabilidade é também uma desvantagem para os fluxos de dados transfronteiriços. A ANPD pode promover a interoperabilidade ao incorporar em seus mecanismos de transferência internacional de dados princípios de acordos multilaterais, como o *Framework* de Privacidade da Organização para Cooperação e Desenvolvimento Econômico (OCDE) e práticas compatíveis com os benchmarks globais.

Portanto, apoiamos fortemente o empenho da ANPD em envolver o Brasil nos esforços cooperativos internacionais para a interoperabilidade e o interesse abrangente da ANPD em encontrar as maneiras mais eficazes de reduzir as barreiras ao fluxo internacional de dados, mantendo fortes proteções para dados pessoais. Ao mesmo tempo que incentivamos a ANPD a emitir orientações que esclareçam que as atuais transferências de dados com base nas melhores práticas globais podem continuar, desde que atendam aos princípios de proteção de dados estabelecidos pela LGPD. Também incentivamos a ANPD a considerar maneiras de aumentar a clareza sobre as circunstâncias em que as disposições de transferência da LGPD se aplicam.

2.Qual é a melhor forma de promover a convergência e a interoperabilidade entre instrumentos contratuais de transferência internacional de dados com instrumentos de outras jurisdições? E como a ANPD pode atuar nesse sentido?

Esforços multilaterais para facilitar os fluxos de dados transnacionais - como as negociações da OCDE em direção a princípios comuns sobre o acesso confiável do governo aos dados - são vitais para promover a convergência e a interoperabilidade,

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

assim como o comércio ou outros acordos internacionais que promovem fluxos de dados confiáveis.

Também é importante que os instrumentos contratuais para transferências internacionais de dados sejam consistentes com as Cláusulas Contratuais Padrão da União Europeia, que foram atualizadas em 2021 para levar em conta os desenvolvimentos recentes na GDPR. Desde que os instrumentos contratuais atendam aos requisitos da LGPD, tais instrumentos devem ser reconhecidos como aceitáveis para manter a responsabilidade e legitimar as transferências de dados transfronteiriços. Além de promover convergência e interoperabilidade, essa abordagem promoveria uma forma mais conectada e simples de as organizações atuarem no Brasil.

Existem também padrões e certificações internacionais relevantes, como a ISO/IEC 27001 e o primeiro código de prática internacional do mundo para privacidade na nuvem, a ISO/IEC 27018, que podem ser promovidos pela ANPD, alavancando uma combinação responsiva de salvaguardas.

Por fim, será importante buscar decisões de adequação – tanto para o Brasil ser reconhecido por outros países como capaz de oferecer um nível adequado de proteção de dados, quanto pela ANPD determinar quais outros países oferecem um nível adequado de proteção de dados. Isso servirá para impulsionar a convergência regulatória e elevar ainda mais o país no cenário do comércio internacional. Caso a ANPD considere implementar decisões de adequação, é vital que se busque alinhamento com as abordagens de outras jurisdições relevantes.

3.Quais são os instrumentos mais eficazes e mais utilizados para viabilizar a transferência internacional de dados por grandes e pequenas empresas ou organizações?

De acordo com uma pesquisa da DigitalEurope em novembro de 2020, avaliando como os dados pessoais são transferidos da Europa para o resto do mundo, as cláusulas contratuais padrão (SCCs) foram consideradas de longe o mecanismo mais usado para transferências de dados. De todas as empresas pesquisadas, estima-se que 85% usem SCCs, enquanto outros mecanismos de transferência, como decisões de adequação, regras corporativas vinculantes (BCRs) ou derrogações (por exemplo, consentimento) representam pouco mais de 5% das transferências[4].

[4] https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

As SCCs são especialmente úteis porque, por meio de sua padronização e pré-aprovação são uma ferramenta "pronta" e de fácil implementação. Isso é particularmente importante para PMEs ou outras empresas que podem não ter recursos para negociar contratos individuais com cada um de seus parceiros comerciais. As SCCs também se distinguem de outros mecanismos de conformidade que exigem autorização prévia de uma autoridade nacional de proteção de dados (por exemplo, contratos ad hoc para transferências de dados) ou normalmente são mais caros de implementar (por exemplo, esquemas de certificação). Para serem mais eficazes, as SCCs devem ser proporcionais, flexíveis e interoperáveis – pois essas qualidades suportam melhor os fluxos de dados por organizações de diferentes tamanhos e setores.

Outros mecanismos de transferência também podem ser eficazes. Por exemplo, os esquemas de certificação têm o potencial de fornecer interoperabilidade, mantendo altos padrões de proteção de dados. Esses esquemas de certificação podem fornecer opções de transferência mais adaptadas a tipos específicos de produtos ou serviços e, assim, criar segurança adicional para pessoas e empresas que implementam e usam esses produtos e serviços. Várias jurisdições já reconheceram e adotaram diferentes caminhos para permitir o uso de esquemas de certificação.

Além disso, é importante reconhecer que explorar determinações de adequação de acordo com a seção 33, inciso I, da LGPD, terá amplo impacto e abrangência, legitimando a transferência internacional de dados para organizações de todos os portes e para cenários de casos mais amplos. Isso está alinhado com a capacidade da Comissão Europeia de determinar, de acordo com o artigo 45 do GDPR, se um país fora da UE oferece um nível adequado de proteção de dados.

4.Quais são os principais benefícios e impactos das transferências internacionais de dados e quais as melhores alternativas para abordá-los em cada um dos instrumentos contratuais de transferência de dados incluídos na LGPD e na prática internacional?

A Microsoft e nossos clientes nos setores público e privado dependem da capacidade de transferir dados globalmente para, entre outras coisas, fornecer melhores serviços aos clientes, operar nossos negócios com mais eficiência, permitir que nossos funcionários trabalhem de forma mais produtiva, gerenciar nossas cadeias de suprimentos e trabalhar com nossos parceiros de forma mais eficaz.

Mais amplamente, os fluxos de dados transfronteiriços são críticos para o desenvolvimento do Brasil, para a economia global, para o bem-estar das pessoas e suas comunidades e para a funcionalidade das operações e serviços de negócios. Por exemplo, sem fluxos de dados transfronteiriços, tecnologias transformacionais como inteligência artificial, Internet das Coisas e blockchain – todas alimentadas por grandes quantidades de dados e atendendo a uma variedade de mercados e usuários – não prosperarão. Os indivíduos também contam com fluxos de dados para acessar saúde, educação e outros serviços essenciais – e têm feito isso mais do que nunca desde o início da pandemia de COVID-19.

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

Finalmente, os fluxos de dados transfronteiriços fortalecem a segurança cibernética e proporcionam resiliência a ataques destrutivos, como observamos recentemente em nosso relatório sobre as primeiras lições da guerra na Ucrânia[5]. Os ataques cibernéticos geralmente são transnacionais e rápidos, portanto, a segurança cibernética exige compartilhamento de dados rápido e eficaz em uma base global e a capacidade de desembolsar ativos digitais em uma nuvem global. Impedir essas transferências de dados dificulta a coordenação internacional necessária e pode levar a maiores ameaças à segurança e à privacidade.

Em suma, vivemos em um mundo em que os fluxos de dados transnacionais se tornaram indispensáveis. Empresas e organizações de todos os tamanhos e em todos os cantos do mundo dependem do fluxo de dados através das fronteiras para administrar seus negócios e atender seus clientes.

5.Quais critérios e/ou requisitos devem ser considerados na regulamentação de cada um dos seguintes mecanismos internacionais de transferência de dados e por quê?

cláusulas contratuais padrão; cláusulas contratuais específicas; e regras corporativas obrigatórias.

A resposta a seguir aborda as questões 5, 7, 8 e 9.

Acima de tudo, as regras que regem as transferências internacionais de dados devem ter como objetivo garantir que os dados pessoais permaneçam suficientemente protegidos, não importa para onde vão. A regulamentação dos mecanismos internacionais de transferência de dados deve ser projetada para promover um bom comportamento de proteção de dados por parte dos controladores e processadores que foram encarregados de proteger e respeitar os dados pessoais.

Mais especificamente, os critérios e requisitos para os mecanismos internacionais de transferência de dados devem ser projetados para lidar com riscos específicos aos dados com regras ponderadas e propositais, em vez de restrições amplas que podem não ser necessárias em uma determinada circunstância.

Com isso em mente, vamos nos concentrar em critérios específicos para regular as transferências de dados por meio de SCCs, que também podem se aplicar aos outros mecanismos:

[5] https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-thecyber-war/

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

Flexibilidade: Recomendamos que a ANPD se concentre em garantir que as SCCs alcancem o resultado desejado – um alto nível de proteção de dados consistente com a LGPD – em vez de necessariamente aderir a uma linguagem rígida e predefinida. Essa flexibilidade permitirá que as organizações que já investiram na construção de SCCs que atendem a padrões tão altos possam implantá-los para ajudar a garantir a proteção dos dados dos indivíduos brasileiros;

Orientação: Incentivamos a ANPD a emitir orientações claras e práticas que comuniquem os princípios de flexibilidade descritos acima, para ajudar a garantir que as organizações entendam como criar e implementar efetivamente as SCCs de uma forma que melhor se adapte às suas circunstâncias particulares, mantendo a intenção da LGPD;

Funções e responsabilidades: As regras devem levar em conta as funções e responsabilidades distintas dos controladores e processadores: os processadores lidam com dados em nome e sob a direção dos controladores. Como resultado, os processadores não têm a capacidade de tomar a maioria das decisões com relação aos dados pessoais – e muitas vezes não têm visibilidade dos tipos de dados que estão sendo executados por meio de seus serviços. Ao mesmo tempo, as regras desenvolvidas pela ANPD devem ser flexíveis o suficiente para serem implementadas em vários cenários de controlador/processador. Uma possibilidade seria adotar um documento "modular" que possa ser adaptado ao caso específico, semelhante ao que a União Europeia tem feito em suas SCCs recentemente atualizados a partir de 2021. Essas SCCs permitem que as partes escolham entre quatro módulos: Controlador-Controlador (Módulo 1), Controlador-Processador (Módulo 2), Processador-Processador (Módulo 3) e Processador-Controlador (Módulo 4); e

Interoperabilidade: Conforme mencionado na resposta à pergunta 2, é importante garantir que os contratos de transferência de dados conforme a LGPD sejam o mais consistentes possível com as SCCs. Tais acordos, desde que atendam aos requisitos da LGPD, devem ser reconhecidos como instrumentos aceitáveis para manter a responsabilidade e legitimar as transferências de dados internacionais.

Notavelmente, também será importante adotar a iteração regulatória dos mecanismos de transferência de dados à medida que aprendemos como a LGPD e outras estruturas globais de privacidade operam na prática. As estruturas regulatórias não devem ser vistas como um projeto "único e feito" – à medida que a tecnologia, a sociedade, os modelos de negócios e outras normas evoluem, o "primeiro rascunho" de qualquer lei pode ficar desatualizado. As primeiras abordagens devem, portanto, ser aprimoradas ao longo do tempo por meio de iterações baseadas em várias contribuições de partes interessadas relevantes, incluindo outros formuladores de políticas, indústria, sociedade civil e academia.

6. Em que medida os elementos a serem considerados pela ANPD na avaliação do nível de proteção de dados de países estrangeiros ou organismos internacionais para

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

fins de adequação (artigo 34 da LGPD) também devem ser considerados no âmbito das regras para instrumentos contratuais?

Incentivamos a ANPD a reconhecer que instrumentos contratuais entre entidades (como SCCs), que estabelecem protocolos sólidos de proteção de dados, devem ajudar a eliminar a necessidade de requisitos rigorosos da legislação local. Isso ocorre porque a localização dos dados é normalmente menos relevante para sua proteção do que o tipo, qualidade e eficácia das medidas de proteção aplicadas aos dados, incluindo mecanismos técnicos e controles organizacionais. Essas medidas podem incluir criptografia, minimização de dados, ferramentas e controles de segurança cibernética, correção oportuna de vulnerabilidades identificadas, tecnologias de aprimoramento de privacidade, obrigações contratuais e assim por diante. Como exemplo dessa proteção, em 2020, a Microsoft reforçou suas já fortes proteções para dados pessoais de clientes com uma nova linguagem contratual em torno de nossa iniciativa *Defending Your Data*[6], onde nos comprometemos a contestar todas as solicitações governamentais de dados de clientes do setor público ou corporativo e fornecer compensação monetária aos usuários desses clientes se divulgarmos seus dados em resposta a uma solicitação governamental que viole a GDPR.

Por outro lado, as leis locais são mais relevantes no contexto de transferências de dados com base em determinações de adequação. As avaliações de adequação devem ter uma visão abrangente, em vez de tratar qualquer fator isolado como dispositivo. A GDPR e as estruturas legais internacionais predominantes, incluindo o *Framework* de Privacidade da OCDE e as Diretrizes de Privacidade da APEC, fornecem uma referência relevante para estruturas internacionais de transferência de dados.

7. As cláusulas contratuais padrão devem ser rígidas e com conteúdo pré-definido, ou sua regulamentação deve permitir certa flexibilidade quanto ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?

Consulte a questão 5.

8. Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas contratuais padrão para transferências internacionais de dados? Existem ferramentas relevantes que podem ser usadas para esse fim (por exemplo, árvore de decisão, formulários, caixas de seleção)? Existem experiências sobre o tema que possam servir de exemplo para a ANPD?

Consulte a questão 5.

[6] https://blogs.microsoft.com/on-the-issues/2020/11/19/defending-your-data-edpb-gdpr/

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

9. É necessário ter regras diferentes dependendo do tipo de agentes de processamento (por exemplo, módulos específicos para controladores ou processadores) como exportadores ou importadores de dados em transferências internacionais de dados com base em cláusulas contratuais? Se sim, quais seriam?

Consulte a questão 5.

17. Quais são as melhores alternativas para promover a conformidade regulatória (inclusive em relação ao importador) em relação às transferências internacionais de dados?

Recomendamos que a ANPD emita orientações práticas para explicar como os mecanismos de transferência devem ser implementados de acordo com as regulamentações da LGPD e da ANPD, bem como informações aos titulares dos dados sobre como seus direitos de privacidade são protegidos pela lei.

19. Que obrigações devem ser atribuídas ao importador e exportador em caso de acesso aos dados por autoridades públicas estrangeiras?

Juntamente com outros players relevantes da indústria de tecnologia, a Microsoft anunciou os *Trusted Cloud Principles*[7], que buscam parcerias com governos para resolver conflitos internacionais de leis que impedem inovação, segurança e privacidade, e para estabelecer e garantir proteções básicas para organizações que armazenam e processam dados na nuvem. A iniciativa estabelece os seguintes princípios que são relevantes para o propósito desta consulta:

(i) **Os governos devem envolver os clientes em primeiro lugar**, apenas com pequenas exceções. Os governos devem buscar dados diretamente de clientes corporativos em vez de provedores de serviços em nuvem, exceto em circunstâncias excepcionais.

(ii) **Os clientes devem ter o direito de notificação**. Quando os governos procuram acessar dados de clientes diretamente de provedores de serviços em nuvem, os clientes desses provedores de serviços em nuvem devem ter o direito de serem avisados antecipadamente sobre o acesso do governo a seus dados, o que só pode ser adiado em circunstâncias excepcionais;

(iii) **Os provedores de nuvem devem ter o direito de proteger os interesses dos clientes.** Deve haver um processo claro para os provedores de serviços em nuvem contestarem as solicitações de acesso do governo aos dados dos clientes, incluindo a notificação das autoridades relevantes de proteção de dados;

[7] https://trustedcloudprinciples.com/principles/

Microsoft do Brasil Comércio e Importação
de Software e Video Games Ltda.
Av. Juscelino Kubitschek, 1.909, 16º andar
São Paulo - SP
Brasil

(iv) **Os governos devem abordar os conflitos de lei.** Os governos devem criar mecanismos para levantar e resolver conflitos entre si, de modo que a conformidade legal dos provedores de serviços em nuvem em um país não constitua uma violação da lei em outro; e

(v) **Os governos devem apoiar fluxos de dados transfronteiriços.** Os governos devem apoiar o fluxo de dados transfronteiriço como um mecanismo de inovação, eficiência e segurança e evitar requisitos de residência de dados.

É fundamental que os governos apoiem as estruturas legais internacionais para resolver as leis conflitantes relacionadas ao acesso, privacidade e soberania de dados, bem como que permitam que os governos solicitem dados por meio de um processo transparente que cumpra leis e direitos humanos internacionalmente reconhecidos. A harmonização regulatória e as estruturas legais internacionais são essenciais para resolver possíveis conflitos e garantir uma proteção de dados forte, em vez de se concentrar em regulamentações locais.

20. Quais são os mecanismos mais adequados para fornecer aos titulares de dados informações claras e relevantes sobre a possível transferência de seus dados pessoais para fora do Brasil, bem como para garantir a proteção adequada dos direitos dos titulares de dados em transferências internacionais de dados? Como esses instrumentos devem ser implementados?

Veja a resposta às questões 6 e 17.

Signature: Alessandra Del Debbio (CELA Alessandra Del Debbio (CELA) (Jun 30, 2022 14:53 ADT))

Email: aledd@microsoft.com

Contribuições Microsoft. ANPD. Transf. intl dados pessoais

Final Audit Report 2022-06-30

Created:	2022-06-30
By:	Loren Spindola (CELA) (loren.spindola@microsoft.com)
Status:	Signed
Transaction ID:	CBJCHBCAABAAWwzypu0WQQM-UNOTSnAwrZNTIUUuP7eS

"Contribuições Microsoft. ANPD. Transf. intl dados pessoais" History

Document created by Loren Spindola (CELA) (loren.spindola@microsoft.com) 2022-06-30 - 5:49:27 PM GMT

Document emailed to Alessandra Del Debbio (CELA) (aledd@microsoft.com) for signature 2022-06-30 - 5:51:18 PM GMT

Email viewed by Alessandra Del Debbio (CELA) (aledd@microsoft.com)
2022-06-30 - 5:53:24 PM GMT

Document e-signed by Alessandra Del Debbio (CELA) (aledd@microsoft.com)
Signature Date: 2022-06-30 - 5:53:37 PM GMT - Time Source: server

Agreement completed.

2022-06-30 - 5:53:37 PM GMT

OAB/MG - Tomada de subsídios sobre Transferências Internacionais
Poliane Almeida <[redacted]
Qui, 30/06/2022 1[redacted]
Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

Prezados,

Em nome da OAB/MG - Comissão de Proteção de Dados, gostaríamos de anexar o nosso material complementar às respostas fornecidas pelo site (Participa + Brasil) para compor o processo de Tomada de subsídios sobre Transferências Internacionais de dados pessoais.

Estamos à disposição para contribuir.

Atenciosamente
OAB/MG
Adv. Poliane Almeida Silva Dias

A Comissão Estadual de Proteção de Dados Pessoais da Ordem dos Advogados do Brasil, Seccional Minas Gerais (OAB/MG), vem, por meio deste, honrosamente, apresentar ponderações acerca de algumas das questões com as quais percebeu poder contribuir na Tomada de Subsídios ANPD nº 02/2022.

Prestadas as homenagens desta Seccional à ilustrada Autoridade Nacional de Proteção de Dados e ao seu respeitável quadro, expõem-se adiante sugestões pertinentes às questões de nºs 1, 2, 3, 7, 8, 16 e 20.

---

1. Quais os obstáculos atualmente para que as empresas transfiram dados do Brasil para outros países? E de outros países para o Brasil?

Iniciam-se com a falta de conscientização sobre a cultura e hábito da proteção de dados pela maioria das empresas brasileiras, principalmente, pelo desconhecimento da própria Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e a sua aplicação na prática. Diante da recente vigência da Lei, com menos de dois anos, e a falta de uma regulamentação específica da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) sobre o tema, as transferências internacionais de dados pessoais vêm sendo feitas, sobretudo, com o amparo de cláusulas contratuais, obedecendo aos requisitos legais e com a implementação de medidas técnicas e administrativas para a proteção destes dados de acordo com os princípios da Lei e os direitos dos titulares. Não há, por enquanto, definição pelo Órgão de controle de quais países ou organismos internacionais proporcionam grau de proteção de dados pessoais adequados.

Certamente, com a definição da chamada decisão de adequação pela ANPD, relacionada a estes países e organismos com grau de proteção elevado, propiciará maior facilidade à transferência para os contemplados. Garantir-se-á, assim, melhor coordenação entre todos os atores envolvidos – incluindo a supervisão por parte das autoridades competentes.

Ressalta-se, por oportuno, que não só as grandes empresas transferem dados pessoais internacionalmente, mas as médias e pequenas também. Isso dificulta o cumprimento de todas as medidas exigidas nos demais casos previstos na Lei, inclusive dado ao próprio tratamento diferenciado dispensado a tais agentes. Outro obstáculo surge quando não há um país ou organismo internacional previamente definido como apto para a transferência, pois se torna necessária a realização de contratos específicos, padrões ou com normas corporativas globais.

De igual forma, o inverso, transferência de dados pessoais de outros países para o Brasil, também encontra obstáculos pela falta de cultura, conhecimento e aplicação da LGPD, fazendo com que o Brasil não seja um país reconhecido ainda como adequado para a decisão de adequação de nível internacional.

No que se refere às cláusulas contratuais específicas, padrão ou corporativa, o Brasil na grande maioria das empresas ainda não possuem sequer a adequação completa da LGPD, sendo difícil

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

exigir a adoção das medidas necessárias e cláusulas efetivas que protejam os dados pessoais, pois na sua essência é necessário atender os princípios e outras regras da Legislação, em especial as bases legais próprias para a transferência internacional de dados.

A regulamentação dos instrumentos contratuais, obedecendo a critérios e padrões internacionais de transferência de dados, certamente, ajudará o Brasil não só a exportar os seus dados, como, também, na importação, porquanto harmonizar-se-á nossa legislação e a respectiva regulamentação com o que é exigido pelos outros países.

2. Qual a melhor maneira de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições? E como a ANPD pode atuar nesse sentido?

A ANPD deve orientar e divulgar materiais em seu site para ajudar os agentes de tratamento a elaborarem cláusulas contratuais específicas para determinadas situações de transferência, em consonância com a LGPD, e outras legislações sobre proteção de dados de outros países, para que com uma proximidade maior destas regras voltadas para a salvaguarda apropriada para a transferência internacional, o Brasil possa se inserir no mesmo ritmo de proteção e interoperabilidade nas transferências, atendendo também às exigências de outras jurisdições.

Na LGPD, não havendo o reconhecimento pela ANPD de países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado, a transferência somente poderá ser feita nas hipóteses do art. 33, incisos II a IX e, no que se refere aos instrumentos contratuais, somente as alíneas “a”, “b” e “c” do inciso II, tratam deste assunto ao disciplinar que:

Art. 33 A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
(...)
II quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
a) Cláusulas contratuais específicas para determinada transferência;
b) Cláusulas-padrão contratuais;
c) Normas corporativas globais;
(...)

De igual modo, as cláusulas contratuais padrões devem ser elaboradas pela própria ANPD, com a posterior divulgação em seu site, para que os controladores possam se valer do material no caso da realização de uma transferência internacional de dados. A ANPD assume, desde a vigência da Lei, papel de suma relevância na conscientização e propagação da cultura da proteção de dados pessoais e à privacidade. Regulamentar a transferência internacional é mais uma das relevantes missões que a (agora autarquia especial, vide Medida Provisória nº 1.124/2022) enfrentará – no ponto, de se elogiar o caráter dialético e democrático com o qual a (então) Autoridade vem conduzindo seus trabalhos, reunindo perspectivas das mais distintas e plurais em tomadas de subsídios como essa, buscando o melhor resultado aos sujeitos tutelados pela LGPD.

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

Quanto às normas corporativas globais, por envolver estatutos internos, regras de governança e administração de cada empresa, apenas as diretrizes essenciais devem ser divulgadas pela ANPD, para que as empresas que tenham atuação internacional possam, além de manter as suas próprias regras, se adequarem também às exigências legais e regulamentadas por aquela.

Conclui-se, portanto, que compete à ANPD quanto aos 03 tipos de instrumentos contratuais, facilitar a utilização, dispondo de orientações, modelos, exigências mínimas e outras medidas de salvaguarda para a proteção dos dados pessoais e transferência internacional, a fim de colocar o Brasil como reconhecidamente um país de nível adequado de proteção.

3. Quais os instrumentos mais efetivos e os mais utilizados para legitimar a transferência de dados pessoais internacionalmente por grandes e por pequenas empresas ou organizações?

De forma simples e objetiva, aquele que, em um primeiro momento se mostra o mecanismo mais efetivo para transferências internacionais seguras, e que garantem o cumprimento e a efetivação dos direitos e liberdades dos titulares é o mecanismo estampado no artigo 33, inciso I do caput da lei 13.709, abaixo transcrito:

"I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei"[1]

Para que se possa avaliar qual o grau de proteção de uma proteção de dados pessoais de um país, não basta apenas olhar se tal país possui uma legislação geral de proteção de dados pessoais, uma autoridade independente ou normas setoriais que possuam algum grau de proteção de dados pessoais. Não necessariamente será exigido de um país terceiro que possua leis e proteções idênticas àquelas trazidas pela LGPD;, nas palavras de Leonardi:

"Dada a influência Europeia, é de se esperar que a ANPD utilize como referência o conceito europeu de 'nível adequado de proteção', por meio do qual se entende que um país não precisa assegurar nível de proteção idêntico, mas 'substancialmente equivalente'."[2]

O próprio artigo 34 da LGPD enumera fatores que deverão ser considerados no momento em que a ANPD decidir por analisar o grau de proteção de dados pessoais de um país terceiro para que possa definir o grau de proteção de dados de um país, que será uma ampla análise ampla e geral, que deverá levar em conta: normas de proteção de dados gerais e setoriais, observância dos princípios e dos direitos dos titulares presentes na LGPD pelo país terceiro ou organismo internacional que receba transferências de dados com aplicação da LGPD, adoção de medidas de

[1] Retirado do artigo 33 da LGPD, inciso I.
Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm
[2] Tratado de Proteção de Dados Pessoais – página 292, Transferência Internacional de Dados Pessoais, Leonardi, Marcel.

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

segurança previstas em regulamento (que, até o momento, ainda não foi feito), garantias judiciais e institucionais para respeito dos titulares de dados, dentre outros.

A decisão de adequação é um método muito mais efetivo do que os demais, pelo fato de que para que possa ter uma decisão de adequação em relação a país terceiro ou mesmo a organismo internacional, deverá ser feito um longo processo de análise de todo o ordenamento jurídico relativo a proteção de dados de país terceiro ou órgão internacional relativo a proteção de dados pessoais, sua jurisprudência sobre tema e até mesmo as práticas de proteção de dados para se saber sobre a possibilidade ou não de o referido terceiro dar aos titulares garantias "substancialmente equivalentes" àquelas trazidas pela LGPD e pelo ordenamento jurídico brasileiro com relação a proteção de dados pessoais.

Com uma decisão de adequação em relação a um país ou um organismo internacional, este estará comprovadamente com as adequações da ANPD, garantindo o cumprimento de requisitos necessários para garantir os direitos dos titulares e princípios da LGPD – ocorrendo também, em tese, profunda análise do sistema jurídico regulatório do país terceiro.

Apesar de não existir uma hierarquia entre os mecanismos de transferência internacional de dados pessoais na LGPD, nos resta claro que uma decisão de adequação é o principal meio para realização de transferências internacionais seguras. Inclusive, esse é o posicionamento da doutrina:

"Os demais mecanismos de transferência mencionados a seguir podem ser utilizados quando o nível de proteção do país estrangeiro envolvido na transferência de dados pessoais não é considerado adequado pela ANPD."[3]

No entanto, apesar de as decisões de adequação serem o meio de transferência internacional mais efetivo para garantir proteção aos direitos e liberdades dos titulares, não é um método simples, pois, como já explicitado, exige ampla análise das normas, jurisprudências e práticas relativas a proteção de dados pessoais do país terceiro para ser emitida.

Ainda, deve ser tomada uma decisão de adequação individual com relação a cada país terceiro ou organismo internacional com o qual se pretenda realizar transferências internacionais de dados pessoais, o que pode não ser uma medida tão efetiva ao curto prazo.

As transferências internacionais de dados são cada vez mais comuns, em especial nos dias de hoje, em razão da globalização e da nova era digital, na qual a grande maioria das empresas possui contratos com prestadores de serviços para armazenamento de dados em nuvem ou com prestadores de serviços de marketing, gestão de clientes ou mesmo gestão de recursos humanos, que utilizam serviços em nuvem, cujo servidor está localizado fora do território nacional.

[3] Tratado de Proteção de Dados Pessoais – página 293, Transferência Internacional de Dados Pessoais, Leonardi, Marcel.

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

Apenas a título de exemplo, cite-se matéria da TI Inside[4], o mercado de infraestrutura como serviço cresceu 41,4% em 2021, totalizando US$ 90,9 bilhões, acima dos US$ 64,3 bilhões em 2020. De acordo com Sid Nag, Analista e Vice-Presidente de Pesquisa do Gartner:

"A Nuvem oferece suporte à escalabilidade e à composição que as tecnologias e aplicações avançadas exigem, ao mesmo tempo em que permite que as empresas atendam às necessidades emergentes, como soberania, integração de dados e experiência aprimorada do cliente."

Tendo em conta referida fala, bem como o nosso contexto atual, é evidente que as transferências internacionais de dados pessoais acontecem com enorme frequência e devem ocorrer com frequência cada vez maior nos próximos anos, é de suma importância que se busque uma solução rápida para que as transferências internacionais continuem a ocorrer, de forma a garantir o desenvolvimento econômico e tecnológico e a inovação e também a autodeterminação informativa e o direito fundamental à proteção de dados pessoais dos titulares.

Por tal razão, e pelo fato de que a ANPD e a proteção de dados pessoais no Brasil ainda estão em seus primeiros passos, imperioso é, buscarmos por uma solução mais amplas para garantir que as transferências internacionais possam ser feitas segundo os moldes da LGPD e para garantir a segurança dos dados dos titulares de dados pessoais.

O artigo 33 da LGPD traz, além das decisões de adequação, enorme lista com outras 11 hipóteses para legitimar uma transferência internacional de dados pessoais.

Tendo em vista a natureza do presente parecer, e a sua busca por uma solução que visa a criação de uma solução, em um curto espaço de tempo, que possa auxiliar na realização de transferências internacionais e garantir a proteção de dados pessoais exigida pelo sistema brasileiro, ou ao menos uma proteção "substancialmente equivalente", iremos focar, a partir de agora nas cláusulas-padrão contratuais, do inciso II, alínea b, do caput do artigo 33 da LGPD.

Não se discorre, no presente ensaio, sobre as derrogações, que são, nas palavras de Angelo Gamba Prata de Carvalho[5],

"que se caracteriza, em verdade, pelo afastamento do manto da proteção de dados do diploma, porém, sempre em homenagem a outros objetivos de interesse público previstos de maneira taxativa pelos incisos III a VII do art. 33 da LGPD..."

[4] Mercado Mundial de infraestrutura como serviço em nuvem pública cresce 41,4%. Acesso em 07/06/2022. Disponível em: https://tiinside.com.br/06/06/2022/mercado-mundial-de-infraestrutura-como-servico-em-nuvem-publica-cresce-414/

[5] Transferência Internacional de Dados na Lei Geral de Proteção de Dados – Força normativa e efetividade diante do cenário transnacional. CARVALHO, Angelo Gamba Prata de. Página 629. Lei Geral de Proteção de Dados Pessoais e suas repercussões no direito Brasileiro.

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

Em verdade, as situações previstas nos incisos III a IX, constituem situações específicas, são passíveis de ocorrer no mundo real, sem a necessidade da criação de um instrumento específico, como o cumprimento de um contrato ou o consentimento do titular, ou então situações restritas a órgãos públicos ou que dependem de autorização específica da ANPD.

O que se pretende no presente ensaio, mais uma vez, é auxiliar na criação de um mecanismo efetivo para uma transferência internacional de dados segura, com aplicação ampla e que possa ser colocado em circulação pela autoridade o mais rápido possível.

II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
a) cláusulas contratuais específicas para determinada transferência;b) cláusulas-padrão contratuais;c) normas corporativas globais;d) selos, certificados e códigos de conduta regularmente emitidos;

Com relação aos elementos acima citados, as cláusulas contratuais específicas não se mostram, salvo melhor juízo, o melhor instrumento ao presente momento, pois tais cláusulas deverão ser elaboradas para uma determinada transferência e ainda deverão ser verificadas e aprovadas pela ANPD, segundo o próprio caput do artigo 35 da LGPD.

Com isso, pode haver morosidade no processo de aprovação de cada conjunto de cláusulas contratuais especificas enviados para a ANPD por diversos controladores do Brasil, o que vai contra uma ideia inicial de um meio que vise facilitar as transferências internacionais de dados pessoais.

Com relação às normas corporativas globais, as palavras de Leonardi[6] rapidamente nos mostram seu significado, e a não aplicabilidade das mesmas no presente caso:

"As chamadas 'normas corporativas globais' são outra opção disponível para casos de transferência internacional de dados pessoais entre empresas do mesmo Grupo Econômico."

Ainda nas palavras do autor, apesar de a LGPD ser silente, espera-se que, assim como no modelo europeu, as normas corporativas globais tenham que ser também aprovadas pela ANPD, o que, somado ao fato de que cada conjunto de normas corporativas globais seja específico para um grupo econômico, mostra que o referido mecanismo também não seja uma solução geral a ser adotada.

Quanto aos selos, certificados e códigos regularmente emitidos, a ANPD ainda não criou sequer procedimentos que deverão ser adotados, ou mesmo critérios utilizados para sua aprovação, o que mostra que também não são uma solução para o presente momento.

[6] Tratado de Proteção de Dados Pessoais – página 294, Transferência Internacional de Dados Pessoais, Leonardi, Marcel

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

Por fim, temos as cláusulas-padrão contratuais, que nada mais são do que "*cláusulas-modelo elaboradas pela ANPD, contendo obrigações das partes envolvidas na transferência e os direitos dos titulares dos dados a serem transferidos*".[7]

Tais cláusulas contratuais, diferentemente de cláusulas específicas ou de normas corporativas globais, possuem um conteúdo mais geral, o que dispensa aprovação de seu conteúdo pela ANPD a todo momento, possibilitando a criação de um único documento aprovado pela ANPD, e assim, trazendo maior segurança jurídica para as transferências internacionais.

Podemos, inclusive, nos espelhar no modelo europeu, no qual os órgãos competentes disponibilizam referidas cláusulas online.

No entanto, apesar de as Cláusulas-padrão contratuais serem, inicialmente um modelo, elas podem ser alteradas de acordo com o caso concreto, segundo Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE Versão 2.0, documento do EDPB, da seguinte forma:

"Se o exportador pretender adotar medidas complementares em combinação com as cláusulas contratuais-tipo, não é necessário solicitar autorização à autoridade de controlo competente para adicionar este tipo de cláusulas ou garantias complementares, desde que as medidas complementares identificadas não contradigam, direta ou indiretamente, as cláusulas-tipo de proteção de dados e sejam suficientes para assegurar que o nível de proteção garantido pelo RGPD não é comprometido."[8]

Portanto, além de seu caráter ligeiramente mais geral do que os demais mecanismos de transferência internacional de dados pessoais, as cláusulas-padrão contratuais devem ser aprovadas pela ANPD, e ser seguidas em sua integralidade pelos agentes de tratamento envolvidos na transferência internacional,[9] é possível que sejam adicionadas cláusulas ao seu conteúdo, desde que não contradigam as cláusulas iniciais, e tais alterações, segundo o EDPB, não precisam ser solicitadas à Autoridade, podendo ser aprovadas posteriormente.

Portanto, o método mais seguro para transferências internacionais de dados pessoais são as decisões de adequação, que dão maior segurança em que sejam cumpridos os requisitos da LGPD. No entanto, as decisões de adequação ainda não estão prontas, e serão feitas ao longo do tempo.

---

[7] Tratado de Proteção de Dados Pessoais – página 293, Transferência Internacional de Dados Pessoais, Leonardi, Marcel

[8] Recomendações 01/2020 relativas às medidas complementares aos instrumentos de transferência para assegurar o cumprimento do nível de proteção dos dados pessoais da UE Versão 2.0, página 26. Acesso em 07/06/2022. Disponível em: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_pt

[9] Tratado de Proteção de Dados Pessoais – página 293, Transferência Internacional de Dados Pessoais, Leonardi, Marcel

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

E no momento, necessitamos de uma solução mais rápida e geral para que possam ser realizadas transferências internacionais seguras. Portanto, as cláusulas-padrão contratuais se mostram uma saída melhor ao atual momento.

7. As cláusulas-padrão contratuais devem ser rígidas e com conteúdo pré-definido ou a sua regulamentação deve permitir uma determinada flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado?

As cláusulas-padrão contratuais devem sim ser rígidas para possibilitarem uma real proteção aos direitos dos titulares e dos princípios da legislação de proteção de dados pessoais em países terceiros, mas devem também possui um conteúdo pré-definido, pois o nome "cláusulas-padrão" nos leva a entender que seu conteúdo será padrão, igual para todos os casos e com um conteúdo previamente definido pela ANPD.

Caso o conteúdo de uma cláusula-padrão contratuais fosse demasiado flexibilizado pela ANPD e agentes de tratamento pudessem alterar o seu conteúdo a todo e qualquer momento, as cláusulas-padrão contratuais perderiam a sua natureza e seriam semelhantes às cláusulas trazidas na alínea a, do inciso II do caput do artigo 33 da LGPD, as cláusulas contratuais específicas para cada transação.

O que deve ser ponderado nos casos de cláusulas-padrão contratuais é a possibilidade de incrementação de seu conteúdo conforme o caso concreto, de ocorrer adaptação do conteúdo das cláusulas-padrão ao caso concreto, desde que os direitos dos titulares e os princípios das normas de proteção de dados do Brasil continuem sendo respeitados. Assim mostra, inclusive, o Considerando 109 do GDPR, lei que inspirou e ainda serve de referência para o sistema de proteção de dados nacional:

"A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção."[10]

[10] Considerando 109 GDPR. Acesso em 08/06/2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

Ou seja: a depender do caso concreto, deverão ser adicionadas cláusulas mais detalhadas aos contratos que envolvam as cláusulas-padrão contratuais, para que o contrato seja adequado à realidade jurídico/normativa de cada país que venha a receber os dados pessoais.

Para se saber quais cláusulas ou mesmo quais medidas deverão ser incluídas no contrato, o EDPB sugere, na já mencionada Guideline 01/2020, uma sequência de passos para análise do cenário fático/jurídico de país terceiro, para saber se a transferência é viável com as cláusulas-padrão pré-elaboradas pela ANPD, se para possibilitar a transferência serão necessárias alterações/adições de cláusulas contratuais e/ou medidas de segurança adicionais ou se as transferências deverão ser interrompidas em razão de falta de possibilidade de se garantir padrão similar de proteção aos da LGPD. Referido passo a passo é descrito da seguinte forma:

Etapa 1: Conhecer as transferências

Para saber o que lhe poderá ser exigido para poder prosseguir as suas transferências ou para realizar novas transferências de dados pessoais, o exportador *(aquele que envia os dados pessoais para o exterior)* de dados deve começar por se assegurar de que tem **pleno conhecimento das suas transferências**. O registo (mapeamento de dados/processos) e o levantamento de todas as transferências podem constituir um exercício complexo para as entidades envolvidas em transferências múltiplas, diversas e regulares com países terceiros e que utilizam diversos subcontratantes e subcontratantes ulteriores. **Conhecer as suas transferências é uma primeira etapa essencial para cumprir as obrigações que incumbem ao exportador de dados por força do princípio da responsabilidade.**

Etapa 2: Identificar os instrumentos de transferências utilizados

Independentemente do instrumento de transferência do artigo 46.º do RGPD (na LGPD, seria o artigo 33) escolhido, o exportador deve assegurar-se de que, em termos gerais, os dados pessoais transferidos beneficiam de um nível de proteção essencialmente equivalente.

Os instrumentos de transferência do artigo 46.º do RGPD contêm principalmente garantias adequadas de natureza contratual que podem ser aplicadas a transferências para todos os países terceiros. A situação existente no país terceiro para o qual o exportador transfere dados pode ainda exigir que este complemente os referidos instrumentos de transferência e as garantias aí contidas com medidas adicionais («medidas complementares») para assegurar um nível de proteção essencialmente equivalente.

Se a transferência não puder basear-se legalmente numa decisão de adequação, nem uma derrogação do artigo 49.º, é necessário prosseguir para a etapa 3. (Traduzindo para a LGPD, se a transferência de dados for pautada em alguma das hipóteses do inciso II do caput do artigo 33, deverá o agente de tratamento prosseguir para a próxima etapa do teste).

Etapa 3: Avaliar se o instrumento de transferência do artigo 46.º do RGPD utilizado é eficaz tendo em conta todas as circunstâncias da transferência (No caso da LGPD, instrumentos do artigo 33, inciso II)

O instrumento de transferência do artigo 46.º do RGPD selecionado deve ser eficaz, assegurando que o nível de proteção garantido pelo RGPD não é comprometido pela transferência.

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

Em especial, a proteção conferida aos dados pessoais transferidos para o país terceiro deve ser essencialmente equivalente à que é garantida no EEE pelo RGPD, lido à luz da Carta dos Direitos Fundamentais da EU. (Onde se lê RGPD, substituir por LGPD e Carta de Direitos substituir por Constituição Federal).

Por conseguinte, o exportador deve, se necessário, em colaboração com o importador (aquele que recebe os dados pessoais), avaliar se existe algo no direito ou na prática do país terceiro que possa afetar a eficácia das garantias adequadas (das garantias que criam a possibilidade de cumprimento dos princípios da LGPD e da garantia de exercício de direitos dos titulares naquela transferência) do instrumento de transferência do artigo 46.º do RGPD que utilizou, no contexto da transferência específica.

Esta avaliação deve conter elementos relativos ao acesso aos dados das autoridades públicas do país terceiro do importador, tais como:

- elementos que indiquem se as autoridades públicas do país terceiro do importador podem procurar aceder aos dados com ou sem o conhecimento do importador de dados, à luz da legislação, prática e precedentes comunicados;
- elementos que indiquem se as autoridades públicas do país terceiro do importador poderão ter acesso aos dados através do importador de dados ou através dos fornecedores de telecomunicações ou canais de comunicação, à luz da legislação, dos poderes legais, dos recursos técnicos, financeiros e humanos de que dispõem e dos precedentes comunicados.

Para auxiliar na investigação do contexto jurídico de país terceiro ou organismo internacional que irá receber os dados pessoais, o parecer em análise insere os seguintes tópicos, como um guia:

O contexto jurídico e/ou as práticas aplicáveis dependerão das circunstâncias específicas da transferência, nomeadamente:

- as finalidades para as quais os dados são transferidos e tratados (por ex., marketing, RH, armazenamento, apoio informático, ensaios clínicos);
- os tipos de entidade envolvidos no tratamento (pública/privada; responsável pelo tratamento/subcontratante);
- o setor no qual a transferência ocorre (por ex., adtech, telecomunicações, financeiro, etc.);
- as categorias de dados pessoais transferidos (por ex., os dados pessoais relativos a crianças podem ser abrangidos pelo âmbito de aplicação de uma legislação específica do país terceiro)42;
- se os dados serão armazenados no país terceiro ou se existe acesso remoto aos dados armazenados na UE ou no EEE;
- o formato dos dados a transferir (ou seja, texto corrido/pseudonimizado ou encriptado);
- a possibilidade de ocorrência de transferências ulteriores dos dados do país terceiro em causa para outro país terceiro

Etapa 4: Adotar medidas complementares

Se resultar da avaliação efetuada pelo exportador na etapa 3 que o instrumento de transferência do artigo 46.º do RGPD escolhido não é eficaz, o exportador deverá determinar, caso necessário em colaboração com o importador, se existem medidas complementares que, em combinação com as garantias contidas nos instrumentos de transferência, possam assegurar que os dados transferidos beneficiem no país

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

terceiro de um nível de proteção essencialmente equivalente ao que é garantido na UE. As «medidas complementares» são, por definição, complementares das garantias já previstas no instrumento de transferência do artigo 46.º do RGPD e de quaisquer outros requisitos de segurança aplicáveis (por ex., medidas técnicas de segurança) estabelecidos no RGPD.

O exportador deve identificar, caso a caso, as medidas complementares que podem ser eficazes para um conjunto de transferências para um país terceiro específico quando utiliza um instrumento de transferência específico do artigo 46.º do RGPD. O exportador não precisa de repetir a avaliação sempre que efetuar a mesma transferência de um tipo específico de dados para o mesmo país terceiro. Alguns dos dados previstos para transferência podem exigir medidas complementares, ao passo que outros podem não exigir essas medidas (tendo em conta a aplicação formal e/ou prática da legislação do país terceiro). O exportador poderá basear-se nas suas avaliações e conclusões anteriores nas etapas 1, 2 e 3 supra e verificar, com base nas suas conclusões, a potencial eficácia das medidas complementares para garantir o nível de proteção exigido.
Em princípio, as medidas complementares podem ter um caráter contratual, técnico ou organizativo.

Etapa 5: Etapas do processo a seguir quando o exportador identifica medidas complementares eficazes
As etapas do processo que o exportador pode ter de seguir se tiver identificado medidas complementares eficazes a adotar variam consoante o instrumento de transferência do artigo 46.º do RGPD que estiver a utilizar ou pretender utiliza.

Cláusulas-tipo de proteção de dados [artigo 46.º, n.º 2, alíneas c) e d), do RGPD]

Se o exportador pretender adotar medidas complementares em combinação com as cláusulas contratuais-tipo, não é necessário solicitar autorização à autoridade de controlo competente para adicionar este tipo de cláusulas ou garantias complementares, desde que as medidas complementares identificadas não contradigam, direta ou indiretamente, as cláusulas-tipo de proteção de dados e sejam suficientes para assegurar que o nível de proteção garantido pelo RGPD não é comprometido.71 O exportador e o importador de dados devem assegurar que as cláusulas adicionais não podem ser interpretadas de modo a restringir os direitos e obrigações previstos nas cláusulas contratuais-tipo ou, de qualquer outro modo, reduzir o nível de proteção dos dados. O exportador deve poder demonstrar o que precede, incluindo a inequivocidade de todas as cláusulas, em conformidade com o princípio da responsabilidade e a sua obrigação de proporcionar um nível suficiente de proteção dos dados. As autoridades de controlo competentes têm o poder de rever as cláusulas complementares sempre que necessário (por ex., em caso de reclamação ou de um inquérito de iniciativa própria).

Se o exportador pretender alterar as próprias cláusulas-tipo de proteção de dados ou se as medidas complementares adicionadas «contradisserem», direta ou indiretamente, as cláusulas contratuais-tipo, deixa de se considerar que o exportador recorreu às cláusulas-tipo contratuais72 e este deve solicitar uma autorização à autoridade de controlo competente, nos termos do artigo 46.º, n.º 3, alínea a), do RGPD.

Etapa 6: Reavaliar com frequência adequada
O exportador deve controlar, permanentemente e sempre que adequado em colaboração com os importadores de dados, os desenvolvimentos no país terceiro para o qual transferiu dados pessoais que possam afetar a sua avaliação inicial do nível de proteção e as decisões que tenha consequentemente adotado em relação às suas transferências. A responsabilidade é uma obrigação permanente.

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

8. Qual seria o formato mais adequado para a ANPD disponibilizar modelos de cláusulas-padrão contratuais para transferências internacionais de dados? Há ferramentas que poderiam ser interessantes para tal? (por exemplo, árvore de decisões, formulários, checkboxes, etc)? Existem experiências sobre o tema que poderiam servir de exemplo para a ANPD?

Acredita-se que o formato mais adequado para disponibilização dos modelos de cláusulas-padrão seria através da ferramenta do Word. Pois, é totalmente acessível e popular no Brasil. Sugere-se também que os documentos estejam em modo editável, adaptáveis pelos agentes, caso queiram acrescentar outras cláusulas ou garantias adicionais, desde que não choquem, direta ou indiretamente, com as cláusulas contratuais sugeridas pela ANPD (sem prejuízo de nenhum dos direitos ou das liberdades fundamentais dos titulares dos dados).

Sugere-se ainda que a ANPD disponibilize uma página exclusiva para o tema de Transferência Internacional de Dados. Abaixo, indicações de alguns mecanismos de ajuda aos agentes de tratamento para esclarecimento e direcionamento sobre qual modelo adotar:

- Resumo da matéria em passo a passo (como perguntas e respostas): São elaboradas perguntas estratégicas, e suas respostas levarão conhecimento aos agentes de tratamento. Após os esclarecimentos (inclusive com exemplos práticos hipotéticos) os mesmos conseguirão avaliar a necessidade da utilização das cláusulas-padrão:

Com base nas boas práticas adotadas pela Autoridade do Reino Unido – ICO1, temos que ela descreve perguntas chaves sobre o tema.
Exemplo: Quais são as restrições às transferências internacionais? Existe outra possibilidade de realização do seu negócio sem que ocorra a transferência internacional?
A cada pergunta respondida poderá existir links de direcionamento para modelos de cláusula-padrão ou demais conteúdo.

- Checkboxes com avaliação de caso concreto: Com perguntas básicas sobre o tratamento de dados, e sobre os agentes para quem se pretende transferir as informações. À medida que o agente de tratamento vai respondendo as perguntas (com sim ou não), ao final o resultado demostra o tipo de cláusula que ele deverá utilizar. Estará também descrito informações sobre o modelo de contrato que deverá ser aplicado e um link para o modelo em Word editável.

- Mapa mundial de adequação: Seguindo as boas práticas da Autoridade Francesa – CNIL2, deve-se elaborar um mapa mundial com descrição dos países adequados, países parcialmente adequados, países com Autoridade instituída, países com leis de proteção de dados e países sem lei específica.

Cada país terá sua cor de referência na legenda. Ao clicar no país que deseja transferir os dados, abre-se uma caixa ao lado trazendo informações relevantes e links de mais conteúdo e/ou modelo de contrato-padrão sugerido.

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

- Infográfico ilustrativo: Poderia ser elaborado um infográfico ilustrativo e simplificado com perguntas. A resposta do agente indicará qual a seta e caminho o agente deverá seguir (mecanismo de perguntas e resposta se sim ou não).

Sempre nos resultados poderá ser apresentado ainda mais conteúdo e o link do respectivo contrato aplicável. Segue um exemplo encontrado no site Eden Legal.

Referências

1 ICO - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#arewemaking (acessado em junho de 2022).

2 CNIL - https://www.cnil.fr/en/data-protection-around-the-world (acessado em junho de 2022).

3 EDEN LEGAL - https://www.edenlegal.com/blog/post.php?s=2016-07-20-infographic-international-data-transfers-from-the-eu (acessado em junho de 2022).

16. Quais as melhores alternativas para a resolução de conflitos entre agentes de tratamento e entre estes e titulares de dados envolvendo instrumentos contratuais de transferências internacionais de dados? Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de conflitos? Como?

Sugere-se a criação e a constituição de organismo intergovernamental ou órgão no âmbito de entidade intergovernamental já existente, competente para a resolução administrativa de tais conflitos. A entidade pode ser debatida e estruturada a partir de acordo multilateral inspirado nos tratados e convenções internacionais afetas à propriedade intelectual. Exemplificativamente, assim como os escritórios de propriedade intelectual em cada País signatário do Acordo e do Protocolo de Madrid, Acordo de Haia e ou Tratado de Cooperação em Matéria de Patentes têm e exercem interface direta com o Escritório Internacional da Organização Mundial da Propriedade Intelectual sito em Genebra, as respectivas autoridades nacionais de proteção de dados nutririam, nessa proposta, o fluxo e o intercâmbio de procedimentos – coordenando sua atuação conforme parâmetros de referido órgão ou entidade intergovernamental.

O fomento e a receita poderiam surgir de fundos solidários e compulsórios entre agentes que transfiram internacionalmente dados pessoais, compostos de contribuições proporcionais às especificidades do agente, do volume de dados pessoais, de avaliação econômica, patrimonial e financeira da empresa, conglomerado ou grupo econômico e a classe e espécies de dados pessoais transferidos. Isso, sem prejuízo de contribuição também por parte dos países e/ou blocos regionais signatários. O fundo mútuo destinar-se-ia à operacionalização da

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

entidade/órgão intergovernamental, incumbida de mediar, conciliar e dirimir conflitos entre agentes de tratamento e entre estes e titulares de dados.

Quando entre agentes de tratamento, a competência para a resolução do conflito verificar-se-ia conforme disposição em contrato. Nada dispondo esse e se tratando de contrato por adesão, da jurisdição da parte aderente ou da parte que não redigiu o contrato, se identificável. Tratando-se de contrato paritário, a competência seria verificada nos termos do foro eleito contratualmente e, no silêncio do contrato, no país em que sediado o proponente (em paralelo ao §2º do art. 9º da Lei de Introdução às Normas do Direito Brasileiro).

No que toca a conflitos envolvendo titulares, dada a hipossuficiência das pessoas naturais, faz-se necessário franquear a estas o acesso a tal entidade no país em que domiciliada, facilitando o acesso à jurisdição administrativa. Ainda, há de se pensar em mecanismos que garantam a acessibilidade e proteção adequada às partes hipossuficientes, garantindo o devido processo legal e o contraditório, assim como assegurando que as partes estão em simetria técnica e informacional com a disponibilização de pessoal competente e qualificado para orientação e esclarecimento, mitigando vantagens sistêmicas em prol de grandes litigantes. Sugere-se, ainda, sejam disponibilizados profissionais que orientem os titulares a serem mais práticos, eficientes e com uma boa ideia sobre os procedimentos.

O procedimento deve ocorrer eletronicamente em sua íntegra, permitindo apresentação de alegações, postulações e documentos. Sugere-se que a instância final seja órgão da Autoridade Nacional de Proteção de Dados Pessoais no Brasil e congêneres nos demais países signatários dos eventuais acordos multilaterais.

O procedimento poderia se dar no formato de resolução de disputas online (também conhecidas como ODR – *Online Dispute Resolution*). Há, no Brasil, exemplo de sucesso na seara do Direito do Consumidor; trata-se da plataforma *www.consumigor.gov.br*, lançada pelo Ministério da Justiça e Segurança Pública, em 2015. Na plataforma, partes (consumidores e empresas) dialogam e tentam resolver o conflito antes de uma solução heterocompositiva.

Nas questões afetas à proteção de dados pessoais em nível internacional e às transferências nesse particular, agentes de tratamento e pessoas naturais poderiam tentar solucionar o conflito, antes de uma decisão heterocompositiva pela entidade intergovernamental.

Vantagem desse modelo seria a otimização na gestão do tempo. Por meio de interações assíncronas, em detrimento de audiências, reuniões ou ligações, abrevia-se o procedimento e logra-se maior controle do momento voltado a essa atividade compositiva.

Assim como na plataforma *www.consumidor.gov.br*, a reclamação é apresentada contra a parte supostamente infratora ou ofensora, tendo essa até prazo razoável para analisar a reclamação e respondê-la. A parte solicitante pode avaliar o atendimento, encerrá-lo dando-se por satisfeita,

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

contrapropor medida diversa ou solicitar o encaminhamento do caso a órgão decisório, que conhecerá e apreciará a demanda, podendo determinar medidas cautelares ou satisfativas, providências, sanções, recomendações ou requisições.

Como os dados são públicos, viabilizaria pesquisa e criação de índices de solução, índices de satisfação, índices de prazo médio de resposta por fornecedor, propiciando sistema de monitoramento efetivo, que premia e propaga boas práticas na solução de demandas.

Os agentes que transferem internacionalmente dados pessoais se cadastrariam obrigatoriamente perante a plataforma, mediante portal operado e disponibilizado junto a cada autoridade dos respectivos países signatários. O arranjo, execução e coordenação de tal sistema poderiam ser capitaneados pela Autoridade Nacional de Proteção de Dados (ANPD) no exercício da competência disposta no inciso IX do art. 55-J da Lei Geral de Proteção de Dados Pessoais (LGPD).

Referências

1. HUSEK, Carlos Roberto. Curso de direito internacional público. — 14ª. ed. — São Paulo: LTr, 2017;

2. ÓPICE BLUM, Renato; MALDONADO, Viviane Nóbrega (coords). LGPD: Lei Geral de Proteção de Dados Comentada 2ª. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

20. Quais os mecanismos mais adequados para fornecer aos titulares a informação clara e relevante sobre a eventual transferência de seus dados pessoais para fora do Brasil bem como para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais? Como esses instrumentos devem ser implementados?

A necessidade de transferência internacional deve ser suficiente e claramente esclarecida ao titular, assim como quais dados estão envolvidos em tais transferências. Além das bases legais sob as quais são tratados os dados pessoais, objeto da transferência internacional, deve se garantir informação clara e transparente acerca da observância aos requisitos do art. 33 da LGPD.

Sugere-se que esses pontos sejam objeto de destaque nas políticas de privacidade, em contratos, termos de uso e, acaso autorizados pela via do consentimento, seja esse formalizado em estrita observância ao inciso VIII do art. 33 da LGPD.

Para que a informação seja útil a quem dela precisa ou para que surta os efeitos desejados, o destinatário das informações precisa ser o ponto focal, parte ativamente considerada na elaboração desses documentos de cunho jurídico ou técnico. O foco no usuário destinatário (em

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

especial a pessoa natural) dá, atualmente, a tônica nos modelos de negócio, nos comportamentos e no mercado. No caso dos contratos e demais documentos em que o receptor das informações é o cidadão-médio, leigo, mais importante se faz o emprego de medidas que facilitem a compreensão do conteúdo dos instrumentos. Medidas como fluxogramas, diagramas, exemplos, ilustrações, gráficos, tabelas, vídeos, animações, inteirações, *gamificação* e outras formas eficazes de comunicação são recomendáveis. A adoção de medidas tais concretiza, inclusive, a transparência – obrigação que se reflete em vários aspectos do Direito, notadamente nas relações de consumo e no âmbito da privacidade e da proteção de dados pessoais.

Outro aspecto de grande importância é a extensão do documento: documentos muito extensos tendem a não comunicar de forma eficaz o que se pretende. A capacidade de síntese e a noção do resultado pretendido são reflexos da empatia e do foco no leitor. Naturalmente, não se deve pretender suprimir informações, mas ter em mente que o contato do leitor com o documento de forma amigável e produtiva é o que vai viabilizar a produção do resultado pretendido.

Tais esclarecimentos, cláusulas, termos ou políticas devem privilegiar sempre frases curtas e na ordem direta. Além de auxiliarem na agilidade da análise do documento, apoiam o processo de compreensão, considerando que existem tantas interpretações possíveis quanto há leitores. Quanto mais objetiva for a exposição, menos margem para interpretações diversas daquela objetivada.

Linguagem acessível também está intimamente ligada à transparência, a qual, como dito, é privilegiada em vários aspectos da vida cotidiana e da ordem jurídica, seja no Brasil, seja em outros países. Partes em uma relação precisam compreender a extensão de seus direitos e deveres para que possam exercitar sua vontade e seus direitos da personalidade de forma livre e inequívoca. A falta de transparência tem consequências jurídicas indesejadas, e pode macular a própria relação contratual, pelo que são necessários os cuidados devidos com a apresentação e explicação do escopo, finalidade e necessidade da transferência internacional.

Também se faz pertinente a atuação educacional da ANPD, em continuidade às publicações, guias orientativos e fascículos já expedidos, no exercício da atribuição do art. 55-J, inciso VI da LGPD, promovendo à população orientação sobre questões pertinentes à transferência internacional de dados. Assim, municia-se a população para que esta também passe a fiscalizar tais operações internacionais de seu interesse.

Referências

1. FRANCO, Isabel (org). Guia Prático de Compliance. – 1ª ed. – Rio de Janeiro: Forense, 2020;

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

2. ÓPICE BLUM, Renato; MALDONADO, Viviane Nóbrega (coords). LGPD: Lei Geral de Proteção de Dados Comentada. 2ª. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.

MELISSA BARRIONI E OLIVEIRA
Presidente da Comissão de Proteção de Dados da OAB/MG

STELLA MUNIZ CAMPOS ELIAS
Vice Presidente da Comissão de Proteção de Dados da OAB/MG

RAFAEL SOARES MAGALHÃES
Diretor do Núcleo de Legislação e Jurisprudência da Comissão de Proteção de Dados da OAB/MG

MARIO PENIDO CAMPOS
Membro da Comissão de Proteção de Dados da OAB/MG

POLIANE ALMEIDA SILVA DIAS
Membro da Comissão de Proteção de Dados da OAB/MG

RICARDO GOMES FIGUEIROA
Membro da Comissão de Proteção de Dados da OAB/MG

SAVIO LUIZ MARTINS PEREIRA:09430908650 Assinado de forma digital por SAVIO LUIZ MARTINS PEREIRA:09430908650 Dados: 2022.06.29 09:34:12 -03'00'

SÁVIO LUIZ MARTINS PEREIRA
Membro da Comissão de Proteção de Dados da OAB/MG

ZapSign aab1a2ed-ba9e-4685-9176-f10c24bb0707. Documento assinado eletronicamente, conforme MP 2.200-2/2001 e Lei 14.063/2020.

COMMENTS OF THE AMERICAN BAR ASSOCIATION ANTITRUST LAW SECTION AND INTERNATIONAL LAW SECTION ON THE AUTORIDADE NACIONAL DE PROTECÃO DE DADOS (ANPD) CALL FOR CONTRIBUTIONS ON INTERNATIONAL TRANSFERS OF PERSONAL DATA

The views expressed herein are being presented on behalf of the Sections of Antitrust Law and International Law. They have not been reviewed or approved by the House of Delegates or the Board of Governors of the American Bar Association and, accordingly, should not be construed as representing the position of the Association.

June 30, 2022

The Antitrust Law Section and International Law Section (the "Sections") of the American Bar Association respectfully submit these comments in response to the ANPD's call for input on the regulation of international transfers of personal data under Brazil's General Data Protection Law (LGPD).

The Sections welcome the ANPD's open process. In releasing this call for public comment, the ANPD has encouraged a robust and informed dialogue on how to manage international data transfers. These comments are intended to further this dialogue and reflect the Sections' experience in international and cross-border data protection issues. The Sections' long involvement in these issues rests on the participation of both private and public sector lawyers, economists, and market participants, reflecting the interests of all those who engage in, benefit from, and enforce legal rights relating to digital as well as traditional commerce in which personal data plays an important role.

The Sections also welcome ANPD's questions about achieving consistency with other international data transfer regimes. In these Comments, the Sections make several suggestions that we believe both further the goals of modernization and harmonization and serve the desired balance between individual privacy and the development of information markets and services that benefit Brazilian nationals and the development of a global marketplace.

The Antitrust Law Section is the world's largest professional organization for antitrust and competition law, trade regulation, consumer protection, and data privacy as well as related aspects of economics. Section members, numbering over 7,600, come from all over the world and include attorneys and non-lawyers from private law firms, in-house counsel, non-profit organizations, consulting firms, federal and state government agencies, as well as judges, professors, and law students. The Antitrust Law Section provides a broad variety of programs and publications concerning all facets of antitrust and the other listed fields. Numerous members of the Antitrust Law Section have extensive experience and expertise regarding similar laws of non-U.S. jurisdictions. For thirty years, the Antitrust Law Section has provided input to enforcement agencies around the world conducting consultations on topics within the Section's scope of expertise.[1]

[1] Past comments of the Antitrust Law Section are available at https://www.americanbar.org/groups/antitrust_law/resources/comments_reports_amicus_briefs/.

The International Law Section focuses on international legal issues, the promotion of the rule of law, and the provision of legal education, policy, publishing, and practical assistance related to cross-border activity. Its members total over 10,000, including private practitioners, in-house counsel, attorneys in governmental and inter-government entities, and legal academics, and represent over 100 countries. The International Law Section's more than 50 substantive committees cover competition law, trade law, and data privacy and data security law worldwide as well as areas of law that often intersect with these areas, such as regulatory compliance, mergers and acquisitions and joint ventures. Throughout its century of existence, the International Law Section has provided input on debates relating to international legal policy.[2] The International Law Section has provided input for decades to authorities around the world.[3]

I. Executive Summary

Data is a critical element of the modern global economy. Effective regulation of the cross-border transfer of personal data must balance several interests, including: (1) businesses' increasing need for, and reliance on, the flow of data around the globe as a means of maintaining competitiveness and innovation; (2) individuals' rights to have control over their personal data; and (3) governments' imperatives to protect individual data rights as well as their own interests in national security, economic security, law enforcement, and other public interests. Examples of regulation of cross-border data transfers include the European Union General Data Protection Regulation (GDPR) model; the APEC privacy framework; China's Personal Information Protection Law and information security regulations; and the more liberal transfer model in the United States. All models are still evolving.

Brazil today is one of the largest countries by population with a federal data protection law in force. Considering that Brazil is also one of the largest economies worldwide, with many multinational and national companies doing business locally and around the globe, it is of paramount importance that its data transfer regulation be consistent with international standards and best practices.

The Sections respectfully make the following suggestions:

- ***Contractual instruments:*** The ANPD can promote convergence and interoperability by approving standard contractual clauses (SCCs) as an option for cross-border data transfers in the absence of an adequacy finding, binding corporate rules (BCRs), or mechanism similar to the proposed Trans-Atlantic Data Privacy Framework. SCCs are currently the most commonly used instrument by companies and organizations of all sizes, and usher in uniformity for data transfers internationally. In principle, SCCs that allow parties to use annexes to provide more detailed information on the data transfer—with different provisions based on whether the transfer is controller to controller, controller to processor, processor to processor, or processor to controller—provide a workable approach to maintaining uniformity.
- ***Binding Corporate Rules:*** The Sections suggest that the ANPD develop requirements for

[2] American Bar Association, International Law Section Policy, available at https://www.americanbar.org/groups/international_law/policy/about/.

[3] Past comments of the International Law Section are available at https://www.americanbar.org/groups/ international_law/policy/blanket_authorities_initiatives/.

BCRs that would be applicable for corporate groups. The ANPD should also develop mechanisms to analyze and approve BCRs. BCRs and SCCs are applied in different situations—they are largely complementary approaches—and therefore their requirements should be different from one another. The ANPD could build on standards already established by the European Commission for BCR submission and approval. The definition of a corporate group for the purpose of application of BCRs should be in line with the rules that are established by Brazil's antitrust authority, CADE, under the competition laws.

- ***Adequacy criteria and contractual instruments:*** The former EU-U.S. Privacy Shield and proposed successor, the Trans-Atlantic Data Privacy Framework, provide a model for ensuring adequacy at company level. This approach includes alignment with the adequacy criteria and providing recourse to resolve data subject and controller/processor complaints.
- ***Managing access by foreign public authorities to data:*** The Sections urge the ANPD to ensure that any obligations imposed on the data exporter in relation to government access are reasonable and practical. Most notably, the ANPD should take a realistic view in assessing contractual, organizational, or technical safeguards to ensure that access by government authorities is lawful. Data importers could contractually be required to inform the data exporter of such foreign government access only if (1) the data importer knew or should have known of such access; and (2) is permitted by law to provide notice to the data exporter of such access.
- ***Accountability for the handling of data in a foreign jurisdiction:*** The Sections recommend that data subjects be informed of changes in the location of processing that materially increase risks to their privacy interests. Any right to intervene should be limited to situations in which harm can result from the material change, such as if the location to which the data is imported has been identified to present a risk. Conflicts between the data subject and a processing agent should be addressed by means of a regulatory scheme or, as the ANPD suggested in the inquiry, through multilateral cooperation processes between data protection authorities. Resolution of disputes between processing agents should be addressed by contractual provisions similar to those in the GDPR SCCs, ensuring that they are aligned with other data protection regimes.

II. Specific Suggestions

1. Contractual Instruments

ANPD question (2): "What is the best way to promote convergence and interoperability between contractual instruments for international data transfers with instruments from other jurisdictions? And how can ANPD act in this regard?"

Standard contractual clauses are commonly used tools to promote interoperability between the EEA and non-EEA jurisdictions in addition to independent privacy assessments completed by the parties to the contract. SCCs are standard terms that are integrated into contracts between data controllers and/or processors. On June 4, 2021, the European Commission published new SCCs to

govern international data transfers from EEA controllers or processors to non-EEA controllers or processors.[4]

The ANPD can promote convergence and interoperability by approving SCCs for all cross-border data transfers and requiring companies and organizations to conduct their own privacy assessments; but SCCs should be one option that companies can choose if they are appropriate for a given data transfer. As discussed below, other approaches—such as the APEC Cross-Border Privacy Rules and the proposed Trans-Atlantic Data Privacy Framework—also deserve the ANPD's consideration. Any additional requirements to assess privacy risks arising from a cross-border transfer should reflect specific gaps between other jurisdictions' regulations and requirements set forth by the LGPD.

ANPD question (3): "What are the most effective and the most used instruments to enable international data transfers by large and small companies or organizations?"

SCCs are currently the instrument most commonly used by companies and organizations of all sizes and provide uniformity for data transfers internationally. Because not all companies or organizations have the same resources, the ability to rely on the same clauses allows small businesses to keep pace with large multinational companies and organizations. However, SCCs should not be the sole or presumed means of transferring personal data from Brazil. For instance, BCRs may be a better fit for multinational companies and organizations with the proper resources and a need to conduct long-term intra-company transfers. BCRs are discussed further below.

ANPD question (7): "Should the standard contractual clauses be rigid and with predefined content, or should their regulation allow certain flexibility concerning the text of the clauses, specifying the desired results, and allowing changes as long as they do not conflict with the standard text made available?"

Under the European Commission's model, SCCs cannot be modified by the parties "except (i) to select modules and/or specific options offered in the text, (ii) to complete the text where necessary (indicated by square brackets), e.g. to indicate the competent courts and supervisory authority, and to specify time periods, (iii) to fill in the Annexes or (iv) to add additional safeguards that increase the level of protection for the data."[5] This approach helps to maintain uniformity, provided that data importers and exporters may use annexes to provide more detailed information on the data transfer.

ANPD Question (8): "What would be the most appropriate format for ANPD to make available models of standard contractual clauses for international data transfers? Are there any relevant tools that could be used to this end (e.g., decision tree, forms, checkboxes)? Are there any experiences on the theme that could serve as an example for ANPD?"

An appropriate format for the ANPD to make SCCs available would be as an editable document in common formats. Providing SCCs in common, editable formats would also allow

[4] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

[5] https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf.

companies and organizations to add required information, including any annexes that provide details about the specific data transfer at issue.

"9) Is it necessary to have different rules depending on the type of processing agents (e.g., specific modules for controllers or processors) as data exporters or importers in international data transfers based on contractual clauses? If so, what would they be?"

The SCCs should reflect all potential arrangements between controllers and processors, as with the SCCs that the European Commission approved in 2021. The four sets of SCCs—controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller—establish contractual obligations that align with each party's underlying legal obligations, e.g., with respect to data subject rights, liability, and supervision.

2. Binding Corporate Rules

ANPD question (10): "Are there requirements that need to be different for Binding Corporate Rules from those usually required for Standard Contractual Clauses? If so, what would they be?"

Even though BRCs and SCCs have similar purposes, they are applied in different situations and should be governed by different requirements. While SCCs can be applied for companies with less complex data flows, BCRs are more suitable for scenarios with a higher level of complexity and more data subjects.

To promote consistency internationally and efficiency for companies that have already obtained approval for BCRs under the GDPR, the Sections suggest following the criteria set forth in Article 47 (2) of GDPR,[6] which include:

> *(i) the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;*
>
> *(ii) the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;*
>
> *(iii) the application of the general data protection principles;*
>
> *(iv) the complaint procedures;*
>
> *(v) the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority; and*
>
> *(vi) the appropriate data protection training to personnel having permanent or regular access to personal data.*

[6] https://gdpr-info.eu/art-47-gdpr/.

Although BCRs are a valuable and effective tool for data protection, the approval process under the GDPR has proven to be a significant barrier to using them. The Sections understand that companies will need to provide information and documents to demonstrate how their transfer will comply with the LGPD and prove the existence of company structure (formally and technically) capable of guaranteeing the application of such rules. However, the ANPD could consider ways to provide a more efficient review and approval procedure. Otherwise, the regulatory approval of BCRs would create a large obstacle for companies whose economic activities are directly affected by their data transferring capabilities.

ANPD question (11): "How should a corporate group be defined for the purpose of application of Binding Corporate Rules?"

The Sections submit that the definition of a corporate group for the purpose of application of BCRs should be in line with other relevant Brazilian legislation. In particular, the Sections suggest application of the rules that CADE has established within the scope of Brazil's competition laws. CADE's Resolution No. 33/2022 sets two conditions to define what should be considered as a corporate group:

1. Companies that are in common, internal or external control; and
2. Companies in which a company holds, directly or indirectly, at least 20% (twenty percent) of the capital stock or voting capital.[7]

In addition, CADE has already decided that the existence of relevant influence in the decision making of a company can also be considered for the definition of a corporate group. This idea is very similar to how the GDPR describes corporate groups:

> *"(37) A group of undertakings should cover a controlling undertaking and its controlled undertakings, whereby the controlling undertaking should be the undertaking which can exert a dominant influence over the other undertakings by virtue, for example, of ownership, financial participation or the rules which govern it or the power to have personal data protection rules implemented. An undertaking which controls the processing of personal data in undertakings affiliated to it should be regarded, together with those undertakings, as a group of undertakings."*

We understand that the use of these parameters to determine the concept of corporate group would be essential to: (i) follow the concepts that are already incorporated in Brazilian legislation and used by other relevant authorities, without creating completely new and complex rules; and (ii) maintain a certain level of harmony with the parameters that are already set in the GDPR.

ANPD question (13): "What are the risks and benefits of allowing transfers between different economic groups whose binding corporate rules have been approved by ANPD?"

[7] The Sections note that the 20% ownership rule expands the scope of corporate groups beyond definitions applicable in many other countries, sometimes creating complexity when the rule is applied in the pre-merger notification context. Nevertheless, the Sections believe the benefit of uniform application of the group definition across competition and data protection law outweighs potential disadvantages of its expansive scope.

BCRs have become a more attractive option after the EU's invalidation of the EU-U.S. Privacy Shield framework and to avoid the inefficiencies of SCCs for certain types of cross-border data transfers. There are, however, complex trade-offs involved with allowing data transfers under BCRs of different economic groups. The benefits and risks of this approach include the following:

Advantages:

1. Once approved, BCRs allow and facilitate consistent and continuous international data transfers within the economic groups.
2. BCRs significantly increase flexibility, as in case of changes in a company's flow of data transfers or the company structure. In addition, once approved by the data protection authority the updates generally do need not be approved again.
3. BCRs can reduce the exposure of the organization by setting a high standard for data protection compliance with the law, understanding the requirements of BCRs, and improving the company's internal data privacy policy.
4. From a brand perspective, the implementation of BCRs sends a public signal about the seriousness of the company when data protection responsibilities are mentioned, and that the company desires to be transparent with the authority and regulators.
5. The approval of BCRs is an attractive option for economic groups to achieve compliance with data protection laws worldwide and can help organizations obtain international certificates of compliance with privacy standards.

Disadvantages:

1. Based on experience in other jurisdictions, it can take a long time to obtain the approval of BCRs (up to 18 months).
2. BCRs can be used only for international transfers within the same economic group. That means that other data export protection solutions will be required when transferring personal data to third parties.
3. Since the BCRs are not used universally, they may not be appropriate for all types and situations of international data transfer.

ANPD question (14): "Are there any experiences with the verification and approval of specific contractual clauses and binding corporate rules that could serve as an example for ANPD?"

The European Union and United Kingdom institutions provide several relevant documents regarding their procedures for approval of BCRs. The new SCCs approved in the EU and UK do not require verification or approval for their use by companies. The Sections recommend that the ANPD follow that same approach regarding SCCs.

To start the approval procedure for BCRs, the European data protection authorities analyze forms submitted by interested companies and decide whether they comply with the legal

requirements of Articles 47 and 63 of the GDPR and documents approved by the Article 29 Working Party and endorsed by the EDPB.[8]

The European Data Protection Board (EDPD) develops an opinion on the approval of the BCR based on a draft decision from the competent authority. If it complies with the law, the competent authority will approve the request.

The EDPB[9] and ICO[10] provide a section on their websites with all approved BCRs and the companies that use the instrument. The EDPB's published list indicates BCRs that the European authorities have approved since 2018 and contains the decisions and further information for each approved BCR.

3. Adequacy determinations

ANPD question (6): "To what extent should the elements to be considered by ANPD in assessing the level of data protection of foreign countries or international bodies for adequacy purposes (article 34 of the LGPD) also be taken into account within the scope of the rules for contractual instruments?"

Article 34 of the LGPD provides that in the Assessment of the Data Protection Level of the Recipient Country(ies) the ANPD "will take into consideration: I - the general and sectoral rules of the legislation in force in the country of destination or in the international body; II - the nature of the data; III - compliance with the general principles of protection of personal data and rights of the holders provided for in this Law; IV - the adoption of security measures provided for in the regulation; V - the existence of judicial and institutional guarantees to respect personal data protection rights; and VI - other specific circumstances relating to the transfer."

To a large extent, this is the model used for the EU-U.S. Privacy Shield framework and the successor program that has been agreed to in principle, the Trans-Atlantic Data Privacy Framework.[11] Key elements of this approach include compliance with (and annual recertification of compliance with) the GDPR principles while allowing businesses to create compliance programs appropriate and proportional to their activities and operations.[12] Another key element of this framework is a dispute resolution mechanism to provide EU data subjects with recourse against violations of their rights. This approach provides specificity as well as flexibility to determine adequacy on a business-specific level, taking into account the size and scope of a company. This approach also allows companies that are subject to multiple national and regional

---

8 https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en.

9 https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en.

10 https://ico.org.uk/for-organisations/binding-corporate-rules/.

11 https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/25/fact-sheet-united-states-and-european-commission-announce-trans-atlantic-data-privacy-framework/.

12 *See* GDPR Recital 4 ("The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.").

data protection regulations to use and build on privacy programs that govern compliance with applicable laws.

4. Managing access by foreign public authorities to data

ANPD question (19): "What obligations should be assigned to the importer and exporter in case of access to data by foreign public authorities?"

Access to data by foreign public authorities has been a key issue under the EU GDPR model. The Court of Justice of the European Union (CJEU) invalidated the EU–U.S. Privacy Shield framework in the *Schrems II* case[13] because it found that Privacy Shield did not provide data protection at a level "essentially equivalent" to European legal standards, based on the CJEU's view of the breadth of certain US surveillance authorities and the limitations on individual redress under Privacy Shield. Following *Schrems II*, the European Commission and EDPB released measures for EU-based entities to undertake prior to transferring data outside the European Economic Area (EEA). One of the steps is to assess the proposed transfer under the surveillance laws of the recipient country to determine whether an adequate level of protection is afforded. This assessment is to be carried out under the European Essential Guarantees for Surveillance Measures Recommendations issued by the EDPB in November 2020.[14] Thus, the EU has imposed obligations on the data exporter to be implemented before the data is exported and thus prior to access by a foreign public authority.

The Sections submit that the ANPD should ensure that any transfer risk assessment obligations imposed on the data exporter be reasonable and practical. Most notably, the ANPD should take a realistic view of the effectiveness of contractual, organizational, or technical supplementary measures to ensure that access requests by foreign governments are lawful. The Sections also respectfully urge the ANPD to allow the data exporter to take a risk-based approach relying on (i) the likelihood that the data exporter is actually subject to the legal requirement to provide foreign governments access in light of the nature of exporter's business and (ii) the likelihood that even if it is, a foreign government will in fact make an access request in light of the type of data collected. In many instances, that risk is minimal.

As to the obligations of the data importer, the ANPD could consider requiring notification of the data exporter of foreign government access only if (1) the data importer knew or should have known of such access, and (2) is permitted by law to provide notice to the data exporter of such access.

5. Accountability for the handling of data in a foreign jurisdiction

---

[13] *Data Protection Commissioner v. Facebook Ireland Limited, Maximillian Schrems* (C-311/18) July 16, 2020. Privacy Shield replaced the Safe Harbor framework which was invalidated by the CJEU in 2015 in *Schrems I* because it did not restrict the US government's ability to collect and use personal data or grant individuals sufficient legal remedies when their personal data was collected by the US government.

[14] https://edpb.europa.eu/our-work-tools/our-documents/recommendations/recommendations-022020-european-essential-guarantees_en.

ANPD question (15): "What are the data subject's rights in case of changes in the original configuration of the transfer? In which situations is it essential to communicate directly with the data subjects or to enable some type of intervention by them?"

ANPD question (20): "What are the most appropriate mechanisms to provide data subjects with clear and relevant information about the possible transfer of their personal data outside of Brazil as well as to ensure the adequate protection of data subjects' rights in international data transfers? How should these instruments be implemented?"

The Sections suggest that the ANPD focus on materiality as a guide to creating additional notice or other requirements relating to changes in cross-border data transfer arrangements. Where the data importer is a processor, many of the likely changes to the configuration of the data transfer would be of a minimal, non-material nature. Because data processors, which are the likely data importers, are obligated to process data according to the data controller's instructions, the data processor cannot make significant changes to the configuration of the transfer without appropriate instruction from the data controller.

However, it is possible to identify situations where change to the processing would be so significant that it would be considered a change to the terms under which the data subject provided the data – for example, if the location to which the data is imported is changed. In those scenarios, requiring the data exporter to notify the data subject could be appropriate. Finally, any notice requirement should take into account research and experience with providing *effective* notice.[15]

ANPD question (16): "What are the best alternatives for resolving conflicts between processing agents and/or between those agents and data subjects involving contractual instruments for international data transfers? Could bilateral, multilateral or international cooperation between data protection authorities assist in conflict resolution? If so, how?"

As a general matter, contracts between processing agents do not create rights for third parties, i.e., data subjects. The SCCs[16] recognized by the EU, UK, and Switzerland address this issue through their third-party beneficiary provisions. It is reasonable to create a similar set of clauses to address such transfers under the LGPD. It is important to assure, however, that they are aligned with other data protection regimes, including the APEC Cross-Border Privacy Rules.[17]

III. Conclusion

The Sections appreciate the opportunity to provide this comment and would be pleased to answer any questions about the matters discussed herein.

---

15 *See, e.g.*, Amanda Grannis, *You Didn't Even Notice! Elements of Effective Online Privacy Policies*, 42 FORDHAM URB. L.J. 1109 (2015), *available at* https://ir.lawnet.fordham.edu/ulj/vol42/iss5/1; *We Read 150 Online Privacy Policies. They were an Incomprehensible Disaster*, N.Y. TIMES, June 12, 2019.

16 *See* n.4 above.

17 https://www.apec.org/About-Us/About-APEC/Fact-Sheets/What-is-the-Cross-Border-Privacy-Rules-System.

Anexos complementares para Tomada de Subsídios junto à ANPD | Transferência Internacional de Dados

Joana Cavalheiro Teixeira [redacted]

Qui, 30/06/2022 16:33

Para:

- ANPD - Normatizacao <normatizacao@anpd.gov.br>

5 anexos (4 MB)

(EYG) Política de Processamento de Regras Corporativas Vinculantes.pdf; (EYG) Política de Processamento das Regras Corporativas Vinculativas do Reino Unido.pdf; (EYG) Política de Controladoria de Regras Corporativas Vinculativas.pdf; (EYG) Política de Controladoria de Regras Corporativas Vinculativas do Reino Unido.pdf; DECISÃO DE EXECUÇÃO (UE) 2021-914 DA COMISSÃO.pdf;

Prezados, boa tarde.

Seguem os anexos complementares as minhas respostas quanto à tomada de subsídios sobre transferências internacionais de dados pessoais.

Precisando de algum esclarecimento adicional, fico à disposição.

Atenciosamente,

Joana Cavalheiro Teixeira

EY
Data Protection Binding Corporate Rules Processor Policy

30 September 2020

Building a better working world

Contents

Introduction to the Data Protection Binding Corporate Rules Processor Policy **3**

Part I: Background and actions **4**

Part II: The Rules **7**

PART III: Appendices **13**

Appendix 1 13

Data privacy roles and responsibilities 13

Appendix 2 16

Subject Access Request Procedure 16

Appendix 3 19

Assessment of Compliance Protocol 19

Appendix 4 21

Complaint Handling Procedure 21

Appendix 5 23

Cooperation Procedure 23

Appendix 6 24

Updating Procedure 24

Appendix 7 25

Privacy Training Program 25

Appendix 8 26

Law Enforcement Data Access Procedure 26

Introduction to the Data Protection Binding Corporate Rules Processor Policy

EY has established a foundation for the privacy of all personal data, which is processed worldwide in its global personal data privacy program ("**global privacy program**"). The global privacy program comprises a series of policies and procedures, which set out the principles to be applied to the processing of personal data within EY.

One of the policies forming part of the global privacy program is this Data Protection Binding Corporate Rules Processor Policy ("**Processor Policy**"). In this Processor Policy, we use "**EY**" to refer to the global organization of independent member firms ("**EY Member Firm**")[1] and other entities in the EY organization ("**EY Network entity**"),[2] which are bound to comply with the requirements of Ernst & Young Global Limited ("**EYG**"). EYG is the central governance entity of the EY organization and coordinates EY Network entities and the cooperation among them.

This Processor Policy has been created to establish EY's approach to compliance with European[3] data protection law and specifically to transfers of personal data between EY Network entities where such EY Network entities are acting as processors.

All EY Network entities[4] and their partners, directors, employees, new hires, individual contractors and temporary staff ("**EY Personnel**") must comply with, and respect, this Processor Policy when processing[5] personal data as a processor, irrespective of the country in which they are located.

This Processor Policy applies to data received from a controller established in the EU which is not an EY Network Entity ("**Controllers**") and then processed by EY Network entities as processor or sub-processor.

The Processor Policy contains 15 rules ("**Rules**") that govern the processing of personal data of current, past and prospective EY Personnel, clients, suppliers, subcontractors and any other third parties ("**EY Data**").

This Processor Policy applies to all EY Data wherever it is processed as part of the regular business activities of EY. Transfers of personal data take place between EY Network entities during the normal course of business and such data may be stored in centralized databases accessible by EY Network entities from anywhere in the world. Each EY Network entity and its EY Personnel shall respect the instructions regarding the data processing and the security and confidentiality measures as provided in the contract or other binding document that such EY Network entity enters into with the Controller.

This Processor Policy is accessible on EY's website at ey.com/bcr.

[1] EY Member Firm means any corporation, partnership or other entity or organization that is admitted from time to time as members of Ernst & Young Global Limited pursuant to the regulations of Ernst & Young Global Limited.
[2] EY Network entity means any one of the network of entities comprising Ernst & Young Global Limited, EYGN Limited, EYGM Limited, EYGS LLP, EYGI B.V., EY Global Finance, Inc. and their members. It also means any entity controlled by any such entity, under common control with any such entity, or controlling such entity or any corporation, partnership, or other business organization that is a member firm or a subsidiary of the entity, or which is directly or indirectly a majority owned or controlled subsidiary of the entity, together with any partner, director, employee or agent of any such entity. For the purposes of this definition, "control" means (a) ownership, either directly or indirectly, of equity securities entitling either such entity to exercise in the aggregate of at least 50% of the voting power of such entity in question; or (b) possession, either directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity in question, whether through ownership of securities, by contract or otherwise.
[3] For the purpose of this Processor Policy, reference to Europe means the European Economic Area (EEA) and Switzerland and European should be construed accordingly.
[4] The list of the EY Network entities providing services to Clients who are bound by the Processor Policy is accessible on EY's website at ey.com/uk/en/home/legal via "View a list of EY member firms and affiliates".
[5] "Processing" in European data protection law means any set of operations performed upon personal data, whether or not by automatic means. This is interpreted widely to include collecting, storing, organizing, destroying, amending, consulting, destroying and disclosure of the personal data.

All Rights Reserved – EY

Part I: Background and actions

What is data protection law?

Data protection law gives people the right to control how their "**personal data**"[6] is used. When EY processes EY Data, this is covered and regulated by data protection law.

Data protection law distinguishes between the concepts of "**controller**" and "**processor**". The controller determines, alone or jointly with others, the purposes and the means of the processing of personal data. The processor, on the other hand, processes personal data on behalf of the controller.

For the majority of professional services, EY is acting as a controller, processing personal data in accordance with its own strict professional obligations. For a limited type of professional services, EY will be acting as a processor under the detailed instructions of the Controller. For services where an EY Network Entity acts as a controller in relation to another EY Network entity acting as controller or as 'internal processor', EY shall comply with the Data Protection Binding Corporate Rules Controller Policy ("**Controller Policy**") as published on ey.com/bcr. For services where EY acts as a processor, this Processor Policy applies.

How does data protection law affect EY internationally?

European data protection law does not allow the transfer of personal data to countries outside Europe that do not ensure an adequate level of data protection[7]. Some of the countries in which EY operates are not regarded by European supervisory authorities as providing an adequate level of protection for individuals' data privacy rights.

When EY acts as a processor, the Controller retains the responsibility to comply with European data protection law. Controllers in Europe will pass certain data protection obligations on to EY in the contracts or other binding documents EY has with them. Consequently, if EY fails to comply with the terms of a contract or other binding document it enters into with a Controller, the Controller may be in breach of applicable data protection law and EY may face a claim for breach of contract, which may result in the payment of compensation or other judicial remedies.

In such cases, if a Controller demonstrates that it has suffered damage, and that it is likely that the damage has occurred due to a breach of the Processor Policy by an EY Network entity outside Europe (or a third party sub-processor established outside Europe), that Controller is entitled to enforce the Processor Policy against EY and, in such cases, the obligation will be on the EY Network entity accepting liability (namely the EY Network entity that is a party to the contract or other binding document with the Controller) to demonstrate that the EY Network entity outside Europe (or the third party sub-processor established outside Europe) is not responsible for the breach, or that no such breach took place.

What is EY doing about it?

EY must take proper steps to ensure that it processes personal data on an international basis in a safe and lawful manner. This Processor Policy sets out a framework to satisfy the standards contained in European data protection law and, in particular, to provide an adequate level of protection for all personal data processed in Europe and transferred to EY Network entities outside Europe, where the personal data is collected by a Controller in Europe.

Although the legal obligations under European law apply only to personal data processed in Europe, EY will apply this Processor Policy globally whenever it acts as a processor, and in **all cases** where EY processes EY Data both manually and by automatic means.

EY will apply the Rules contained in this Processor Policy whenever it acts as a processor on behalf of a Controller. Where the Controller relies upon this Processor Policy as providing adequate safeguards, an obligation to comply with this Processor Policy will be included in the contract or other binding document EY has with the Controller and a copy of this Processor Policy will be incorporated into such contracts or other binding documents or referenced with a possibility of electronic access. If the Controller chooses not

[6] Personal data means any information relating to an identified or identifiable natural person in line with the definition in the EU Data Protection Regulation 2016/679.
[7] Several exceptions to this rule can be applicable.

All Rights Reserved – EY

to rely upon this Processor Policy, that Controller is responsible for putting in place another adequate safeguard to protect the personal data.

All EY Network entities who process personal data in a capacity as processor under the instructions of a Controller, must comply with the Rules set out in **Part II** of this Processor Policy together with the policies and procedures set out in the appendices in **Part III** of this Processor Policy.

For the avoidance of doubt:

- Where EY acts as a controller (or as processor under the instructions of another EY Network Entity), EY shall comply with the Controller Policy as published on ey.com/bcr. EY Network entities may act as both a controller and a processor and must therefore comply with both the Processor Policy and the Controller Policy.
- For some internal administrative processes and for compliance with regulatory requirements, EY will always act as a controller in its own right (e.g., compliance with regulatory requirements, to check conflicts, for quality, risk management or financial accounting purposes and for the provision of internal administrative or IT support services). For such processes, EY shall comply with the Controller Policy.

What does this mean in practice for personal data processed in the EEA?

Under European data protection law, individuals both within and outside Europe whose personal data is processed in Europe by a Controller and transferred to an EY Network entity outside Europe under the Processor Policy have certain rights. These individuals may enforce the Rules set out in this Processor Policy as third-party beneficiaries where they are not able to bring a claim against the Controller in respect of a breach of any of the commitments in this Processor Policy by an EY Network entity (or by a sub-processor) acting as a processor (for example in case the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law).

In such cases, these individuals' rights are as follows:

- **Complaints**: Individuals may complain to the Controller established in Europe in accordance with the Complaint Handling Procedure (as set out in Appendix 4 of this Processor Policy) and to a European supervisory authority in the jurisdiction of the Controller responsible for exporting the data outside Europe.
- **Liability**: Individuals may bring proceedings against the Controller responsible for exporting the data outside Europe:
  - In the courts of the country where the Controller responsible for exporting the data is established
  - In the jurisdiction from which the personal data was transferred

    Or
  - In the courts of the jurisdiction of the EEA Member State where the individual resides
- **Compensation**: Individuals may seek appropriate redress from the Controller established in Europe and responsible for exporting the data (including the remedy of any breach of this Processor Policy by an EY Network entity outside Europe) and where appropriate, receive compensation from the Controller established in Europe and responsible for exporting the data for any damage suffered as a result of a breach of this Processor Policy by:
  - An EY Network entity established outside Europe.

    Or
  - Any third-party processor that is established outside Europe and is acting on behalf of an EY Network entity inside Europe or outside Europe, in accordance with the determination of the court or other competent authority.
- **Transparency**: Individuals may obtain a copy of this Processor Policy by accessing the Processor Policy on EY's website: ey.com/bcr.

In the event of a claim being made in which an individual has suffered damage, where that individual can demonstrate that it is likely that the damage has occurred because of a breach of the Processor Policy, EY has agreed that the burden of proof to show that (i) an EY Network entity outside Europe or (ii) any third-party sub-processor who is established outside Europe and who is acting on behalf of an EY Network entity

outside Europe is not responsible for the breach, or that no such breach took place, will rest with the EY Network entity responsible for exporting the personal data to the EY Network entity outside Europe.

Data protection roles and responsibilities

The EY Global Privacy Leader[8] is the person who has overall responsibility for compliance with the Processor Policy and any other supporting policies and procedures.

Area Privacy Leaders are responsible for overseeing compliance with this Processor Policy by the EY Network entities within their area on a day-to-day basis.

A description of the roles and responsibilities of the EY global privacy team is set out in Appendix 1.

Further information

If you have any questions regarding the provisions of this Processor Policy, your rights under this Processor Policy or any other data privacy issues, you may contact the EY Global Privacy Leader who will either deal with the matter or forward it to the appropriate person or department within EY at the following address:

EY Global Privacy Leader

Email: global.data.protection@ey.com

Address: Office of the General Counsel (GCO), 6 More London Place, London, SE1 2DA.

The Global Privacy Leader is responsible for ensuring that changes to this Processor Policy are notified to the EY Network entities and to individuals whose personal data is processed by EY via the EY website at ey.com/bcr.

[8] At present EY's Global Lead Counsel Privacy and Security serves as the Global Privacy Leader as referenced in the BCRs.

Part II: The Rules

The Rules are divided into two sections. Section A addresses the basic principles of European data protection law EY must observe when EY processes personal data as a processor.

Section B deals with the practical commitments made by EY to the competent supervisory authority (the "Autoriteit Persoonsgegevens" in the Netherlands) in connection with this Processor Policy.

Section A

Rule 1 — Compliance with local law

Rule 1A — EY will first and foremost comply with local law where it exists.

EY will comply with any applicable legislation relating to personal data and will ensure that, where personal data is processed as a processor, this is done in accordance with applicable local law.

Where local legislation relating to personal data requires a higher level of protection for personal data, such legislation will take precedence over this Processor Policy.

Where there is no law or the law does not meet the standards set out by the Rules in this Processor Policy, EY's position will be to process personal data adhering to the Rules in this Processor Policy.

Rule 1B — EY will cooperate and assist a Controller to comply with its obligations under local law in a reasonable time and to the extent reasonably possible.

EY will, within a reasonable time and to the extent reasonably possible, as required under the contract or other binding document it has entered into with a Controller, assist such Controller to comply with its obligations under applicable data protection law.

Rule 2 — Ensuring transparency and using personal data for a known purpose only

Rule 2A — EY will assist a Controller to comply with the requirements to *explain to individuals* how their data will be used and to be transparent about data processing activities.

The Controller has a duty to explain to individuals how their personal data will be processed (for example, by providing a privacy notice or privacy statement). EY will assist a Controller, insofar as this is possible, to comply with this requirement.

EY will follow this Rule 2A unless there is a legitimate basis for not doing so, for example, where it is necessary to safeguard national security or defense, for the prevention or detection of crime, legal proceedings or where otherwise permitted by law.

Rule 2B — EY will only obtain and use personal data on behalf of and in accordance with the instructions of the Controller.

EY will only process personal data on behalf of and in compliance with the (lawful) instructions of a Controller, as specified in the contract or other binding document it has with such Controller. Where the Controller relies upon this Processor Policy as providing adequate safeguards, an obligation to comply with this Processor Policy will be included in the contract or other binding document and a copy of this Processor Policy will be incorporated into such contract or other binding document or referenced with a possibility of electronic access. Where the personal data is subject to European data protection law, the contract or other binding document between EY and the Controller will include the required elements as provided by article 28 of the EU General Data Protection Regulation ("GDPR").

If EY is unable to comply with this Rule or its obligations under this Processor Policy, EY will inform the Controller promptly of this fact. The Controller may then take appropriate action (such as suspending the transfer of personal data and terminating the contract or other binding document it has with EY).

All Rights Reserved — EY

Rule 3 — Ensuring data quality

Rule 3A — EY will assist the Controller to keep personal data *accurate* and *up to date*.

EY will act upon the instructions of the Controller in order to help and assist such Controller to comply with its obligations to keep personal data accurate and up to date. EY shall execute any necessary measures when asked by the Controller in order to have the personal data updated or corrected.

When required to do so on instruction from a Controller, as required under the terms of the contract or other binding document with that Controller, EY will delete, anonymize, update or correct personal data.

EY will notify other EY Network entities or any third-party sub-processors to whom the personal data has been disclosed accordingly so that they can also update their records.

Rule 3B — EY will only keep personal data in a form which permits identification for *as long as is necessary*.

Personal data will always be retained and/or deleted or anonymized to the extent required by law, regulation and professional standards, under the instructions of the Controller (provided such instructions do not conflict with such law, regulation and professional standards) and in line with the applicable EY service lines and any local retention policies applying to an EY Network entity. EY will dispose of personal data only in a secure manner in accordance with EY global security policies.

On the termination of the provision of professional services to a Controller, EY will — at the choice and at the request of the Controller — return all the personal data transferred and the copies thereof to the Controller or destroy all the personal data (except for backup copies) and certify to the Controller that it has done so. If applicable legislation or professional regulations prevent EY from returning or destroying the personal data to a Controller, EY will ensure that such personal data remains confidential.

Rule 3C — EY will only keep personal data which is *relevant* to EY.

EY will identify the minimum amount of personal data that is required in order to properly fulfil its purpose. EY will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Rule 4 — Taking appropriate security measures

Rule 4A — EY will always adhere to its *IT Security Policies* and the information security measures as specified in the contract or other binding document with a Controller.

EY will comply with the requirements contained in EY global security policies as revised and updated from time to time together with any other information security procedures relevant to a business area or function, as well as with information security measures specified in a contract or other binding document it enters into with a Controller.

The technical and organizational security measures as implemented by EY will be designed to implement data protection principles and to facilitate compliance with data protection by design and by default.

Rule 4B — EY will ensure that providers of services to EY also adopt appropriate and equivalent security measures.

European law expressly requires that where a provider of a service to EY has access to EY Data, strict contractual obligations, evidenced in writing and dealing with the security of that data, are imposed to ensure that such service providers act only on EY's instructions when using that data and that they have in place appropriate technical and organizational security measures to safeguard the personal data.

Rule 4C — EY will notify a Controller of any personal data breach in relation to personal data processed on behalf of the Controller in accordance with and to the extent required by applicable law and in accordance with the terms of the contract or other binding document with that Controller.

All Rights Reserved — EY

EY will notify a Controller of any personal data breach in relation to personal data processed on behalf of that Controller in accordance with and to the extent required by applicable law and the terms of the contract or other binding document with that Controller. A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Where a breach is subject to European data protection law, EY will notify the Controller without undue delay after becoming aware of a personal data breach.

Rule 4D — EY will ensure that sub-processors undertake to comply with provisions that are consistent with the terms in its contract or other binding document with a Controller and this Processor Policy, specifically with regard to the adopting of security measures.

EY may only appoint sub-processors who provide appropriate and equivalent technical and organizational security measures that are applicable to their use of the personal data to which such sub-processor will have access in accordance with the terms of the contract or other binding document EY has with the Controller.

To comply with this Rule, where a sub-processor has access to EY Data, EY will impose strict contractual obligations, in writing, on the sub-processor regarding (i) the security of such data, consistent with those contained in this Processor Policy and with the terms of the contract or other binding document EY has with the Controller, (ii) the sub-processor's obligation to act only on EY's instructions when using EY Data and (iii) such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by EY in this Processor Policy.

Rule 4E — EY will comply with the requirements of a Controller regarding the appointment of any sub-processor.

EY will inform the Controller where processing, undertaken on its behalf in the context of providing services, will be conducted by a sub-processor and will comply with the particular requirements of a Controller with regard to the appointment of sub-processors as set out under the terms of the contract or other binding document with that Controller. EY will ensure that up-to-date information regarding its appointment of sub-processors is available to the Controller at all times so that its general consent is obtained. If, on reviewing this information, a Controller objects to the appointment of a sub-processor to process personal data on behalf of EY, that Controller will be entitled to take such steps as are consistent with the terms of the contract or other binding document it has with EY.

Rule 5 — Honoring individuals' rights

Rule 5A — EY will assist the Controller to comply with the rights of individuals to be informed whether any personal data about them is being processed.

EY will act in accordance with the instructions of the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to respect the rights of individuals.

Rule 5B — EY will handle requests from individuals to rectify, restrict the processing of personal data, receive data in a machine-readable format or to object to the processing of their personal data in accordance with the instructions of the Controller and — where applicable — with the *Individual's Rights Request Procedure*.

Individuals have the rights to ask for rectification of the personal data EY holds about them where it is inaccurate or incomplete. In certain circumstances, individuals may also request erasure, the restriction of or object to the processing of their personal data or to receive personal data in a machine-readable format and have the right to transmit those data to another controller (data portability).

EY will act in accordance with the terms of the contract or other binding document it has with the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to respect the rights of individuals. If an EY Network entity receives a request from an individual, it will manage such request in accordance with the contract or other binding document it has with the Controller, which may include transferring the request to the relevant Controller and not responding to such request. Where

All Rights Reserved — EY

EY is authorized to do so or is required by law, EY will adhere to the *Individual's Rights Request Procedure* (as set out in Appendix 2).

Rule 6 — Ensuring adequate protection for international transfers

Rule 6 — EY will *not* transfer personal data to external third parties *outside* Europe *without ensuring adequate protection* for the data.

In principle, international transfers of personal data to third parties outside Europe are not allowed without appropriate steps being taken by EY, such as contractual clauses, in order to protect the personal data that is being transferred.

Rule 7 — Safeguarding the use of sensitive personal data

Rule 7A — EY will only process sensitive personal data as instructed by a Controller and only if such processing is *absolutely necessary*.

"**Sensitive personal data**" is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation. Legal restrictions may also apply to criminal convictions, social security files, government identification numbers or financial account numbers under applicable laws. Sensitive personal data needs to be handled with additional care, in order to respect local customs and applicable local laws. In particular, EY will:

- Only process sensitive personal data under the instructions of the Controller
- Avoid collection of sensitive personal data where it is not required for the purposes for which the data is collected or subsequently processed
- Limit access to sensitive personal data to appropriate persons (by either masking or making anonymous or pseudonymous the data, where appropriate) in accordance with the security standards established in EY Global Information Security Policies and the instructions of the Controller

Rule 7B — EY will only process sensitive personal data where the Controller has obtained the individual's *explicit consent* unless the Controller has a legitimate basis for doing so consistent with the requirements of applicable data protection laws.

In principle, individuals must give their explicit consent to the processing of their sensitive personal data. This consent must be obtained by the Controller, unless the Controller has a legitimate basis for processing sensitive data. Consent to process sensitive personal data must be specific, informed, unambiguous and freely given. The responsibility to obtain the consent of the individuals is on the Controller.

Rule 8 — Automated individual decisions

Rule 8 — Individuals have the right not to be subject to a decision based solely on automated processing and to know the logic involved in such decision as well as the significance and the envisaged consequences of such processing. EY will assist Controllers in taking necessary measures to protect the legitimate interests of individuals.

Under European data protection law, no decision which produces legal effects concerning an individual or significantly affects that individual can be based solely on the automated processing of that individuals' personal data (including profiling), unless such decision is: (i) necessary for entering into, or performance of, a contract between the individual and the data controller; (ii) authorized by law; or (iii) based on the individual's explicit consent. EY will act in accordance with the instructions of the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to inform individuals.

Section B — Practical Commitments

Rule 9 — Training

Rule 9 — EY will provide appropriate *training* to EY Personnel who have *permanent or regular access* to personal data, who are involved in the processing *of personal data* or in the *development of tools* used to process personal data.

EY will take reasonable and appropriate steps to communicate with EY Personnel and to provide appropriate training on the requirements of this Processor Policy in accordance with the Privacy Training Program set out in Appendix 7.

Rule 10 — Records of processing and data protection impact assessments

Rule 10 — EY will keep a record of categories of processing activities carried out on behalf of the Controller. EY will assist the Controller in carrying out a data protection impact assessment if the processing activities are likely to result in a high risk to the rights and freedoms of natural persons.

EY Network entities keep a record of processing activities. This record will be in writing, including in electronic form, and will be made available to supervisory authorities on request.

Rule 11 — Assessment of compliance

Rule 11A — EY will comply with the *Assessment of Compliance Protocol* set out in *Appendix 3*.

Rule 11B — EY will — at the request of a Client acting as a Controller — allow its data processing facilities to be audited in relation to the processing activities of the Controller.

EY will allow its data processing facilities to be audited at the request of a Client. Such audit may consist of:

- The provision by EY of written information (including, without limitation, questionnaires, related independent SOC2 audit reports or reports of a similar nature and information security policies) that may include information relating to sub-processors

  Or

- Interviews with EY's IT personnel

Such audit may be carried out by the Client or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, provided such members are not working for direct competitors of EY.

For the avoidance of doubt, no access to any part of IT systems or infrastructure will be permitted due to strict confidentiality obligations towards Clients.

Rule 12 — Complaint handling

Rule 12 — EY will comply with the *Complaint Handling Procedure* set out in *Appendix 4*.

Rule 13 — Cooperation with supervisory authorities

Rule 13 — EY will comply with the *Cooperation Procedure* set out in *Appendix 5*.

Rule 14 — Update of the rules

Rule 14 — EY will comply with the *Updating Procedure* set out in *Appendix 6*.

Rule 15 — Actions in case of national legislation preventing respect for the Processor Policy

All Rights Reserved — EY

Rule 15A — EY will ensure that where it believes that existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller, or its obligations under the Processor Policy, or its obligations under the contract or other binding document with the Controller, EY will promptly inform the Controller, the Global Privacy Leader and the supervisory authority competent for the Controller unless otherwise prohibited.

Where EY has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller, or its obligations under this Processor Policy or the obligations under the contract or other binding document it has with the Controller, it will promptly notify this to:

- The Controller, who is entitled to suspend the data transfer and terminate the contract or other binding document with EY
- The EY Global Privacy Leader
- The supervisory authority competent for the Controller

Rule 15B — EY will ensure that where it receives a *legally binding request for disclosure* **of personal data, which is subject to this Processor Policy, EY will:**

- **Notify the** *Controller promptly unless prohibited from doing so by a law enforcement authority*
- **Put the request on hold and notify the Autoriteit Persoonsgegevens for this Processor Policy and the appropriate supervisory authority competent for the Controller unless prohibited from doing so by a law enforcement authority or agency**
- **Comply with the Law Enforcement Data Access Procedure set out in Appendix 8**

EY will assess each data access request by any law enforcement authority or state security body (the "**requesting authority**") on a case-by-case basis. EY will use best efforts to inform the requesting authority about EY obligations under European data protection law and to obtain the right to waive this prohibition.

EY will put such request on hold for a reasonable delay in order to notify the supervisory authority competent for the Controller and the Autoriteit Persoonsgegevens (together the competent supervisory authorities) for this Processor Policy prior to disclosing the data to the requesting authority. EY shall clearly inform the competent supervisory authorities about the request, including information about the data requested, the requesting authority and the legal basis for the disclosure.

If, despite having used best efforts, EY is not in a position to notify the competent supervisory authorities and to put the request on hold, in such case, EY will provide on an annual basis general information about the requests it has received to the competent supervisory authorities (e.g., number of applications for disclosure, type of data requested and requesting authority if possible), to the extent it has been authorized by the said requesting authority to disclose such information to third parties. Transfers of personal data by an EY Network entity to any public authority will never be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

All Rights Reserved — EY

PART III: Appendices

Appendix 1

Data protection roles and responsibilities

Data Protection Network

1. EY Global Privacy Leader

1.1 The EY Global Privacy Leader is responsible for:

- Advising the Global General Counsel, Risk Management Executive Committee and other EYG leaders on data privacy matters
- Recommending modifications to the global privacy program, as regulations and the business environment evolve, and to other EY policies, practices or agreements relating to data privacy for Risk Management Executive Committee approval
- Maintaining the compliance of EY global systems with applicable data protection rules, including the Controller Policy and this Processor Policy (analysis of systems, definition of actions and ongoing compliance)
- Coordinating a community of EY Area Privacy Leaders (see below) for the purpose of competency building, collaboration on implementation of and revisions as necessary to the global privacy program (including the Processor Policy and Controller Policy), sharing of leading practices, monitoring of relevant applicable regulations, and consistency of communications between EY Network entities and their respective local regulators with the global privacy program
- Collaborating with EY Talent, Risk Management, General Counsel, and Global IT teams, service lines and other relevant functions on data privacy matters
- With the assistance of the Area Privacy Leaders, overseeing the compliance of EY Network entities with the global privacy program (including the Controller Policy and this Processor Policy)
- With the assistance of the Area Privacy Leaders, developing and providing communications and uniform training material and support
- With the assistance of the Area Privacy Leaders, providing guidance to EY Network entities in implementing and modifying local data privacy policies and compliance programs.

2. Area Privacy Leaders

2.1 EY Area Privacy Leaders work with the EY Global Privacy Leader to evaluate and develop global policy and processes. The Area Privacy Leaders will coordinate the implementation of the Processor Policy locally. In particular, they are responsible for the following within their respective Areas:

- Providing assistance to Regional Privacy Leaders and Local Privacy Leaders to identify local business, and legal and regulatory risks surrounding data privacy issues
- Providing assistance to Regional Privacy Leaders and Local Privacy Leaders on local privacy matters, including developing local data privacy policies, as necessary
- Developing and implementing consistent solutions on a global or area basis to mitigate data privacy risks
- Coordinating the development and implementation of a data privacy program in their area that complies with the global privacy program (including the Controller Policy and this Processor Policy)
- Advising the General Counsel's Office and relevant executive and country management on data privacy issues

All Rights Reserved – EY

- Escalating within the General Counsel's Office and relevant executive, Regional and country management any significant compliance issues and plans for their resolution, as well as implications of local data privacy regulations
- Advising the EY Global Privacy Leader of any local data privacy regulations in their Area that may have international or cross-border implications, which are not adequately addressed by the global privacy program (which includes the Processor Policy)
- Confirming to the EY Global Privacy Leader, EY Network entity compliance with the global privacy program and, in particular, the Processor Policy
- Collaborating with relevant Talent, Risk Management, General Counsel and IT teams, service lines, and other relevant functions on data privacy matters
- Periodically monitoring the effectiveness of the Area Privacy functions

3. Regional / Local Privacy Leaders

3.1 EY may appoint Regional / Local Privacy Leaders to assist with the coordination and implementation of Global standards locally.

3.2 The Regional / Local Privacy Leader remains knowledgeable about the relevant country, region and state laws, governmental regulations, professional practice obligations, and regulatory guidance, which relate to data privacy compliance and are applicable to the EY Network entities of the Region.

3.3 The Regional / Local Privacy Leader handles subject access requests and complaints under the Processor Policy and may refer such request or complaint to the Area Privacy Leader or the Global Privacy Leader as needed.

Data Protection Officers

1.1 EY Network entities that are subject to the EU General Data Protection Regulation ("GDPR") shall designate a Data Protection Officer ("DPO") where they have determined that 1) its core activities consist of processing operations which require regular and systematic monitoring of individuals on a large scale; or 2) the core activities consist of processing on a large scale of sensitive personal data (Rule 7A) and personal data relating to criminal convictions and offences.

1.2 Various EY Network entities may appoint one DPO, for example a DPO acting on behalf of all EY Network entities in one Region.

1.3 The DPO may be the same person as the Regional or Local Privacy Leader but the role may also be undertaken by a separate individual.

1.4 Where a DPO is acting on behalf of multiple EY Network entities, such EY Network entity will appoint a Local Privacy Leader who will assist the DPO in the exercise of its responsibilities. The DPO may delegate its responsibilities to the Local Privacy Leader who may perform these responsibilities under supervision and on behalf of the DPO.

1.5 A DPO will have the following responsibilities:

- Informing and advising the EY Network entity and EY Personnel with respect to obligations under the GDPR and other EU data protection provisions;
- Monitoring the EY Network Entity's compliance with the GDPR and other EU data protection provisions, the regulations of Ernst & Young Global Limited insofar as they relate to the protection of personal data and any other applicable policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of EY Personnel and conducting and/or arranging for internal audits as appropriate;
- When requested, advising on data protection impact assessments;
- Working and cooperating with the EY Network Entity's designated representative where applicable and serving as the contact point for the representative on issues relating to the processing of personal data;
- Being available to respond to inquiries from individuals relating to data protection practices and data subjects' rights, including withdrawal of consent, the right to be forgotten, and related rights;

- Assisting in the developing and monitoring of local procedures for personal data breach handling, and being available as a first point of contact to assist with responding to any breaches of personal data, including assessing whether the data breach must be notified to supervisory authorities and/or individuals;
- Keeping up-to-date the EY Network Entity's record of processing;
- Keeping up-to-date its in-depth knowledge of the GDPR, including GDPR guidance issued by supervisory authorities and relevant legal decisions that may impact the EY Network Entity's processing of personal data;
- Providing an annual report for the EY Network Entity's leadership (as applicable).

1.6 The DPO may fulfill other tasks and duties, provided such tasks and duties do not result in a conflict of interests.

1.7 EY will publish the contact details of EY Network Entities' DPOs on EY's website ey.com.

Appendix 2

Individual's Rights Request Procedure

1. Subject Access Request Procedure

1.1 European data protection law gives individuals whose personal data is processed the right to be informed whether any personal data about them is being processed by an organization. This is known as the right of subject access.

1.2 When EY processes personal data on behalf of a Controller, EY is considered to be a processor of the data and the Controller will be primarily responsible for meeting the legal requirements as a controller. If an EY Network entity receives a subject access request, the EY Network entity will manage such request in accordance with the contract or other binding document it has with the Controller. This may include transferring the request to the Controller and not responding to such request. Where EY is authorized to do so or is required by law, EY will adhere to the terms of this Individual's Rights Request Procedure.

1.3 Where a subject access request is subject to European data protection law, such a request will be dealt with by EY in accordance with this Individual's Rights Request Procedure (referred to as "**valid request**" in this procedure). A subject access request is subject to European data protection law where the EY Network entity or the Controller is established in the EU or where the processing activities are related to the offering of goods or services to individuals in the EU or to the monitoring of their behavior as far as their behavior takes place within the EU. Where applicable local data protection law differs from any aspect of this Individual's Rights Request Procedure, the local data protection law will prevail.

1.4 An individual making a valid request to an EY Network entity is entitled to:

1.4.1 Be informed whether the EY Network entity holds and is processing personal data about that individual and, where that is the case, access such personal data

1.4.2 Be given a description of the personal data; the purposes for which they are being held and processed; the recipients or classes of recipient to whom the personal data is, or may be, disclosed by the EY Network entity (in particular recipients in third countries); the envisaged period for which the personal data is stored or — if this is not possible — the criteria used to determine that period; the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing; the right to lodge a complaint with a supervisory authority and — where personal data are not collected from the individual — any available information as to their resource

1.4.3 Receive — free of charge — a copy of the personal data undergoing processing; for any further copies requested by the individual, a reasonable fee based on administrative costs may be charged

1.5 The request must be made in writing[9], which can include email. Where the individual makes the request by electronic means, the personal data shall be provided in a commonly-used electronic form, unless otherwise requested by the individual.

1.6 The EY Network entity must respond to a valid request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The individual will be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

1.7 The EY Network entity is not obliged to comply with a subject access request unless the EY Network entity is supplied with such information which it may reasonably require in order to confirm the identity of the individual making the request and to locate the information which that person seeks.

[9] Unless the local data protection law provides that an oral request may be made, in which case EY will document the request and provide a copy to the individual making the request before dealing with it

2. Procedure

2.1 Receipt of a subject access request

2.1.1 If any member of EY Personnel receives a request from an individual for access to his or her personal data, they must first pass the communication to the Controller. If the EY Network entity is authorized to deal with such request directly or is required by law, they must then pass the communication to the Local Privacy Leader or DPO (where applicable) indicating the date on which the request was received together with any other information that may assist the Local Privacy Leader or DPO (where applicable) to deal with the request.

2.1.2 The request does not have to be official or mentioned as data protection law to qualify as a subject access request.

2.2 Initial steps

2.2.1 The Local Privacy Leader or DPO (where applicable) will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

2.2.2 The Local Privacy Leader or DPO (where applicable) will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

2.3 Exemptions to subject access

2.3.1 A valid request may be refused on the following grounds:

a. Where the Controller instructs the EY Network entity not to deal with such request directly

b. If the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that EY Network entity is located

Or

c. Where the subject access is not subject to European data protection law

2.4 The Search and the response

2.4.1 The Local Privacy Leader or DPO (where applicable) will arrange a search of all relevant electronic and paper-filing systems.

2.4.2 The Local Privacy Leader or DPO (where applicable) may refer any complex cases to the Area Privacy Leader or ultimately to the Global Privacy Leader for advice, particularly where the request includes information relating to third parties or where the release of personal data may prejudice commercial confidentiality or legal proceedings.

2.4.3 The information requested will be collated by the Local Privacy Leader or DPO (where applicable) into a readily understandable format (internal codes or identification numbers used at EY that correspond to personal data shall be translated before being disclosed). A covering letter will be prepared by the Local Privacy Leader or DPO (where applicable), which includes information required to be provided in response to a subject access request.

2.4.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. The other information referred to in 1.4 above must still be provided. In such circumstances, the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

2.5 Requests for erasure, amendment, cessation of processing or to port information

2.5.1 If a request is received for the deletion of that individual's personal data, such a request must be considered and dealt with as appropriate by the Local Privacy Leader or DPO (where applicable). If a request is received advising of a change in that individual's personal data,

All Rights Reserved – EY

such information must be rectified or updated accordingly if the EY Network entity is satisfied that there is a legitimate basis for doing so.

2.5.2 If the request is to cease processing that individual's personal data because the rights and freedoms of the individual are prejudiced by virtue of such processing by the EY Network entity, or on the basis of other compelling legitimate grounds, the matter will be referred by the Local Privacy Leader or DPO (where applicable) to the Area Privacy Leader and ultimately to the Global Privacy Leader to assess. Where the processing undertaken by the EY Network entity is required by law, the request will not be regarded as valid.

2.5.3 If a request is to receive personal data in a structured, commonly used and machine-readable format and to have that data transmitted to another controller, such a request must be considered and dealt with as appropriate by the Local Privacy Leader or DPO (where applicable).

2.6 All queries relating to this procedure are to be addressed to the Local Privacy Leader or DPO (where applicable).

All Rights Reserved – EY

Appendix 3

Assessment of Compliance Protocol

1. Background

1.1 The purpose of this Processor Policy is to safeguard personal data transferred between the EY Network entities where EY acts as a processor. This Processor Policy requires approval from the supervisory authorities in the European member states from which the personal data is transferred. One of the requirements of the supervisory authorities is that EY assesses compliance with this Processor Policy and satisfies certain conditions in so doing, and this Appendix describes how EY deals with such requirements.

1.2 One of the roles of the EY Global Privacy Leader and also the Area Privacy Leader is to provide guidance about the processing of personal data subject to this Processor Policy and to assess the processing of personal data by the EY Network entities for potential privacy-related risks. The processing of personal data with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an ongoing basis. Accordingly, although this Appendix describes the formal assessment process adopted by EY to ensure compliance with this Processor Policy as required by the supervisory authorities, this is only one way in which EY ensures that the provisions of the Processor Policy are observed and corrective actions are taken as required.

2. Approach

2.1 Scope of assessment

2.1.1 The EY Global Risk Management function ("Risk Management") will be responsible for carrying out assessments of compliance with this Processor Policy and will ensure that such assessments address all aspects of this Processor Policy (including methods of ensuring that corrective actions will take place). The assessments will comprise a review of the performance of particular functions within the business and also an assessment of the EY Network entity adopting a risk-based approach. Risk Management will be responsible for ensuring that the results of the assessment are brought to the attention of the EY Global Privacy Leader who will ensure that any actions identified to implement this Processor Policy take place correctly. The Global Privacy Leader will ensure that any reports indicating unsatisfactory compliance in relation to the Processor Policy will be brought to the attention of the Global General Counsel who attends the meetings of the Global Executive.

2.1.2 EY Clients (or auditors acting on their behalf) may assess compliance with the commitments made in this Processor Policy in accordance with the terms of the relevant Client's contract with an EY Network entity. The assessment of compliance may consist of:

- The provision by EY of written information (including, without limitation, questionnaires, related independent SOC2 audit reports or reports of a similar nature and information security policies) that may include information relating to sub-processors

  Or

- Interviews with EY IT personnel

2.1.3 EY will not provide a Client with access to any part of IT systems or infrastructure which process personal data of other Clients.

2.2 Timing

2.2.1 Review of compliance with the global privacy program, including the Processor Policy, will take place on a regular basis at the instigation of Risk Management and as required by the terms of the relevant Client's contract with EY. The scope of the compliance assessment will be decided by EY's independent Global Internal Audit team with input from the Global General Counsel's Office.

2.3 Auditors

2.3.1 Review of compliance with this Processor Policy will be undertaken by Risk Management and responsibility for compliance with this Processor Policy on a day-to-day basis will be undertaken by the EY Global Privacy Leader and the Area Privacy Leaders.

2.3.2 In the event that a Client exercises its right to assess EY for compliance with this Processor Policy, such assessment may be undertaken by that Client, or by independent and suitably experienced auditors selected by that Client, as required and defined by the terms of the relevant Client's contract with an EY Network entity.

2.4 Report

2.4.1 Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, EY will:

a. Provide copies of the results of any assessment of compliance with the Processor Policy to the competent European supervisory authority

b. Provide a copy of the results to the Client, to the extent that an assessment relates to personal data EY processes on behalf of that Client

2.4.2 EY will also provide a copy of the results of any assessment of compliance to the EY Global Privacy Leader who will be responsible for liaising with the European supervisory authorities for this purpose. In addition, EY has agreed that in accordance with the provisions of clause 5 of the Cooperation Procedure,[10] supervisory authorities may assess compliance by EY with this Processor Policy. The EY Global Privacy Leader will also be responsible for liaising with the European supervisory authorities for this purpose.

[10]Clause 5 states: Where any EY Network entity is located within the jurisdiction of a supervisory authority based in Europe, EY agrees that that supervisory authority may audit that EY Network entity for the purpose of reviewing compliance with the BCR, in accordance with the applicable law of the country in which the EY Network entity is located, or, in the case of an EY Network entity located outside Europe, in accordance with the applicable law of the European country from which the personal data is transferred under the BCR, on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of EY.

All Rights Reserved – EY

Appendix 4

Complaint Handling Procedure

1. Background

1.1 This Processor Policy safeguards personal data transferred between EY Network entities where such entity acts as a processor. The content of this Processor Policy is determined by the supervisory authorities in the European member states from which the personal data is transferred and one of their requirements is that EY must have a Complaint Handling Procedure in place. The purpose of this procedure is to explain how complaints brought by an individual whose personal data is processed by EY under this Processor Policy are dealt with.

2. How individuals can bring complaints

2.1 Individuals can bring complaints in writing by contacting the General Counsel's Office ("GCO") or the Global Privacy Leader, 6 More London Place, London, SE1 2DA, or via email at global.data.protection@ey.com.

2.2 Where a complaint relates to the processing of personal data by EY acting as a processor, EY will communicate the details of the complaint to the Controller promptly and will act in accordance with the terms of the contract or other binding document between the Controller and EY. If the Controller requires EY to deal with the complaint, the below mentioned steps will be applicable.

2.3 In circumstances where a Controller has disappeared, no longer exists or has become insolvent, individuals whose personal data is processed by EY on behalf of that Controller have the right to complain to the EY Network entity that is processing the data. EY will deal with such complaints in accordance with the below mentioned steps.

3. Who handles complaints?

3.1 The local GCO or Regional or Local Privacy Leader will handle all complaints arising under the Processor Policy in conjunction with executive leadership and the Global Privacy Leader, and will liaise with colleagues from relevant business and support units as appropriate to deal with complaints.

4. What is the response time?

4.1 The local GCO or Regional or Local Privacy Leader will acknowledge receipt of a complaint to the individual concerned within five working days (after having received confirmation from the Controller that it requires EY to deal with the complaint), investigating and making a substantive response within one month. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the local GCO or Regional or Local Privacy Leader will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided, which will not exceed six months from the date the complaint was brought.

4.2 The response will indicate whether the complaint is considered justified or whether it is rejected, as well as the consequences of such response.

5. When a complainant disputes a finding

5.1 If the complainant disputes the response (or any aspect of a finding) of the local GCO or Regional or Local Privacy Leader, the complainant notifies the local GCO or Regional or Local Privacy Leader accordingly. The matter will then be referred to the Region or Area GCO contact or ultimately to the Global Privacy Leader as appropriate who will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. The Region, Area GCO contact or Global Privacy Leader will respond to the complainant within one month of the referral. As part of the review, the Region or Area GCO contact or Global Privacy Leader may arrange to meet the parties in an attempt to resolve the complaint. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Region, Area GCO contact or Global Privacy Leader will advise the complainant accordingly and provide a reasonable estimate

All Rights Reserved – EY

for the timescale within which a response will be provided, which will not exceed three months from the date the complaint was referred.

5.2 If the complaint is upheld, the EY Region or Area GCO contact or Global Privacy Leader will arrange for any necessary steps to be taken as a consequence.

6. Right to complain to a European supervisory authority and to lodge an application with a court of competent jurisdiction

6.1 In addition to the right to bring a claim to EY in accordance with this Complaint Handling Procedure, individuals whose personal data is processed in accordance with European data protection law have the right to complain to a European supervisory authority and to lodge an application with a court of competent jurisdiction. This also applies if the individual is not satisfied with the way in which the complaint relating to this Processor Policy has been resolved by EY.

All Rights Reserved – EY

Appendix 5

Cooperation Procedure

1. This Cooperation Procedure sets out the way in which EY will cooperate with the European supervisory authorities in relation to this Processor Policy.
2. Where required, EY will make the necessary personnel available for dialogue with a European supervisory authority in relation to this Processor Policy.
3. EY will actively review and consider:
   - Any decisions made by relevant European supervisory authorities on any data protection law issues that may affect the Processor Policy
   - The views of the Article 29 Working Party as outlined in its published guidance on Binding Corporate Rules for Processors
4. EY will provide upon request copies of the results of any assessment of compliance of the Processor Policy to a European supervisory authority of competent jurisdiction subject to applicable law and respect for the confidentiality and trade secrets of the information provided.
5. EY agrees that:
   - Where any EY Network entity is located within the jurisdiction of a supervisory authority based in Europe, that supervisory authority may audit that EY Network entity for the purpose of reviewing compliance with this Processor Policy, in accordance with the applicable law of the country in which the EY Network entity is located, or, in the case of an EY Network entity located outside Europe, in accordance with the applicable law of the European country from which the personal data is transferred under this Processor Policy.
   - Where any EY Network entity is processing personal data on behalf of a Controller located within the jurisdiction of a supervisory authority based in Europe, that supervisory authority may audit that EY Network entity for the purpose of reviewing compliance with this Processor Policy, in accordance with the applicable law of the country in which the Controller is located on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of EY.
6. EY agrees to abide by a formal decision of the applicable supervisory authority where a right to appeal is not exercised on any issues related to the interpretation and application of this Processor Policy.

All Rights Reserved – EY

Appendix 6

Updating Procedure

1. Background

1.1 This Updating Procedure sets out the way in which EY will communicate changes to this Processor Policy to the European supervisory authorities, Controllers, data subjects and to the EY Network entities bound by this Processor Policy.

2. Material changes

2.1 EY will communicate in advance any material changes to this Processor Policy to the Autoriteit Persoonsgegevens and any other relevant European supervisory authorities as soon as reasonably practicable.

2.2 Where a change to this Processor Policy materially affects the conditions under which EY processes personal data on behalf of a Controller under the terms of the contract or other binding document EY has with that Controller, EY will communicate the proposed change to the Controller before it is implemented, and with sufficient notice to enable the affected Controller to object. The Controller may then suspend the transfer of personal data to EY and terminate its relationship with EY, in accordance with the terms of its contract or other binding document with EY.

3. Administrative changes

3.1 EY will communicate changes to this Processor Policy, which are administrative in nature (including changes in the list of EY Network entities) or which have occurred as a result of a change of applicable data protection law in any European country, through any legislative, court or supervisory authority measure, to the Autoriteit Persoonsgegevens and other relevant supervisory authorities at least once a year. EY will also provide a brief explanation of the reasons for any notified changes to this Processor Policy.

4. Communicating changes to the Processor Policy

4.1 EY will communicate all changes to this Processor Policy, whether administrative or material in nature, to the EY Network entities bound by this Processor Policy, and material changes to the Controller and data subjects who benefit from this Processor Policy.

4.2 Communication internally will be via the EY internal communications process which comes from the EY Global Leader, Risk Management and the EY Global Vice Chair and General Counsel, cascading down to the Area Privacy Leaders, Regional Privacy Leaders and General Counsel's Offices, and Local Privacy Leaders and Local General Counsel's Offices. Such communication includes publication on EY's intranet and on EY's external site: ey.com/bcr.

4.3 EY will communicate to the Autoriteit Persoonsgegevens any substantial changes to the list of EY Network entities once a year. Otherwise, EY will communicate an up-to-date list of entities to the Autoriteit Persoonsgegevens and any other relevant European supervisory authorities when required.

5. Logging changes to the Processor Policy

5.1 This Processor Policy contains a change log which sets out the date on which this Processor Policy is revised and the details of any revisions that have been made.

5.2 The Global Privacy Leader will maintain an up-to-date list of the EY Network entities this Processor Policy is applicable to. EY will ensure that all new EY Network entities are bound by this Processor Policy before a transfer of personal data to them takes place. Each EY Network entity will maintain an up-to-date list of all sub-processors it has appointed to process personal data on behalf of a Controller.

All Rights Reserved – EY

Appendix 7

Privacy Training Program

1. Background

1.1 EY trains EY Personnel on the basic principles of data protection, confidentiality and information security awareness. Training and awareness will be provided through posting messages and videos on EY's intranet and daily news articles, as well as by making available web-based training courses.

1.2 EY Personnel who have permanent or regular access to personal data, and who are involved in the processing of personal data or in the development of tools to process personal data receive additional, tailored training on the Policies and specific data protection issues relevant to their role. This web-based training is further described below.

2. Responsibility for the privacy training program

2.1 The EY Global Privacy Leader has overall responsibility for privacy training at EY, with input from colleagues from other functional areas, including Information Security, Talent and other departments, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the Processor Policy and that it is appropriate for individuals who have permanent or regular access to personal data, and who are involved in the processing of personal data or in the development of tools to process personal data.

2.2 Communication and training should cover data privacy elements such as:

- Basic principles
- Importance of data privacy
- Definitions
- Personal and sensitive personal data
- Data privacy considerations with respect to information security

3. About the training courses

3.1 EY has developed a global Web-Based Learning (WBL) that is available for all EY Personnel. The course is designed to be both informative and user-friendly, generating interest in the topics covered. At the end of the WBL, EY Personnel must correctly answer a series of multiple choice questions for the course to be deemed complete.

3.2

3.3 EY management supports the completion of the WBL and is responsible for ensuring that individuals within the organization are given appropriate time to complete the course. Local management determines which members of EY Personnel in their respective country will be mandated to complete the WBL. Compliance will be monitored. New hires are required to complete the training as part of their induction program.

4. Awareness

4.1 EY will regularly provide reinforcement content to EY Personnel reminding them of their responsibilities regarding data protection, confidentiality and information security awareness. Such content will be provided through posting messages and videos on EY's intranet, posters in EY network entities' offices and daily news emails provided to all EY Personnel.

All Rights Reserved – EY

Appendix 8

Law Enforcement Data Access Procedure

1. Background

1.1 This Law Enforcement Data Access Procedure sets out EY's policy for responding to a request received from a law enforcement or other government authority (together the "**Requesting Authority**") to disclose personal data processed by EY on behalf of a Controller (hereafter "**Data Production Request**"). Where EY receives a Data Production Request, it will handle that Data Protection Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal data than is required by this Procedure, EY will comply with the relevant requirements of applicable data protection law(s).

2. General principle on Data Production Requests

2.1 As a general principle, EY does not disclose personal data in response to a Data Production Request unless either:

- It is under a compelling legal obligation to make such disclosure

  Or

- Taking into account the circumstances and the privacy rights of any affected individuals, there is an imminent risk of serious harm that merits disclosure in any event

2.2 Even where disclosure is required, EY's policy is that the Controller should have the opportunity to protect the personal data requested because it has the greatest interest in opposing, or is in the better position to comply with, a Data Production Request.

2.3 For that reason, unless it is legally compelled to do so or there is an imminent risk of serious harm, EY will first consult with the competent supervisory authorities and provide the Controller with details of the Data Production Request. EY will cooperate with the competent supervisory authorities and the Controller to address the Data Production Request.

3. Data Production Request Review

3.1 If EY receives a Data Production Request, the recipient of the request must pass it to EY's Regional or Local Privacy Leader or DPO (where applicable) and Regional or Local General Counsel immediately upon receipt, indicating the date on which it was received together with any other information which may assist EY's Regional or Local Privacy Leader or DPO (where applicable) and Regional or Local General Counsel to deal with the request.

3.2 The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Production Request.

3.3 EY's Regional or Local Privacy Leader or DPO (where applicable) and Regional or Local General Counsel will carefully review each and every Data Production Request individually and on a case-by-case basis, and will deal with the request to determine the nature, urgency, scope and validity of the Data Production Request under applicable laws and to identify whether action may be needed to challenge the Data Production Request.

4. Notice of a Data Production Request

4.1 After assessing the nature, urgency, scope and validity of the Data Protection Request, EY will notify and provide the Controller with the details of the Data Production Request prior to disclosing any personal data, unless legally prohibited or where the imminent risk of serious harm prohibits prior notification.

4.2 EY will also put the request on hold in order to notify and consult with the competent supervisory authorities, unless legally prohibited or where the imminent risk of serious harm prohibits prior notification.

All Rights Reserved – EY

4.3 Where EY is prohibited from notifying the competent supervisory authorities and suspending the request, EY will use its best efforts (taking into account the nature, urgency, scope and validity of the request) to inform the Requesting Authority about its obligations under applicable data protection law(s) and to obtain the right to waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that EY can consult with the Autoriteit Persoonsgegevens and may also, in appropriate circumstances, include seeking a court order to this effect. EY will maintain a written record of the efforts it takes.

5. Transparency reports

5.1 In cases where EY is prohibited from notifying the competent supervisory authorities about a Data Production Request, it commits to providing the competent supervisory authorities with a confidential annual report (i.e., "Transparency Report"), which reflects to the extent permitted by applicable laws, the number and type of Data Production Requests it has received for the preceding year and the Requesting Authorities who made those requests.

6. Queries

6.1 All queries relating to this Procedure are to be addressed to the EY Global Privacy Leader at global.data.protection@ey.com.

All Rights Reserved – EY

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2020 EYGM Limited.
All Rights Reserved.

EYG no. 010400-18Gbl
BCR no. 2869
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

EY
Data Protection
United Kingdom
Binding Corporate Rules
Processor Policy

1 January 2021

Building a better working world

Contents

Introduction to the UK Data Protection Binding Corporate Rules Processor Policy 3

Part I: Background and actions 4

Part II: The Rules 7

PART III: Appendices 13

Appendix 1 13

Data privacy roles and responsibilities 13

Appendix 2 16

Subject Access Request Procedure 16

Appendix 3 19

Assessment of Compliance Protocol 19

Appendix 4 21

Complaint Handling Procedure 21

Appendix 5 23

Cooperation Procedure 23

Appendix 6 24

Updating Procedure 24

Appendix 7 25

Privacy Training Program 25

Appendix 8 26

Law Enforcement Data Access Procedure 26

Introduction to the UK Data Protection Binding Corporate Rules Processor Policy

EY has established a foundation for the privacy of all personal data, which is processed worldwide in its global personal data privacy program ("**global privacy program**"). The global privacy program comprises a series of policies and procedures, which set out the principles to be applied to the processing of personal data within EY.

One of the policies forming part of the global privacy program is this UK Data Protection Binding Corporate Rules Processor Policy ("UK **Processor Policy**"). In this UK Processor Policy, we use "**EY**" to refer to the global organization of independent member firms ("**EY Member Firm**")[1] and other entities in the EY organization ("**EY Network entity**"),[2] which are bound to comply with the requirements of Ernst & Young Global Limited ("**EYG**"). EYG is the central governance entity of the EY organization and coordinates EY Network entities and the cooperation among them.

This UK Processor Policy has been created to establish EY's approach to compliance with United Kingdom (the **"UK"**) data protection law and specifically to transfers of personal data between EY Network entities where such EY Network entities are acting as processors.

All EY Network entities[3] and their partners, directors, employees, new hires, individual contractors and temporary staff ("**EY Personnel**") must comply with, and respect, this UK Processor Policy when processing[4] personal data as a processor, irrespective of the country in which they are located.

This UK Processor Policy applies to data received from a controller established in the UK which is not an EY Network Entity ("**Controllers**") and then processed by EY Network entities as processor or sub-processor.

The UK Processor Policy contains 15 rules ("**Rules**") that govern the processing of personal data of current, past and prospective EY Personnel, clients, suppliers, subcontractors and any other third parties ("**EY Data**").

This UK Processor Policy applies to all EY Data wherever it is processed as part of the regular business activities of EY. Transfers of personal data take place between EY Network entities during the normal course of business and such data may be stored in centralized databases accessible by EY Network entities from anywhere in the world. Each EY Network entity and its EY Personnel shall respect the instructions regarding the data processing and the security and confidentiality measures as provided in the contract or other binding document that such EY Network entity enters into with the Controller.

This UK Processor Policy is accessible on EY's website at ey.com/bcr.

[1] EY Member Firm means any corporation, partnership or other entity or organization that is admitted from time to time as members of Ernst & Young Global Limited pursuant to the regulations of Ernst & Young Global Limited.
[2] EY Network entity means any one of the network of entities comprising Ernst & Young Global Limited, EYGN Limited, EYGM Limited, EYGS LLP, EYGI B.V., EY Global Finance, Inc. and their members. It also means any entity controlled by any such entity, under common control with any such entity, or controlling such entity or any corporation, partnership, or other business organization that is a member firm or a subsidiary of the entity, or which is directly or indirectly a majority owned or controlled subsidiary of the entity, together with any partner, director, employee or agent of any such entity. For the purposes of this definition, "control" means (a) ownership, either directly or indirectly, of equity securities entitling either such entity to exercise in the aggregate of at least 50% of the voting power of such entity in question; or (b) possession, either directly or indirectly, of the power to direct or cause the direction of the management and policies of such entity in question, whether through ownership of securities, by contract or otherwise.
[3] The list of the EY Network entities providing services to Clients who are bound by the UK Processor Policy is accessible on EY's website at ey.com/uk/en/home/legal via "View a list of EY member firms and affiliates".
[4] "Processing" in UK data protection law means any set of operations performed upon personal data, whether or not by automatic means. This is interpreted widely to include collecting, storing, organizing, destroying, amending, consulting, destroying and disclosure of the personal data.

Part I: Background and actions

What is data protection law?

Data protection law gives people the right to control how their "**personal data**"[5] is used. When EY processes EY Data, this is covered and regulated by data protection law.

Data protection law distinguishes between the concepts of "**controller**" and "**processor**". The controller determines, alone or jointly with others, the purposes and the means of the processing of personal data. The processor, on the other hand, processes personal data on behalf of the controller.

For the majority of professional services, EY is acting as a controller, processing personal data in accordance with its own strict professional obligations. For a limited type of professional services, EY will be acting as a processor under the detailed instructions of the Controller. For services where an EY Network Entity acts as a controller in relation to another EY Network entity acting as controller or as 'internal processor', EY shall comply with the UK Data Protection Binding Corporate Rules Controller Policy ("UK **Controller Policy**") as published on ey.com/bcr. For services where EY acts as a processor, this UK Processor Policy applies.

How does data protection law affect EY internationally?

UK data protection law does not allow the transfer of personal data to countries outside the UK that do not ensure an adequate level of data protection[6]. Some of the countries in which EY operates are not regarded by the UK supervisory authority, the Information Commissioner's Office (the **"ICO"**), as providing an adequate level of protection for individuals' data privacy rights.

When EY acts as a processor, the Controller retains the responsibility to comply with UK data protection law. Controllers in the UK will pass certain data protection obligations on to EY in the contracts or other binding documents EY has with them. Consequently, if EY fails to comply with the terms of a contract or other binding document it enters into with a Controller, the Controller may be in breach of applicable data protection law and EY may face a claim for breach of contract, which may result in the payment of compensation or other judicial remedies.

In such cases, if a Controller demonstrates that it has suffered damage, and that it is likely that the damage has occurred due to a breach of the UK Processor Policy by an EY Network entity outside the UK (or a third party sub-processor established outside the UK), that Controller is entitled to enforce the UK Processor Policy against EY and, in such cases, the obligation will be on the EY Network entity accepting liability (namely the EY Network entity that is a party to the contract or other binding document with the Controller) to demonstrate that the EY Network entity outside the UK (or the third party sub-processor established outside the UK) is not responsible for the breach, or that no such breach took place.

What is EY doing about it?

EY must take proper steps to ensure that it processes personal data on an international basis in a safe and lawful manner. This UK Processor Policy sets out a framework to satisfy the standards contained in UK data protection law and, in particular, to provide an adequate level of protection for all personal data processed in the UK and transferred to EY Network entities outside the UK, where the personal data is collected by a Controller in the UK.

EY will apply the Rules contained in this UK Processor Policy whenever it acts as a processor on behalf of a Controller. Where the Controller relies upon this UK Processor Policy as providing adequate safeguards, an obligation to comply with this UK Processor Policy will be included in the contract or other binding document EY has with the Controller and a copy of this UK Processor Policy will be incorporated into such contracts or other binding documents or referenced with a possibility of electronic access. If the Controller chooses not to rely upon this UK Processor Policy, that Controller is responsible for putting in place another adequate safeguard to protect the personal data.

[5] Personal data means any information relating to an identified or identifiable natural person in line with the definition in the UK Data Protection Act 2018

[6] Several exceptions to this rule can be applicable.

All EY Network entities who process personal data in a capacity as processor under the instructions of a Controller, must comply with the Rules set out in **Part II** of this UK Processor Policy together with the policies and procedures set out in the appendices in **Part III** of this UK Processor Policy.

For the avoidance of doubt:

- Where EY acts as a controller (or as processor under the instructions of another EY Network Entity), EY shall comply with the UK Controller Policy as published on ey.com/bcr. EY Network entities may act as both a controller and a processor and must therefore comply with both the UK Processor Policy and the UK Controller Policy.
- For some internal administrative processes and for compliance with regulatory requirements, EY will always act as a controller in its own right (e.g., compliance with regulatory requirements, to check conflicts, for quality, risk management or financial accounting purposes and for the provision of internal administrative or IT support services). For such processes, EY shall comply with the UK Controller Policy.

What does this mean in practice for personal data processed in the UK?

Under UK data protection law, individuals both within and outside the UK whose personal data is processed in the UK by a Controller and transferred to an EY Network entity outside the UK under the UK Processor Policy have certain rights. These individuals may enforce the Rules set out in this UK Processor Policy as third-party beneficiaries where they are not able to bring a claim against the Controller in respect of a breach of any of the commitments in this UK Processor Policy by an EY Network entity (or by a sub-processor) acting as a processor (for example in case the Controller has factually disappeared or ceased to exist in law or has become insolvent, unless any successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law).

In such cases, these individuals' rights are as follows:

- **Complaints**: Individuals may complain to the Controller established in the UKin accordance with the Complaint Handling Procedure (as set out in Appendix 4 of this UK Processor Policy) and to the ICO .
- **Liability**: Individuals may bring proceedings against the Controller responsible for exporting the data outside the UK in the courts of the the UK
- **Compensation**: Individuals may seek appropriate redress from the Controller established in the UK and responsible for exporting the data (including the remedy of any breach of this UK Processor Policy by an EY Network entity outside the UK) and where appropriate, receive compensation from the Controller established in the UKand responsible for exporting the data for any damage suffered as a result of a breach of this UK Processor Policy by:
  - An EY Network entity established outside the UK.

    Or
  - Any third-party processor that is established outside the UKand is acting on behalf of an EY Network entity inside the UKor outside the UK, in accordance with the determination of the court or the ICO.
- **Transparency**: Individuals may obtain a copy of this UK Processor Policy by accessing the UK Processor Policy on EY's website: ey.com/bcr.

In the event of a claim being made in which an individual has suffered damage, where that individual can demonstrate that it is likely that the damage has occurred because of a breach of the UK Processor Policy, EY has agreed that the burden of proof to show that (i) an EY Network entity outside the UK or (ii) any third-party sub-processor who is established outside the UK and who is acting on behalf of an EY Network entity outside the UK is not responsible for the breach, or that no such breach took place, will rest with the EY Network entity responsible for exporting the personal data to the EY Network entity outside the UK.

Data protection roles and responsibilities

The EY Global Privacy Leader[7] is the person who has overall responsibility for compliance with the UK Processor Policy and any other supporting policies and procedures.

[7] At present EY's Global Lead Counsel Privacy and Security serves as the Global Privacy Leader as referenced in the BCRs.

Area Privacy Leaders are responsible for overseeing compliance with this UK Processor Policy by the EY Network entities within their area on a day-to-day basis.

A description of the roles and responsibilities of the EY global privacy team is set out in Appendix 1.

Further information

If you have any questions regarding the provisions of this UK Processor Policy, your rights under this UK Processor Policy or any other data privacy issues, you may contact the EY Global Privacy Leader who will either deal with the matter or forward it to the appropriate person or department within EY at the following address:

EY Global Privacy Leader

Email: global.data.protection@ey.com

Address: Office of the General Counsel (GCO), 6 More London Place, London, SE1 2DA.

The Global Privacy Leader is responsible for ensuring that changes to this UK Processor Policy are notified to the EY Network entities and to individuals whose personal data is processed by EY via the EY website at ey.com/bcr.

Part II: The Rules

The Rules are divided into two sections. Section A addresses the basic principles of UK data protection law EY must observe when EY processes personal data as a processor.

Section B deals with the practical commitments made by EY to the ICO in connection with this UK Processor Policy.

Section A

Rule 1 — Compliance with local law

Rule 1A — EY will first and foremost comply with local law where it exists.

EY will comply with any applicable legislation relating to personal data and will ensure that, where personal data is processed as a processor, this is done in accordance with applicable local law.

Where local legislation relating to personal data requires a higher level of protection for personal data, such legislation will take precedence over this UK Processor Policy.

Where there is no law or the law does not meet the standards set out by the Rules in this UK Processor Policy, EY's position will be to process personal data adhering to the Rules in this UK Processor Policy.

Rule 1B — EY will cooperate and assist a Controller to comply with its obligations under local law in a reasonable time and to the extent reasonably possible.

EY will, within a reasonable time and to the extent reasonably possible, as required under the contract or other binding document it has entered into with a Controller, assist such Controller to comply with its obligations under applicable data protection law.

Rule 2 — Ensuring transparency and using personal data for a known purpose only

Rule 2A — EY will assist a Controller to comply with the requirements to *explain to individuals* how their data will be used and to be transparent about data processing activities.

The Controller has a duty to explain to individuals how their personal data will be processed (for example, by providing a privacy notice or privacy statement). EY will assist a Controller, insofar as this is possible, to comply with this requirement.

EY will follow this Rule 2A unless there is a legitimate basis for not doing so, for example, where it is necessary to safeguard national security or defense, for the prevention or detection of crime, legal proceedings or where otherwise permitted by law.

Rule 2B — EY will only obtain and use personal data on behalf of and in accordance with the instructions of the Controller.

EY will only process personal data on behalf of and in compliance with the (lawful) instructions of a Controller, as specified in the contract or other binding document it has with such Controller. Where the Controller relies upon this UK Processor Policy as providing adequate safeguards, an obligation to comply with this UK Processor Policy will be included in the contract or other binding document and a copy of this UK Processor Policy will be incorporated into such contract or other binding document or referenced with a possibility of electronic access. Where the personal data is subject to UK data protection law, the contract or other binding document between EY and the Controller will include the required elements as provided by article 28 of the UK General Data Protection Regulation ("UK GDPR").

If EY is unable to comply with this Rule or its obligations under this UK Processor Policy, EY will inform the Controller promptly of this fact. The Controller may then take appropriate action (such as suspending the transfer of personal data and terminating the contract or other binding document it has with EY).

Rule 3 — Ensuring data quality

Rule 3A — EY will assist the Controller to keep personal data *accurate* and *up to date*.

EY will act upon the instructions of the Controller in order to help and assist such Controller to comply with its obligations to keep personal data accurate and up to date. EY shall execute any necessary measures when asked by the Controller in order to have the personal data updated or corrected.

When required to do so on instruction from a Controller, as required under the terms of the contract or other binding document with that Controller, EY will delete, anonymize, update or correct personal data.

EY will notify other EY Network entities or any third-party sub-processors to whom the personal data has been disclosed accordingly so that they can also update their records.

Rule 3B — EY will only keep personal data in a form which permits identification for *as long as is necessary*.

Personal data will always be retained and/or deleted or anonymized to the extent required by law, regulation and professional standards, under the instructions of the Controller (provided such instructions do not conflict with such law, regulation and professional standards) and in line with the applicable EY service lines and any local retention policies applying to an EY Network entity. EY will dispose of personal data only in a secure manner in accordance with EY global security policies.

On the termination of the provision of professional services to a Controller, EY will — at the choice and at the request of the Controller — return all the personal data transferred and the copies thereof to the Controller or destroy all the personal data (except for backup copies) and certify to the Controller that it has done so. If applicable legislation or professional regulations prevent EY from returning or destroying the personal data to a Controller, EY will ensure that such personal data remains confidential.

Rule 3C — EY will only keep personal data which is *relevant* to EY.

EY will identify the minimum amount of personal data that is required in order to properly fulfil its purpose. EY will only process personal data that is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

Rule 4 — Taking appropriate security measures

Rule 4A — EY will always adhere to its *IT Security Policies* and the information security measures as specified in the contract or other binding document with a Controller.

EY will comply with the requirements contained in EY global security policies as revised and updated from time to time together with any other information security procedures relevant to a business area or function, as well as with information security measures specified in a contract or other binding document it enters into with a Controller.

The technical and organizational security measures as implemented by EY will be designed to implement data protection principles and to facilitate compliance with data protection by design and by default.

Rule 4B — EY will ensure that providers of services to EY also adopt appropriate and equivalent security measures.

UK law expressly requires that where a provider of a service to EY has access to EY Data, strict contractual obligations, evidenced in writing and dealing with the security of that data, are imposed to ensure that such service providers act only on EY's instructions when using that data and that they have in place appropriate technical and organizational security measures to safeguard the personal data.

Rule 4C — EY will notify a Controller of any personal data breach in relation to personal data processed on behalf of the Controller in accordance with and to the extent required by applicable law and in accordance with the terms of the contract or other binding document with that Controller.

EY will notify a Controller of any personal data breach in relation to personal data processed on behalf of that Controller in accordance with and to the extent required by applicable law and the terms of the contract or other binding document with that Controller. A personal data breach means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data. Where a breach is subject to UK data protection law, EY will notify the Controller without undue delay after becoming aware of a personal data breach.

Rule 4D — EY will ensure that sub-processors undertake to comply with provisions that are consistent with the terms in its contract or other binding document with a Controller and this UK Processor Policy, specifically with regard to the adopting of security measures.

EY may only appoint sub-processors who provide appropriate and equivalent technical and organizational security measures that are applicable to their use of the personal data to which such sub-processor will have access in accordance with the terms of the contract or other binding document EY has with the Controller.

To comply with this Rule, where a sub-processor has access to EY Data, EY will impose strict contractual obligations, in writing, on the sub-processor regarding (i) the security of such data, consistent with those contained in this UK Processor Policy and with the terms of the contract or other binding document EY has with the Controller, (ii) the sub-processor's obligation to act only on EY's instructions when using EY Data and (iii) such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by EY in this UK Processor Policy.

Rule 4E — EY will comply with the requirements of a Controller regarding the appointment of any sub-processor.

EY will inform the Controller where processing, undertaken on its behalf in the context of providing services, will be conducted by a sub-processor and will comply with the particular requirements of a Controller with regard to the appointment of sub-processors as set out under the terms of the contract or other binding document with that Controller. EY will ensure that up-to-date information regarding its appointment of sub-processors is available to the Controller at all times so that its general consent is obtained. If, on reviewing this information, a Controller objects to the appointment of a sub-processor to process personal data on behalf of EY, that Controller will be entitled to take such steps as are consistent with the terms of the contract or other binding document it has with EY.

Rule 5 — Honoring individuals' rights

Rule 5A — EY will assist the Controller to comply with the rights of individuals to be informed whether any personal data about them is being processed.

EY will act in accordance with the instructions of the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to respect the rights of individuals.

Rule 5B — EY will handle requests from individuals to rectify, restrict the processing of personal data, receive data in a machine-readable format or to object to the processing of their personal data in accordance with the instructions of the Controller and — where applicable — with the *Individual's Rights Request Procedure*.

Individuals have the rights to ask for rectification of the personal data EY holds about them where it is inaccurate or incomplete. In certain circumstances, individuals may also request erasure, the restriction of or object to the processing of their personal data or to receive personal data in a machine-readable format and have the right to transmit those data to another controller (data portability).

EY will act in accordance with the terms of the contract or other binding document it has with the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to respect the rights of individuals. If an EY Network entity receives a request from an individual, it will manage such request in accordance with the contract or other binding document it has with the Controller, which may include transferring the request to the relevant Controller and not responding to such request. Where

EY is authorized to do so or is required by law, EY will adhere to the *Individual's Rights Request Procedure* (as set out in Appendix 2).

Rule 6 — Ensuring adequate protection for international transfers

Rule 6 — EY will *not* transfer personal data to external third parties *outside* the United Kingdom *without ensuring adequate protection* for the data.

In principle, international transfers of personal data to third parties outside the UK are not allowed without appropriate steps being taken by EY, such as contractual clauses, in order to protect the personal data that is being transferred.

Rule 7 — Safeguarding the use of sensitive personal data

Rule 7A — EY will only process sensitive personal data as instructed by a Controller and only if such processing is *absolutely necessary*.

"**Sensitive personal data**" is data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, and data concerning a natural person's sex life or sexual orientation. Legal restrictions may also apply to criminal convictions, social security files, government identification numbers or financial account numbers under applicable laws. Sensitive personal data needs to be handled with additional care, in order to respect local customs and applicable local laws. In particular, EY will:

- Only process sensitive personal data under the instructions of the Controller
- Avoid collection of sensitive personal data where it is not required for the purposes for which the data is collected or subsequently processed
- Limit access to sensitive personal data to appropriate persons (by either masking or making anonymous or pseudonymous the data, where appropriate) in accordance with the security standards established in EY Global Information Security Policies and the instructions of the Controller

Rule 7B — EY will only process sensitive personal data where the Controller has obtained the individual's *explicit consent* unless the Controller has a legitimate basis for doing so consistent with the requirements of applicable data protection laws.

In principle, individuals must give their explicit consent to the processing of their sensitive personal data. This consent must be obtained by the Controller, unless the Controller has a legitimate basis for processing sensitive data. Consent to process sensitive personal data must be specific, informed, unambiguous and freely given. The responsibility to obtain the consent of the individuals is on the Controller.

Rule 8 — Automated individual decisions

Rule 8 — Individuals have the right not to be subject to a decision based solely on automated processing and to know the logic involved in such decision as well as the significance and the envisaged consequences of such processing. EY will assist Controllers in taking necessary measures to protect the legitimate interests of individuals.

Under UK data protection law, no decision which produces legal effects concerning an individual or significantly affects that individual can be based solely on the automated processing of that individuals' personal data (including profiling), unless such decision is: (i) necessary for entering into, or performance of, a contract between the individual and the data controller; (ii) authorized by law; or (iii) based on the individual's explicit consent. EY will act in accordance with the instructions of the Controller and undertake any reasonably necessary measures to enable the Controller to comply with its duty to inform individuals.

Section B — Practical Commitments

Rule 9 — Training

Rule 9 — EY will provide appropriate *training* to EY Personnel who have *permanent or regular access* to personal data, who are involved in the processing *of personal data* or in the *development of tools* used to process personal data.

EY will take reasonable and appropriate steps to communicate with EY Personnel and to provide appropriate training on the requirements of this UK Processor Policy in accordance with the Privacy Training Program set out in Appendix 7.

Rule 10 — Records of processing and data protection impact assessments

Rule 10 — EY will keep a record of categories of processing activities carried out on behalf of the Controller. EY will assist the Controller in carrying out a data protection impact assessment if the processing activities are likely to result in a high risk to the rights and freedoms of natural persons.

EY Network entities keep a record of processing activities. This record will be in writing, including in electronic form, and will be made available to the ICO on request.

Rule 11 — Assessment of compliance

Rule 11A — EY will comply with the *Assessment of Compliance Protocol* set out in *Appendix 3*.

Rule 11B — EY will — at the request of a Client acting as a Controller — allow its data processing facilities to be audited in relation to the processing activities of the Controller.

EY will allow its data processing facilities to be audited at the request of a Client. Such audit may consist of:

- The provision by EY of written information (including, without limitation, questionnaires, related independent SOC2 audit reports or reports of a similar nature and information security policies) that may include information relating to sub-processors

  Or

- Interviews with EY's IT personnel

Such audit may be carried out by the Client or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, provided such members are not working for direct competitors of EY.

For the avoidance of doubt, no access to any part of IT systems or infrastructure will be permitted due to strict confidentiality obligations towards Clients.

Rule 12 — Complaint handling

Rule 12 — EY will comply with the *Complaint Handling Procedure* set out in *Appendix 4*.

Rule 13 — Cooperation with the ICO

Rule 13 — EY will comply with the *Cooperation Procedure* set out in *Appendix 5*.

Rule 14 — Update of the rules

Rule 14 — EY will comply with the *Updating Procedure* set out in *Appendix 6*.

Rule 15 — Actions in case of national legislation preventing respect for the UK Processor Policy

Rule 15A — EY will ensure that where it believes that existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller, or its obligations under the UK Processor Policy, or its obligations under the contract or other binding document with the Controller, EY will promptly inform the Controller, the Global Privacy Leader and the ICO unless otherwise prohibited.

Where EY has reasons to believe that the existing or future legislation applicable to it may prevent it from fulfilling the instructions received from the Controller, or its obligations under this UK Processor Policy or the obligations under the contract or other binding document it has with the Controller, it will promptly notify this to:

- The Controller, who is entitled to suspend the data transfer and terminate the contract or other binding document with EY
- The EY Global Privacy Leader
- The ICO

Rule 15B — EY will ensure that where it receives a *legally binding request for disclosure* **of personal data, which is subject to this UK Processor Policy, EY will:**

- **Notify the** *Controller promptly unless prohibited from doing so by a law enforcement authority*
- **Put the request on hold and notify the ICO for this UK Processor Policy unless prohibited from doing so by a law enforcement authority or agency**
- **Comply with the Law Enforcement Data Access Procedure set out in Appendix 8**

EY will assess each data access request by any law enforcement authority or state security body (the "**requesting authority**") on a case-by-case basis. EY will use best efforts to inform the requesting authority about EY obligations under UK data protection law and to obtain the right to waive this prohibition.

EY will put such request on hold for a reasonable delay in order to notify the ICO for this UK Processor Policy prior to disclosing the data to the requesting authority. EY shall clearly inform the ICO about the request, including information about the data requested, the requesting authority and the legal basis for the disclosure.

If, despite having used best efforts, EY is not in a position to notify the ICO and to put the request on hold, in such case, EY will provide on an annual basis general information about the requests it has received to the ICO (e.g., number of applications for disclosure, type of data requested and requesting authority if possible), to the extent it has been authorized by the said requesting authority to disclose such information to third parties. Transfers of personal data by an EY Network entity to any public authority will never be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

PART III: Appendices

Appendix 1

Data protection roles and responsibilities

Data Protection Network

1. EY Global Privacy Leader

1.1 The EY Global Privacy Leader is responsible for:

- Advising the Global General Counsel, Risk Management Executive Committee and other EYG leaders on data privacy matters
- Recommending modifications to the global privacy program, as regulations and the business environment evolve, and to other EY policies, practices or agreements relating to data privacy for Risk Management Executive Committee approval
- Maintaining the compliance of EY global systems with applicable data protection rules, including the UK Controller Policy and this UK Processor Policy (analysis of systems, definition of actions and ongoing compliance)
- Coordinating a community of EY Area Privacy Leaders (see below) for the purpose of competency building, collaboration on implementation of and revisions as necessary to the global privacy program (including the UK Processor Policy and UK Controller Policy), sharing of leading practices, monitoring of relevant applicable regulations, and consistency of communications between EY Network entities and their respective local regulators with the global privacy program
- Collaborating with EY Talent, Risk Management, General Counsel, and Global IT teams, service lines and other relevant functions on data privacy matters
- With the assistance of the Area Privacy Leaders, overseeing the compliance of EY Network entities with the global privacy program (including the UK Controller Policy and this UK Processor Policy)
- With the assistance of the Area Privacy Leaders, developing and providing communications and uniform training material and support
- With the assistance of the Area Privacy Leaders, providing guidance to EY Network entities in implementing and modifying local data privacy policies and compliance programs.

2. Area Privacy Leaders

2.1 EY Area Privacy Leaders work with the EY Global Privacy Leader to evaluate and develop global policy and processes. The Area Privacy Leaders will coordinate the implementation of the UK Processor Policy locally. In particular, they are responsible for the following within their respective Areas:

- Providing assistance to Regional Privacy Leaders and Local Privacy Leaders to identify local business, and legal and regulatory risks surrounding data privacy issues
- Providing assistance to Regional Privacy Leaders and Local Privacy Leaders on local privacy matters, including developing local data privacy policies, as necessary
- Developing and implementing consistent solutions on a global or area basis to mitigate data privacy risks
- Coordinating the development and implementation of a data privacy program in their area that complies with the global privacy program (including the UK Controller Policy and this UK Processor Policy)

- Advising the General Counsel's Office and relevant executive and country management on data privacy issues
- Escalating within the General Counsel's Office and relevant executive, Regional and country management any significant compliance issues and plans for their resolution, as well as implications of local data privacy regulations
- Advising the EY Global Privacy Leader of any local data privacy regulations in their Area that may have international or cross-border implications, which are not adequately addressed by the global privacy program (which includes the UK Processor Policy)
- Confirming to the EY Global Privacy Leader, EY Network entity compliance with the global privacy program and, in particular, the UK Processor Policy
- Collaborating with relevant Talent, Risk Management, General Counsel and IT teams, service lines, and other relevant functions on data privacy matters
- Periodically monitoring the effectiveness of the Area Privacy functions

3. Regional / Local Privacy Leaders

3.1 EY may appoint Regional / Local Privacy Leaders to assist with the coordination and implementation of Global standards locally.

3.2 The Regional / Local Privacy Leader remains knowledgeable about the relevant country, region and state laws, governmental regulations, professional practice obligations, and regulatory guidance, which relate to data privacy compliance and are applicable to the EY Network entities of the Region.

3.3 The Regional / Local Privacy Leader handles subject access requests and complaints under the UK Processor Policy and may refer such request or complaint to the Area Privacy Leader or the Global Privacy Leader as needed.

Data Protection Officers

1.1 EY Network entities that are subject to the UK Data Protection Act 2018 shall designate a Data Protection Officer ("DPO") where they have determined that 1) its core activities consist of processing operations which require regular and systematic monitoring of individuals on a large scale; or 2) the core activities consist of processing on a large scale of sensitive personal data (Rule 7A) and personal data relating to criminal convictions and offences.

1.2 Various EY Network entities may appoint one DPO, for example a DPO acting on behalf of all EY Network entities in one Region.

1.3 The DPO may be the same person as the Regional or Local Privacy Leader but the role may also be undertaken by a separate individual.

1.4 Where a DPO is acting on behalf of multiple EY Network entities, such EY Network entity will appoint a Local Privacy Leader who will assist the DPO in the exercise of its responsibilities. The DPO may delegate its responsibilities to the Local Privacy Leader who may perform these responsibilities under supervision and on behalf of the DPO.

1.5 A DPO will have the following responsibilities:

- Informing and advising the EY Network entity and EY Personnel with respect to obligations under the UK Data Protection Act 2018;
- Monitoring the EY Network Entity's compliance with the UK Data Protection Act 2018, the regulations of Ernst & Young Global Limited insofar as they relate to the protection of personal data and any other applicable policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of EY Personnel and conducting and/or arranging for internal audits as appropriate;
- When requested, advising on data protection impact assessments;
- Working and cooperating with the EY Network Entity's designated representative where applicable and serving as the contact point for the representative on issues relating to the processing of personal data;

- Being available to respond to inquiries from individuals relating to data protection practices and data subjects' rights, including withdrawal of consent, the right to be forgotten, and related rights;
- Assisting in the developing and monitoring of local procedures for personal data breach handling, and being available as a first point of contact to assist with responding to any breaches of personal data, including assessing whether the data breach must be notified to the ICO and/or individuals;
- Keeping up-to-date the EY Network Entity's record of processing;
- Keeping up-to-date its in-depth knowledge of the UK Data Protection Act and the GDPR, including data protection guidance issued by the ICO and relevant legal decisions that may impact the EY Network Entity's processing of personal data;
- Providing an annual report for the EY Network Entity's leadership (as applicable).

1.6 The DPO may fulfill other tasks and duties, provided such tasks and duties do not result in a conflict of interests.

1.7 EY will publish the contact details of EY Network Entities' DPOs on EY's website ey.com.

Appendix 2

Individual's Rights Request Procedure

1. Subject Access Request Procedure

1.1 UK data protection law gives individuals whose personal data is processed the right to be informed whether any personal data about them is being processed by an organization. This is known as the right of subject access.

1.2 When EY processes personal data on behalf of a Controller, EY is considered to be a processor of the data and the Controller will be primarily responsible for meeting the legal requirements as a controller. If an EY Network entity receives a subject access request, the EY Network entity will manage such request in accordance with the contract or other binding document it has with the Controller. This may include transferring the request to the Controller and not responding to such request. Where EY is authorized to do so or is required by law, EY will adhere to the terms of this Individual's Rights Request Procedure.

1.3 Where a subject access request is subject to UK data protection law, such a request will be dealt with by EY in accordance with this Individual's Rights Request Procedure (referred to as "**valid request**" in this procedure). A subject access request is subject to UK data protection law where the EY Network entity or the Controller is established in the UK or where the processing activities are related to the offering of goods or services to individuals in the UK or to the monitoring of their behaviour as far as their behaviour takes place within the UK. Where applicable local data protection law differs from any aspect of this Individual's Rights Request Procedure, the local data protection law will prevail.

1.4 An individual making a valid request to an EY Network entity is entitled to:

1.4.1 Be informed whether the EY Network entity holds and is processing personal data about that individual and, where that is the case, access such personal data

1.4.2 Be given a description of the personal data; the purposes for which they are being held and processed; the recipients or classes of recipient to whom the personal data is, or may be, disclosed by the EY Network entity (in particular recipients in third countries); the envisaged period for which the personal data is stored or — if this is not possible — the criteria used to determine that period; the existence of the right to request from the Controller rectification or erasure of personal data or restriction of processing; the right to lodge a complaint with the ICO and — where personal data are not collected from the individual — any available information as to their resource

1.4.3 Receive — free of charge — a copy of the personal data undergoing processing; for any further copies requested by the individual, a reasonable fee based on administrative costs may be charged

1.5 The request must be made in writing[8], which can include email. Where the individual makes the request by electronic means, the personal data shall be provided in a commonly-used electronic form, unless otherwise requested by the individual.

1.6 The EY Network entity must respond to a valid request without undue delay and in any event within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. The individual will be informed of any such extension within one month of receipt of the request, together with the reasons for the delay.

1.7 The EY Network entity is not obliged to comply with a subject access request unless the EY Network entity is supplied with such information which it may reasonably require in order to confirm the identity of the individual making the request and to locate the information which that person seeks.

[8] Unless the local data protection law provides that an oral request may be made, in which case EY will document the request and provide a copy to the individual making the request before dealing with it

2. Procedure

2.1 Receipt of a subject access request

2.1.1 If any member of EY Personnel receives a request from an individual for access to his or her personal data, they must first pass the communication to the Controller. If the EY Network entity is authorized to deal with such request directly or is required by law, they must then pass the communication to the Local Privacy Leader or DPO (where applicable) indicating the date on which the request was received together with any other information that may assist the Local Privacy Leader or DPO (where applicable) to deal with the request.

2.1.2 The request does not have to be official or mentioned as data protection law to qualify as a subject access request.

2.2 Initial steps

2.2.1 The Local Privacy Leader or DPO (where applicable) will make an initial assessment of the request to decide whether it is a valid request and whether confirmation of identity, or any further information, is required.

2.2.2 The Local Privacy Leader or DPO (where applicable) will then contact the individual in writing to confirm receipt of the subject access request, seek confirmation of identity or further information, if required, or decline the request if one of the exemptions to subject access applies.

2.3 Exemptions to subject access

2.3.1 A valid request may be refused on the following grounds:

a. Where the Controller instructs the EY Network entity not to deal with such request directly

b. If the refusal to provide the information is consistent with the data protection law within the jurisdiction in which that EY Network entity is located

Or

c. Where the subject access is not subject to UK data protection law

2.4 The Search and the response

2.4.1 The Local Privacy Leader or DPO (where applicable) will arrange a search of all relevant electronic and paper-filing systems.

2.4.2 The Local Privacy Leader or DPO (where applicable) may refer any complex cases to the Area Privacy Leader or ultimately to the Global Privacy Leader for advice, particularly where the request includes information relating to third parties or where the release of personal data may prejudice commercial confidentiality or legal proceedings.

2.4.3 The information requested will be collated by the Local Privacy Leader or DPO (where applicable) into a readily understandable format (internal codes or identification numbers used at EY that correspond to personal data shall be translated before being disclosed). A covering letter will be prepared by the Local Privacy Leader or DPO (where applicable), which includes information required to be provided in response to a subject access request.

2.4.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. The other information referred to in 1.4 above must still be provided. In such circumstances, the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form.

2.5 Requests for erasure, amendment, cessation of processing or to port information

2.5.1 If a request is received for the deletion of that individual's personal data, such a request must be considered and dealt with as appropriate by the Local Privacy Leader or DPO (where applicable). If a request is received advising of a change in that individual's personal data,

such information must be rectified or updated accordingly if the EY Network entity is satisfied that there is a legitimate basis for doing so.

2.5.2 If the request is to cease processing that individual's personal data because the rights and freedoms of the individual are prejudiced by virtue of such processing by the EY Network entity, or on the basis of other compelling legitimate grounds, the matter will be referred by the Local Privacy Leader or DPO (where applicable) to the Area Privacy Leader and ultimately to the Global Privacy Leader to assess. Where the processing undertaken by the EY Network entity is required by law, the request will not be regarded as valid.

2.5.3 If a request is to receive personal data in a structured, commonly used and machine-readable format and to have that data transmitted to another controller, such a request must be considered and dealt with as appropriate by the Local Privacy Leader or DPO (where applicable).

2.6 All queries relating to this procedure are to be addressed to the Local Privacy Leader or DPO (where applicable).

Appendix 3

Assessment of Compliance Protocol

1. Background

1.1 The purpose of this UK Processor Policy is to safeguard personal data transferred between the EY Network entities where EY acts as a processor. This UK Processor Policy requires approval from the ICO. One of the requirements of the ICO is that EY assesses compliance with this UK Processor Policy and satisfies certain conditions in so doing, and this Appendix describes how EY deals with such requirements.

1.2 One of the roles of the EY Global Privacy Leader and also the Area Privacy Leader is to provide guidance about the processing of personal data subject to this UK Processor Policy and to assess the processing of personal data by the EY Network entities for potential privacy-related risks. The processing of personal data with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an ongoing basis. Accordingly, although this Appendix describes the formal assessment process adopted by EY to ensure compliance with this UK Processor Policy as required by the ICO, this is only one way in which EY ensures that the provisions of the UK Processor Policy are observed and corrective actions are taken as required.

2. Approach

2.1 Scope of assessment

2.1.1 The EY Global Risk Management function ("Risk Management") will be responsible for carrying out assessments of compliance with this UK Processor Policy and will ensure that such assessments address all aspects of this UK Processor Policy (including methods of ensuring that corrective actions will take place). The assessments will comprise a review of the performance of particular functions within the business and also an assessment of the EY Network entity adopting a risk-based approach. Risk Management will be responsible for ensuring that the results of the assessment are brought to the attention of the EY Global Privacy Leader who will ensure that any actions identified to implement this UK Processor Policy take place correctly. The Global Privacy Leader will ensure that any reports indicating unsatisfactory compliance in relation to the UK Processor Policy will be brought to the attention of the Global General Counsel who attends the meetings of the Global Executive.

2.1.2 EY Clients (or auditors acting on their behalf) may assess compliance with the commitments made in this UK Processor Policy in accordance with the terms of the relevant Client's contract with an EY Network entity. The assessment of compliance may consist of:

- The provision by EY of written information (including, without limitation, questionnaires, related independent SOC2 audit reports or reports of a similar nature and information security policies) that may include information relating to sub-processors

  Or

- Interviews with EY IT personnel

2.1.3 EY will not provide a Client with access to any part of IT systems or infrastructure which process personal data of other Clients.

2.2 Timing

2.2.1 Review of compliance with the global privacy program, including the UK Processor Policy, will take place on a regular basis at the instigation of Risk Management and as required by the terms of the relevant Client's contract with EY. The scope of the compliance assessment will be decided by EY's independent Global Internal Audit team with input from the Global General Counsel's Office.

2.3 Auditors

2.3.1 Review of compliance with this UK Processor Policy will be undertaken by Risk Management and responsibility for compliance with this UK Processor Policy on a day-to-day basis will be undertaken by the EY Global Privacy Leader and the Area Privacy Leaders.

2.3.2 In the event that a Client exercises its right to assess EY for compliance with this UK Processor Policy, such assessment may be undertaken by that Client, or by independent and suitably experienced auditors selected by that Client, as required and defined by the terms of the relevant Client's contract with an EY Network entity.

2.4 Report

2.4.1 Upon request and subject to applicable law and respect for the confidentiality and trade secrets of the information provided, EY will:

a. Provide copies of the results of any assessment of compliance with the UK Processor Policy to the ICO; and

b. Provide a copy of the results to the Client, to the extent that an assessment relates to personal data EY processes on behalf of that Client

2.4.2 EY will also provide a copy of the results of any assessment of compliance to the EY Global Privacy Leader who will be responsible for liaising with the ICO for this purpose. In addition, EY has agreed that in accordance with the provisions of clause 5 of the Cooperation Procedure,[9] the ICO may assess compliance by EY with this UK Processor Policy. The EY Global Privacy Leader will also be responsible for liaising with the ICO for this purpose.

[9]Clause 5 states: Where any EY Network entity is located within the the UK, EY agrees that that the ICO may audit that EY Network entity for the purpose of reviewing compliance with the BCR, in accordance with the applicable law of the UK.

Appendix 4

Complaint Handling Procedure

1. Background

1.1 This UK Processor Policy safeguards personal data transferred between EY Network entities where such entity acts as a processor. The content of this UK Processor Policy is determined by the ICO and one of the requirements is that EY must have a Complaint Handling Procedure in place. The purpose of this procedure is to explain how complaints brought by an individual whose personal data is processed by EY under this UK Processor Policy are dealt with.

2. How individuals can bring complaints

2.1 Individuals can bring complaints in writing by contacting the General Counsel's Office ("GCO") or the Global Privacy Leader, 6 More London Place, London, SE1 2DA, or via email at global.data.protection@ey.com.

2.2 Where a complaint relates to the processing of personal data by EY acting as a processor, EY will communicate the details of the complaint to the Controller promptly and will act in accordance with the terms of the contract or other binding document between the Controller and EY. If the Controller requires EY to deal with the complaint, the below mentioned steps will be applicable.

2.3 In circumstances where a Controller has disappeared, no longer exists or has become insolvent, individuals whose personal data is processed by EY on behalf of that Controller have the right to complain to the EY Network entity that is processing the data. EY will deal with such complaints in accordance with the below mentioned steps.

3. Who handles complaints?

3.1 The local GCO or Regional or Local Privacy Leader will handle all complaints arising under the UK Processor Policy in conjunction with executive leadership and the Global Privacy Leader, and will liaise with colleagues from relevant business and support units as appropriate to deal with complaints.

4. What is the response time?

4.1 The local GCO or Regional or Local Privacy Leader will acknowledge receipt of a complaint to the individual concerned within five working days (after having received confirmation from the Controller that it requires EY to deal with the complaint), investigating and making a substantive response within one month. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the local GCO or Regional or Local Privacy Leader will advise the complainant accordingly and provide a reasonable estimate for the timescale within which a response will be provided, which will not exceed six months from the date the complaint was brought.

4.2 The response will indicate whether the complaint is considered justified or whether it is rejected, as well as the consequences of such response.

5. When a complainant disputes a finding

5.1 If the complainant disputes the response (or any aspect of a finding) of the local GCO or Regional or Local Privacy Leader, the complainant notifies the local GCO or Regional or Local Privacy Leader accordingly. The matter will then be referred to the Region or Area GCO contact or ultimately to the Global Privacy Leader as appropriate who will review the case and advise the complainant of his or her decision either to accept the original finding or to substitute a new finding. The Region, Area GCO contact or Global Privacy Leader will respond to the complainant within one month of the referral. As part of the review, the Region or Area GCO contact or Global Privacy Leader may arrange to meet the parties in an attempt to resolve the complaint. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Region, Area GCO contact or Global Privacy Leader will advise the complainant accordingly and provide a reasonable estimate

for the timescale within which a response will be provided, which will not exceed three months from the date the complaint was referred.

5.2 If the complaint is upheld, the EY Region or Area GCO contact or Global Privacy Leader will arrange for any necessary steps to be taken as a consequence.

6. Right to complain to the ICO and to lodge an application with a UK court

6.1 In addition to the right to bring a claim to EY in accordance with this Complaint Handling Procedure, individuals whose personal data is processed in accordance with UK data protection law have the right to complain to the ICO and to lodge an application with a UK court. This also applies if the individual is not satisfied with the way in which the complaint relating to this UK Processor Policy has been resolved by EY.

Appendix 5

Cooperation Procedure

1. This Cooperation Procedure sets out the way in which EY will cooperate with the ICO in relation to this UK Processor Policy.
2. Where required, EY will make the necessary personnel available for dialogue with the ICO in relation to this UK Processor Policy.
3. EY will actively review and consider:
   - Any decisions made by the ICO on any data protection law issues that may affect the UK Processor Policy
   - The views of the ICO as outlined in its published guidance on Binding Corporate Rules
4. EY will provide upon request copies of the results of any assessment of compliance of the UK Processor Policy to the ICO subject to applicable law and respect for the confidentiality and trade secrets of the information provided.
5. EY agrees that:
   - Where any EY Network entity is located within the UK, the ICO may audit that EY Network entity for the purpose of reviewing compliance with this UK Processor Policy, in accordance with UK law or, in the case of an EY Network entity located outsidethe UK, in accordance with UK law (under which the personal data is transferred pursuant to this UK Processor Policy).
   - Where any EY Network entity is processing personal data on behalf of a Controller located within the UK, the ICO may audit that EY Network entity for the purpose of reviewing compliance with this UK Processor Policy, in accordance with UK law on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of EY.
6. EY agrees to abide by a formal decision of the ICO where a right to appeal is not exercised on any issues related to the interpretation and application of this UK Processor Policy.

Appendix 6

Updating Procedure

1. Background

1.1 This Updating Procedure sets out the way in which EY will communicate changes to this UK Processor Policy to the ICO, Controllers, data subjects and to the EY Network entities bound by this UK Processor Policy.

2. Material changes

2.1 EY will communicate in advance any material changes to this UK Processor Policy to the ICO as soon as reasonably practicable.

2.2 Where a change to this UK Processor Policy materially affects the conditions under which EY processes personal data on behalf of a Controller under the terms of the contract or other binding document EY has with that Controller, EY will communicate the proposed change to the Controller before it is implemented, and with sufficient notice to enable the affected Controller to object. The Controller may then suspend the transfer of personal data to EY and terminate its relationship with EY, in accordance with the terms of its contract or other binding document with EY.

3. Administrative changes

3.1 EY will communicate changes to this UK Processor Policy, which are administrative in nature (including changes in the list of EY Network entities) or which have occurred as a result of a change of applicable data protection law in the UK, through any legislative, court or the ICO measure, to the ICO at least once a year. EY will also provide a brief explanation of the reasons for any notified changes to this UK Processor Policy.

4. Communicating changes to the UK Processor Policy

4.1 EY will communicate all changes to this UK Processor Policy, whether administrative or material in nature, to the EY Network entities bound by this UK Processor Policy, and material changes to the Controller and data subjects who benefit from this UK Processor Policy.

4.2 Communication internally will be via the EY internal communications process which comes from the EY Global Leader, Risk Management and the EY Global Vice Chair and General Counsel, cascading down to the Area Privacy Leaders, Regional Privacy Leaders and General Counsel's Offices, and Local Privacy Leaders and Local General Counsel's Offices. Such communication includes publication on EY's intranet and on EY's external site: ey.com/bcr.

4.3 EY will communicate to the ICO any substantial changes to the list of EY Network entities once a year. Otherwise, EY will communicate an up-to-date list of entities to the ICO.

5. Logging changes to the UK Processor Policy

5.1 This UK Processor Policy contains a change log which sets out the date on which this UK Processor Policy is revised and the details of any revisions that have been made.

5.2 The Global Privacy Leader will maintain an up-to-date list of the EY Network entities this UK Processor Policy is applicable to. EY will ensure that all new EY Network entities are bound by this UK Processor Policy before a transfer of personal data to them takes place. Each EY Network entity will maintain an up-to-date list of all sub-processors it has appointed to process personal data on behalf of a Controller.

Appendix 7

Privacy Training Program

1. Background

1.1 EY trains EY Personnel on the basic principles of data protection, confidentiality and information security awareness. Training and awareness will be provided through posting messages and videos on EY's intranet and daily news articles, as well as by making available web-based training courses.

1.2 EY Personnel who have permanent or regular access to personal data, and who are involved in the processing of personal data or in the development of tools to process personal data receive additional, tailored training on the Policies and specific data protection issues relevant to their role. This web-based training is further described below.

2. Responsibility for the privacy training program

2.1 The EY Global Privacy Leader has overall responsibility for privacy training at EY, with input from colleagues from other functional areas, including Information Security, Talent and other departments, as appropriate. They will review training from time to time to ensure it addresses all relevant aspects of the UK Processor Policy and that it is appropriate for individuals who have permanent or regular access to personal data, and who are involved in the processing of personal data or in the development of tools to process personal data.

2.2 Communication and training should cover data privacy elements such as:

- Basic principles
- Importance of data privacy
- Definitions
- Personal and sensitive personal data
- Data privacy considerations with respect to information security

3. About the training courses

3.1 EY has developed a global Web-Based Learning (WBL) that is available for all EY Personnel. The course is designed to be both informative and user-friendly, generating interest in the topics covered. At the end of the WBL, EY Personnel must correctly answer a series of multiple choice questions for the course to be deemed complete.

3.2 EY management supports the completion of the WBL and is responsible for ensuring that individuals within the organization are given appropriate time to complete the course. Local management determines which members of EY Personnel in their respective country will be mandated to complete the WBL. Compliance will be monitored. New hires are required to complete the training as part of their induction program.

4. Awareness

4.1 EY will regularly provide reinforcement content to EY Personnel reminding them of their responsibilities regarding data protection, confidentiality and information security awareness. Such content will be provided through posting messages and videos on EY's intranet, posters in EY network entities' offices and daily news emails provided to all EY Personnel.

Appendix 8

Law Enforcement Data Access Procedure

1. Background

1.1 This Law Enforcement Data Access Procedure sets out EY's policy for responding to a request received from a law enforcement or other government authority (together the "**Requesting Authority**") to disclose personal data processed by EY on behalf of a Controller (hereafter "**Data Production Request**"). Where EY receives a Data Production Request, it will handle that Data Protection Request in accordance with this Procedure. If applicable data protection law(s) require a higher standard of protection for personal data than is required by this Procedure, EY will comply with the relevant requirements of applicable data protection law(s).

2. General principle on Data Production Requests

2.1 As a general principle, EY does not disclose personal data in response to a Data Production Request unless either:

- It is under a compelling legal obligation to make such disclosure

  Or

- Taking into account the circumstances and the privacy rights of any affected individuals, there is an imminent risk of serious harm that merits disclosure in any event

2.2 Even where disclosure is required, EY's policy is that the Controller should have the opportunity to protect the personal data requested because it has the greatest interest in opposing, or is in the better position to comply with, a Data Production Request.

2.3 For that reason, unless it is legally compelled to do so or there is an imminent risk of serious harm, EY will first consult with the ICO and provide the Controller with details of the Data Production Request. EY will cooperate with the ICO and the Controller to address the Data Production Request.

3. Data Production Request Review

3.1 If EY receives a Data Production Request, the recipient of the request must pass it to EY's Regional or Local Privacy Leader or DPO (where applicable) and Regional or Local General Counsel immediately upon receipt, indicating the date on which it was received together with any other information which may assist EY's Regional or Local Privacy Leader or DPO (where applicable) and Regional or Local General Counsel to deal with the request.

3.2 The request does not have to be made in writing, made under a Court order, or mention data protection law to qualify as a Data Production Request.

3.3 EY's Regional or Local Privacy Leader or DPO (where applicable) and Regional or Local General Counsel will carefully review each and every Data Production Request individually and on a case-by-case basis, and will deal with the request to determine the nature, urgency, scope and validity of the Data Production Request under applicable laws and to identify whether action may be needed to challenge the Data Production Request.

4. Notice of a Data Production Request

4.1 After assessing the nature, urgency, scope and validity of the Data Protection Request, EY will notify and provide the Controller with the details of the Data Production Request prior to disclosing any personal data, unless legally prohibited or where the imminent risk of serious harm prohibits prior notification.

4.2 EY will also put the request on hold in order to notify and consult with the ICO, unless legally prohibited or where the imminent risk of serious harm prohibits prior notification.

4.3 Where EY is prohibited from notifying the ICO and suspending the request, EY will use its best efforts (taking into account the nature, urgency, scope and validity of the request) to inform the Requesting Authority about its obligations under applicable data protection law(s) and to obtain the right to

waive this prohibition. Such efforts may include asking the Requesting Authority to put the request on hold so that EY can consult with the ICO and may also, in appropriate circumstances, include seeking a court order to this effect. EY will maintain a written record of the efforts it takes.

5. Transparency reports

5.1 In cases where EY is prohibited from notifying the ICO about a Data Production Request, it commits to providing the ICO with a confidential annual report (i.e., "Transparency Report"), which reflects to the extent permitted by applicable laws, the number and type of Data Production Requests it has received for the preceding year and the Requesting Authorities who made those requests.

6. Queries

6.1 All queries relating to this Procedure are to be addressed to the EY Global Privacy Leader at global.data.protection@ey.com.

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

© 2020 EYGM Limited.
All Rights Reserved.

EYG no. 010400-18Gbl
BCR no. 2869
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

RE: E-mail à ANPD | Tomada de Subsídios - Transferência internacional de dados pessoais
ANPD - Normatizacao <normatizacao@anpd.gov.br>
Sex, 01/07/2022 16:20
Para:

- Ibrac <ibrac@ibrac.org.br>

Prezados, boa tarde.

Acusamos recebimento da petição contendo o esclarecimento a respeito das contribuições. Agradecemos, desde já, a participação dos senhores e senhoras na Tomada de Subsídios acerca da Norma sobre Transferência Internacional.

Atenciosamente,

Coordenação-Geral de Normatização
Autoridade Nacional de Proteção de Dados

De: Ibrac <ibrac@ibrac.org.br>
Enviado: quinta-feira, 30 de junho de 2022 18:12
Para: ANPD - Normatizacao <normatizacao@anpd.gov.br>

[redacted]

Assunto: E-mail à ANPD | Tomada de Subsídios - Transferência internacional de dados pessoais

Prezados,

Com relação à submissão de comentários e sugestões no contexto da Tomada de Subsídios para a elaboração do regulamento sobre transferências internacionais de dados pessoais, em nome do Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional – Ibrac, segue, em anexo, uma petição que esclarece que as contribuições de MARCELA MATTIUZZO na Tomada de Subsídios sobre Transferência Internacional, submetidas por meio da plataforma “Participa + Brasil”, foram feitas em nome do Ibrac.

Permanecemos à disposição e agradecemos a oportunidade!

Atenciosamente,
Bruno Drago | Diretor Presidente do Ibrac
Mateus Piva Adami | Diretor de Regulação do Ibrac
Denis Alves Guimarães | Coordenadora de Regulação do Ibrac
José Leça | Coordenador de Regulação do Ibrac
Letícia Lins de Alencar | Coordenadora de Regulação do Ibrac
Marcela Mattiuzzo | Coordenadora de Regulação do Ibrac

Instituto Brasileiro de Estudos de Concorrência, Consumo e Comércio Internacional
t. 55 11 3872-2609
ibrac@ibrac.org.br
www.ibrac.org.br

Contribuições no Documento Opine - Aqui

Número: OP-175501

Data: 19/05/2022 - 06:47

Resumo:
:"","174354":"","174356":"","174359":"","174360":"","174361":"","174362":"","174363":"","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373":"","174375":"","174376":"","174378":"","174379":"","174380":"

Contribuinte: Caio Matheus Cintra Moreira

Número: OP-179914

Data: 14/06/2022 - 08:52

Resumo: :"Primeiramente, destacamos que foi acertada a iniciativa da ANPD de possibilitar que toda a sociedade contribua na tomada de subsídios sobre a regulamentação de transferência internacional de dados, dado o profundo impacto da regulamentação para todos os atores envolvidos. Dito isso, alguns obstáculos para transferências internacionais de dados pessoais, de natureza prática ou jurídica, se destacam, entre os quais: (i) A ausência de regulamentação dos mecanismos de transferência previstos na LGPD, inclusive a ausência de definição dos graus de proteção de dados pessoais dos países estrangeiros; (ii) A existência de regulações complexas diferentes em vários países é um dos principais obstáculos que dificulta o atendimento a todos os requisitos legais impostos no contexto da transferência internacional de dados e pode, além de impactar as atividades de um agente de tratamento e a própria possibilidade de transferir dados pessoais, trazer risco para os agentes; (iii) Ausência de legislação de proteção de dados pessoais em países estrangeiros; (iv) Falta de clareza sobre o que de fato representa uma transferência internacional de dados para fins de aplicação das restrições e hipóteses específicas previstas na LGPD, destacando que não deve ser considerada transferência internacional, no mínimo, a hipótese em que o "importador" dos dados também já esteja sujeito à LGPD; (v) Mecanismos de transferência que, muito embora previstos na legislação, mostram-se muito complexos, morosos e custosos para implementação prática, podendo, inclusive, gerar efeitos indesejáveis de "data localization" ou trazer risco desarrazoado aos agentes; (vi) Legislações extremamente restritivas que vedem transferências internacionais ou que, mesmo não vedando, não forneçam instrumentos de transferência eficientes e de implementação prática viável; (vii) Mesmo mecanismos importantes e bastante utilizados não são simples de implementar, como cláusulas-padrão contratuais extremamente engessadas ou que incluam obrigações desarrazoadas para os agentes de tratamento; (viii) Práticas comerciais de agentes de tratamento que vedam a transferência internacional de dados para certas regiões

ou países, em razão de decisões das Autoridades de Proteção de Dados e/ou regras internas desses agentes; (ix) A ausência de decisões de adequação da legislação de proteção de dados do Brasil em relação a outros países e vice-versa. Nesse contexto, entendemos que a ANPD deveria: (i) priorizar o reconhecimento do nível de proteção de dados dos principais países estrangeiros ou organismos internacionais, em atenção ao inciso I do caput do artigo 33 da LGPD, inclusive considerando as decisões de adequação já proferidas em outras localidades, como a União Europeia; (ii) considerar que a exportação ou transferência de dados pessoais para fora do Brasil não é uma atividade inerentemente de risco. Só porque o dado pessoal está saindo do território brasileiro não significa que está imediatamente menos protegido, o que dependerá, por exemplo, dos instrumentos utilizados para a transferência, nível de proteção do país destinatário e da parte receptora, com a qual o dado está sendo compartilhado; (iii) destacar a importância das demais hipóteses previstas no art. 33, incisos III a IX da LGPD que autorizam a transferência internacional sem a necessidade de adoção de mecanismos contratuais adicionais; (iv) na construção de cláusulas-padrão contratuais, observar as regulamentações e experiências já existentes no Brasil para que possam ser utilizadas como referencial nesse contexto de transferência internacional e reconhecidas como instrumentos válidos de transferência, tal como as previstas nas Resoluções CMN n° 4893/21 e Resolução BCB n° 85/2021, que dispõem sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras, instituições de pagamento e demais instituições autorizadas a funcionar pelo Banco Central do Brasil. ","174354":"Em primeiro lugar, frisa-se que a existência da interoperabilidade é imprescindível, tanto dentro do território brasileiro quanto internacionalmente, e deve ser realizada o máximo possível, já que traz maior segurança e previsibilidade jurídica aos instrumentos já existentes e validados. Nesse sentido, a ANPD deve levar em consideração em sua regulação específica a extensão em que irão se alinhar com outras regulamentações aplicáveis de outros reguladores no país (como, por exemplo, o Banco Central), que possam impactar a transferência internacional. Importante que, na análise de convergência e interoperabilidade entre instrumentos contratuais brasileiros com os de outras jurisdições seja adotada, o quanto possível, a flexibilização, com possibilidade de: a) sem prejuízo da construção das cláusulas-padrão contratuais flexíveis pela ANPD que devem considerar as especificidades do país, considerar a possibilidade de equiparação e aceitação de cláusulas-padrão e outros instrumentos das demais jurisdições adotadas pelos agentes de tratamento, sempre que cabível e mantida a segurança jurídica necessária; b) possibilitar a realização de adaptações necessárias nos instrumentos existentes, visando garantir a convergência, mas mantendo-se, neste caso, a segurança jurídica; c) aceitação de selos e certificados que sejam globalmente reconhecidos, os quais poderiam, inclusive, ser parte integrante de contratos que, porventura, abarquem diferentes regulações internacionais; d) buscar, na medida do possível, convergência conceitual e terminológica. Ademais, em adição à regulamentação a ser emitida objeto da presente Tomada de Subsídios, sugere-se que a ANPD disponibilize em seu sítio a indicação das principais legislações internacionais a respeito de transferências internacionais, de modo a facilitar o acesso e entendimento por parte dos agentes de tratamento. Por fim, a ANPD pode

celebrar acordos de cooperação com outras autoridades de dados e disponibilizar essa informação no seu site, a exemplo da lista divulgada no site do Banco Central do Brasil das autoridades financeiras de outros países com as quais o regulador mantém acordo para troca de informações. ","174356":"Os instrumentos contratuais mais utilizados são, em primeiro lugar, as cláusulas-padrão, e em segundo as BCCs (“Binding Corporate Rules” – normas corporativas globais aplicadas entre empresas do mesmo grupo econômico em diferentes países). No entanto, importante destacar que as outras hipóteses previstas nos demais incisos do art. 33 da LGPD são também igualmente válidas e importantes para legitimar as transferências por entidades de todos os portes. Nesse contexto, em respeito ao disposto na LGPD, que não determina hierarquia entre esses mecanismos, não deve ser estabelecida obrigatoriedade ou priorização quanto ao uso de alguma das hipóteses previstas no art. 33, da LGPD. Além disso, a flexibilidade na forma de implementação das cláusulas ajuda na sua adoção, de modo que as cláusulas-padrão contratuais possam ser incorporadas de diferentes formas a outros contratos, por exemplo, como anexos, cláusulas contratuais no corpo do contrato ou incorporação por referência, ao invés de incluir todo o texto das cláusulas-padrão no instrumento contratual. ","174359":"É inegável a importância de se garantir o livre fluxo de dados, com menor fricção possível e proteção dos dados pessoais do titular, para as atividades e o desenvolvimento social e econômico do país – e não só da economia digital, bem como para possibilitar que os próprios titulares colham os benefícios gerados por meio desse fluxo informacional. Nessa linha, importantes são os benefícios quanto a aspectos de inovação e de integração com o comércio internacional, cada vez mais globalizado. O Brasil é um país que necessita estar integrado internacionalmente, fomentando sua presença no comércio internacional. Ademais, inúmeras empresas internacionais estão no Brasil e necessitam estar conectadas internacionalmente. Assim, a transferência de dados pessoais de maneira eficiente e por meio de estruturas simples, mas que protejam o titular, é essencial para permitir o incremento da economia brasileira. Quanto aos impactos, além da direta relação com os obstáculos já indicados na resposta à pergunta n. 1, destaca-se também a possível dificuldade para negociação e implementação prática dos mecanismos contratuais de transferência que vierem a ser regulamentados pela ANPD, especialmente se forem demasiadamente engessados, podendo, inclusive, inviabilizar práticas comerciais. A realidade dos atores que utilizarão esses modelos também deve ser levada em consideração, a fim de que as cláusulas façam sentido na prática do tratamento de dados e possam ser efetivamente cumpridas. Importante considerar que a implementação de instrumentos a serem previstos pela ANPD deve ocorrer para relações contratuais constituídas após a sua publicação e, ainda assim, com prazo de vacância condizente com a complexidade do tema, uma vez que a implementação efetiva dos mecanismos será complexa na prática. ","174360":"Qualquer critério/requisito a ser adotado deve ser pautado na flexibilidade, de modo que a regulamentação de cada mecanismo supracitado não envolva esforço desproporcional ou mesmo inviabilidade de atendimento por parte de importadores e/ou exportadores. Uma vez que as cláusulas contratuais específicas dependem de avaliação individual pela ANPD, possivelmente o mecanismo será pouco utilizado, além de onerar a ANPD. Já as normas corporativas globais seriam aplicadas em espectro mais restrito de transferências e, caso sejam excessivamente engessadas, podem encarecer ou mesmo

inviabilizar a sua adoção. Sugerimos que a ANPD priorize a definição de cláusulas-padrão contratuais, que podem ser aplicadas de forma mais ampla do que os demais instrumentos contratuais acima citados. A ANPD deve ainda buscar múltiplos mecanismos para permitir que as transferências de dados atendam às necessidades das empresas em todos os níveis: a.

Normas corporativas globais ("BCRs"): ¿ Somos favoráveis ao reconhecimento de BCRs já existentes e em vigor em outras jurisdições que oferecem o mesmo nível de proteção da LGPD, como, por exemplo, na União Europeia; ¿ Incentivamos a ANPD, ao definir critérios para aprovação das BCRs, observando o contexto brasileiro, evite a criação de novos requisitos específicos apenas para o Brasil ou que crie requisitos muito onerosos, para que as BCRs aprovadas de uma empresa em outra jurisdição funcionem no Brasil e não criem conflitos entre diferentes conjuntos de BCRs; ¿ Incentivamos a ANPD a definir critérios claros e viáveis para revisão e aprovação de BCRs, que contemple, inclusive, um processo acelerado para aprovação/adoção/reconhecimento de BCRs já aprovados em outras jurisdições que oferecem o mesmo nível de proteção da LGPD. b. Cláusulas Contratuais Padrão ("SCCs"): ¿ Incentivamos a ANPD a seguir a mesma abordagem de formatação baseada em módulos usada em alguns locais, como na União Europeia, que pode se adaptar prontamente à natureza das funções que cada parte está desempenhando em um determinado acordo (por exemplo, Controlador/Controlador, Controlador/Operador etc.), como um dos modelos possíveis para garantir maior flexibilidade na adoção de cláusulas padrão contratuais; ¿ Garanta flexibilidade na forma de implementação das cláusulas, de modo que possam ser incorporadas de diferentes formas a outros contratos, por exemplo, como anexos, cláusulas contratuais no corpo do contrato ou incorporação por referência, ao invés de incluir todo o texto das cláusulas-padrão no instrumento contratual; c. Certificações ¿

Incentivamos a ANPD a reconhecer a validade das aprovações e certificações recebidas de outras jurisdições que oferecem o mesmo nível de proteção da LGPD, pois novamente afirmam que ocorreu uma revisão regulatória robusta de processos e controles (por exemplo, "APEC Cross-Border Privacy Rules System"). De qualquer forma, os critérios a serem adotados pela ANPD não devem burocratizar os instrumentos e possibilitar a sua adoção, podendo ser baseados, por exemplo, em análise de risco (risk based approach) e accountability (prestação de contas e responsabilização), sendo que, para empresas que integrem o mesmo grupo econômico, as normas corporativas poderiam ser definidas e seu cumprimento monitorado pelo próprio grupo, com possibilidade de fiscalização pela ANPD, caso necessário. ","174361":"Sugere-se que os elementos previstos no artigo 34 da LGPD sejam considerados a nível principiológico, como o próprio artigo sugere, sem exigências de atendimento a regramentos específicos. Ademais, o art. 34, da LGPD prevê a avaliação específica de aspectos legais e regulamentares de outros países, o que entendemos não ser totalmente aplicável ao caso, uma vez que os instrumentos contratuais de transferência devem ser passíveis de utilização em qualquer país ou organismo internacional que não tenha uma decisão de adequação, nos termos do art. 33, I, da LGPD. ","174362":"Se por um lado as cláusulas-padrão totalmente rígidas, a exemplo das cláusulas-padrão contratuais adotadas na União Europeia, podem auxiliar na definição de padrão de proteção pré-estabelecido ou na fiscalização do seu cumprimento pela ANPD, por outro lado podem representar uma restrição excessiva ao fluxo informacional, onerando os agentes de tratamento e impactando a livre

iniciativa e a autonomia privada nas contratações. Entendemos que um modelo que permita flexibilidade na adoção das cláusulas-padrão com conteúdo adequado é um objetivo desejável, na medida em que propiciará a devida proteção dos dados pessoais e, também, a sua adoção em diferentes cenários. Também é importante considerar as regulamentações existentes no Brasil que podem ser utilizadas como referencial em caso de transferências internacionais. Citamos como exemplo as regras definidas pelo Banco Central do Brasil e pelo Conselho Monetário Nacional para a contratação de serviços relevantes de armazenamento e processamento de dados e de computação em nuvem por instituições financeiras e demais autorizadas a funcionar pelo Banco Central do Brasil. Nesse contexto, tais normas regulatórias indicam o conteúdo que as cláusulas dessas contratações específicas devem ter, sem prescrever a redação das cláusulas, permitindo maior flexibilidade para a sua adoção. Assim, sugerimos que a ANPD avalie a adoção de um modelo em que o conteúdo mínimo das cláusulas seja indicado – conteúdo esse que deve ser observar a razoabilidade e aplicação prática -, contemplando os requisitos essenciais e principiológicos para a transferência internacional, inclusive com a redação dessas cláusulas disponíveis para uso pelos agentes de tratamento, bem como outras disposições que podem ser adotadas de forma flexível, inclusive em relação à redação, e adequadas ao contexto da contratação e do fluxo de dados específico, mas preservando o mínimo exigível. Importante ressaltar a necessidade de a ANPD também observar, no que for cabível, ao avaliar os impactos e definir a regulamentação sobre transferência internacional, o disposto na Lei n. 13.874/19 (“Lei de Liberdade Econômica”) que estabelece normas de proteção à livre iniciativa e ao livre exercício de atividade econômica e disposições sobre a atuação do Estado como agente normativo e regulador. ","174363":"O modelo das cláusulas pode ser disponibilizado no site da ANPD para uso pelos agentes de tratamento. Havendo a possibilidade de flexibilizar as cláusulas – o que entendemos recomendável -, ou mesmo utilizar cláusulas-padrão “modulares” a serem adaptadas ao caso concreto, esses módulos também podem ser disponibilizados, além de ferramentas que facilitem a sua adoção, como checklist ou questionários, por exemplo, ou outras ferramentas de avaliação de sua aplicabilidade considerando critérios de relevância ou risco. Citamos como exemplo a experiência da Nova Zelândia, que permite a flexibilização das cláusulas, além de fornecer ferramentas que auxiliam na definição do instrumento de transferência internacional. Também reforçamos o exemplo do Banco Central do Brasil, já indicado em outras respostas, que orienta sobre o conteúdo das cláusulas em determinadas contratações, sem prescrever a redação. Por fim, sugerimos a edição de um guia orientativo sobre transferências internacionais. ","174364":"Pode ser recomendável a criação de regras diferenciadas, mas desde que observada a flexibilidade necessária para não inviabilizar a prática da transferência internacional. É também possível adotar um modelo único que considere os diversos cenários/papéis dos agentes de tratamento, mas deixando claro as cláusulas/disposições que se aplicariam a depender do papel exercido pelo agente. Pensamos que é também importante manter os padrões de responsabilização de prestação de contas trazidos pela LGPD, sem importar para onde ou de onde os dados serão transferidos. Além disso, os Controladores devem garantir que seus operadores e suboperadores respeitem e protejam os dados pessoais a eles confiados, cumprindo os critérios e padrões trazidos pela LGPD. Nesse sentido, os

operadores devem obeceder às instruções do Controlador e garantir a segurança dos dados pessoais presentes em seus sistemas. Esses requisitos já estão presentes na LGPD – qualquer requisito específico quanto às transferências internacionais deve ser estritamente adaptado para lembrar e exigir dos agentes de tratamento que suas obrigações já existentes não terminam nas fronteiras do Brasil. ","174367":"Como as normas corporativas globais são aplicáveis a empresas de um mesmo grupo econômico, entende-se viável garantir maior flexibilidade nesse caso, como citado na resposta à questão 5. Nesse contexto, por exemplo, poder-se-ia avaliar a dispensa da aprovação ou mesmo de submissão prévia junto à ANPD, o que pode, inclusive, exigir recursos de que a Autoridade não dispõe neste momento e gerar um gargalo que inviabilize a adoção desse mecanismo. Além disso, a ANPD também poderia dispensar da aprovação normas corporativas globais que sigam modelo orientativo, não vinculante, disponibilizado pela ANPD (seja por meio de template ou de conteúdo mínimo indicativo que deva constar das normas corporativas globais), bem como daquelas normas corporativas globais já aprovadas em outros países, especialmente os que venham a ser considerados com nível de proteção adequado pela ANPD. Para tanto, sugere-se a interpretação do caput do artigo 35 da LGPD concomitante com o disposto no seu §2°, de modo que a ANPD poderia optar por emitir orientações a serem observadas nesse caso, requisitando evidências e/ou informações complementares, caso necessário. Esses mecanismos podem facilitar a adoção deste instrumento, ainda subutilizado em outas jurisdições razão do processo moroso, complexo e custoso para a sua aprovação. Outros pontos importantes são: (i) O conteúdo das normas corporativas globais deve ser flexível, na medida em que considera as especificidades de determinado grupo, mas é possível que a ANPD oriente sobre o conteúdo mínimo e forneça exemplos não vinculantes; (ii) É benéfico reconhecer mecanismos e políticas já adotados e implementados por grupos empresariais para as transferências internacionais; (iii) as normas corporativas globais devem ser aplicáveis às empresas do grupo que venham a ser expressamente indicadas, e não necessariamente para todo o grupo; (iv) a ANPD deve manter constante diálogo com o agente de tratamento na avaliação de normas corporativas globais, de modo que haja espaço para a construção e adaptação levando em conta o contexto dos tratamentos e dos agentes. ","174368":"Sugere-se observar, com as adaptações cabíveis, a definição indicada no sítio do Information Commissioner's Office (ICO) em relação a Binding Corporate Rules, ao prescrever que se destinam a "grupos empresariais multinacionais, grupos de empresas ou um grupo de empresas que exerçam uma atividade econômica conjunta, como franquias, joint ventures ou parcerias profissionais". As informações supracitadas estão disponíveis em: https://ico.org.uk/for-organisations/binding-corporate-rules/ O critério sugerido acima é adequadamente amplo e não precisa estar vinculado a conceitos de grupo econômico previstos na legislação nacional, como na lei de sociedades anônimas, por exemplo. Podem ser avaliadas as relações societárias dos agentes de tratamento envolvidos, de controle societário, controle comum ou conjunto, ou mesmo entre coligadas, mas deve-se considerar também situações fáticas e outras conformações corporativas. De qualquer forma, é essencial que as normas não sejam aplicáveis de forma automática ou obrigatória a todas as empresas do grupo, dependendo de sua indicação e adesão formal às normas corporativas globais. Por fim, destacamos que o conceito de grupo econômico a ser adotado no caso das normas

corporativas globais não necessariamente deve ser o mesmo em outras situações previstas na LGPD em relação ao grupo econômico, pois trata de situação específica de transferência internacional. ","174369":"Sugere-se que sejam exigidas informações sobre a categoria dos dados pessoais que serão objeto da transferência internacional, sem a necessidade de indicar de forma granular esses dados.","174371":"Parece-nos bastante benéfico permitir transferências internacionais entre grupos econômicos distintos cujas normas corporativas globais tenham sido aprovadas pela ANPD. Depreende-se que os grupos terão passado pela avaliação da ANPD para a aprovação de suas normas corporativas globais, que garantiriam o grau de proteção adequado ao titular dos dados, especialmente no caso das transferências intragrupo. ","174372":"É sabido que as cláusulas específicas para determinada transferência são muito pouco usadas, pois dependem de aprovação prévia, caso a caso, pela autoridade de dados competente. De qualquer forma, a ANPD pode avaliar a experiência de outros países e jurisdições que possuem mecanismo similar, seja para as cláusulas específicas ou para normas corporativas globais, especialmente outras jurisdições que adotam modelos distintos e mais flexíveis do que a utilizado pela União Europeia. Ressaltamos, inclusive, que o modelo de aprovação prévia é demasiado oneroso, tanto para as empresas, quanto para a Autoridade, que deve dedicar recursos para que tal avaliação não seja demorada e inviabilize ou encareça demais o processo. ","174373":"Os direitos a serem exercidos pelo titular são aqueles previstos na LGPD e não seriam modificados ou impactados em caso de alterações na configuração original da transferência, uma vez que os agentes que realizam a transferência deverão continuar a observar as garantias e os direitos dos titulares. Entendemos que não é necessário comunicar diretamente o titular, mesmo que haja alteração na configuração original da transferência. Eventuais informações sobre a possibilidade de transferência internacional de dados seria fornecida pelo agente de tratamento exportador pelos mecanismos de transparência adotados usualmente, como em sua política de privacidade. ","174375":"Sugere-se observar os mecanismos de resolução de conflitos existentes, a exemplo do Poder Judiciário e da arbitragem, para resolução de conflitos entre os agentes de tratamento. Ademais, deve-se respeitar as competências territoriais e de jurisdição já estabelecidas pelo Código Civil, pelo Direito Internacional Público e Privado, pois prevalecem sobre qualquer regulamentação a respeito desse tema. No que toca ao titular dos dados, importante destacar que este pode acionar o controlador, reclamar perante a ANPD e, também, socorrer-se do Poder Judiciário no caso de conflitos. Entendemos que acordos bilaterais, multilaterais ou acordos de cooperação entre autoridades de proteção de dados podem ser instrumentos importantes na resolução de conflitos, seja em relação aos agentes ou aos titulares. ","174376":"A melhor alternativa é por meio de obrigação assumida contratualmente, ou seja, assumindo-se via contrato a obrigação de observar requisitos para fins de conformidade. Selos, certificados e códigos de conduta, inclusive emitidos e aceitos globalmente, podem se tornar opções importantes para promover a conformidade e, também, viabilizar as transferências internacionais de forma mais fluída.","174378":"Sugere-se observar as disposições contratuais e, também, as regras já existentes no Brasil, notadamente as disposições do Código Civil aplicáveis à matéria e as definições quanto à responsabilidade solidária previstas na própria LGPD (artigo 42), quando aplicável.","174379":"Importante observar, antes de liberação de qualquer acesso, se a determinação recebida está de acordo

com as legislações aplicáveis e observa as formalidades exigidas para esses casos. ","174380":"Entendemos que a melhor forma para dar transparência aos titulares sobre a possibilidade de transferência internacional de seus dados e as hipóteses é por meio da política de privacidade. É essencial destacar que informação clara e relevante não se confunde com o fornecimento ao titular de informações granulares, detalhadas e exaustivas sobre agentes de tratamento específicos ou países destino de transferências internacionais. Isso se revela impossível na prática, além de extrapolar e, muito, o que seria uma informação relevante. O cenário de transferências internacionais é dinâmico, sendo impossível fornecer informações demasiadamente detalhadas em políticas de privacidade, sob o risco da informação se tornar incorreta e obsoleta e, também, de revelar segredos empresariais. Assim, caso a regulamentação venha a abordar este ponto, para além da regulamentação dos mecanismos de transferência, deve permitir flexibilidade na forma de dar transparência ao titular dos dados. Finalmente, os exportadores já devem observar a LGPD e dispor de canais e meios de contato para que o titular dos dados possa pedir informações ao controlador e/ou exercer os seus direitos garantidos pela LGPD.

Contribuinte: Luciana Taschner

Número: OP-180005

Data: 14/06/2022 - 14:03

Resumo: :"Falta de regulamentação das salvaguardas previstas no art. 33 da LGPD, limitando a utilização imediata aos incisos IV e VIII, do referido artigo, e aos arts. 33, IX cc. art. 7º, II, V e VI, hipóteses que não se enquadram na maioria das transferências de dados internacionais que ocorrem nas empresas.","174354":"Utilizar como parâmetro as normas internacionais, como as já estabelecidas pela União Europeia, bem como as recomendações da OCDE, Comitê Consultivo da Convenção 108, GPA, GPEN e rede ibero-americana, a exemplo da assinatura de Memorando de Entendimento com a Agência Espanhola de Proteção de Dados, em 2021, sem prejuízo de parcerias bilaterais com países como EUA, Reino Unido e Alemanha. .Acordos de cooperação técnica e memorandos de entendimento firmados pela ANPD com outros países e autoridades permitirão a adoção de mecanismos de cooperação internacional que facilitem a aplicação das legislações nacionais correspondentes na matéria de proteção de dados pessoais, voltados para o conhecimento e intercâmbio das melhores práticas e experiências, em relação a conflitos de jurisdição com países terceiros.","174356":"A escolha do instrumento mais efetivo dependerá da relação firmada entre as partes, bem como da complexidade das operações de tratamento a serem realizadas. Merecem destaques: • Normas corporativas globais (art. 33, II, c, LGPD): na prática, considerando o cenário da União Europeia, sua aplicação pode ser considerada dificultosa, considerando que o grupo empresarial que desejar implementar tal instrumento, deverá submetê-lo a um processo de aprovação da autoridade competente da UE (Article 63, GDPR). Ou seja, quando envolver filiais situadas em diversos países, é possível que seja necessário obter aprovação de diversas autoridades competentes, o que torna o processo moroso e oneroso. Por outro lado, uma vez implementadas, costumam ser mais fáceis de ser

mantidas, considerando a completude de informações contidas em seu bojo. Ainda, permitem um nível de flexibilidade maior em relação aos demais mecanismos de transferência, na medida em que a autoridade não precisa aprovar "non-material updates". • Cláusulas-padrão contratuais (art. 33, II, b): podem ser utilizadas como estratégia para transferências internacionais entre empresas distintas e cujo país terceiro, receptor dos dados, não ofereça níveis de proteção considerados adequados. Por ser um modelo pré-aprovado e avaliado previamente pela Autoridade, não é necessário que as empresas despendam tempo excessivo com negociações, visto tratar-se de um modelo fechado, mais seguro e simples. Ainda, de acordo com o IAPP-EY Annual Privacy Governance Report 2019, as SCCs costumam ser particularmente importantes para pequenas e médias empresas que podem não ter recursos suficientes para negociar contratos individualmente com cada parceiro comercial. A mesma pesquisa afirma que no cenário europeu, dentre os mecanismos de transferência internacional, 88% dos stakeholders afirmam utilizar as cláusulas contratuais padrão como salvaguarda principal, sendo estas, portanto, as mais utilizadas pelas empresas no âmbito da GDPR, e para as quais a ANPD pode dedicar particular importância no cenário brasileiro. Ainda considerando aspectos provenientes do cenário internacional, embora as SCCs sejam amplamente utilizadas por empresas menores e em casos de compartilhamento bilateral de dados, seu uso por grandes multinacionais pode ser impraticável a depender do contexto e frequência da transferência internacional de dados realizada, tendo em vista que: (i) as SCCs podem não ser adequadas para situações em que haja uma rede complexa de atividades de tratamento; (ii) empresas maiores com muitas afiliadas no exterior poderão ter que implementar centenas de SCCs para abranger todas as atividades de transferência internacional realizadas, o que pode ser extremamente custoso; (iii) alguns Estados-Membros da União Europeia exigem formalidades adicionais, como preenchimento e aprovação das SCCs pela autoridade supervisora, tornando o processo moroso e oneroso. • Cláusulas Contratuais específicas: em situações que não sejam viáveis normas corporativas globais ou cláusulas-padrão contratuais, o uso de cláusulas contratuais específicas pode se apresentar como uma salvaguarda eficaz, tendo em vista que são ajustáveis a qualquer tipo de relação e capazes de abranger qualquer nível de complexidade das transferências internacionais. Trata-se, portanto, de um subterfúgio menos oneroso e mais flexível, que pode ser implementado por todas as empresas, independentemente de seu porte.","174359":"• Possibilidade de armazenamento e operação internacional, o que pode representar economia nos custos do negócio; • Viabilização de transações de exportação/importação, com o estabelecimento de fluxos de dados entre países, instrumento chave para o desenvolvimento da economia digital e da inovação; • Possibilidade de mais serviços oferecidos ao consumidor, com acesso a um número maior de bens a um custo mais baixo, estimulando, assim, a livre concorrência; • Possibilidade de que pequenas empresas também tenham acesso a informações e serviços provenientes do cenário internacional, e possam se manter competitivas no mercado, reduzindo, por exemplo, a necessidade de altos investimentos com infraestrutura digital local. Ou seja, a depender da maneira como os mecanismos disponibilizados pela LGPD forem regulamentados pela ANPD, poderão ser instrumentos facilitadores à economia, ou poderão criar entraves e custos operacionais de modo a inviabilizar modelos de negócio e barrar o desenvolvimento econômico e a inovação dos agentes de tratamento. É importante que a

regulamentação esteja em harmonia com o cenário internacional, sobretudo Europa e EUA, já que grande parte do mercado e dos players internacionais já vêm se estruturando nesse sentido. É também relevante que a ANPD preveja medidas de segurança que sejam consideradas razoáveis (art. 34, IV, LGPD) para sustentar transferências internacionais, bem como critérios a serem observados em relação à transferência internacional, considerando o porte da empresa, a natureza dos dados e as categorias dos titulares envolvidos. Ainda, é necessário que a ANPD busque firmar acordos diplomáticos no âmbito internacional com outras autoridades reguladoras, de modo a viabilizar que sejam admitidos no exterior os instrumentos elaborados pelo Brasil e validados pela ANPD.","174360":"a. cláusulas-padrão contratuais: Por serem instrumentos jurídicos mais utilizados pelas empresas na União Europeia e serem de fácil utilização, merecem destaque pela ANPD, mitigando entraves jurídicos e divergências em sua aplicação, já que grande parte de empresas multinacionais já se baseiam nas regras adotadas internacionalmente. Logo, sugerimos que a ANPD edite um modelo de cláusulas-padrão para transferência internacional de dados pensado para as situações em que já exista em contrato firmado entre as partes a previsão de aplicação das cláusulas-tipo da Comissão Europeia, ou seja, um rol de disposições complementares – mas não conflitantes – com as europeias. Nesta linha, sugerimos a observância dos critérios estabelecidos no art. 46, II, c, do GDPR, além de documentos já disponibilizados pelo EDPB, inclusive Q&A, acerca da aplicação e utilização desses mecanismos de transferência. Sugerimos, ainda, a definição de parâmetros de utilização que não sejam excessivamente burocráticos e acabem tornando o uso do documento inviável para empresas multinacionais. Recomendamos, também, que a estruturação das cláusulas-padrão se dê de forma clara e concisa para que empresas de pequeno porte possam utilizar sem tantos entraves, e para que não tenham dificuldades de compreensão. Quanto à estrutura a ser utilizada, a Comissão Europeia concebeu as SCCs para serem instrumentos dinâmicos e adaptáveis compostos por: cláusulas fixas, que se destinam a permanecer inalteradas independentemente das partes a elas submetidas; módulos, adaptáveis ao agente de tratamento (controlador ou operador) que figurará como exportador ou importador; e cláusulas e anexos em branco (“livres”), que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados, entre outras). É nesse sentido que recomendamos que a ANPD siga na elaboração do referido documento, de modo a serem dinâmicos e adaptáveis conforme a necessidade das partes envolvidas na transferência internacional. Ainda, vale mencionar que o EDPB apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas contratuais padrão, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção dos dados pessoais transferidos. É recomendável que a ANPD também oriente os agentes de tratamento em relação a tais medidas suplementares, o que os auxiliará na implementação de salvaguardas efetivas para garantir a proteção dos dados sob transferência internacional, bem como para garantir sua confidencialidade, disponibilidade e integridade. b. cláusulas contratuais específicas: Deve indicar a salvaguarda da LGPD que consubstancia a operação (arts. 33 a 36, da LGPD), especificando a sua finalidade, discriminando as responsabilidades

dos agentes de tratamento e o fluxo de dados, além também de indicar como serão garantidos os direitos e liberdades dos titulares de dados. Sugerimos a adoção de critérios que permitam um nível maior de flexibilidade em relação aos demais mecanismos de transferência, adotando, por exemplo, a linha das BCRs, cujas atualizações "non-material" não precisariam ser aprovadas pela Autoridade ou mesmo aspectos que, se alterados e caso não conflitem com premissas bases definidas pela Autoridade, dispensariam também referida aprovação. c. normas corporativas globais: Devem levar em conta os critérios para transferência internacional provenientes do cenário internacional, considerando que várias empresas situadas no Brasil têm sede fora do país e já vem adotando critérios da própria Comissão Europeia e GDPR. Assim, sugerimos a utilização de parâmetros estabelecidos no art. 47 do GDPR, especialmente os relacionados ao conteúdo das normas corporativas globais, contendo em seu bojo aspectos como (i) a estrutura e os contatos do grupo empresarial ou do grupo de empresas envolvidas numa atividade econômica conjunta e de cada uma das entidades que o compõe; (ii) as transferências ou conjunto de transferências de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, o tipo de titulares de dados afetados e a identificação do país ou países terceiros em questão; (iii) o seu caráter juridicamente vinculativo; (iv) evidências que demonstrem o compromisso da organização empresarial em observar os princípios previstos no art. 6º da LGPD, sobretudo o princípio da transparência; (v) documentos que evidenciem que os Encarregados de todas as empresas do grupo que aderirem às normas estão alinhados em relação às salvaguardas que deverão ser implementadas para garantir proteção aos dados pessoais submetidos a transferência internacional; (vi) outros documentos que demonstrem a estrutura de governança da organização e seu nível de conformidade. Além disso, recomenda-se que a ANPD determine para quais contextos serão admitidas normas corporativas globais (a exemplo da União Europeia, há dois tipos de BCRs, as de controlador e as de operador); e (ii) como se dará o processo de submissão do documento e consequente aprovação pela Autoridade das normas corporativas globais, se assim entender a ANPD, e seguindo a linha do adotado no contexto europeu, de maneira a estabelecer o máximo possível de diretrizes para que este processo se torne mais simplificado e até mesmo menos moroso para os agentes. De toda forma, o material disponibilizado no site da Comissão Europeia e as diretrizes do WP29 fornecem estrutura sugerida para um conjunto de BCRs, a fim de auxiliar empresas na elaboração das suas próprias regras e poderá servir de auxílio à ANPD neste processo. No mais, para empresas cuja sede é fora do Brasil e que já tenham normas corporativas globais implementadas, espera-se que o papel da ANDP seja o de validar o documento para ser implementado no âmbito do Brasil, de modo que a organização não tenha que produzir um segundo documento com a mesma função. Assim, sugerimos endereçamento deste ponto também pela ANPD. Vale ressaltar que até o momento, a lista publicada pela EDPB indica que desde 2018, 30 normas corporativas globais foram aprovadas pelas autoridades supervisoras sob o GDPR, para as quais o EDPB emitiu sua respectiva opinião/decisão vinculante. Tais instrumentos também podem servir como base para a ANPD. ","174361":"Entendemos que os elementos previstos no art. 34 da LGPD devem ser utilizados nos instrumentos contratuais de forma macro, se limitando àqueles critérios que não impactem na fácil e objetiva aplicabilidade do instrumento contratual em questão.

Assim, entendemos que nos instrumentos contratuais devem ser considerados, pela ANPD, a natureza dos dados que serão transferidos (art. 34, II, LGPD), as medidas de segurança que serão adotadas (art. 34, IV, LGPD), além de outros fatores específicos inerentes à transferência (art. 34, VI, LGPD) que possam demandar a elevação do nível de proteção para que sejam resguardadas a confidencialidade, disponibilidade e integridade dos dados sob transferência. Por fim, em linha com o art. 34, I da LGPD, é recomendável que a ANPD oriente os agentes de tratamento a fim de que os exportadores adotem medidas que visem garantir que os importadores os informem previamente caso o país destinatário dos dados pessoais apresente normas que possam submeter a riscos os dados pessoais transferidos, o que inclui divulgações indevidas e/ou divulgações a autoridades/órgãos públicos.","174362":"Embora seja necessário um conteúdo pré-definido para que as empresas possam utilizar as cláusulas-padrão de maneira segura, objetiva e facilitada, é importante que seu conteúdo não seja rígido, mas modular, a fim de que o documento possa se amoldar às especificidades do contexto da transferência, de modo que possam ser mencionadas informações relevantes como os tipos de dados que serão transferidos, e de modo que o documento seja adaptável considerando os agentes de tratamento envolvidos na operação, sobretudo o tipo de agente que ocupará o papel de exportador, e o tipo de agente que figurará como importador. É possível, ainda, que agentes adicionais que venham a fazer parte da cadeia de atividades de tratamento, se valham das disposições das SCCs12, o que poderá permitir que se concentre em um único instrumento as normas a serem seguidas e observadas por toda a cadeia de agentes envolvidos na transferência internacional. As chamadas docking clauses permitem que um importador ou exportador, a partir da autorização das partes originalmente signatárias do instrumento jurídico, adentre às condições estabelecidas nas SCCs, desde que assinado um Anexo específico.","174363":"Aquele que permita ao agente de tratamento a escolha do clausulado de forma a abranger as especificidades da sua atividade de tratamento com determinado parceiro, mas que ao mesmo tempo desse segurança jurídica de que de fato foi adotada a cláusula mais pertinente para aquela relação. Recorrendo à experiência internacional, a Comissão Europeia, ao adotar SCCs, optou pela modelagem das cláusulas, de modo que o documento é composto por (i) cláusulas fixas, que permanecem inalteradas independentemente das partes a elas submetidas; (ii) módulos adaptáveis a depender do agente de tratamento (controlador ou operador) que figurará como exportador ou importador; e (iii) cláusulas e anexos em branco, que devem ser preenchidos pelas partes com informações relevantes (por exemplo, natureza de dados transferidos, categorias de titulares dos dados envolvidos, entre outras). A simplificação do modo como poderá se dar a modulação poderá evitar, inclusive, que o agente as cláusulas de forma errônea, considerando o cenário fático. Por outro lado, a ICO, no International Data Transfer Agreement, disponibiliza ao agente de tratamento uma árvore de decisões, além de checkboxes para preenchimento, de forma um pouco mais fechada e direcionada. O formato adotado pelo ICO, por ter adaptações mais limitadas, pode ser capaz de evitar que as partes adicionem informações equivocadas no documento e o tornem inaplicável ou não aderente ao caso concreto. Em todo caso, independentemente do critério a ser adotado pela ANPD, sugerimos um documento que seja autoexplicativo e contemple o que a autoridade espera (ao menos nos campos de livre preenchimento) em cada cenário relativo às transferências

internacionais.","174364":"Entendemos ser necessário adotar módulos diferenciados, considerando o agente que figurará como exportador, e o agente que figurará como importador. Em linha com a resposta dada para a questão 7 e considerando que as obrigações atribuídas pela LGPD a cada agente de tratamento e suas responsabilidades são diferentes, bem como considerando o nível de autonomia que possuem para o tratamento de dados pessoais, entendemos ser importante que haja regras específicas para cada agente na transferência internacional de dados. Recomendamos que sejam adotados os requisitos já observados pela Comissão Europeia no documento Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, bem como em seus anexos relacionados.","174367":"Considerando o escopo diverso de aplicação de ambos os mecanismos bem como a complexidade do fluxo de dados e quantidade de agentes de tratamento envolvidos a depender do contexto da transferência, entendemos que os requisitos de ambos os instrumentos também devem ser distintos. Isto porque as Normas Corporativas Globais (Binding Corporate Rules, no contexto europeu) costumam ser direcionadas a empresas multinacionais, com um fluxo maior de atividades de tratamento e mais agentes envolvidos na operação, ao passo que as cláusulas-padrão contratuais (Standard Contractual Clauses, no âmbito da União Europeia), são mais comumente utilizadas para relações com agentes em menor quantidade, e uma menor complexidade no fluxo das atividades de tratamento. Em linha com a ideia de uma harmonização internacional, sugerimos que, no que couber no âmbito de aplicação da LGPD, sejam utilizados os requisitos e parâmetros já estabelecidos pela Comissão Europeia para aprovação de ambos os instrumentos. Em suma, as cláusulas-padrão contratuais necessitariam de uma construção e elaboração prévias pela Autoridade, de forma que uma vez tornadas públicas, estariam “pré-aprovadas” para utilização dos agentes. Seus requisitos de aplicabilidade devem englobar a adequada escolha de seus módulos específicos pelo agente exportador, caso este seja o formato escolhido pela ANPD, bem como deve ser exigido que o exportador e o importador avaliem previamente, se há leis ou normas do país terceiro que poderiam impactar em sua eficácia. É recomendável, ainda, que o exportador tenha a obrigação de avaliar se as referidas cláusulas-padrão não contradizem com cláusulas estabelecidas nos instrumentos contratuais específicos firmados entre as partes, ou em outros mecanismos complementares eventualmente adotados para viabilizar a transferência internacional. As Normas Corporativas Globais, por outro lado, decorrerão de uma ação positiva do agente de tratamento, no sentido de submeter o documento, elaborado de forma mais personalizada para o seu negócio, ao processo de aprovação da Autoridade. No que tange as referidas normas, é recomendável que a Autoridade disponha sobre informações específicas que deverão constar no referido documento, tais como: (i) políticas e procedimentos da Organização que demonstrem seu compromisso com a observância dos princípios previstos no art. 6º da LGPD; (ii) documento que evidencie as medidas de transparência que utiliza, bem como a maneira pela qual possibilita que os titulares exerçam seus direitos, à luz da LGPD; (iii) documentos que evidenciem o caráter vinculante das normas dentro da Organização; (iv) documentos que evidenciem que os Encarregados de todas as empresas do grupo que aderirem às normas estão alinhados em relação às

salvaguardas que deverão ser implementadas para garantir proteção aos dados pessoais submetidos a transferência internacional; (v) outros documentos que demonstrem a estrutura de governança da organização e seu nível de conformidade. ","174368":"• Existência de uma estrutura corporativa única17 ou com influência significativa de ao menos uma empresa nas decisões de outra, como direção, controle ou administração; • Combinação de recursos ou esforços19 para alcançar interesses em comum; • Adoção de mecanismo aplicável a todas as empresas do grupo envolvidas e aos funcionários, de natureza juridicamente vinculante. Referidos critérios permitem que sejam abrangidos grupos de empresas multinacionais com subsidiárias e afiliadas, franquias, consórcios, joint ventures ou parcerias profissionais, para os quais o ICO indica a aplicação das binding corporate rules.","174369":"O nível de detalhamento deve ser coerente com as demais obrigações já impostas pela LGPD, seja para fins de atendimento aos princípios de transparência e livre acesso ao titular, e exercício de direito de acesso, seja para demonstração de conformidade pelo agente de tratamento, como por meio do registro das atividades. Nesse último aspecto de responsabilização e prestação de contas, a sugestão também tem por base o art. 30 do GDPR, que apresenta detalhamento acerca das informações que devem constar no registro de atividades, bem como em orientações do EDPS. Adicionalmente, as informações mínimas exigidas poderão ser complementadas com dados específicos acerca do compartilhamento de dados pessoais, com base em recomendação do ICO. Diante dessas considerações, sugere-se como informações mínimas: • os tipos de dados pessoais; • as categorias de titulares envolvidos • a finalidade específica do tratamento; • o período de retenção; • a identificação dos agentes de tratamento envolvidos; • o país em que está localizado o agente de tratamento; • a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares; e • as medidas de segurança tecnológica e organizacional implementadas em relação ao compartilhamento dos dados pessoais.","174371":"Prejuízos: • Incompatibilidade entre procedimentos; • Possibilidade de os meios de supervisão e fiscalização não serem implementados com a mesma eficácia entre os agentes de tratamento envolvidos. • Pluralidade de legislações. • Maior burocracia para efetivar a transferência internacional. • Maior exposição dos negócios ao risco. • Maior dificuldade de fluxo de dados. • Maior burocracia para atualização das regras entre os agentes de tratamento. Benefícios: • Minimização de divergências com base na LGPD • Maior harmonia na forma de interpretação e aplicação da LGPD nos processos de supervisão e fiscalização. • Possibilidade de utilização de instrumento adicional, como uma cláusula contratual, para demandar uma avaliação das normas corporativas da outra parte ou eleger um conjunto de normas a ser observado por ambas. • Redução de burocracias no compartilhamento e a possibilidade de um fluxo de dados pessoais facilitado para empresas que já demostraram possuir procedimento internos eficientes. • Menor exposição dos negócios ao risco. • Potencializa o fluxo de dados, preservando a segurança; • São mais fáceis de serem mantidas e atualizadas, na medida em ANPD não precisaria aprovar alterações não materiais, economizando tempo e custos. ","174372":"Na UE, até o momento, a lista publicada pela EDPB indica que, desde 2018, 30 normas corporativas globais foram aprovadas pelas autoridades supervisoras sob GDPR, para as quais o EDPB emitiu sua respectiva opinião/decisão vinculante. Ainda, o mesmo EDPB apresenta recomendações acerca de medidas suplementares (técnicas, organizacionais e contratuais) para transferências

internacionais, as quais não estão vinculadas à verificação ou aprovação de cláusulas contratuais padrão, cláusulas contratuais específicas ou normas corporativas globais, mas podem ser implementadas pelos exportadores a fim de elevar o nível de proteção. ","174373":"Inicialmente, é importante que se estabeleça uma referência para o que serão consideradas “alterações na configuração original” da transferência internacional. Isso porque é natural que mudanças sejam realizadas a fim de otimizar o fluxo de informações e a continuidade das atividades. Deste modo, a primeira premissa estabelecida seria que apenas alterações substanciais, como: finalidades materialmente diferentes das originais, adentrem no escopo apresentado, com base na conexão e compatibilidade entre as finalidades; alterações de países envolvidos na transferência que implique na mudança de legislação; e alterações que representem riscos aos direitos e liberdades dos titulares. Partindo da premissa apresentada, os direitos dos titulares que poderão ser invocados nesse contexto são: (a) direito de acessar os dados que são tratados pelos agentes de tratamento nessa nova configuração; (b) direito de oposição ao novo tratamento, caso a nova configuração descumpra a LGPD; (c) direito de anonimização, bloqueio ou eliminação, caso o titular entenda que o novo tratamento seja excessivo, desnecessário ou ocorra em desconformidade com a LGPD; (d) direito de correção, caso os dados estejam incompletos, inexatos ou desatualizados para a nova configuração; (e) caso o tratamento tenha fundamento no consentimento, o direito de revogação a qualquer tempo; e (f) o direito de peticionar perante a ANPD caso a nova configuração implique em violação à lei. Como referência, a Comissão Europeia esclarece acerca dos direitos de titulares em casos de transferências internacionais baseadas em cláusulas contratuais padrão, reforçando especialmente o direito de que os titulares sejam informados acerca do tratamento, bem como sobre o direito de obtenção de uma cópia das cláusulas conforme utilizadas, nos termos do art. 15 (3) do GDPR. Quanto à necessidade de comunicação dos titulares sobre a nova configuração da transferência, além do direito abrangente de que os titulares sejam informados sobre operações de tratamento, as circunstâncias que tornariam a comunicação direta imprescindível seria apenas quando o tratamento seja fundamentado no consentimento e a alteração disser respeito à finalidade, forma e duração do tratamento, bem como controlador responsável pelo tratamento, com base no art. 8º, §6º da LGPD. Referido artigo também faz menção às alterações referentes a “informações acerca do uso compartilhado”, sugere-se que a interpretação seja feita de forma flexível para não burocratizar eventual troca de agentes de tratamento e de países que não atraia risco aos titulares. Ademais, nesse aspecto, entende-se que aplicar-se-ia o direito de obter informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados, o qual deve ser provocado ativamente pelo titular.","174375":"Dividimos a questão em três pontos: (a) resolução de conflitos entre agentes de tratamento, envolvendo instrumentos contratuais; (b) resolução de conflitos entre agentes de tratamento e titulares, envolvendo instrumentos contratuais; e (c) medidas para auxílio da ANPD na resolução de conflitos internacional. Primeiramente, para resolução de conflitos entre agentes de tratamento, entendemos que o meio viável seria a indicação em contrato pela utilização de arbitragem, conciliação ou mediação, elegendo previamente a lei e jurisdição aplicáveis. No que tange à resolução de conflitos entre agentes de tratamento e titulares, quando a transferência tiver por base um instrumento contratual, a ANPD poderá

prever como orientação que os agentes de tratamento determinem no contrato responsabilidades acerca: do fluxo de comunicação entre as partes para atendimento a requisições de titulares; da existência de meios facilitados para que o titular contate cada uma das partes; e da existência de procedimentos internos para lidar com as requisições dentro de um prazo razoável. Ademais, dentro do papel de conscientização que compete à ANPD, entendemos que é relevante a indicação aos agentes de tratamento e titulares, por meio de guias e orientações, acerca dos meios alternativos de resolução dos conflitos sobre privacidade, para que possam optar livremente, tais como mediação e conciliação. Quanto ao último ponto, acerca das alternativas para atuação da ANPD frente às questões internacionais para resolução de conflitos, a melhor alternativa poderia ser a promoção de ações de cooperação com autoridades internacionais de natureza semelhante à ANPD, ação cuja competência resta evidenciada no art. 55-J, IX da ANPD e que já tem sido colocada em prática. Ademais, há uma lista extensa e não exaustiva de frameworks de cooperação internacional sobre proteção de dados pessoais existentes, aos quais a ANPD poderá integrar.","174376":"A ANPD poderá elaborar ferramentas para auxiliar os agentes de tratamento na gestão e documentação pertinente às transferências internacionais, como a disponibilização de materiais opcionais para os agentes de tratamento, como: (a) guias para utilização das salvaguardas do art. 33 da LGPD; (b) estudos acerca da probabilidade de respeito aos direitos e garantias de titulares nos países (com base em diretrizes de recursos humanos, adesão a acordos internacionais e no estado das leis, por exemplo); (c) guias sobre medidas de segurança e conformidade aplicáveis ao contexto de transferências internacionais; (d) modelos de planilhas para registro das operações que envolvam transferência internacional; (e) modelos de análise de impacto de transferência internacional; (f) checklist de análise de conformidade de terceiro (importador). Vale reforçar o caráter opcional, embora incentivado, das medidas “c” a “f” acima indicadas, a fim de que não se torne uma obrigação adicional.","174378":"Entendemos que o cenário de responsabilização não deva se desviar das responsabilidades que já cabem aos agentes de tratamento a partir de sua atuação fática quanto à atividade desempenhada, ou seja, a depender se figuram como controladores - inclusive com as particularidades de controladores independentes e conjuntos -, operadores ou suboperadores. Para tanto, uma vez verificado que houve transferências posteriores a jurisdições não conhecidas ou até mesmo a outros importadores, o regime de responsabilidade deve seguir o disposto tanto nos artigos 42 a 45 da LGPD, quanto nas orientações já formuladas pela ANPD em seu Guia. Quando houver mudança de jurisdição nas cadeias consecutivas de compartilhamento, estaremos diante de uma nova configuração de exportador-importador, de modo que o novo exportador também assumirá responsabilidade pela observância das regras dispostas nos artigos 33 a 36 da LGPD e regulamentações futuras, ou ainda por regras próprias da legislação aplicável de sua jurisdição, o que poderia afetar a adoção de mecanismos da LGPD pelo novo exportador. Como meio de direcionar essa preocupação sem adicionar ao exportador original responsabilidades adicionais pelas transferências consecutivas, a alternativa encontrada pela Comissão Europeia foi a inclusão de “docking clauses” opcionais nas Standard Contractual Clauses. Por meio desta cláusula, é possível que uma parte que não estava envolvida originalmente na relação, adira ao mesmo conjunto de obrigações e direitos, viabilizando a

atribuição de responsabilidade entre os contratantes, sempre a partir do período de ingresso da terceira parte à relação. A ANPD poderá considerar ainda a possibilidade de inclusão de anexos nacionais, nas cláusulas contratuais padrão ou nas normas corporativas globais, que têm como principal objetivo inclusão de eventuais particularidades contidas em lei nacional, conforme proposto em consulta pública pelo ICO. Já no que tange aos compartilhamentos na mesma jurisdição, entendemos que o importador inicial deve assegurar que terceiros porventura envolvidos se submetam às mesmas proteções resguardadas e exigidas pelo exportador inicial, bem como que os terceiros envolvidos serão documentados no registro de atividades mantido pelo importador. No mesmo sentido, as "docking clauses" opcionais indicadas pela Comissão Europeia também serviriam de exemplo aplicável para solucionar as questões de responsabilidade nesta relação. ","174379":"Entendemos não ser necessário impor obrigações legais adicionais aos agentes de tratamento (importador ou exportador) quando estes tiverem que se sujeitar a uma determinação de autoridades públicas, sob o risco de inviabilizar o fluxo de dados. Considerando a legislação europeia, o EDPB e o EDPS reforçam que em caso de pedidos de acesso dos tribunais e outras autoridades públicas, os importadores devem promover a comunicação antes de responder ao pedido. Tal recomendação, inclusive, é abarcada nas Standard Contractual Clauses. Ainda, a recente declaração conjunta entre Comissão Europeia e os Estados Unidos, possui o objetivo de restituir e aprimorar os princípios para abrigar transferências, dentre os quais estão incluídas regras e salvaguardas vinculativas para limitar o acesso aos dados por autoridades nos Estados Unidos ao que é necessário e proporcional para proteger a segurança nacional. ","174380":"Entendemos que os mecanismos adequados são aqueles instrumentos utilizados para fins de transparência, por meio dos quais os agentes de tratamento elencam as informações relevantes aos titulares de forma clara, adequada e ostensiva, nos termos do art. 9º da LGPD. A título exemplificativo, cita-se o Aviso de Privacidade, cuja disponibilização pode ser feita por meio de canais acessíveis aos titulares, seja nos meios físicos ou digitais, bem como pode ser um instrumento abrangente ou específico para determinada transferência internacional. Ademais, é um documento pelo qual é possível assegurar o acesso gratuito e facilitado. Acerca da forma de apresentação de informações, entendemos que o agente de tratamento poderá optar pelo meio mais adequado à sua realidade e aos meios de interação com o titular, desde que promova ativamente a exposição de informações. Sobre o tema, a doutrina europeia provê recomendações para garantia de transparência, aplicáveis para o contexto de transferências internacionais, as quais dizem respeito: à disposição das informações em camadas, utilização de ferramentas como pop-ups, dashboards, avisos de privacidade específicos (just-in-time), QR codes, entre outros. Vale ressaltar que tais recomendações não possuem caráter vinculante, mas se apresentam como orientações aos agentes de tratamento. Quanto à implementação do mecanismo elegido para conferir transferência, ainda que o agente de tratamento deva se atentar os requisitos do art. 9º da LGPD, não recomendamos a exigência de elementos adicionais obrigatórios para o contexto de transferência internacional, sob pena de que o titular seja impactado com um documento denso ou complexo demais, afastando o objetivo pretendido com o princípio da transparência.

Contribuinte: FIESP - FEDERAÇÃO DAS INDÚSTRIAS DO ESTADO DE SÃO PAULO

Número: OP-180265

Data: 15/06/2022 - 08:55

Resumo: :"Os principais obstáculos, tanto para transferência do Brasil para o exterior ou vice-versa, são a complexidade operacional, o alto custo financeiro e o tempo na adoção prática dos mecanismos de transferência internacional de dados pessoais — previstos tanto na legislação brasileira, quanto na de outros países — e o conflito de jurisdições. Nesse sentido, uma das dificuldades centrais encontradas para transferir dados do Brasil para o exterior, é: (i) a ausência de acordos internacionais; (ii) a ausência de decisões de países adequados e (iii) a falta de regulamentação da ANPD em relação aos seguintes mecanismos de transferência de dados: • Estabelecimento de critérios para verificação de grau adequado de proteção de dados pessoais, de acordo com os arts. 33, I e 34; • Elaboração e publicação das cláusulas-padrão contratuais, bem como a definição dos procedimentos para verificação de cláusulas contratuais específicas para uma determinada transferência, normas corporativas globais ou selos, certificados e códigos de conduta, conforme arts. 33, II e 35; e • Avaliação das normas corporativas globais. Já no que se refere aos obstáculos enfrentados para transferência de dados do exterior para o Brasil, principalmente no contexto europeu, pode-se falar na ausência de reconhecimento do Brasil, por parte da Comissão Europeia de Proteção de Dados Pessoais, como um país que ofereça um nível adequado de proteção de dados pessoais, que acarreta a necessidade de adoção de outros mecanismos de transferência internacional, muitas vezes burocráticos, desproporcionais e operacionalmente complexos a fim de não atravancar a transferência. É muito importante constatar que as exigências rígidas impostas pela União Europeia na aplicação prática dos mecanismos de transferência internacional não são um modelo a ser seguido pelo Brasil, porque implicam na obrigatoriedade de assunção de diversas obrigações, muitas vezes desproporcionais, acarretando um alto custo operacional ou mesmo a impossibilidade de seu cumprimento. Estas barreiras impactam diretamente o desenvolvimento da economia brasileira – notadamente no contexto de exportações de produtos e serviços nacionais – e afetam de modo significativo o desenvolvimento tecnológico e a inovação de diversos setores. Além disso, regulações restritivas igualmente afugentam investimento estrangeiro, pelo óbvio motivo de que é preferível fazer negócios com empresas estabelecidas em países que simplifiquem o livre fluxo de dados, e não o inverso. ","174354":"Entendemos que, conforme exposto acima, temos como impactos o custo operacional e financeiro da adoção de mecanismos complexos, o conflito de jurisdições, a ausência de decisões de adequação e regulamentação de mecanismos importantes. Note que o problema está posto, uma vez que hoje não temos mecanismos regulamentados que propiciem a segurança jurídica para as empresas na execução das transferências internacionais. Nesse sentido, entendemos que a promoção da convergência e interoperabilidade que viabilizem a transferência internacional deverá ser adotada em etapas, de forma a (i) resolver os principais impactos com mecanismos mais ágeis e (ii) desenvolver modelos e mecanismos que atendam de forma mais efetiva tal convergência. A fim de buscarmos uma solução proporcional e mais ágil, neste primeiro momento entendemos que a melhor forma de promover a convergência e interoperabilidade de instrumentos contratuais, a

princípio, é a regulamentação adequada das cláusulas-padrão contratuais. Parece natural que a ANPD queira se basear nos textos das Standard Contractual Clauses da União Europeia para elaboração das cláusulas-padrão contratuais da LGPD. Idealmente, isto implicaria o mesmo tipo de proteção tanto para exportação, quanto para importação de dados. No entanto, entendemos que a mera cópia das disposições das SCCs é completamente equivocada, e que o texto das cláusulas-padrão deve refletir tanto a legislação, quanto a realidade brasileira. Entendemos que o papel da ANPD na regulamentação deste mecanismo de transferência internacional deve ser, sim, a busca pela interoperabilidade, mas sempre levando em considerações adaptações do mecanismo de forma a, de um lado, proteger os interesses dos titulares de dados no Brasil, e de outro, a não criar um obstáculo instransponível ao desenvolvimento tecnológico e ao livre mercado. Vale insistir, aqui, no enorme custo operacional e financeiro atrelado a mecanismos inflexíveis de transferência internacional. A regulação brasileira deve buscar interoperabilidade com outras regulações similares apenas na medida em que simplifique – e não dificulte – a realização de transferências internacionais, sempre proporcionando a proteção necessária aos dados pessoais e consequentemente aos direitos e às liberdades fundamentais dos titulares. Ainda, nesse sentido, devemos avaliar os contextos regulatórios de forma a entendermos a dificuldade prática em torno da obrigatoriedade de se observar diversas legislações estrangeiras em sua integralidade, seja pela própria barreira linguística, seja pelos diversos tipos de especificidades que cada lei possui, o que torna a operação de transferência internacional sobremaneira complexa e desproporcional. O modelo deve buscar um equilíbrio entre a necessidade de se garantir a proteção dos dados pessoais onde quer que o dado pessoal esteja e a forma como isto se operará na prática de forma a viabilizar tais transferências internacionais. Propomos aqui que estes mecanismos sejam baseados em princípios gerais de proteção de dados pessoais e não no cumprimento integral das legislações que muitas vezes possuem diferenças práticas que acarretam em um sem fim de procedimentos e processos capazes de atender tais especificidades. Já em um segundo momento, para buscarmos melhorias de interoperabilidade a ANPD deve buscar acordos internacionais ou regulamentação de códigos de conduta de forma a buscarmos uma homogeneidade internacional quanto ao tema, desenvolvendo um framework de proteção de dados pessoais que não enseje nos contextos de conflitos de jurisdição. ","174356":"O instrumento mais efetivo para legitimar a transferência de dados é quando há o reconhecimento de “país com nível de proteção adequado”, pois, assim, a transferência ocorre livremente, sem necessidade de autorização ou formalização. No caso da União Europeia, quando o país é reconhecido pela Comissão Europeia como adequado, mediante publicação de decisão oficial sobre o tema. Ainda que efetivo, esse instrumento é bastante limitado (somente alguns países foram avaliados pela Comissão), em virtude da demora e dos critérios para o reconhecimento. Além disso, como modelo, existem dois instrumentos muito utilizados: as cláusulas-padrão contratuais e as normas corporativas globais. No primeiro caso, após aprovação pela Autoridade de Proteção de Dados Pessoais, basta a sua inclusão no texto do contrato ou do DPA para que a transferência seja válida, sem nenhuma necessidade que qualquer tipo de aprovação prévia de autoridades de proteção de dados pessoais. Estas cláusulas são publicadas pela autoridade e, posteriormente, inseridas nos contratos que ensejaram a transferência internacional de dados.

A vantagem delas é justamente a simplicidade na execução: basta incluí-las no contrato principal. Contudo, a vantagem apresentada acima pode se tornar em um fardo burocrático e operacional a depender de como as cláusulas-padrão contratuais serão definidas. Isto porque, a depender das obrigações impostas no documento poderemos voltar aos impactos já mencionados. No contexto europeu, falamos das Standard Contractual Clauses (SCC), aprovadas e publicadas pela Comissão Europeia — de acordo com uma pesquisa recente da Comissão Europeia, cerca de 88% dos controladores respondentes utilizam as SCCs como mecanismo principal para a transferência dos dados. Insta destacar que, apesar de as SCCs serem um instrumento comumente utilizado, devemos sempre levar em consideração que o modelo destas SCCs impacta diretamente no custo financeiro e operacional de viabilidade das transferências internacionais. Ou seja, o modelo padrão das SCCs deverá levar em consideração os impactos da inclusão de determinadas obrigações, em especial aquelas relacionadas ao cumprimento integral da legislação brasileira, conforme já mencionamos no item anterior, posto que, tais obrigação exigem, na prática, que as empresas adotem mecanismos separados para atender a cada legislação nacional da origem dos dados. Imagine, por exemplo, uma empresa global que recebe dados provenientes de diversos países, cada grupo de dados deverá seguir um fluxo diferente para atendimento das especificidades de cada legislação de origem, o que torna este controle demasiadamente complexo e, muitas vezes, em decorrência desta complexidade poderá haver falhas e questões que na prática não consigam atingir o objetivo precípuo da regulação da transferência internacional que é o de garantir a proteção dos dados pessoais. Por isso, reiteramos que o modelo das normas contratuais padrão deva ser um modelo mais simplificado que foque no objetivo precípuo de sua existência que é garantir que os princípios da finalidade, transparência, livre acesso, prevenção, segurança, necessidade, qualidade dos dados, não responsabilização, adequação e não discriminação sejam observados no tratamento dos dados pessoais. ","174359":"As vantagens da regulamentação das transferências internacionais de dados pessoais são, de um lado, garantir a efetiva proteção de dados pessoais independentemente da jurisdição onde os dados estão sendo tratados e, de outro lado, garantir maior segurança jurídica aos agentes de tratamento que tratam dados de pessoais localizadas no Brasil (independe de onde estes agentes estejam localizados). A regulamentação adequada dos mecanismos também é vantajosa do ponto de vista do direito internacional, uma vez que ela pode pesar em favor do Brasil em eventual avaliação de adequação do país pela Comissão Europeia. ","174360":"Itens a) e b) No estabelecimento das cláusulas-padrão contratuais, das cláusulas específicas e das normas corporativas globais, o que deve orientar tanto a elaboração, quanto a aprovação destas cláusulas é a obediências aos princípios da LGPD. Além disso, deve-se ter em vista a manutenção da proteção adequada, necessária e suficiente aos titulares dos dados exportados, de acordo com a LGPD. Ou seja, ainda que não se esteja obrigando um país a cumprir integralmente a lei brasileira, os direitos por ela garantidos devem ser resguardados pela cláusulas-padrão. Por fim, a cláusula deve ser capaz de alocar a responsabilidade por violação contratual entre as partes e por definir a qual delas cabe atender os direitos dos titulares de dados localizados no Brasil. Tendo em vista a realidade da esmagadora maioria das empresas brasileiras - as quais ainda desconhecem os elementos principais da LGPD ou enfrentam dificuldades para sua implementação prática – é imperativo que sejam adotados

modelos mais simplificados para estas cláusulas, com enfoque na observância dos princípios e fundamentos da LGPD, e não nas exigências multifacetadas do GDPR. Nesse contexto, uma abordagem baseada em riscos, e não regras idênticas em todos os contextos, pode servir de modelo para melhor equilibrar as obrigações de agentes de tratamento em relação a transferências internacionais. Item c) O ponto principal a ser considerado em relação às normas-corporativas globais são: (i) a capacidade de o grupo econômico demonstrar cumprimento da LGPD em suas atividades corporativas e negociais; e (ii) eficiência da centralização dos canais de comunicação do grupo com os titulares de dados e com as autoridades brasileiras. ","174361":"Em ambos os casos o objetivo é o mesmo: garantir que os dados pessoais de titular localizado no Brasil tenham o mesmo nível de proteção independentemente da jurisdição. Critérios gerais podem ser levados em conta para fins de ambos os mecanismos, como: (i) respeito aos princípios da LGPD; (ii) presença de regras sobre tratamentos que podem entrar em conflito com os princípios (e.g. dados sensíveis, decisões automatizadas); e (iii) regras procedimentais de aplicação das regras de proteção de dados. De toda forma, é importante que a análise do nível de proteção de dados de países ou organismos estrangeiros seja principiológica: o que importa é a proteção dos direitos e das liberdades fundamentais dos titulares no contexto das transferências internacionais e não a letra literal da legislação estrangeira, cuja interpretação e aplicação prática pode não corresponder na prática ao que é previsto no texto. ","174362":"Na União Europeia, as SCCs são propositadamente rígidas pois apresentam vantagem evidente: por causa de sua padronização e aprovação prévia, as SCCs são um mecanismo "pronto para uso" e de fácil implementação: basta incluir o texto integral no contrato principal, sem burocracia adicional. A desvantagem disto é a impossibilidade de realizar ajustes no texto, o que pode impactar negativamente algumas atividades de tratamento. Caso a ANPD opte por deixar o texto flexível, entendemos ser importante que elas não precisem ser novamente aprovadas pela Autoridade — do contrário, elas deixam de ser cláusulas-padrão (Art. 33, II, b) e passam a ser cláusulas específicas (Art. 33, II, a). Em linhas gerais, entendemos que deve ser permitida uma determinada flexibilidade para que possa ser utilizada de forma ampla, mas ao mesmo tempo caso não seja possível que essa flexibilidade seja feita sem ser novamente aprovada pela ANPD é preferível que as cláusulas adotem uma estrutura única para que exista segurança jurídica em sua utilização, sem prejuízo de eventuais variações conforme o grau de risco da transferência internacional. ","174363":"Sobre a apresentação das cláusulas, entendemos que a melhor forma dependerá da abordagem escolhida pela ANPD. Caso a cláusula seja única (independentemente da relação entre os agentes de tratamento), entendemos que não será necessário nenhum tipo de árvore de decisão/formulário/checkbox. Caso o texto seja adaptado para refletir as diversas relações entre agentes do tratamento, a árvore de decisões seria ideal. Ademais, sugerimos que haja um modelo baseado em risco, em que a adoção das cláusulas pode depender desta avaliação, ou seja, para situações em que há um risco baixo poder-se-ia haver cláusulas mais simplificadas ao passo que, nos casos em que houver alto risco as cláusulas deveriam ser mais rigorosas. Nesse sentido, a existência de um mecanismo que seja capaz de mensurar o risco a partir da situação contextual da transferência internacional seria interessante de forma a propiciar uma segurança jurídica quanto a decisão se determinado fluxo é ou não de alto risco. O formato de arquivo mais

adequado para disponibilização de modelos seria algum compatível com os principais processadores de texto disponíveis no mercado, tendo em vista que, em princípio, as cláusulas deverão ser adotadas em sua integralidade, ou seja, “cópia e cola”. Além disso, conforme ocorre no cenário europeu, seria interessante a disponibilização dessas cláusulas já traduzidas para o inglês e o espanhol, a fim de manter uma padronização na tradução dos contratos. Por fim, sugerimos que a ANPD crie, assim como a Comissão Europeia, um documento central com as perguntas mais comuns acerca das cláusulas e sua aplicação, com suas respectivas respostas. Se adotado um modelo baseado em riscos, o documento deve igualmente apresentar critérios que auxiliem os agentes de tratamento a avaliar cenários específicos e compreender os riscos envolvidos. ","174364":"Entendemos que sim, pois a relação entre os agentes de tratamento, assim como as obrigações relativas aos dados pessoais, é diferente. As cláusulas que tratarem dos operadores devem ser mais flexíveis, tendo em vista sua atuação limitada do tratamento dos dados. ","174367":"No caso das Normas Corporativas Globais, a empresa deve comprovar que as políticas internas de proteção de dados pessoais contêm expressamente os princípios gerais previstos na lei. Ponto importante é que o grupo econômico seja capaz de fornecer a transparência necessária aos titulares sobre onde os dados estão localizados e a forma como eles podem exercer seus direitos.","174368":"Entendemos que o conceito deve abranger além de grupo econômico ou empresarial, também, a chamada rede de firmas definida na Resolução Conselho Federal de Contabilidade - CFC Nº 1.201 DE 27.11.2009. ","174369":"I. Respeito aos princípios da LGPD; II. Finalidade legítima do compartilhamento; III. Base legal adequada que justifique o compartilhamento; IV. Alocação de obrigações e responsabilidade entre o agente exportador e o importador dos dados; V. Canal de atendimento adequado para questões LGPD vindas de titulares de dados e de autoridades brasileiras. ","174371":"Ao aprovar as normas corporativas globais, a ANPD reconhece que as políticas internas dos grupos econômicos são adequadas e suficientes para garantir os direitos dos titulares de dados, previstos na legislação nacional. Dessa forma, ao permitir a transferência de grupos distintos, mas ambos com as normas corporativas globais aprovadas, cria-se uma melhora no ambiente de negócios, facilitando a troca de informações e dados entre as empresas, ao mesmo tempo em que se resguardam os direitos dos titulares. Quanto ao risco, este pode ser considerado minimizado ao constatar-se que há uma preocupação mútua entre os grupos de que ambos estejam atuando em conformidade com a lei. ","174372":"A Comissão Europeia de Proteção de Dados disponibiliza, em seu site, todas as normas corporativas globais aprovadas e as respectivas empresas, bem como as cláusulas-padrão contratuais. Tendo em vista a forte influência da legislação europeia sobre a brasileira, elas podem servir como exemplo para a ANPD. ","174373":"Os direitos do titular deverão ser resguardados independentemente do modelo de transferência escolhido. Dentro deste contexto, entendemos que a forma mais eficiente e eficaz de se proporcionar esta garantia é a obrigação do exportador de dados atender tais direitos, sendo certo que o importador deverá atender as solicitações do exportador. Aqui o ideal seria que o exportador seja o responsável primário pelo atendimento a estes direitos. Quanto a comunicação ao titular de dados pessoais só deve ocorrer quando ocorrer uma mudança substancial na finalidade do tratamento dos dados enviados ao exterior. Não sendo substancial esta mudança, dispensa-se a necessidade de

notificação ao titular, a fim de evitar ônus desproporcional aos agentes de tratamento. É importante ponderar que a obrigação de transparência deve ser sempre do agente de tratamento exportador dos dados pessoais, já que compete a ele, por estar diretamente sujeito à LGPD, cumprir com os deveres e princípios da lei local. Informações claras e acessíveis sobre a existência de transferências internacionais devem estar previstas em políticas de privacidade – cuja existência já é amplamente conhecida pelo público em geral – ou documentos similares. ","174375":"As melhores opções para resolução desses conflitos são os métodos alternativos de solução de conflitos, como conciliação, mediação e arbitragem. Priorizar este tipo de mecanismo é uma forma de dinamizar a solução dos conflitos e evitar sobrecarregar a ANPD. Além disso, acordos bi e multilaterais, bem como cooperação entre autoridades de proteção de dados podem auxiliar na resolução de conflitos complexos envolvendo transferência internacional de dados, seja criando procedimentos administrativos comuns, ou estabelecendo qual a jurisdição competente para tratar da disputa. ","174376":"Para promoção da conformidade com a regulamentação, é necessário que a ANPD estabeleça regras claras e mecanismos precisos acerca do que deve ser feito para que a transferência internacional ocorra em conformidade com a LGPD, preferencialmente por meio de modelos padronizados e de acordo com standards internacionais, sempre ressalvada a realidade brasileira e a complexidade operacional desses mecanismos. Ao lado disto, a ANPD tem o papel fundamental em conscientizar, através de Guias Orientativos, as melhores práticas na transferência internacional de dados. Note que a medida de adoção de modelos estandardizados deve levar em consideração a complexidade operacional e o custo financeiro da adoção destes mecanismos. Nesse sentido uma abordagem baseada em risco é essencial para sobrepesar tais entraves burocráticos e custos financeiros. Ainda, considerando o que já foi exposto nesta contribuição quanto a necessidade de buscarmos o equilíbrio entre a garantia da proteção de dados pessoais e a viabilização das transferências internacionais, medidas posteriores de acordos bilaterais e multilaterais entre países e com organismos internacionais também podem ser consideradas como potencializadores de enforcement. Além disso, estes acordos multilaterais podem buscar o desenvolvimento de um framework estandardizado entre países de forma a buscarmos uma maior homogeneidade nas regras de proteção de dados pessoais, reduzindo assim, os riscos de observância integral de diversas jurisdições acerca do tema. Note-se que devemos ter um olhar sobre esses aspectos mais focados na busca pelo equilíbrio entre estas questões, pois mecanismos altamente burocráticos e complexos podem gerar o efeito contrário ao que se pretende com sua utilização. ","174378":"Tendo em vista a complexidade de resolução de conflitos e determinação de jurisdição competente na seara internacional as melhores alternativas são os mecanismos alternativos de resolução de conflito, como arbitragem, mecanismos de ODR (online dispute resolution), parcerias entre autoridades de fiscalização etc. – em todos os cenários, porém, vale ressaltar que a responsabilidade recai sobre o agente de tratamento exportador dos dados, a quem compete a observância dos princípios e das regras da LGPD. ","174379":"No caso do importador, ele deve ser obrigado a informar o exportador dos dados acerca da solicitação imediatamente – ou, quando aplicável, em tempo hábil para que o exportador possa tomar providências adequadas, se cabíveis. ","174380":"O titular deve ser informado da possibilidade de envio de seus dados para um terceiro no exterior e qual a

finalidade deste compartilhamento. Isso deve constar na Política de Privacidade tanto do exportador, quanto do importador, disponibilizada ao titular, em conjunto com as demais informações fornecidas acerca do tratamento. Ainda, o exportador e o importador deverão acordar entre si em relação aos mecanismos de atendimento aos direitos dos titulares. O canal de atendimento deve ser de fácil acesso ao titular, e ambos os agentes devem estar preparados para receber/responder/encaminhar as solicitações que receberem destes titulares.

Contribuinte: JOSE CARLOS RAMOS DE OLIVEIRA JUNIOR

Número: OP-180307

Data: 15/06/2022 - 11:20

Resumo: :"O principal entrave é a falta de reconhecimento do Brasil como país que dá proteção adequadas a dados pessoais, notadamente pela Comissão Europeia. Vale destacar que países da região como Uruguai e Argentina já contam com esse reconhecimento. A participação ativa da ANPD e do governo brasileiro em geral para efetuar gestões junto a países que emitem esse tipo de decisão é fundamental.","174354":"Considerando a posição proeminente da Comissão Europeia no tema de proteção de dados, o caminho mais fácil seria a adaptação dos modelos europeus (“SCCs”) à LGPD, com o mínimo de alterações possível.","174356":"Os mecanismos mais comuns são os regulamentos internos vinculantes e os contratos intragrupo de transferência internacional de dados.","174359":"O fluxo livre de dados pessoais é fundamental no processo de internacionalização de empresas brasileiras, já que permite a centralização do tratamento de dados pessoais (notadamente armazenamento) na sede brasileira. Os mecanismos para permitir esse fluxo livre devem contar com obrigações de cunho tecnológico mínimas para assegurar a integridade e segurança das transferências e do tratamento dos dados, bem como o livre exercício pelos titulares dos direitos assegurados pela LGPD (ou de outras legislações de dados pessoais) onde quer que eles estejam.","174360":"No contexto de transferência internacional, deve ser assegurada a harmonização dos modelos brasileiros de cláusulas, contratos e (eventualmente) normas corporativas com os dos países/grupos mais avançados no tema, novamente tendo como base os da Comissão Europeia.","174361":"","174362":"O conteúdo deve ser o mais rígido possível para assegurar harmonização, mas assim como no modelo europeu devem ser fornecidas opções/módulos dentro do contrato modelo. Eventuais especificidades devem ser tratadas nos anexos, como as descrições das transferências, quem são os controladores etc.","174363":"O contrato modelo deveria ser fornecido em formato MS Word (ou semelhante), que funciona bem na União Europeia. No entanto, formulários que geram um contrato padrão podem ser interessantes, sobretudo para empresas de porte menor.","174364":"Novamente, pode ser utilizado o modelo europeu, incluindo módulos dentro do mesmo modelo, quais sejam, controlador-controlador, controlador-processador, processador-processador e processador-controlador.","174367":"Sim. É necessário assegurar que as entidades do grupo sujeitas às normas globais estejam juridicamente vinculadas a tais normas (por exemplo, mediante ‘contratos de acessão’), e que terceiros e empregados possam exercer seus direitos com base nas normas globais.","174368":"O grupo deve ser composto

da sociedade controladora e suas controladas diretas e indiretas, e coligadas, usando as definições da Lei das S.A. (v.g. art. 243, pars. 1º e 2º). De qualquer forma, isso não dispensa a necessidade de acessão formal de cada entidade partícipe às normas globais.","174369":"Identificação de: (i) partes envolvidas (exportadores/importadores dos dados), (ii) descrição dos dados pessoais e do processamento, (iii) duração do processamento, e (iv) países envolvidos.","174371":"","174372":"Como mencionado, as da Comissão Europeia.","174373":"Caso a transferência siga sendo feita com base nos mecanismos autorizados (por exemplo, contratos modelos ou regulamentos internos, ou para países homologados), não deve ser feita comunicação ao titular, a menos que este exerça seu direito de pedir informações às partes que estejam processando seus dados pessoais.","174375":"","174376":"","174378":"","174379":"","174380":"

Contribuinte: VICTORIA OETINGER CHASSOT

Número: OP-180323

Data: 15/06/2022 - 12:26

Resumo: :"","174354":"","174356":"","174359":"","174360":"","174361":"1. Proposta ¿ Proposição uma metodologia técnica para produzir uma "Diretriz para Recomendações de Avaliação de Adequação" pela Autoridade Brasileira de Proteção de Dados (ANPD). ¿ Nossa recomendação aborda quatro grupos de diferentes aspectos técnicos: i) Grupo 01: Princípios e Diretrizes Europeus Existentes para a Proteção de Dados ii) Grupo 02: Medidas técnicas e organizacionais aplicadas às transferências de dados para evitar ou minimizar o nível de intrusão e acesso não autorizado por órgãos governamentais iii) Grupo 03: Princípios de direito internacional privado no contexto da interpretação de disposições contratuais sobre uma transferência internacional e enfatizando os pactos relevantes ratificados pelo governo brasileiro iv) Grupo 04: Requisitos operacionais para implementação de cláusulas-padrão contratuais (SCC) 2. Aplicação prática ¿ O documento seria a principal metodologia para as seguintes situações específicas de transferência internacional de dados: i) O procedimento oficial da ANPD para qualificar um país estrangeiro ou um organismo internacional como adequado. ii) Uma recomendação de metodologia às organizações para construir procedimentos internos relativos a transferências internacionais de dados (por exemplo, Avaliação de Impacto de Transferência, integração com SCCs ou Regras Corporativas Vinculativas, e linha de base mínima para cláusulas contratuais ad hoc e medidas técnicas suplementares). iii) Como a ANPD avaliará a possibilidade de considerar válidos os contratos de outras jurisdições (EU SCCs, UK IDTA, etc.) sob o regime brasileiro, com a ressalva de um adendo nacional capturando as emendas necessárias sob a LGPD. 3. Metodologia técnica Nesta seção, serão resumidos os destaques que devem ser considerados por cada Grupo citado na Seção 01. 3.1. Grupo 01 ¿ As disposições contratuais devem ao menos descrever as recomendações: i) Instrumento juridicamente vinculante e executável frente a autoridades ou órgãos públicos (por exemplo, Regras Corporativas Vinculantes, SCCs adotadas pelo país exportador de dados, Códigos de Conduta, Esquema de Certificação e cláusulas contratuais

ad-hoc). ii) O que é entendido como limitação de finalidade para impedir o uso dos dados pessoais para fins secundários. iii) Medidas de minimização sobre coleta e uso. iv) Medidas de transparência mostrando para quem e por que os dados estão sendo transferidos. v) Adoção de uma estrutura menos restritiva e mais protetora em relação aos direitos dos titulares, bem como indicação da lista de direitos exercíveis. ¿ As características qualitativas mínimas para considerar um país importador adequado: i) A existência de legislação especial como fundamento para impor obrigações de privacidade e proteção de dados. ii) A existência de sanções dissuasivas de qualquer nível para fazer cumprir as obrigações de privacidade e proteção de dados. iii) A existência de uma Autoridade de Proteção de Dados ou qualquer agência governamental correlata com poderes legais suficientes para monitorar e aplicar independentemente as regras relativas à privacidade e proteção de dados. iv) Um sistema judicial apropriado onde a pessoa interessada pode apresentar reclamações e exercer um nível de reparação apropriado. A consideração deve ser ampla e nem sempre relacionada ao Poder Judiciário em sua forma tradicional (por exemplo, possibilidade de considerar a Adjudicação Administrativa como adequada, dependendo de certas circunstâncias). 3.2. Grupo 02 ¿ Medidas organizacionais e de TI para evitar ou minimizar o acesso não autorizado ou intrusão governamental ilegal: i) Ferramenta técnica de transmissão utilizada para a transferência. Se a ferramenta de transmissão for desenvolvida internamente, identificar as medidas que foram usadas para tratar de salvaguardas de privacidade em um ambiente de desenvolvimento, SDKs e software de sistema. ii) Infraestrutura técnica de TI necessária para garantir o nível desejado de proteção de dados e preservação da confidencialidade, disponibilidade e integridade dos dados pessoais (por exemplo, criptografia, ferramentas de análise de rede, antivírus, firewalls, patches de segurança, proxy reverso, virtualização do sistema ou opções de localização de dados). ¿ Práticas e padrões organizacionais adotados contribuindo para salvaguardar a privacidade e a proteção de dados (por exemplo, Políticas Internas de Privacidade e Segurança, Avaliações de Risco de Privacidade, Privilégios de Acesso à Informação, Política de Senha Forte, Planos de Recuperação de Desastres e Incidentes, Alinhamento com padrões internacionais de privacidade e segurança tais como Relatórios ISOs, NIST e SOC). ¿ Atividades colaterais que possam afetar direta ou indiretamente as salvaguardas de proteção aplicadas (por exemplo, interação com redes sociais, atividades publicitárias, transferências associadas com software de terceiros instalado por funcionários, ou assinaturas de serviços on-line que possam exigir transferências de dados). 3.3. Grupo 03 ¿ Aplicação dos princípios do direito internacional privado (tais como tratados ou convenções) no contexto da interpretação das disposições contratuais i) Definição de uma estrutura padrão internacional comum aceitável, levando em consideração diferentes abordagens regionais (por exemplo, Europa, Estados Unidos, Austrália, ou China). ii) A não aplicação do princípio de não-transactividade ou não-negociação de leis para evitar a compreensão de apenas uma legislação ou jurisdição de privacidade como válida. iii) A aplicação do princípio da extraterritorialidade tornando igualmente válida a transferência tanto pela legislação de importação como pela legislação de exportação de dados. iv) Boa-fé no cumprimento das obrigações internacionais para não criar obstáculos irrazoáveis à promoção de transferências internacionais ou mudanças

inesperadas no entendimento da conformidade legal dos mecanismos utilizados. ¿

Consideração de instrumentos jurídicos do Direito Internacional (soft e hard law) para definir o que é entendido como um comportamento aceitável em privacidade. Os seguintes tratados e convenções poderiam ser relevantes ao entender a adequação de um país ou ao fazer cumprir as disposições contratuais: i) Pacto Internacional sobre os Direitos Econômicos, Sociais e Culturais ii) Pacto Internacional sobre Direitos Civis e Políticos iii)

O Pacto de San José da Costa Rica também chamado de Convenção Americana sobre Direitos Humanos iv) Convenção sobre os Direitos da Criança v) Declaração Universal dos Direitos Humanos vi) As diretrizes para o regulamento dos arquivos de dados pessoais computadorizados vii) O Relatório Especial sobre o Direito à Privacidade (Relatório das Nações Unidas) viii) Os Princípios de Proteção de Dados Pessoais e Privacidade (Memorando das Nações Unidas) ix) As Diretrizes para a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais (Diretrizes de Privacidade da OCDE) x) A Estrutura Revisada de Privacidade da OCDE xi) Estrutura de Privacidade da APEC xii)

Resolução de Madri xiii) Declaração dos Direitos Humanos da ASEAN 3.4.

Grupo 04 ¿ Consideração de diferentes casos de uso e aspectos operacionais da aplicabilidade das SCCs: i) Transferência para um importador não brasileiro que está sujeito ao LGPD de acordo com o Art. 3 (I) e (II) da LGPD. ii) Transferência de subprocessador sujeito à LGPD de volta aos processadores não sujeitos à LGPD. iii) Um controlador fora do Brasil cujo processamento está sujeito à LGPD devido ao Artigo 3 (II) ou (III) a um controlador ou processador fora do Brasil que processa dados em nome de quem os transferiu (por exemplo, fornecendo elementos de segurança ou organizando aspectos administrativos e financeiros da atividade) e não está sujeito à LGPD. ¿ Situações de possibilidade de adesão de terceiros às SCCs (cláusula de ancoragem) e, ao fazê-lo, estabelecer um mecanismo claro para a adesão de novas partes, evitando incertezas legais e negociações onerosas para as organizações. ¿ Situações de possibilidade de fornecer cláusulas específicas e/ou orientação para tratar de forma flexível a responsabilidade das partes (importador/exportador) sob o contrato de transferência para evitar que as organizações se abstenham de entrar em SCCs devido aos riscos relacionados à responsabilidade. ¿ Prazo flexível para permitir que as organizações possam implementar os contratos de transferência uma vez aprovados. ¿ Explicação detalhada das medidas para qualificar um país ou entidade internacional como adequados com base no Artigo 34 da LGPD. Quanto às exigências legais abordadas no artigo 34, é necessário um esclarecimento especial sobre o artigo 34 (II), a natureza dos dados (utilização de critérios especiais como quantidade e tipo de dados, o nível de sensibilidade dos dados, impactos da segurança nacional, desenvolvimento econômico e interesses sociais ou públicos). 4. Lei nacional impondo a necessidade de criar esta metodologia O Guia proposto pode ser entendido como um instrumento regulatório impositivo pela legislação brasileira quando consideramos as disposições gerais projetadas pela Lei Federal 13.655/2018 e pelo Decreto-Lei 4657/1942: ¿

Proibição das entidades administrativas de tomar decisões sobre valores abstratos (Artigo 20 do Decreto- lei 4657/1942). ¿ A necessidade de indicar as consequências da invalidação de um ato ou contrato por uma entidade administrativa (Artigo 21 do Decreto-Lei 4657/1942). ¿ A obrigação de demonstrar as orientações técnicas gerais de algum assunto

antes de tomar qualquer decisão sobre a invalidação de um contrato, ato ou regra administrativa (Artigo 24 do Decreto-lei 4657/1942). ¿ A necessidade de publicar normas e diretrizes complementares para aumentar a segurança jurídica em relação à aplicação da legislação nacional (Artigo 19 do Decreto Presidencial 9830/2019 que regulamenta o Artigo 20 do Decreto-lei 4657/1942).
","174362":"","174363":"","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373":"","174375":"","174376":"","174378":"","174379":"","174380":"

Contribuinte: MARCO AURELIO SOUZA MENDES

Número: OP-180452

Data: 15/06/2022 - 13:43

Resumo: :"Ao nosso ver, o maior obstáculo hoje é a própria inexistência de regras mais específicas sobre a transferência internacional de dados, uma das grandes lacunas de nossa legislação, o que deixa o Brasil “fora do radar” em se tratando de tal tema. Pelo fato de o tema não ser totalmente regulado pela própria lei, as empresas tendem a se sentir receosas em realizar tais transferências, na medida em que desconhecem os mecanismos para tanto validados pela ANPD. Hoje, para que a atividade não seja frustrada, muito do que se faz é utilizar por base o entendimento de outras autoridades e legislações do resto do mundo, porém, há pouca segurança nessa prática. Empresas estrangeiras tendem a questionar o regramento brasileiro, porém, hoje, não é possível responder à pergunta com propriedade. Além disso, é de se considerar que o Brasil hoje não faz parte da lista de países adequados para importação de dados pessoais pela legislação europeia, o que também é um obstáculo para que outros países transfiram dados para o Brasil. O fato de a ANPD hoje não ser um órgão totalmente independente do Poder Executivo também é um importante obstáculo para essa inclusão na lista de países. ","174354":"Acreditamos que, como já vem sendo feito em outros casos por esta Autoridade, a ANPD deve se espelhar em outros modelos já existentes e consolidados em outras jurisdições, sem necessariamente inovar na interpretação e consolidação das regras de transferência internacional. Assim, entende-se que devem ser considerados modelos internacionais vigentes para nortear a regulamentação a ser editada pela ANPD, tais como o Europeu, sendo possível que se façam pequenas modificações nas regras se necessário.","174356":"Em nossa opinião, os instrumentos de maior efetividade e adoção para legitimar as transferências de dados internacionalmente hoje são as cláusulas-padrão contratuais (CPCs), dada a sua maior capacidade de uniformizar regras de proteção de dados de legislações e países diversos. Também é importante destacar que o custo para implementação das CPCs é consideravelmente menor do que dos demais instrumentos, além de que o seu formato de um modelo de cláusulas pré-aprovado permite a reutilização com facilidade pelos menores players, em especial as pequenas empresas.","174359":"Os benefícios vão desde a inclusão do Brasil no ecossistema de transferência internacional de dados pessoais até a necessária segurança jurídica para operar e tratar dados pessoais no país. A ausência de regramento torna o Brasil um país com um grau desnecessário de “obscuridade” em relação ao tema e, portanto, inseguro para ser o receptor ou exportador de

dados pessoais quando necessário. Não podemos esquecer que as regras se mostram ainda mais relevantes em um contexto no qual muitas das atividades empresariais passam pelo livre fluxo de dados pessoais por diferentes países e continentes. ","174360":"a. cláusulas-padrão contratuais; R: Importante definir a lei de regência do contrato (a qual, preferencialmente, deve ser a brasileira), o conceito e o conteúdo das CPCs, bem como o procedimento para elaboração e divulgação de tais cláusulas pela ANPD. b. cláusulas contratuais específicas; e R: Diferenciação entre o conceito das cláusulas contratuais específicas e as padrão, estabelecer o procedimento para aprovação de tais cláusulas pela ANPD, bem como o estabelecimento do prazo para deliberação da autoridade, o qual não deveria exceder 30 dias. c. normas corporativas globais. R: Requisitos mínimos para a formulação das normas corporativas globais, bem como o estabelecimento do prazo para deliberação da autoridade, o qual não deveria exceder 30 dias.","174361":"A Autoridade deve levar em conta todos os elementos presentes no artigo 34, com especial ênfase para os incisos: I, no sentido de exigir que o país de destino possua normas gerais e/ou setoriais na legislação em vigor que proporcionem mínima segurança ao tratamento dos dados; III, para exigir que sejam observados os princípios gerais de proteção de dados e os direitos dos titulares previstos na LGPD; IV, no sentido estabelecer medidas de segurança mínimas a serem adotadas pelo importador; e V, no sentido de exigir que o importador declare a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais.","174362":"Verifica-se a necessidade de encontrar um equilíbrio, uma vez que as cláusulas devem ser instrumentos dinâmicos e adaptáveis conforme a necessidade. A exemplo do que ocorre na Europa, considerando as particularidades de cada transação, os agentes de tratamento devem ter a liberdade de incluir as cláusulas-padrão em um contrato mais abrangente e de acrescentar outras cláusulas ou garantias adicionais, desde que não colidam, direta ou indiretamente, com as cláusulas-padrão. Além disso, deve haver abertura para a indicação do objeto e da duração do tratamento de dados, bem como da sua natureza e da sua finalidade, os tipos de dados pessoais envolvidos, as categorias dos titulares e os direitos e obrigações dos agentes de tratamento. Estrutura sugerida: (I) Disposições fixas, que permaneçam inalteradas independentemente das partes contratantes. As disposições fixas devem atender aos requisitos essenciais previstos no artigo 34, conforme mencionado na resposta acima; (II) Disposições variáveis (módulos), que possam ser adicionadas/retiradas do contrato conforme escolha das partes. Os módulos devem ser redigidos para abarcar as diversas circunstâncias de transferência (Controlador para Controlador; Controlador para Operador; Operador para Controlador; Operador para Operador); e (III) Anexos em branco para preenchimento pelas partes com a indicação das informações específicas e relevantes (categorias de dados e titulares envolvidos, medidas técnicas e organizacionais adotadas pela parte importadora etc.).","174363":"A ANPD deve disponibilizar os modelos editáveis (word) de forma facilmente acessível em seu site, já preparados para cada circunstância de transferência. A árvore de decisões pode ser útil para auxiliar o agente de tratamento a identificar qual modelo se encaixa à sua operação.","174364":"Sim, as responsabilidades aplicáveis ao importador devem ser compatíveis com o seu papel de controlador ou operador, nos termos da LGPD. Exemplificativamente, as questões referentes ao atendimento de direitos de titulares devem estar mais detalhadas nos módulos que regulam a transferência

para um controlador. Assim, as cláusulas para as transferências nas quais o importador seja operador podem ser mais simplificadas. Contudo, o nível mínimo de segurança exigível deve ser o mesmo para todos os agentes.","174367":"Sim. Normas Corporativas Globais deveriam ser usados por conglomerados internacionais, e organizações menores, pelo grau de complexidade, devem continuar usando as cláusulas-padrão contratuais. Para BCRs, deve haver toda uma auditoria de documentos e procedimentos adotados dentro de um grupo econômico para a proteção de dados. Para SCCs, há um conjunto de cláusulas pré-aprovadas pela ANPD, que é um processo muito menos complexo e mais cabível para empresas que fazem a transferências simples e bilaterais. Por outro lado, BCRs são feitas e aprovadas uma só vez. Assim, seria inviável para um grupo econômico que pratica volumosa atividade de transferências internacionais ter SCCs para cada uma delas. SCCs são self-assessment das empresas que aplicam. BCRs são aprovadas pela autoridade com base no que verifica na prática do grupo. BCRs já aprovadas em outro lugar: facilitaria caminho da ANPD.","174368":"Direta ou indiretamente, e de modo permanente, o controle das sociedades + grupos formados contratualmente => GDPR em português: grupo empresarial ou do grupo de empresas envolvidas numa atividade económica conjunta. Outro problema: empresas adquiridas posteriormente: necessariamente seguem procedimentos? O que mais vemos é o choque de culturas e empresas dentro do mesmo grupo atuando de forma diferente. A depender do caso, nova auditoria da nova empresa ou declaração atestando que a nova empresa obrigatoriamente seguirá mesmos procedimentos.","174369":"Políticas de proteção de dados, programa de governança, lista de entidades, diretrizes para tratamento de dados de empregados, documento de responsabilidade da matriz sobre todas as empresas do grupo e compromisso de tornar as regras aplicáveis em todo o grupo, contrato intragrupo sobre o assunto. Como o objetivo é substituir a decisão de adequação, o ideal é requerer exatamente aquilo que é previsto na LGPD, regulações e diretrizes da ANPD. Poderia haver um framework exemplificativo, como fez o WP29, mas as exigências devem ser customizadas para cada grupo econômico.","174371":"Benefícios: facilita a vida de todos (não precisaria de SCCs ou outro mecanismo). Riscos: ausência de contratos entre eles. Para BCRs, intragroup agreement é necessário. Ausência de uniformização dos procedimentos; o que um grupo foi requerido a fazer, não necessariamente poderá ser cumprido pelo outro.","174372":"Hoje, na Europa, 12 meses para conseguir e processo é bastante burocrático, especialmente porque envolve aprovação das demais DPAs, que é um problema que o Brasil não precisaria enfrentar.","174373":"Para os mecanismos de transferências internacionais, assim como todos os princípios da LGPD, devem ser seguidos os mesmos direitos dos artigos 18 a 20 devem ser garantidos aos titulares. Por exemplo, o titular deve estar informado sobre a possibilidade da transferência internacional (transparência) e tal atividade deve estar dentro dos propósitos legítimos (finalidade), assim como deve conseguir obter informações sobre o compartilhamento de seus dados pessoais e revogar seu consentimento quanto à transferência internacional de dados, se essa foi a base legal que justificou a atividade.","174375":"Uma solução possível seria a criação de um núcleo específico junto à ANPD para lidar com a solução de conflitos entre agentes de tratamento e entre estes e titulares envolvendo instrumentos contratuais de transferência internacional de dados. Prática semelhante é inclusive adotada pelo Núcleo de Informação e Coordenação do

Ponto BR (NIC.br), que instituiu, em 30 de setembro de 2010, o Sistema Administrativo de Conflitos de Internet (SACI-Adm), que nada mais é do que um procedimento conduzido por instituições previamente aprovadas pelo NIC.br. Segundo modelo atualmente adotado pelo NIC.br há três instituições credenciadas pelo NIC.br para processar e decidir controvérsias do SACI-Adm: a Associação Brasileira da Propriedade Intelectual (ABPI), a Câmara de Comércio Brasil Canadá (CCBC) e a Organização Mundial da Propriedade Intelectual (OMPI ou WIPO), que, na qualidade de provedoras do serviço de resolução administrativa de disputas, devem aplicar seus respectivos regulamentos aprovados pelo NIC.br, que estarão sempre em consonância com o regulamento geral próprio do SACI-Adm. Acredita-se que a adoção de tal mecanismo se mostrará bastante útil na resolução de conflitos envolvendo instrumentos contratuais de transferência internacional de dados. Além disso, em razão do tema, acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de tais conflitos, em especial com autoridades que já possuem reconhecida experiência na matéria, visto que poderiam contribuir com exemplos e casos práticos já enfrentados, para a resolução dos conflitos.","174376":"Para promover a conformidade com a regulamentação, algumas medidas podem ser tomadas – inclusive com base em experiências já adotadas na União Europeia –, tais como: Pedidos de informação: o importador de dados deve responder, rápida e adequadamente, aos pedidos de informação do exportador de dados relacionados com o tratamento objeto da transferência. Cumprimento do contrato: as partes devem poder demonstrar o cumprimento das presentes cláusulas contratuais. Em particular, o importador de dados deve conservar documentação adequada sobre as atividades de tratamento realizadas por conta do exportador de dados. Disponibilização de informações e auditoria: o importador de dados deve disponibilizar ao exportador de dados todas as informações necessárias para demonstrar o cumprimento das obrigações previstas nas presentes cláusulas e, a pedido deste último, facilitar e contribuir para as auditorias das operações de tratamento abrangidas pelas presentes cláusulas, a intervalos razoáveis ou se houver indícios de incumprimento. Ao decidir sobre uma revisão ou auditoria, o exportador de dados pode ter em conta as certificações pertinentes detidas pelo importador de dados. Auditorias: o exportador de dados pode optar por realizar, ele próprio, a auditoria ou mandatar um auditor independente. As auditorias podem incluir inspeções nos edifícios ou nas instalações físicas do importador de dados, devendo, se for caso disso, ser realizadas com uma antecedência razoável. Comunicação à autoridade: as partes devem disponibilizar as informações referidas nos itens 2 (cumprimento do contrato) e 3 (Disponibilização de informações e auditoria) acima, incluindo os resultados de quaisquer auditorias, à autoridade de controle competente, mediante pedido. ","174378":"Como a LGPD foi ampla e fortemente inspirada na legislação europeia, algumas práticas já utilizadas sob o contexto do GDPR podem ser úteis com relação ao presente tema, inclusive com o intuito de trazer certa harmonização entre as práticas, dado que o Brasil possui grande relação comercial com o bloco europeu. Alguns exemplos de alternativas seriam: Instruções do exportador: O importador de dados só deve divulgar os dados pessoais a terceiros mediante instruções documentadas do exportador de dados. Divulgação dos dados: os dados só podem ser divulgados a terceiros localizados fora do Brasil (no mesmo país que o importador de dados ou em outro país terceiro, a seguir designado como “transferência ulterior”) se o

terceiro estiver ou aceitar estar vinculado as respectivas cláusulas contratuais das quais o importador se obrigou, ao abrigo do módulo adequado, ou, ainda, se: ¿ o destino da transferência ulterior for um país que beneficie de uma decisão de adequação (quando a ANPD emitir as decisões) que abranja tal transferência ulterior; ¿ o terceiro assegurar, de qualquer outra forma, as garantias adequadas nos termos dos artigos 33 a 36 da LGPD, no que diz respeito ao tratamento em questão, ¿ a transferência ulterior for necessária à declaração, ao exercício ou à defesa de um direito do importador num processo judicial no contexto de processos administrativos, regulamentares ou judiciais específicos, ou ¿ a transferência ulterior for necessária para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular. Cumprimento de garantias: Qualquer transferência ulterior está sujeita ao cumprimento, pelo importador de dados, de todas as outras garantias previstas nas respectivas cláusulas contratuais, em particular a limitação da finalidade. ","174379":"Ao se falar em obrigações atribuídas ao importador e ao exportador, assim como no caso acima, algumas práticas já adotadas no contexto do bloco europeu podem ser adotadas no Brasil, inclusive para fins de harmonização dos dois sistemas, em razão das relações comerciais e de negócio existentes entre Brasil e União Europeia, quais sejam: Notificação (solicitação): Sempre que possível, o importador de dados deve notificar o exportador de dados e o titular dos dados se receber um pedido juridicamente vinculativo de uma autoridade pública (incluindo judiciária) ao abrigo da legislação do país de destino para a divulgação dos dados pessoais transferidos nos termos das cláusulas contratuais. Notificação (acesso): Do mesmo modo, o importador de dados deve notificar o exportador de dados e o titular dos dados se tomar conhecimento de qualquer acesso direto das autoridades públicas a tais dados pessoais, em conformidade com a legislação do país terceiro de destino. Impossibilidade de notificação: Se, não obstante todos os seus esforços, o importador de dados não estiver em condições de notificar o exportador de dados e/ou o titular dos dados de pedidos específicos de divulgação, deve fornecer ao exportador de dados o máximo possível de informações pertinentes sobre os pedidos. Documentação dos pedidos: O importador de dados deve igualmente ser obrigado a documentar qualquer pedido de divulgação recebido e a resposta fornecida, e a disponibilizar essa informação ao exportador de dados ou à autoridade de controle competente, ou a ambos, mediante pedido. Fiscalização: Se, na sequência de uma fiscalização da legalidade de tal pedido, de acordo com a legislação do país de destino, o importador de dados concluir que existem motivos razoáveis para considerar que o pedido é ilegal nos termos da legislação do país terceiro de destino, deve contestá-lo, nomeadamente, quando adequado, esgotando todas as possibilidades de recurso disponíveis. Não cumprimento das cláusulas contratuais: Em todo o caso, se o importador de dados deixar de ter capacidade de cumprir com o quanto disposto nas cláusulas contratuais, deve informar o exportador de dados em conformidade, inclusivamente quando tal for consequência de um pedido de divulgação. ","174380":"Com relação aos mecanismos mais adequados, entende-se não haver necessidade de esgotar as possibilidades ao trazer situações específicas na resolução. Um caminho possível seria trazer os requisitos mínimos que devem conter em tal comunicação, assim como o é feito no art. 9º da LGPD, para que os agentes de tratamento responsáveis escolham o melhor mecanismo, seja uma política de privacidade, um aviso de privacidade, um vídeo explicativo, etc. No que diz respeito às formas de assegurar a efetiva

proteção de direitos dos titulares, entende-se que o próprio mecanismo que autoriza a transferência deve prever isso, por meio de menção explícita sobre o tema. Por fim, para implementação dos instrumentos, tudo vai depender da relação existente entre o exportador e a pessoa titular de dados em questão. Por exemplo, se for no âmbito de utilização de um aplicativo/software, por meio de pop-ups banner; se for no âmbito de uma relação de emprego, por meio de uma política ou aviso de privacidade específicos.

Contribuinte: Guilherme Cunha Braguim

Número: OP-180536

Data: 15/06/2022 - 15:11

Resumo:
:"Teste","174354":"","174356":"","174359":"","174360":"","174361":"","174362":"","17436 3":"","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373": "","174375":"","174376":"","174378":"","174379":"","174380":"

Contribuinte: bruno lustosa rodrigues

Número: OP-180698

Data: 16/06/2022 - 17:11

Resumo: :"","174354":"","174356":"","174359":"","174360":"","174361":"COMENTÁRIO SOBRE O ARTIGO 34 - IMPORTANTE O inciso I do artigo 33 define uma das hipóteses que autoriza transferências internacionais: “I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei...”. Dada a inspiração que este capítulo recebeu do Regulamento Europeu, supõe-se que a validação concedida pela ANPD, por si só já seja suficiente para que uma transferência seja realizada sem qualquer exigência adicional. Mesmo que a Lei brasileira não coloque a hipótese de país/organismo adequado como prioridade sobre as outras hipóteses, ainda assim ela será uma das mais utilizadas devido à facilidade operacional que oferece. Após a “aprovação” de um país pela ANPD, o fluxo de dados se torna livre de impedimentos e outras exigências. Para que o conceito de “pais adequado” se concretize, a Lei define, no artigo 34, os critérios que devem ser levados em consideração pela ANPD para avaliar se um país ou organismo internacional proporciona de fato um “grau de proteção de dados pessoais adequado ao previsto” na LGPD. Desta forma, a compreensão do artigo 34 é uma das bases do sistema de transferências internacionais que virá ser definido pela Autoridade. Embora o citado artigo 34 não esteja listado no item 2.3 da Nota Técnica nº 20/2022/CGN/ANPD, trata-se de artigo crucial para a definição do modelo desejado e é sobre ele que versa este comentário. O artigo 34 define como critérios que devem ser levados em consideração no momento da avaliação do nível de proteção de dados de países estrangeiros: I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional; II - a natureza dos

dados; III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei; IV - a adoção de medidas de segurança previstas em regulamento; V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e VI - outras circunstâncias específicas relativas à transferência. O objetivo do artigo 34 é elencar uma lista mínima de elementos que precisam ser observados para avaliar se um país específico apresenta um sistema de leis e regulamentos que respeitem os direitos e liberdades dos titulares de dados condizente com as premissas de proteção da própria LGPD (nos moldes do inspirador artigo 45 do GDPR). Desta forma, todos os elementos listados como critérios de avaliação devem necessariamente se referir à situação do país em análise. Entretanto, a lista do artigo 34 traz os itens: II - a natureza dos dados; IV - a adoção de medidas de segurança previstas em regulamento e VI - outras circunstâncias específicas relativas à transferência. Estes três elementos (natureza dos dados, adoção de medidas de segurança e circunstâncias específicas relativas à transferência) se referem a operações de transferência e não à situação do pais avaliado. Não existe natureza dos dados no país avaliado, nem medidas de segurança específicas e muito menos circunstâncias específicas de uma transferência. Na medida em que um país é considerado adequado, todo e qualquer questionamento sobre: a “natureza dos dados”, a “adoção de medidas de segurança” e “outras circunstâncias específicas relativas à transferência” não apenas se tornam irrelevantes como poderiam vir a comprometer a premissa de que um país já é adequado por si só e apenas isto já afasta qualquer outra exigência. Será necessário algum tipo de retificação no texto da Lei ou esclarecimento da Autoridade, pois a atual redação inviabiliza a aplicação prática dos incisos II, IV e VI, o que poderá causar problemas futuros. Sugiro que seja feita a retificação, na forma que o sistema legislativo brasileiro permite, com fins de adequar os itens da lista ao propósito do artigo que é avaliar o país e não cada transferência individual. ","174362":"Devem ser rígidas e com conteúdo pré-definido, A criatividade do povo é grande e é mais seguro não deixar margem para "livre interpretação".","174363":"","174364":"","174367":"","174368":"","174369":"","174371":"A situação se enquadra nas Cláusulas Contratuais Específicas. Caso haja uma norma para grupos distintos que não seja as Cláusulas Específicas, o mercado ficará confuso entre os limites de cada uma das hipóteses de transferência. Este fato poderia suscitar interpretações errôneas. É mais seguro manter a definição das Normas Corporativas Globais especificamente para grupos empresariais mesmo que pareça lógico imaginar que se ambas foram aprovadas, a junção deveria dar certo.
","174372":"","174373":"","174375":"","174376":"","174378":"Apenas uma ideia que não sei se é viável do ponto de vista jurídico: o exportador deveria ser punido em caso de qualquer evento com os dados exportados. A exemplo do próprio papel de Controlador da LGPD que sempre será responsável pela escolha de seus fornecedores e parceiros, o exportador deve ser responsável pela decisão de exportar os dados. ","174379":"Imagino que sua obrigação NÂO PERMTIR que isto aconteça. O agente tem total responsabilidade, pois como exportador assumiu o risco. Supondo que aconteça, este acesso, mesmo que exigido por lei daquele país, deve ser visto como acesso ilegal e uma violação àquela base de dados. A partir de então a responsabilidade segue na linha da LGPD: comunicação à ANPD e ao

titular. Deve ir além, pois a empresa precisa garantir apoio ao titular para sanar ou reduzir possíveis efeitos do acesso indevido.. ","174380":"

Contribuinte: MARCIA INES GUANABARA DOS REIS

Número: OP-180744

Data: 17/06/2022 - 06:53

Resumo: :"Os obstáculos enfrentados são: O Brasil ainda não ser considerado um país adequado para o tratamento de dados pessoais; A necessidade de clareza na regulamentação vigente podendo a Instituição ter uma abordagem avaliada no risco documentada em Relatórios específicos. Abaixo sugestões para consideração: • Esforço para considerar o Brasil na lista dos países adequados • Considerando a GDPR: Intragrupo – considerar a Política Global • Vendor – cláusula padrão mínima, considerando flexibilização de volume (novos contratos a partir da regulamentação) e definição de um prazo para os contratos do legado Seguindo normativo de Cyber e outros normativos regulatórios, para ser um ambiente certificado, considerar Relatório podendo ser elaborado internamente de avaliação do tema. ","174354":"A maneira razoável para a promoção de convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições poderia considerar uma avaliação em benchmarking de cláusulas de outras jurisdições como orientador. A ANPD poderia: • Divulgar guia orientativo com parâmetros sobre cláusulas contratuais relacionados à interoperabilidade; • Definir conceito claro da interoperabilidade. ","174356":"Os instrumentos mais efetivos e mais utilizados são: • Disposições incluídas como cláusula / anexo no contrato; •Outras hipóteses (ex: obrigação legal / regulatória). ","174359":"• Benefícios: reforço na governança do tratamento dos dados. • Impactos: falta de uniformização e complexidade das diversas regulamentações sobre o tema. ","174360":"a. cláusulas-padrão contratuais; SCCs Flexibilidade de conceitos / exportador / importador de dados b. cláusulas contratuais específicas; e Atenção ao padrão europeu c. normas corporativas globais. Accountability grupo econômico; Normas corporativas (políticas internas, p.ex) Não burocratizar os mecanismos. Normas que abarquem conceitos e critérios de mais de uma jurisdição ou referência regulatória. ","174361":"Devem ser levados em consideração: • Inviabilidade de customizar por local; customizar pelo agente; • Modelos mais simplificados para país com mesmo grau de proteção seria uma alternativa; • Se lei é protetiva, ela integra lacunas contratuais, não necessária a complementação; • Gerais – tratamento de forma principiológica. ","174362":"As cláusulas não deveriam ser rígidas, levando-se em conta a flexibilidade: • Com indicação dos itens necessários para serem regrados (ex: observância de princípios, notificações de incidentes relevantes no caso do Operador; etc) • Considerando o setor envolvido, inclusive regramentos já existentes. ","174363":"• Check-list de tomada de decisões como boas práticas levando em consideração a abordagem baseada no risco; • Orientação não vinculante; • Citar, como exemplo, a segurança cibernética para setor financeiro (regramento Resolução CMN, que já contém espécie de check-list). ","174364":"Sim, é recomendável adequando ao tipo de

relacionamento. Por exemplo caso haja um incidente no operador, o prazo de comunicação ao controlador. Há a obrigatoriedade de comunicação ao órgão regulador pelo controlador, mas é necessário avaliar no país importador se será/é feita esta comunicação. Considerando SCC: ônus excessivo, difícil implementação, obrigações de difícil atendimento. ","174367":"Sim, precisam ser diferentes por terem requisitos diferentes, levando em consideração que nas Normas Corporativas Globais há um conhecimento maior da governança das partes. Como sugestão considerar: •Flexibilidade; Possibilidade de requisitos diferentes; • Sugestão para um guia orientativo; não haver aprovação prévia pela ANPD de toda norma (art. 35, LGPD). • Facilitar o processo para implantação destas normas corporativas; aprovação prévia cria gargalos / barreiras que não fazem sentido para a própria ANPD e para o mercado. ","174368":"Instituição podendo definir os critérios para aplicação da norma corporativa global.","174369":"• Definir categorias conforme guia orientador. • Respeitar segredos comerciais. ","174371":"• Benefícios: Reconhecer outros instrumentos que igualmente tragam proteção.","174372":"• Adoção de processo que assegure a celeridade na verificação e aprovação de cláusulas contratuais e de normas corporativas globais.","174373":"Caso haja uma mudança de controlador da informação. Adicionalmente, se for para execução do contrato, a comunicação poderia ocorrer quando há necessidade de alguma intervenção deste titular. Em caso de alteração de configuração original da transferência, exemplo mudança de empresa terceirizada para atendimento, suporte, esta informação poderia constar no site da Instituição. ","174375":"Como alternativas: • Cooperação internacional entre as autoridades de proteção de dados; • Manual orientador com a relação agente x titular dos dados; • Disposições incluídas como cláusula / anexo no contrato. ","174376":"Alternativas: • Esforço para considerar o Brasil na lista dos países adequados; • Manual orientador; • Flexibilização de volume (novos contratos a partir da regulamentação) e definição de um prazo para a informação atual e do legado • Para ser um ambiente certificado, considerar Relatório podendo ser elaborado internamente de avaliação do tema e/ou certificado. ","174378":"Sem sugestões.","174379":"Como obrigações: • É necessário ter regulamentação aplicável ao caso para cumprimento da determinação da Autoridade; • Importador e Exportador precisam avaliar a ordem considerando a avaliação dos mecanismos de segurança para disponibilização da informação e considerando somente o que for solicitado pela autoridade pública estrangeira. ","174380":"Disponibilização no site da Instituição e/ou contrato com o titular do dado, além da Política de Privacidade/Proteção de Dados. A proteção dos direitos dos titulares precisa ser avaliada com os mecanismos de segurança implementados pelo exportador e com o importador, considerando a relevância deste com avaliação do que é feito, e possível Relatório emitido por empresa externa e/ou selo de certificação.

Contribuinte: ELIEL MIRANDA DA SILVA

Número: OP-180779

Data: 17/06/2022 - 09:21

Resumo: :"O principal obstáculo para as empresas que desejam transferir internacionalmente os dados pessoais dos titulares de dados brasileiros é a falta de mecanismos de proteção aprovados. Para muitos países, a transferência de dados para o Brasil é relativamente simples; no entanto, ao transferir os dados de residentes europeus (países do EEE e Reino Unido), a falta de uma decisão de adequação e o aumento da complexidade para a transferência de dados pessoais em um mundo pós-Schrems II. torna as transferências para o Brasil mais intensivas em recursos.","174354":"Dado que os países europeus (EEE) tendem a ser os mais exigentes, quando se trata de transferências internacionais de dados pessoais, regular essas transferências de maneira que satisfaça às exigências dos reguladores da UE (o Tribunal de Justiça da União Europeia), assegurando que as transferências para o Brasil não prejudicarão os direitos e liberdades dos cidadãos da UE, deve ser uma prioridade para a ANPD. Se essas transferências não forem tratadas antecipadamente, as transferências de dados pessoais a em desconformidade (ou seja, para países não reconhecidos como adequados) podem dificultar a cooperação futura.","174356":"As cláusulas modelo da UE Pré-Schrems II (cláusulas contratuais padrão) provavelmente apresentam o instrumento mais simples e escalável para proteger as transferências internacionais de dados pessoais. De todo modo, importa mencionar que as Avaliações de Impacto de Transferência que têm sido um requisito para o uso continuado das Cláusulas Modelo pós-Schrems II apresentam inconsistências e são um fardo significativo para as empresas.","174359":"As transferências internacionais de dados permitem que as empresas brasileiras utilizem o maior conjunto de fornecedores disponíveis, ajudam a manter os fornecedores locais competitivos e ajudam a garantir que as empresas internacionais possam oferecer facilmente seus serviços digitais aos consumidores brasileiros. Evidentemente existem riscos em qualquer transferência (interna ou internacional) e ter os dados do brasileiro comprometidos em um território com padrões de proteção de dados mais baixos do que eles esperariam localmente é uma preocupação particular; é por isso que é essencial que desenvolvamos mecanismos de salvaguarda que sejam robustos, simples e utilizáveis. Cláusulas contratuais padrão, sustentadas por orientações aprovadas pela ANPD quanto à aplicabilidade da área, oferecem o mecanismo mais flexível e amigável aos negócios para transferências internacionais de dados. ","174360":"","174361":"Os elementos considerados pela ANPD ao avaliar o nível de proteção de dados de países estrangeiros ou organismos internacionais devem ser contemplados em instrumentos contratuais para dar aos que utilizam esses mecanismos a certeza de que são válidos. Idealmente, esses instrumentos deveriam incluir uma lista de regiões/órgãos onde, apesar dos instrumentos contratuais, as transferências para essas áreas ainda seriam proibidas.","174362":"As cláusulas contratuais devem ser rígidas e pré-definidas. Caso contrário, a natureza personalizada de cada acordo provavelmente tornará a conformidade com a proteção de dados um fardo significativo para as empresas brasileiras, especialmente as empresas menores sem o poder de impor os termos do negócio.","174363":"Na medida em que as cláusulas contratuais padrão são modulares, os módulos específicos que compõem um conjunto de cláusulas devem estar disponíveis na primeira página do documento (para ajudar a economizar tempo).","174364":"É possível que apenas um conjunto de cláusulas contratuais englobe as regras dos diferentes agentes de tratamento de dados. Isso pode ajudar a no exercício dos direitos dos titulares de dados brasileiros, na medida que os operadores que extrapolarem as suas atribuições contratuais, ou

seja, que ao realizar o tratamento dos dados ao se tornarem controladores, sejam diretamente responsáveis pelos danos causados aos seus respectivos titulares.","174367":"Binding Corporate Rules (BCRs) são artefatos multidimensionais que precisam refletir os requisitos de várias estruturas legais e regimes regulatórios; como tal, esperaríamos um maior grau de flexibilidade nos BCRs (ou seja, menos restritivos do que o Standard Contratual Clauses - SCC), mas desde que sejam especificamente endossados pela ANPD.","174368":"Um grupo econômico deve ser definido de acordo com a organização que detém o controle da entidade.","174369":"¿ Objeto e natureza do tratamento ¿ Duração do tratamento e mecanismos de exclusão ¿ Finalidade(s) do tratamento ¿Categorias de titulares de dados ¿ Tipos de dados pessoais ¿ Categorias especiais de dados (se aplicável) ","174371":"","174372":"","174373":"Quando a configuração original do material de transferência for alterada, os titulares dos dados devem esperar que os dados sejam i) solicitados para consentimento para a alteração, ii) excluídos ou iii), onde possa haver risco para o titular dos dados. Na hipótese de eventual atualização da configuração, a expectativa é de que o controlador, dentro de um período (por exemplo dentro de um mês) informe obtenha a ciência dos titulares dos dados com relação a mudança.","174375":"Sem um acordo internacional multilateral, os conflitos serão resolvidos localmente. A vantagem disso é que as nuances e sensibilidades locais serão abordadas (pelo menos onde há escala de mercado para garantir o atendimento desses requisitos). No entanto, é provável que isso leve à fragmentação contínua de produtos e serviços.","174376":"Garantir que os requisitos internacionais de transferência de dados sejam simples e compreendidos (ao contrário da confusão que persiste atualmente na Europa) é a melhor maneira de promover a conformidade. Além disso, onde os mecanismos são estabelecidos e foi determinado que eles são válidos, sua validade deve continuar a ser aceita (apesar de contestações legais bem-sucedidas) até que mecanismos alternativos adequados sejam estabelecidos (para ajudar a evitar um vácuo de conformidade).","174378":"Os mecanismos contratuais são o único mecanismo que aborda de forma prática os desafios de prestação de contas quando os dados são transferidos para fora do Brasil.","174379":"As obrigações só devem ser atribuídas quando forem susceptíveis de melhorar significativamente a privacidade do titular dos dados. Quando as autoridades públicas estrangeiras possuem a capacidade de garantir o acesso aos dados, independentemente das ações do exportador ou importador, as obrigações devem ser limitadas a atividades disruptivas, ou seja, se os serviços de segurança estrangeiros quiserem ter acesso aos dados, eles poderão fazê-lo, então a obrigação é simplesmente testar sua determinação e tentar evitar solicitações indesejadas e desnecessárias.","174380":"Para garantir a máxima transparência, a ANPD deve desenvolver uma hierarquização publicamente disponível das regras privacidade de outras jurisdições. Essas informações podem ser compartilhadas com os titulares dos dados por meio de avisos de privacidade, para ajudar a garantir que eles entendam os riscos associados a determinadas transferências.

Contribuinte: Marina Saraiva Pezolito

Número: OP-180803

Data: 17/06/2022 - 12:22

Contribuinte: Bruna Michele Wozne Godoy

Número: OP-180805

Data: 17/06/2022 - 12:45

Resumo: :"Celebramos o reconhecimento, por parte da consulta, da importância dos fluxos de dados transfronteiriços. O Brasil estabelecerá importantes precedentes globais, pois cria mecanismos de transferência que apoiam fluxos de dados responsáveis. As transferências internacionais de dados trazem grandes benefícios sociais e econômicos; e regras que permitem a transferência de dados com garantias adequadas de privacidade ajudarão o Brasil a perceber esses benefícios. Em uma época de crescente protecionismo de dados em todo o mundo, o Brasil deve continuar a promover fortes salvaguardas de privacidade e fluxos internacionais de dados como pilares da economia de dados. O Brasil também deve ser uma voz ativa contra as tendências de localização e outras restrições aos fluxos internacionais de dados que podem limitar o crescimento econômico do país. Este trabalho é crucial para superar os obstáculos à transferência de dados em todo o mundo. No Brasil, as empresas exigem uma série de mecanismos de transferência para apoiar os fluxos globais de dados - e esses mecanismos devem ser construídos com base em fortes salvaguardas de proteção de dados. Apoiamos os esforços da ANPD para implementar as obrigações de transferência da LGPD, assegurando que as organizações disponham de várias opções para usar na transferência internacional de dados, incluindo determinações de adequação, cláusulas contratuais padrão, além de outros mecanismos. Diferentes tipos de organizações e diferentes modelos de negócios exigem o uso de diferentes mecanismos de transferência que não são intercambiáveis. Na prática, as empresas maiores muitas vezes confiam em um ou mais mecanismos de transferência de dados, utilizando a ferramenta mais adaptada às suas necessidades comerciais e à(s) transferência(s) de dados específica(s) em mãos. Já outras empresas acabam contando com apenas um mecanismo, como o das determinações de adequação ou cláusulas contratuais padrão. A criação de uma gama de mecanismos flexíveis de transferência que podem ser utilizados de forma diferente em várias situações ajudará as empresas a transferir dados de forma responsável, de acordo com a legislação brasileira. Um passo importante que a ANPD pode dar antes da publicação de uma nova regulação é conferir segurança jurídica para as transferências internacionais de dados que já ocorrem. Como as disposições da LGPD sobre transferências internacionais de dados exigem a implementação pela ANPD, existe atualmente um grau de incerteza quanto às obrigações legais para essas transferências de dados que ainda não foram reguladas. Portanto, recomendamos que a ANPD elabore orientações confirmando que, neste interregno, as empresas podem continuar a transferir dados de forma responsável internacionalmente com base nas melhores práticas globais, tais como disposições contratuais que garantam a proteção dos dados, independentemente de onde os dados sejam transferidos, e principalmente quando essas práticas forem convergentes com os objetivos gerais da LGPD. Sob o cenário atual - com poucas opções disponíveis - as organizações enfrentam mais desafios para operar em um

ambiente internacional competitivo. Desenvolver regulamentações que operacionalizem os mecanismos de transferência de dados sob a LGPD é, portanto, fundamental para estabelecer segurança jurídica às organizações que fazem negócios no Brasil. ","174354":"Os mecanismos de transferência de dados não podem ser vistos isoladamente. Na medida em que os países do mundo inteiro desenvolvem e atualizam suas leis e regulamentações de proteção de informações pessoais, é fundamental que essas estruturas legais sejam projetadas para proteger efetivamente a privacidade de modo internacionalmente interoperável e flexível o suficiente como resposta à rápida evolução das tecnologias e dos modelos de negócios, sempre priorizando padrões altos de proteção de dados. Isto é particularmente importante no contexto das transferências internacionais de dados, onde as exigências legais interoperáveis impactam na capacidade das organizações de cumprir com essas obrigações em todas as jurisdições. Naturalmente, o contexto e a perspectiva em torno da privacidade e da proteção de dados pessoais podem variar entre diferentes países com base nas diferenças culturais, tradições legais e outros fatores. Ao mesmo tempo, os governos devem apoiar o reconhecimento comum de normas e práticas internacionais que protejam as estruturas de privacidade interoperáveis. Se, em vez disso, os países adotarem políticas fragmentadas sobre questões centrais, isso pode acarretar uma elevação do custo dos negócios para todas as empresas e pode prejudicar a proteção de dados pessoais e a privacidade do consumidor. As empresas que prestam serviços em mais de um país devem identificar - e implementar - exigências adicionais de privacidade e proteção de dados impostas por cada país em que operam, observando como essas obrigações se relacionam às regulamentações de outros países. Leis e regulamentos que promovem a convergência em torno de abordagens internacionalmente reconhecidas para transferências de dados podem ajudar a impulsionar mecanismos interoperáveis de transferência de dados, permitindo às empresas alavancar essas abordagens comuns. Na prática, um novo mecanismo de transferência deve ser suficientemente similar - em estrutura e proteções substantivas - para que as obrigações sob o novo mecanismo possam ser mapeadas para as obrigações sob o novo mecanismo. Isto garante que as empresas possam entender como suas obrigações mudam em todas as jurisdições e lhes permite identificar exigências semelhantes em todas as estruturas legais. Essa abordagem cria um processo de conformidade mais eficiente e impulsiona o investimento em práticas consolidadas que podem ser alavancadas pelas empresas em mais de uma jurisdição. Há um papel importante para os formuladores de políticas na promoção de abordagens interoperáveis de transferência de dados. Recomendamos fortemente que a ANPD reconheça que os mecanismos de transferência contratual existentes podem satisfazer as obrigações da LGPD, caso contenham proteções substantivas suficientemente similares. Muitas empresas globais já adotam mecanismos de transferência baseados em contratos que protegem os dados à medida que eles são transferidos entre países e regiões. Com isso, a ANPD pode reconhecer que esses contratos existentes satisfazem a LGPD se eles contiverem proteções substantivas suficientemente similares àquelas exigidas pela legislação - sem exigir que as empresas renegociem esses contratos para adotar linguagem ou formatos específicos pré-aprovados. Por exemplo, se uma empresa adotou contratos que já incorporam as Cláusulas Contratuais Padrão da União Europeia - SCCs da UE, esse contrato pode conter obrigações suficientes de proteção de dados para satisfazer as exigências de transferência sob

a LGPD. Encorajamos fortemente a ANPD a reconhecer que estes mecanismos contratuais existentes podem satisfazer as exigências substantivas da LGPD e evitar a exigência de que as empresas adotem um novo formulário ou modelo para estas mesmas proteções. Esta abordagem, ao reconhecer o alinhamento entre estes mecanismos existentes e as exigências da LGPD, conduz à harmonização e assegura que as empresas possam alavancar as práticas e mecanismos de conformidade existentes em apoio a produtos, serviços e clientes no Brasil. Além disso, a participação em sistemas de certificação internacional também pode contribuir para o avanço da convergência e da interoperabilidade. É primordial que a ANPD trabalhe para harmonizar os conflitos jurisdicionais potenciais que possam emergir, evitando que estas questões sejam tratadas por organizações individuais. ","174356":"Como empresas globais, os membros da BSA adotaram uma série de mecanismos contratuais para apoiar transferências responsáveis de dados em todo o mundo. Os mecanismos contratuais são particularmente importantes para as empresas porque podem apoiar transferências para países que não possuam uma determinação de adequação e porque podem ser implementados sem buscar aprovação prévia de um regulador, ao contrário das regras corporativas obrigatórias. Portanto, apreciamos a regulamentação prioritária da ANPD que apoia os mecanismos de transferência baseados em contratos. Os membros da BSA adotaram mecanismos de transferência contratual, incluindo: • Cláusulas Contratuais Padrão da União Europeia (EU SCCs); • Acordos internacionais de transferência de dados do Reino Unido (UK IDTAs); e • Regras de Privacidade trans fronteiriças da APEC e as Regras de Privacidade da APEC para Processadores (APEC CBPRs e APEC PRPs) Mecanismos extracontratuais. Embora a consulta atual se concentre nos mecanismos de transferência contratual, também saudamos o reconhecimento pela LGPD das avaliações e certificações de adequação, que reconhecem os mecanismos de transferência duráveis. • Adequação. As determinações de adequação são particularmente importantes para as pequenas e médias empresas que podem não dispor de recursos para adotar mecanismos contratuais padronizados. Ao fazer determinações de adequação, a ANPD pode contribuir para a convergência global ao reconhecer que outros países possuem níveis similares de proteção de dados. No futuro, encorajamos a ANPD a estabelecer um rol de países prioritários para decisões de adequação com base tanto na relevância para a indústria quanto no compromisso de um país com valores de proteção de dados. • Certificações. Em nossa opinião, os esquemas de certificação podem contribuir para um sistema globalmente interoperável e voltado para o mercado que apoie as transferências de dados. A BSA reconhece que os esquemas de certificação voluntária podem fornecer às empresas mecanismos flexíveis para a transferência de dados. Também queremos enfatizar que os esquemas de certificação são mais úteis para organizações se forem reconhecidos e adotados por mais de uma jurisdição - e, portanto, podem permitir que as empresas que utilizam um único esquema de certificação cumpram com as obrigações em múltiplas jurisdições. Encorajamos a ANPD a priorizar estes benefícios práticos ao considerar ainda mais os esquemas de certificação. ","174359":"Elogiamos a ANPD por reconhecer os benefícios das transferências internacionais de dados. Também apoiamos o desenvolvimento de mecanismos que favoreçam o fluxo responsável de dados através das fronteiras. A capacidade de transferir dados através de fronteiras internacionais é fundamental para organizações de todos os

tamanhos e em todos os setores da indústria. Qualquer empresa com funcionários, fornecedores ou escritórios em mais de um país precisa enviar dados internacionalmente todos os dias, inclusive para: • Gerenciar o inventário global através de um sistema centralizado, incluindo o roteamento de produtos entre países; • Analisar as ameaças de cibersegurança em diferentes países para identificar ameaças comuns; • Gerenciar recursos humanos a partir de uma única sede; e • Avaliar o desempenho de produtos e serviços a partir de um único centro de pesquisa. Para as empresas, a transferência de dados através das fronteiras as ajuda a serem mais eficientes e efetivas na entrega dos produtos e serviços que seus clientes exigem. As transferências de dados também sustentam produtos e serviços globais que possibilitam o teletrabalho, colaboração virtual, treinamento on-line e educação on-line, entre muitos outros. Ter acesso a estas ferramentas globais é particularmente importante para as pequenas e médias empresas, que frequentemente as utilizam para alcançar novos mercados e atender novos clientes . As transferências transfronteiriças também são parte integrante das cadeias de fornecimento internacionais, levando as informações através das fronteiras que otimizam a aquisição, finanças, logística, mitigação de riscos e capacidade de resposta . O processo da cadeia de suprimentos para a maioria dos produtos e serviços envolve muitas fases, agentes e países - bem como está sujeito a potenciais rupturas com base no clima, disponibilidade de material, escassez, ameaças geopolíticas ou crises de saúde . No início de 2020, 94% das empresas da Fortune 1000 relataram rupturas na cadeia de suprimentos da COVID-19 , destacando ainda mais a natureza complexa e integrada dessas cadeias e o papel das transferências de dados na mitigação de riscos e na resposta. As transferências de dados não são importantes apenas para as empresas individualmente - elas também sustentam a economia global de hoje. Estima-se que elas contribuam com US$2,8 trilhões para o PIB global, uma parcela que excede o comércio global de bens e que deverá crescer para US$11 trilhões até 2025. As interrupções nos fluxos de dados transfronteiriços têm amplas reverberações que podem levar à redução dos ganhos potenciais do PIB, à redução dos investimentos nos mercados locais, à perda de empregos e consequente queda do bem-estar e ao impacto adverso nos ecossistemas digitais locais e nacionais - em um momento em que a recuperação econômica está no topo da agenda de cada governo. Cabe destacar que o apoio ao fluxo internacional de dados também pode ajudar a desenvolver uma economia digital vibrante e próspera no Brasil. Para alavancar os benefícios que são trazidos pelo fluxo responsável de dados através das fronteiras, recomendamos que a ANPD promova a convergência e interoperabilidade dos mecanismos de transferência de dados, conforme abordado em nossas respostas às Perguntas 2 e 3. Estratégia Digital USAID, 2020–2024, https://www.usaid.gov/usaid-digital-strategy, p. 37 (“Os ecossistemas digitais têm o potencial de dar a comerciantes informais, mulheres empresárias, pequenos agricultores e MPMEs envolvidas no comércio internacional acesso a mercados, informações e financiamento.”). Global Data Alliance, Transferências de Dados Transfronteiriças e Gerenciamento da Cadeia de Suprimentos. De acordo com o Relatório Global sobre Catástrofes Climáticas de 2016, a indústria da cadeia de abastecimento enfrenta anualmente uma média de 260 grandes desastres naturais Erik Sherman, "94% das empresas da Fortune 1000 estão vendo interrupções na cadeia de fornecimento do coronavírus: relatório", Forbes, 21 de fevereiro de 2020. ","174360":"","174361":"Queremos enfatizar

que as determinações de adequação e os instrumentos contratuais são dois mecanismos separados que suportam as transferências internacionais de dados. É importante observar que não há hierarquia para o uso de cada mecanismo previsto no artigo 33 da LGPD, incluindo instrumentos contratuais e adequação. As partes podem escolher um mecanismo que seja adequado para suas transferências. Encorajamos a ANPD a não aplicar os requisitos de um destes mecanismos ao outro mecanismo. Por exemplo, as empresas que adotam compromissos contratuais para transferência de dados não devem ser obrigadas a avaliar o nível de proteção de dados do país estrangeiro para o qual os dados devem ser transferidos. Isso porque os próprios acordos contratuais aplicam proteções substantivas aos dados pessoais, independentemente de onde esses dados sejam transferidos - tornando os compromissos contratuais apropriados para transferências a países que não receberam uma determinação de adequação. Além disso, as empresas (e especialmente as pequenas e médias empresas) não estão equipadas para realizar o tipo de avaliação detalhada e holística das leis e práticas regulatórias de um país estrangeiro. Exigir tal avaliação cria incerteza, pois as empresas têm dificuldades com essa tarefa. Ademais, tal exigência trará poucos benefícios para os consumidores. ","174362":"Encorajamos fortemente a ANPD a priorizar uma abordagem flexível sobre os mecanismos de transferência contratual. Como observado em nossa resposta à pergunta 2, recomendamos que a ANPD reconheça que os mecanismos de transferência contratual existentes satisfazem as obrigações da LGPD se eles possuírem proteções substantivas suficientemente similares. Esta abordagem especificaria os resultados desejados - ou seja, proteger os dados de acordo com as exigências da LGPD - em vez de se concentrar em exigências rígidas para adotar um determinado formato ou uma linguagem específica pré-aprovada. Uma abordagem flexível é particularmente importante para assegurar que as empresas adotem as obrigações substantivas apropriadas. Muitas empresas já celebraram contratos que refletem obrigações legais existentes sob outras jurisdições - e esses compromissos também podem satisfazer as obrigações substantivas sob a LGPD. As empresas devem ser capazes de confiar nessas disposições específicas, desde que elas criem proteções substantivas suficientemente similares àquelas exigidas pela LGPD e não conflitem com nenhuma das exigências da LGPD. ","174363":"Encorajamos a ANPD a priorizar a flexibilidade nos mecanismos de transferência contratual. Como explicado em nossas respostas às Perguntas 2 e 7, o formato apropriado para cláusulas contratuais padrão deve ser suficientemente flexível para reconhecer os acordos existentes que já cumprem as obrigações substantivas da LGPD Além disso, outra abordagem interoperável que a ANPD poderia considerar para alavancar os mecanismos contratuais existentes é criar um modelo de adendo semelhante ao das SCCs da UE. O UK Information Commissioner's Office (UK ICO) adotou recentemente esta abordagem em dois novos conjuntos de cláusulas contratuais modelo que entraram em vigor este ano . Primeiro, a ICO do Reino Unido adotou um conjunto autônomo de 36 páginas de termos contratuais que as empresas poderiam adotar para apoiar as transferências de dados do Reino Unido . Em segundo lugar, a ICO do Reino Unido adotou um adendo de nove página que as empresas podem acrescentar aos contratos existentes que incorporam as SCCs da UE; isto permite que as empresas adotem a linguagem adicional no adendo para apoiar as transferências de dados do Reino Unido . A adoção tanto de um conjunto autônomo de SCCs quanto de um adendo cria opções flexíveis para empresas que

transferem dados do Reino Unido, inclusive para empresas menores (que podem não ter outros mecanismos contratuais em vigor e, portanto, não fazem uso do adendo) e maiores (que podem já ter mecanismos contratuais existentes que são prontamente modificados pelo adendo). A criação de adendos - que reconhecem as proteções substantivas no mecanismo de transferência contratual subjacente e adotam um conjunto de proteções adicionais concebidas para satisfazer as exigências de uma segunda jurisdição - é outra abordagem interoperável para as transferências de dados, concebida para funcionar em todas as jurisdições. Incentivamos a ANPD a considerar ainda mais este modelo, que pode ajudar a garantir que os mecanismos contratuais adotados por diferentes jurisdições possam trabalhar juntos na prática para promover altos padrões de proteção de dados. Ao mesmo tempo, onde os mecanismos contratuais existentes podem satisfazer as obrigações da LGPD, o uso de adendos não deve ser exigido. Ver UK ICO, Acordo Internacional de Transferência de Dados e Orientação Ver UK ICO, Acordo Internacional de Transferência de Dados Ver UK ICO, International Data Transfer Addendum to the EU Commission Standard Contractual Clauses ","174364":"Se a ANPD adotar novas SCCs brasileiras, nós a encorajamos a considerar a gama de diferentes entidades que transferem dados e a gama de diferentes transferências realizadas entre essas entidades. Qualquer novo mecanismo contratual deve suportar transferências entre dois controladores, de um controlador para um processador, de um processador para um controlador, ou entre processadores. As transferências de dados ocorrem sob muitas formas e, portanto, é crucial que os mecanismos contratuais de transferência possam ser usados em toda a gama de cenários de transferência. Por exemplo, a UE atualizou recentemente seus SCCs para adotar uma abordagem modular que as organizações podem empregar nestes diferentes tipos de transferências. Quer a ANPD adote ou não uma abordagem modular, qualquer nova SCC no Brasil deve ser suficientemente flexível para ser usada em cada um destes cenários","174367":"","174368":"","174369":"","174371":"","174372":"Embora esta questão se refira à "verificação" de cláusulas contratuais específicas e regras corporativas vinculantes, em vez de verificação de cláusulas contratuais padrão, queremos enfatizar que o processo de utilização de arranjos contratuais não deve envolver uma pré-aprovação pela ANPD. Ao contrário, as empresas devem ser capazes de adotar compromissos contratuais que reflitam as proteções substantivas exigidas pela LGPD sem solicitar à ANPD a aprovação prévia de cada conjunto de termos contratuais. Isto assegura que as empresas possam adotar mecanismos de transferência contratual prontamente, sem criar uma enchente de pedidos de aprovação que requeiram atenção por parte da ANPD e retardam a adoção de mecanismos para salvaguardar os dados transferidos. Em vez disso, a ANPD deve estabelecer requisitos específicos para as cláusulas contratuais e declarar que qualquer contrato que atenda a esses requisitos satisfaz as obrigações da LGPD que regem as transferências de dados. Quanto à aprovação de regras corporativas obrigatórias (BCRs), a ANPD poderia considerar acelerar a consideração das BCRs que já foram aprovadas por outras jurisdições cujas leis são análogas às da LGPD. ","174373":"","174375":"","174376":"Encorajamos a ANPD a promover a conformidade regulamentar, emitindo uma série de orientações para a indústria sobre como os mecanismos de transferência devem ser implementados sob a LGPD. Por exemplo, a ANPD pode criar um website com conteúdo para grupos da indústria aprenderem mais sobre

os mecanismos de transferência . O website também pode ser atualizado com orientações específicas para setores definidos ou para pequenas e médias empresas. Exortamos a ANPD a trabalhar com as partes interessadas durante todo o processo de adoção de regulamentos sobre transferências internacionais de dados, e para identificar áreas onde haja amplo consenso entre as partes interessadas de que orientações regulatórias adicionais sejam úteis. Para um exemplo, consulte o site da ICO do Reino Unido sobre orientação para organizações, incluindo obrigações de proteção de dados após a saída do Reino Unido da União Europeia. ","174378":"","174379":"A consulta pergunta sobre as obrigações do importador e exportador no caso de acesso aos dados por autoridades públicas estrangeiras. No caso de acesso por um governo estrangeiro, a obrigação apropriada para um importador de dados é notificar prontamente o exportador de dados caso receba um pedido legalmente vinculante de uma autoridade pública ou tribunal no terceiro país para divulgar os dados pessoais transferidos. Ao mesmo tempo, qualquer obrigação desse tipo deve reconhecer que um importador pode ser proibido por sua lei nacional de fornecer certas informações ao exportador. Nesta circunstância, a obrigação do importador deve ser a de notificar o exportador imediatamente após a expiração de qualquer proibição, conforme permitido pela lei aplicável. Em circunstâncias onde não há proibição de notificar o exportador que um pedido foi recebido pelas autoridades públicas estrangeiras, pode haver, no entanto, restrições sobre o tipo de informação que o importador pode fornecer ao exportador quando solicitado. Portanto, recomendamos que qualquer obrigação relacionada a tal notificação evite criar uma lista rígida de itens em uma notificação, mas, em vez disso, reconheça que tal notificação deve incluir certas informações, com uma quantidade razoável de detalhes, na medida do possível, nos termos da legislação aplicável. Isto cria mais flexibilidade para os importadores de dados fornecerem avisos aos exportadores, mesmo que o importador possa ser proibido de fornecer tipos específicos de informações. ","174380":"A consulta também pergunta sobre formas apropriadas de fornecer aos titulares de dados informações claras e relevantes sobre a transferência de seus dados para fora do Brasil. Encorajamos a ANPD a se concentrar no fornecimento de informações aos consumidores que incluam um contexto significativo - sem exigir que as empresas forneçam aos titulares dos dados longas listas de tipos de dados ou empresas que possam acabar não ajudando no entendimento do indivíduo sobre como seus dados são tratados. Por exemplo, recomendamos contrariamente à inclusão de qualquer exigência de fornecer aos titulares dos dados as identidades de todos os terceiros aos quais os dados pessoais podem ser divulgados. O fornecimento de tais informações resultaria em uma longa lista que poderia obscurecer informações relevantes para os titulares dos dados. Além disso, fornecer tal lista pode ser extremamente difícil para as empresas (dada a quantidade de terceiros que podem ser contratados para apoiar um determinado serviço, e a necessidade de trocar entre terceiros durante a prestação desse serviço). Isto retiraria recursos de outras atividades que promovem a proteção e a privacidade dos dados. Além disso, encorajamos fortemente a ANPD a abster-se de criar requisitos rígidos ou exigir que formatos específicos sejam seguidos para o compartilhamento de informações sobre transferências de dados. Por exemplo, as empresas devem ser autorizadas a compartilhar as informações necessárias com os titulares dos dados por meio de websites. Como discutido em nossa resposta à pergunta

17, a orientação para a indústria também pode ser útil na criação de ferramentas que ajudem as empresas a implementar políticas de acordo com suas obrigações.

Contribuinte: LUCAS LUCCHESI CORREA MACHADO

Número: OP-180822

Data: 17/06/2022 - 14:28

Resumo: :"The Global Data Alliance (GDA)[1] saúda a oportunidade de fornecer feedback à Autoridade Nacional de Proteção de Dados (ANPD) sobre a regulamentação das transferências internacionais de dados sob a Lei Brasileira de Proteção de Dados Pessoais (LGPD). A Global Data Alliance apoia políticas que ajudam a incutir confiança na economia digital sem impor restrições indevidas de dados transfronteiriços ou exigências de localização que minam a segurança dos dados, a inovação, o desenvolvimento econômico e o comércio internacional. As empresas membros da Aliança são investidores significativos no Brasil, investindo coletivamente milhões de dólares e empregando milhares de cidadãos brasileiros. As empresas membros da GDA são ativas no Brasil nos setores aeroespacial, automotivo, bens de consumo, eletrônicos, energia, serviços financeiros, saúde, mídia, cadeia de suprimentos e telecomunicações. Confiando na capacidade de transferir dados e acessar tecnologia através de redes transnacionais de TI, os membros da Aliança também ajudam a oferecer serviços financeiros, tecnologias de software empresarial e recursos de saúde, científicos e educacionais no Brasil.[2] A capacidade de transferir dados de forma segura através de redes digitais transnacionais é de importância central para muitos objetivos de políticas nacionais. As transferências de dados apoiam a recuperação da COVID-19, conectividade digital, cibersegurança, prevenção de fraudes, antilavagem de dinheiro e outras atividades relacionadas com a proteção da saúde, privacidade, segurança e conformidade regulamentar. Esta capacidade também apoia a prosperidade econômica compartilhada. O acesso transfronteiriço a mercados, compradores, fornecedores e outros parceiros comerciais permite que empresas brasileiras de todos os setores se envolvam em transações internacionais mutuamente benéficas com empresas estrangeiras. As transferências de dados, que são críticas em cada estágio da cadeia de valor para empresas de todos os tamanhos, apoiam as cadeias de fornecimento globais e promovem a produtividade, a segurança e a responsabilidade ambiental. Esta capacidade também apoia a inovação e a pesquisa e desenvolvimento transnacional (P&D), assim como a proteção e aplicação da propriedade intelectual. O progresso científico e tecnológico exige o intercâmbio de informações e ideias através das fronteiras: Como a OMC declarou, "para que os dados floresçam como um insumo para a inovação, eles se beneficiam do fluxo o mais livre possível, dadas as políticas necessárias de proteção à privacidade necessárias".[3] Elogiamos a ANPD por reconhecer a importância dos fluxos internacionais de dados e por reconhecer que os mecanismos de transferência de dados se tornaram um instrumento-chave, tanto para a proteção dos direitos dos indivíduos, quanto para o desenvolvimento da economia digital e do comércio internacional. Incentivamos que sejam priorizados os mecanismos de transferência que se baseiam em níveis altos de confiança e de proteção de dados. Nossos comentários

concentram-se em três aspectos da consulta: • Reconhecimento dos benefícios das transferências internacionais de dados. • Promoção da convergência e da interoperabilidade entre os mecanismos de transferência contratual. • Sugestão de alternativas práticas para implementar esses requisitos. Celebramos o reconhecimento, por parte da consulta, da importância dos fluxos de dados transfronteiriços. O Brasil estabelecerá importantes precedentes globais, pois cria mecanismos de transferência que apoiam fluxos de dados responsáveis. As transferências internacionais de dados trazem grandes benefícios sociais e econômicos; e regras que permitem a transferência de dados com garantias adequadas de privacidade ajudarão o Brasil a perceber esses benefícios. Em uma época de crescente protecionismo de dados em todo o mundo, o Brasil deve continuar a promover fortes salvaguardas de privacidade e fluxos internacionais de dados como pilares da economia de dados. O Brasil também deve ser uma voz ativa contra as tendências de localização e outras restrições aos fluxos internacionais de dados que podem limitar o potencial de inovação do país. Este trabalho é crucial para superar os obstáculos à transferência de dados em todo o mundo. No Brasil, as empresas exigem uma série de mecanismos de transferência para apoiar os fluxos globais de dados - e esses mecanismos devem ser construídos com base em fortes salvaguardas de proteção de dados. Apoiamos os esforços da ANPD para implementar as obrigações de transferência da LGPD, assegurando que as organizações disponham de várias opções para usar na transferência internacional de dados, incluindo determinações de adequação, cláusulas contratuais padrão, além de outros mecanismos. Diferentes tipos de organizações e diferentes modelos de negócios exigem o uso de diferentes mecanismos de transferência que não são intercambiáveis. Na prática, as empresas maiores muitas vezes confiam em um ou mais mecanismos de transferência de dados, utilizando a ferramenta mais adaptada às suas necessidades comerciais e à(s) transferência(s) de dados específica(s) em mãos. Já outras empresas acabam contando com apenas um mecanismo, como o das determinações de adequação ou cláusulas contratuais padrão. A criação de uma gama de mecanismos flexíveis de transferência que podem ser utilizados de forma diferente em várias situações ajudará as empresas a transferir dados de forma responsável, de acordo com a legislação brasileira. Um passo importante que a ANPD pode dar antes da publicação de uma nova regulação é conferir segurança jurídica para as transferências internacionais de dados que já ocorrem. Como as disposições da LGPD sobre transferências internacionais de dados exigem a implementação pela ANPD, existe atualmente um grau de incerteza quanto às obrigações legais para essas transferências de dados que ainda não foram reguladas. Portanto, recomendamos que a ANPD elabore orientações confirmando que, neste interregno, as empresas podem continuar a transferir dados de forma responsável internacionalmente com base nas melhores práticas globais, tais como disposições contratuais que garantam a proteção dos dados, independentemente de onde os dados sejam transferidos, e principalmente quando essas práticas forem convergentes com os objetivos gerais da LGPD. Sob o cenário atual - com poucas opções disponíveis - as organizações enfrentam mais desafios para operar em um ambiente internacional competitivo. Desenvolver regulamentações que operacionalizem os mecanismos de transferência de dados sob a LGPD é, portanto, fundamental para estabelecer segurança jurídica às organizações que fazem negócios no Brasil. [1]A Global Data Alliance é uma coalizão intersetorial de empresas que

estão comprometidas com altos padrões de responsabilidade de dados e que dependem da capacidade de transferir dados ao redor do mundo para inovar e criar empregos. Os membros da Aliança estão sediados em todo o mundo e são ativos nos setores de fabricação avançada, aeroespacial, automotivo, bens de consumo, eletrônicos, serviços financeiros, saúde, mídia e entretenimento, recursos naturais, cadeia de suprimentos e telecomunicações, entre outros. A BSA | Software Alliance administra a Global Data Alliance. Para mais informações sobre a Global Data Alliance, acesse: https://www.globaldataalliance.org/downloads/aboutgda.pdf [2]A transferência ininterrupta de dados através das fronteiras internacionais permite a implantação de tecnologias e serviços modernos e emergentes que sustentam a economia, em todos os setores e em nível local, nacional e internacional. Isto inclui tecnologias e serviços possibilitados pelas transferências de dados, tais como análise de dados relacionados à IA e tecnologias de aprendizado de máquinas, bem como computação em nuvem, blockchain e novas tecnologias que melhoram a privacidade. Essas tecnologias e serviços, que são frequentemente acessados além fronteiras ou dependem de dados transferidos além fronteiras (ou ambos), apoiam muitas atividades e prioridades econômicas importantes, incluindo trabalho remoto e colaboração virtual, educação à distância, telemedicina, segurança cibernética, monitoramento e prevenção de fraudes, antilavagem de dinheiro, investigação de produtos falsificados perigosos e uma ampla gama de outras atividades relacionadas com a proteção da saúde, privacidade, segurança e propriedade intelectual. [3] OMC, Políticas Governamentais para a Promoção da Inovação na Era Digital, 2020 World Trade Report (2020), em https://www.wto.org/english/res_e/booksp_e/wtr20_e/wtr20-0_e.pdf
","174354":"Na medida em que os países do mundo inteiro desenvolvem e atualizam suas leis e regulamentações de proteção de informações pessoais, é fundamental que essas estruturas legais sejam projetadas para proteger efetivamente a privacidade de modo internacionalmente interoperável e flexível o suficiente como resposta à rápida evolução das tecnologias e dos modelos de negócios, sempre priorizando padrões altos de proteção de dados. Isto é particularmente importante no contexto das transferências internacionais de dados, onde as exigências legais interoperáveis impactam na capacidade das organizações de cumprir com essas obrigações em todas as jurisdições. Naturalmente, o contexto e a perspectiva em torno da privacidade e da proteção de dados pessoais podem variar entre diferentes países com base nas diferenças culturais, tradições legais e outros fatores. Ao mesmo tempo, os governos devem apoiar o reconhecimento comum de normas e práticas internacionais que protejam as estruturas de privacidade interoperáveis. Se, em vez disso, os países adotarem políticas fragmentadas sobre questões centrais, isso pode acarretar uma elevação do custo dos negócios para todas as empresas e pode prejudicar a proteção de dados pessoais e a privacidade do consumidor. As empresas que prestam serviços em mais de um país devem identificar - e implementar - exigências adicionais de privacidade e proteção de dados impostas por cada país em que operam, observando como essas obrigações se relacionam às regulamentações de outros países. Leis e regulamentos que promovem a convergência em torno de abordagens internacionalmente reconhecidas para transferências de dados podem ajudar a impulsionar mecanismos interoperáveis de transferência de dados, permitindo às empresas alavancar essas abordagens comuns. Na prática, um novo mecanismo de transferência deve ser suficientemente similar - em estrutura e proteções substantivas -

para que as obrigações sob o novo mecanismo possam ser mapeadas para as obrigações sob o antigo mecanismo. Isto garante que as empresas possam entender como suas obrigações mudam em todas as jurisdições e lhes permite identificar exigências semelhantes em todas as estruturas legais. Essa abordagem cria um processo de conformidade mais eficiente e impulsiona o investimento em práticas consolidadas que podem ser alavancadas pelas empresas em mais de uma jurisdição. Há um papel importante para os formuladores de políticas na promoção de abordagens interoperáveis de transferência de dados. Recomendamos fortemente que a ANPD reconheça que os mecanismos de transferência contratual existentes podem satisfazer as obrigações da LGPD, caso contenham proteções substantivas suficientemente similares. Muitas empresas globais já adotam mecanismos de transferência baseados em contratos que protegem os dados à medida que eles são transferidos entre países e regiões. Com isso, a ANPD pode reconhecer que esses contratos existentes satisfazem a LGPD se eles contiverem proteções substantivas suficientemente similares àquelas exigidas pela legislação - sem exigir que as empresas renegociem esses contratos para adotar linguagem ou formatos específicos pré-aprovados. Por exemplo, se uma empresa adotou contratos que já incorporam as SCCs da UE, esse contrato pode conter obrigações suficientes de proteção de dados para satisfazer as exigências de transferência sob a LGPD. Encorajamos fortemente a ANPD a reconhecer que estes mecanismos contratuais existentes podem satisfazer as exigências substantivas da LGPD e evitar a exigência de que as empresas adotem um novo formulário ou modelo para estas mesmas proteções. Esta abordagem, ao reconhecer o alinhamento entre estes mecanismos existentes e as exigências da LGPD, conduz à harmonização e assegura que as empresas possam alavancar as práticas e mecanismos de conformidade existentes em apoio a produtos, serviços e clientes no Brasil (*4). Além disso, a participação em sistemas de certificação internacional também pode contribuir para o avanço da convergência e da interoperabilidade. É primordial que a ANPD trabalhe para harmonizar os conflitos jurisdicionais potenciais que possam emergir, evitando que estas questões sejam tratadas por organizações individuais *4: Uma das principais questões a serem abordadas em futuros esforços regulatórios deve ser a de procurar assegurar a interoperabilidade entre as regulamentações brasileiras e as da UE, dos EUA e de outras jurisdições. Como o Brasil considera a possibilidade de novas exigências regulatórias, encorajamos o estabelecimento de períodos de carência razoáveis e o devido respeito à previsibilidade comercial e à segurança jurídica.","174356":"Como empresas globais, os membros da GDA adotaram uma série de mecanismos contratuais para apoiar transferências responsáveis de dados em todo o mundo. Os mecanismos contratuais são particularmente importantes para as empresas porque podem apoiar transferências para países que não possuam uma determinação de adequação e porque podem ser implementados sem buscar aprovação prévia de um regulador, ao contrário das regras corporativas obrigatórias. Portanto, apreciamos a regulamentação prioritária da ANPD que apoia os mecanismos de transferência baseados em contratos. Os membros da GDA adotaram mecanismos de transferência contratual, incluindo: • Cláusulas Contratuais Padrão da União Europeia (EU SCCs); • Acordos internacionais de transferência de dados do Reino Unido (UK IDTAs); e • Regras de Privacidade trans fronteiriças da APEC e as Regras de Privacidade da APEC para Processadores (APEC CBPRs e APEC PRPs) Mecanismos extracontratuais.

Embora a consulta atual se concentre nos mecanismos de transferência contratual, também saudamos o reconhecimento pela LGPD das avaliações e certificações de adequação, que reconhecem os mecanismos de transferência duráveis. • Adequação. As determinações de adequação são particularmente importantes para as pequenas e médias empresas que podem não dispor de recursos para adotar mecanismos contratuais padronizados. Ao fazer determinações de adequação, a ANPD pode contribuir para a convergência global ao reconhecer que outros países possuem níveis similares de proteção de dados. No futuro, encorajamos a ANPD a estabelecer um rol países prioritários para decisões de adequação com base tanto na relevância para a indústria quanto no compromisso de um país com valores de proteção de dados. • Certificações. Em nossa opinião, os esquemas de certificação podem contribuir para um sistema globalmente interoperável e voltado para o mercado que apoie as transferências de dados. A GDA reconhece que os esquemas de certificação voluntária podem fornecer às empresas mecanismos flexíveis para a transferência de dados. Também queremos enfatizar que os esquemas de certificação são mais úteis para organizações se forem reconhecidos e adotados por mais de uma jurisdição - e, portanto, podem permitir que as empresas que utilizam um único esquema de certificação cumpram com as obrigações em múltiplas jurisdições. Encorajamos a ANPD a priorizar estes benefícios práticos ao considerar ainda mais os esquemas de certificação.
","174359":"Elogiamos a ANPD por reconhecer os benefícios das transferências internacionais de dados. Também apoiamos o desenvolvimento mecanismos que favoreçam o fluxo responsável de dados através das fronteiras. A capacidade de transferir dados através de fronteiras internacionais é fundamental para empresas de todos os tamanhos e em todos os setores da indústria. Qualquer empresa com funcionários, fornecedores ou escritórios em mais de um país precisa enviar dados internacionalmente todos os dias, inclusive para: • Contribuir para as atividades de inovação, pesquisa e desenvolvimento (P&D) e melhoria de produtos oferecidos em múltiplas jurisdições, e garantir a consistência e eficiência operacional (por exemplo, em recursos humanos); • Monitorar a confiabilidade e segurança dos produtos para consumidores ou usuários; •Assegurar a conformidade legal e regulatória; • Apoiar a resiliência e a visibilidade da cadeia de fornecimento; • Manter visibilidade e capacidade de resposta rápida frente às ameaças cibernéticas de segurança em diferentes países (*5). Para as empresas, a transferência de dados através das fronteiras as ajuda a serem mais eficientes e efetivas na entrega dos produtos e serviços que seus clientes exigem. As transferências de dados também sustentam produtos e serviços globais que suportam teletrabalho, colaboração virtual, treinamento on-line e educação on-line, entre muitos outros. Ter acesso a estas ferramentas globais é particularmente importante para as pequenas e médias empresas, que frequentemente as utilizam para alcançar novos mercados e atender novos clientes (*6) . As transferências transfronteiriças também são parte integrante das cadeias de fornecimento internacionais, que devem mover as informações através das fronteiras para otimizar o fornecimento, finanças, logística, mitigação de riscos e capacidade de resposta (*7). O processo da cadeia de fornecimento para a maioria dos produtos e serviços envolve muitas fases, partes e países - bem como potenciais rupturas com base no clima, disponibilidade de material, escassez, ameaças geopolíticas ou crises de saúde emergentes (*8). No início de 2020, 94% das empresas da Fortune 1000 relataram rupturas na

cadeia de abastecimento da COVID-19 (*9), destacando ainda mais a natureza complexa e integrada das cadeias de abastecimento e o papel das transferências de dados na mitigação de riscos e na resposta. As transferências de dados não são importantes apenas para as empresas individualmente - elas também sustentam a economia global de hoje. Estima-se que as transferências de dados contribuam com US$2,8 trilhões para o PIB global, uma parcela que excede o comércio global de mercadorias e que deverá crescer para US$11 trilhões até 2025 (*10). As interrupções nos fluxos de dados transfronteiriços têm amplas reverberações que podem levar à redução dos ganhos potenciais do PIB, à redução dos investimentos nos mercados locais, à perda de empregos e consequente perda de bem-estar e ao impacto adverso nos ecossistemas digitais locais e nacionais - em um momento em que a recuperação econômica está no topo da agenda de cada governo. Cabe destacar que o apoio ao fluxo internacional de dados também pode ajudar a desenvolver uma economia digital vibrante e próspera no Brasil. Para alavancar os benefícios que são trazidos pelo fluxo responsável de dados através das fronteiras, recomendamos que a ANPD promova a convergência e interoperabilidade dos mecanismos de transferência de dados, conforme abordado em nossas respostas às Perguntas 2 e 3. *5: No setor de saúde especificamente, outra prioridade importante é facilitar a transferência de dados usados em ensaios clínicos, avaliações de segurança de produtos, fornecimento de suporte técnico a pacientes ou provedores de saúde e monitoramento de aplicações relevantes. *6: USAID Digital Strategy, 2020-2024, https://www.usaid.gov/usaid-digital-strategy, p. 37 ("Ecossistemas digitais têm o potencial de equipar comerciantes informais, mulheres empreendedoras, pequenos agricultores e MPMEs envolvidas no comércio internacional com acesso a mercados, informações e finanças"). *7: Global Data Alliance, Transferências transfronteiriças de Dados & Gerenciamento de cadeia de suprimentos em, https://www.globaldataalliance.org/downloads/03182021gdaprimersupplychain.pdf *8: De acordo com o Relatório Global sobre Catástrofes Climáticas de 2016, a indústria da cadeia de abastecimento enfrenta anualmente uma média de 260 grandes desastres naturais *9: Erik Sherman, “94% das empresas da Fortune 1000 estão enfrentando rupturas na cadeia de suprimentos por conta do coronavírus: relatório,” Forbes, 21 de devereiro de 2020. Disponível em: https://fortune.com/2020/02/21/fortune-1000-coronavirus-china-supply-chain-impact *10: OCDE, Medindo o Valor Econômico e dos Fluxos de Dados Transfronteiriços, 297 OECD Digital Economy Papers 24 (agosto de 2020).","174360":"","174361":"Queremos enfatizar que as determinações de adequação e os instrumentos contratuais são dois mecanismos separados que suportam as transferências internacionais de dados. É importante observar que não há hierarquia para o uso de cada mecanismo previsto no artigo 33 da LGPD, incluindo instrumentos contratuais e adequação. As partes podem escolher um mecanismo que seja adequado para suas transferências. Encorajamos a ANPD a não aplicar os requisitos de um destes mecanismos ao outro mecanismo. Por exemplo, as empresas que adotam compromissos contratuais para transferência de dados não devem ser obrigadas a avaliar o nível de proteção de dados do país estrangeiro para o qual os dados devem ser transferidos. Isso porque os próprios acordos contratuais aplicam proteções substantivas aos dados pessoais, independentemente de onde esses dados sejam transferidos - tornando os compromissos contratuais apropriados para

transferências a países que não receberam uma determinação de adequação. Além disso, as empresas (e especialmente as pequenas e médias empresas) não estão equipadas para realizar o tipo de avaliação detalhada e holística das leis e práticas regulatórias de um país estrangeiro. Exigir tal avaliação cria incerteza, pois as empresas têm dificuldades com essa tarefa. Ademais, tal exigência trará poucos benefícios para os consumidores. ","174362":"Encorajamos fortemente a ANPD a priorizar uma abordagem flexível sobre os mecanismos de transferência contratual. Como observado em nossa resposta à pergunta 2, recomendamos que a ANPD reconheça que os mecanismos de transferência contratual existentes satisfazem as obrigações substantivas da LGPD se eles possuírem proteções substantivas suficientemente similares. Esta abordagem especificaria os resultados desejados - ou seja, proteger os dados de acordo com as exigências da LGPD - em vez de se concentrar em exigências rígidas para adotar um determinado formato ou uma linguagem específica pré-aprovada. Uma abordagem flexível é particularmente importante para assegurar que as empresas adotem as obrigações substantivas apropriadas. Muitas empresas já celebraram contratos que refletem obrigações legais existentes sob outras jurisdições - e esses compromissos também podem satisfazer as obrigações sob a LGPD. As empresas devem ser capazes de confiar nessas disposições específicas, desde que elas criem proteções substantivas suficientemente similares àquelas exigidas pela LGPD e não conflitem com nenhuma das exigências da LGPD (*11). *11: Também observamos que, como a transferência de dados pode envolver um grupo de empresas em um país, de um lado, e outro grupo de empresas em outro país, de outro, pode valer a pena avaliar a possibilidade de SCCs que permitam às holdings e aos acionistas controladores vincular suas respectivas afiliadas nacionais. ","174363":"Encorajamos a ANPD a priorizar a flexibilidade nos mecanismos de transferência contratual. Como explicado em nossas respostas às Perguntas 2 e 7, o formato apropriado para cláusulas contratuais padrão deve ser suficientemente flexível para reconhecer os acordos existentes que já cumprem as obrigações substantivas da LGPD Além disso, outra abordagem interoperável que a ANPD poderia considerar para alavancar os mecanismos contratuais existentes é criar um modelo de adendo que pode ser adicionado a outros mecanismos contratuais, tais como um adendo às SCCs da UE. O UK Information Commissioner's Office (UK ICO) adotou recentemente esta abordagem em dois novos conjuntos de cláusulas contratuais modelo que entraram em vigor este ano (*12). Primeiro, a ICO do Reino Unido adotou um conjunto autônomo de 36 páginas de termos contratuais que as empresas poderiam adotar para apoiar as transferências de dados do Reino Unido (*13). Em segundo lugar, a ICO do Reino Unido adotou um adendo separado de nove páginas, que as empresas podem acrescentar aos contratos existentes que incorporam as SCCs da UE; isto permite que as empresas adotem a linguagem adicional no adendo para apoiar as transferências de dados do Reino Unido (*14). A adoção tanto de um conjunto autônomo de SCCs quanto de um adendo cria opções flexíveis para empresas que transferem dados do Reino Unido, inclusive para empresas menores (que podem não ter outros mecanismos contratuais em vigor e, portanto, não fazer uso do adendo) e maiores (que podem já ter mecanismos contratuais existentes que são prontamente modificados pelo adendo). A criação de adendos - que reconhecem as proteções substantivas no mecanismo de transferência contratual subjacente e adotam um conjunto de proteções adicionais destinadas a satisfazer as

exigências de uma segunda jurisdição - é outra abordagem interoperável para transferências de dados, concebida para funcionar em todas as jurisdições (*15). Incentivamos a ANPD a considerar ainda mais este modelo, que pode ajudar a garantir que os mecanismos contratuais adotados por diferentes jurisdições possam trabalhar juntos na prática para promover altos padrões de proteção de dados. *12: Ver UK ICO, Acordo Internacional de Transferência de Dados e Orientação, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. *13: Ver UK ICO, Acordo Internacional de Transferência de Dados e Orientação, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. *14: Ver UK ICO, Acordo Internacional de Transferência de Dados e Orientação, https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. *15: Recomendamos garantir que as empresas possam aderir a um modelo de adendo. Assim, as partes poderiam prever que seus acordos contratuais incorporem o modelo de adendo por referência, observando que o acordo pode prever termos mais específicos sobre determinadas questões.","174364":"Se a ANPD adotar novas SCCs brasileiras, nós a encorajamos a considerar a gama de diferentes entidades que transferem dados e a gama de diferentes transferências realizadas entre essas entidades. Qualquer novo mecanismo contratual deve suportar transferências entre dois controladores, de um controlador para um processador, de um processador para um controlador, ou entre processadores (*16) . As transferências de dados ocorrem sob muitas formas e, portanto, é crucial que os mecanismos contratuais de transferência possam ser usados em toda a gama de cenários de transferência. Por exemplo, a UE atualizou recentemente seus SCCs para adotar uma abordagem modular que as organizações podem empregar nestes diferentes tipos de transferências. Quer a ANPD adote ou não uma abordagem modular, qualquer nova SCC no Brasil deve ser suficientemente flexível para ser usada em cada um destes cenários. *16: Também notamos que em relações complexas entre empresas, uma determinada entidade pode ter diferentes papéis em diferentes contextos, com respeito a diferentes conjuntos de informações e em diferentes momentos, inclusive como controlador, processador, importador e/ou exportador.","174367":"","174368":"","174369":"","174371":"","174372":"Embora esta questão se refira à "verificação" de cláusulas contratuais específicas e regras corporativas vinculantes, em vez de verificação de cláusulas contratuais padrão, queremos enfatizar que o processo de utilização de arranjos contratuais não deve envolver uma pré-aprovação pela ANPD. Ao contrário, as empresas devem ser capazes de adotar compromissos contratuais que reflitam as proteções substantivas exigidas pela LGPD sem solicitar à ANPD a aprovação prévia de cada conjunto de termos contratuais. Isto assegura que as empresas possam adotar mecanismos de transferência contratual prontamente, sem criar uma enchente de pedidos de aprovação que requeiram atenção por parte da ANPD e retardam a adoção de mecanismos para salvaguardar os dados transferidos. Evitar tal sistema de aprovações prévias será importante para garantir que a carga de trabalho da ANPD permaneça gerenciável e que as empresas sejam capazes de concentrar seus esforços e recursos em garantir padrões robustos de responsabilidade e conformidade de dados. Em vez disso, a ANPD deve estabelecer

requisitos específicos para as cláusulas contratuais e declarar que qualquer contrato que atenda a esses requisitos satisfaz as obrigações da LGPD que regem as transferências de dados. Quanto à aprovação de regras corporativas obrigatórias (BCRs), a ANPD poderia considerar acelerar a consideração das BCRs que já foram aprovadas por outras jurisdições cujas leis são análogas às da LGPD. ","174373":"","174375":"","174376":"Encorajamos a ANPD a promover a conformidade regulamentar, emitindo uma série de orientações para a indústria sobre como os mecanismos de transferência devem ser implementados sob a LGPD. Por exemplo, a ANPD pode criar um website com conteúdo para grupos da indústria aprenderem mais sobre os mecanismos de transferência. O website também pode ser atualizado com orientações específicas para setores definidos ou para pequenas e médias empresas. Exortamos a ANPD a trabalhar com as partes interessadas durante todo o processo de adoção de regulamentos sobre transferências internacionais de dados, e para identificar áreas onde haja amplo consenso entre as partes interessadas de que orientações regulatórias adicionais sejam úteis (*17) . Conforme as empresas constroem ativamente seus controles internos e buscam orientação da ANPD, recomendamos também que a fiscalização se concentre, pelo menos inicialmente, em casos de negligência grave ou má conduta deliberada. *17: Por exemplo, desde que os critérios de privacidade e anonimato do paciente sejam devidamente respeitados, há uma clara prestação de serviços de saúde e outros benefícios para as patentes brasileiras quando os fabricantes de dispositivos médicos têm acesso adequado aos dados gerados pelos usuários brasileiros sobre esses dispositivos.","174378":"","174379":"A consulta pergunta sobre as obrigações do importador e exportador no caso de acesso aos dados por autoridades públicas estrangeiras. No caso de acesso por um governo estrangeiro, a obrigação apropriada para um importador de dados é notificar prontamente o exportador de dados caso receba um pedido legalmente vinculante de uma autoridade pública ou tribunal no terceiro país para divulgar os dados pessoais transferidos. Ao mesmo tempo, qualquer obrigação desse tipo deve reconhecer que um importador pode ser proibido por sua lei nacional de fornecer certas informações ao exportador. Nesta circunstância, a obrigação do importador deve ser a de notificar o exportador imediatamente após a expiração de qualquer proibição, conforme permitido pela lei aplicável. Em circunstâncias onde não há proibição de notificar o exportador que um pedido foi recebido pelas autoridades públicas estrangeiras, pode haver, no entanto, restrições sobre o tipo de informação que o importador pode fornecer ao exportador quando solicitado. Portanto, recomendamos que qualquer obrigação relacionada a tal notificação evite criar uma lista rígida de itens em uma notificação, mas, em vez disso, reconheça que tal notificação deve incluir certas informações, com uma quantidade razoável de informações, na medida do possível, nos termos da legislação aplicável. Isto cria mais flexibilidade para os importadores de dados fornecerem avisos aos exportadores, mesmo que o importador possa ser proibido de fornecer tipos específicos de informações (*18). *18: Também recomendamos que os pedidos de acesso aos dados sob a LGPD sejam respondidos de modo a evitar o conflito com outras estruturas legais, incluindo restrições comerciais contra pessoas ou países que constam da lista negra. ","174380":"Encorajamos a ANPD a se concentrar no fornecimento de informações aos consumidores que incluam um contexto significativo - sem exigir que as empresas forneçam aos titulares de dados longas listas de tipos de dados ou empresas que

possam acabem não ajudando no entendimento do indivíduo sobre como seus dados são tratados. Por exemplo, recomendamos contrariamente à inclusão de qualquer exigência de fornecer aos titulares de dados as identidades de todos os terceiros aos quais os dados pessoais podem ser divulgados. O fornecimento de tais informações resultaria em uma longa lista que poderia obscurecer informações relevantes para os titulares dos dados. Além disso, fornecer tal lista pode ser extremamente difícil para as empresas (dada a quantidade de terceiros que podem ser contratados para apoiar um determinado serviço, e a necessidade de trocar entre terceiros durante a prestação desse serviço). Isto retiraria recursos de outras atividades que promovem a proteção e a privacidade dos dados. Além disso, encorajamos fortemente a ANPD a abster-se de criar requisitos rígidos ou exigir que formatos específicos sejam seguidos para o compartilhamento de informações sobre transferências de dados. Por exemplo, as empresas devem ser autorizadas a compartilhar as informações necessárias com os titulares de dados por meio de websites. Como discutido em nossa resposta à pergunta 17, a orientação para a indústria também pode ser útil na criação de ferramentas que ajudem as empresas a implementar políticas de acordo com suas obrigações. * * * Mais uma vez, agradeço o seu foco na promoção de mecanismos interoperáveis para apoiar as transferências internacionais de dados. Acolhemos com satisfação uma oportunidade de continuarmos a nos engajar com a ANPD nestas importantes questões. Por favor, dirija quaisquer perguntas ou comentários ao Sr. Antonio Eduardo Mendes da Silva, Gerente do Brasil, BSA | The Software Alliance, no endereço pitanga@bsa.org. Sinceramente, Antônio Eduardo Mendes da Silva Country Manager, Brasil BSA | The Software Alliance

Contribuinte: Emily Sayuri Arnaud Yamaguti

Número: OP-181445

Data: 21/06/2022 - 07:59

Resumo: :"The LGPD Chapter V, Article 33, outlines several mechanisms that would allow companies to transfer data internationally, including not limited to: a) when transferring to countries where the degree of protection is adequate to the LGPD; b) standard contractual clauses; and c) regularly issued seals, certificates, and codes of conduct. However, U.S. industry stakeholders have communicated that it remains unclear if their existing standard contractual clauses are compliant, if international certifications such as the Global Cross-Border Privacy Rules (CBPR) System will be recognized, and if the ANPD intends to develop new frameworks or certifications. Furthermore, companies have expressed both interest and concerns regarding if the ANPD intends to conduct adequacy-based assessments of countries' data protection laws. If the ANPD determines the United States provides an adequate level of data protection for transfers of personal data this would streamline compliance for companies, but there is also concern that adequacy assessments require considerable time and resources, meaning companies would still require clarity in the interim regarding approved data transfer mechanisms. ","174354":"The United States supports interoperable approaches to privacy regulations that provide effective and enforceable privacy protections while also being flexible to accommodate different legal regimes. On

April 21, seven members of the APEC Cross-Border Privacy Rules (CBPR) System, including the United States, announced the establishment of the Global CBPR Forum to introduce a global certification based on CBPR program requirements. The United States Government has engaged extensively with the ANPD on the CBPR certification. We encourage the ANPD to consider explicitly recognizing the CBPR System as a data transfer mechanism under LGPD Article 33, Section II. We also encourage Brazil to consider joining the Global CBPR Forum to directly contribute to developing the certification and to extend its benefits to Brazilian companies and consumers. Promotion and expansion of the CBPR System is a key part of the United States' efforts to establish interoperable frameworks to facilitate cross-border data flows. The CBPR System requirements ensure that baseline common protections travel with and are enforceable across participating jurisdictions. This helps to ensure that data is shared responsibly and securely, while also ensuring that different regulatory approaches to data protection do not create burdensome barriers to cross-border data flows that are critical to modern trade and economic cooperation. Additionally, the structure of the CBPR System enables enforcement cooperation between the participating economies' data protection authorities and/or consumer protection agencies. Overall, the CBPR System presents a mechanism for building global interoperability between different legal regimes because it focuses on results, ensures that baseline common protections travel with data, provides for flexibility in implementation, and ensures data protections are enforceable across participating economies. A multilateral data privacy certification, like CBPR System, provides many benefits, including 1) establishing consistent requirements across jurisdictions; 2) enabling enforcement cooperation; and 3) ensuring that different approaches to data protection do not create barriers to cross border data flows. This flexibility connects data privacy regimes across diverse economies. The CBPR System establishes how a multilateral framework can scale to include economies with different domestic legal regimes for data protection. ","174356":"International certifications like the CBPR System are the most effective and legitimate instruments for international data transfers and offer the most collective long-term benefits for large and small companies. The CBPR program requirements are based on core data privacy principles first reflected in the OECD Privacy Guidelines and now in data privacy regimes around the world, including Brazil. Consequently, countries that recognize the CBPR certification affirm that its program requirements align with most domestic data protection and privacy requirements. Similarly, in obtaining the CBPR certification, a company must adapt its privacy policies to meet CBPR program requirements, which then brings them into alignment with internationally-recognized privacy principles and multiple domestic laws simultaneously. Lastly, while standard contractual clauses (SCCs) are a useful tool, the need to tailor them to different markets can be burdensome, especially for small companies. This makes the CBPR certification more cost-effective and scalable for companies of any size and more scalable given the multilateral nature and common baseline requirements of the CBPR System.","174359":"Cross-border data flows are increasingly crucial to supporting digitally-enable trade, international consumer transactions, research and development, and innovation in emerging technologies such as artificial intelligence, Internet of Things, and 5G. According to a 2018 report from the Brookings Institution, cross-border data flows currently

drive 22% of global economic output and will add up to $11 trillion to global GDP by 2025. Firms across all industries depend on data flows for their operations, supply chains, business models, marketing and customer services. This includes automobile manufacturers, banks, airlines, hospitals, and grocery store chains, as well as individuals, startups, and small businesses that also now leverage cross-border data flows to access global markets and global value chains. Additionally, cross-border data flows are critical to cooperation on health and scientific research studies, cooperation in international regulatory development, and other areas outside of trade and economics. At the same time, because the international data flows often involve personally identifiable information, we must also recognize privacy and data protection as essential for individuals. International certifications such as the CBPR System offer the best instrument for balancing the needs of companies in the modern global economy and protecting consumers' privacy and ensuring responsible use of their data. A key feature of the CBPR System is the concept of accountability—companies that participate must have their privacy policies and practices verified by a third party which generates trust among consumers. The CBPR certification signals accountability to governments and consumers by requiring certified companies to obtain third party verification by a recognized Accountability Agent that verify companies are complying with internationally-recognized privacy standards. Accountability Agents continuously monitor a certified company's compliance with CBPR program requirements. They also receive and investigate complaints and resolve disputes between consumers and certified companies and can refer complaints to participating jurisdictions' enforcement bodies if complaints cannot be resolved or a company's violations continue. ","174360":"a. standard contractual clauses; Standard contractual clauses (SCCs) can be useful for companies as an instrument for complying with domestic data protection and privacy laws and regulations on international data transfers if approved by domestic enforcement bodies. However, unless these SCC can be applied across multiple jurisdictions as a compliance mechanism, companies must tailor or adapt their SCCs to each individual jurisdiction where they have business operations. This can be time-consuming and resource-intensive for any company, but for small companies in particular, the lack of a common framework for these SCCs may discourage them from operating in certain markets. Consequently, Brazil should strongly consider also recognizing international certifications like the CBPR System in addition to instruments like SCCs and Binding Corporate Rules (BCRs). Several large, multinational U.S. companies that operate in Brazil have the CBPR certification and use this as an enforceable compliance mechanism for data transfers between the participating APEC CBPR System economies – Australia, Canada, Japan, Mexico, the Philippines, Singapore, South Korea, Taiwan, and the United States. Allowing CBPR-certified companies to use the certification in Brazil would remove the administrative hurdle of requiring these companies to establish a separate compliance mechanism for data transfers in and out of Brazil, while also offering a menu of data transfer instruments to companies established in or seeking to enter the Brazilian market. b. specific contractual clauses; and In our conversations with ANPD staff they have indicated that they are looking at various other countries' instruments, like the European Commission's SCCs and New Zealand's Model Contractual Clauses, as templates for creating similar instruments tailored to Brazil's domestic context. The United States applauds this due diligence and

meticulous approach, as each country should ensure that approved data transfer instruments are enforceable under domestic law and include comprehensive data protection and privacy requirements for companies using those instruments. However, if the ANPD chooses to develop a Brazil-specific SCC, we encourage the ANPD to consider whether the requirements and privacy protections in those SCCs will be interoperable with and enforceable for all parties to the SCC under the laws and regulations of major markets like the United States and European Union. For example, the U.S. Federal Trade Commission (FTC) has noted that SCCs typically lack an effective enforcement mechanism for data importers - the controller or processor located in a third country that receives personal data from the data exporter - that sign on to SCCs. Conversely, certification like the CBPR include a two-tiered oversight and enforcement system – the third-party Accountability Agents and the regulatory agency – that can monitor if all parties covered under a company's CBPR certification are complying with CBPR requirements, and enforce violations. Additionally, if the ANPD develops a Brazil-specific SCC, they should provide clear guidelines from the outset regarding if companies that are already CBPR-certified or compliant with the EU SCCs will still need to certify to the Brazilian SCC to transfer data internationally. Companies benefit from clear and comprehensible requirements regarding data transfers to different jurisdictions and any data transfer instruments, including a specific SCC, should enable rather than hinder data transfers. c. binding corporate rules. Multiple U.S. companies that utilize BCRs have emphasized that this instrument is widely recognized by countries globally and is legally sound. However, these companies have also noted that the BCRs are not scalable in that, similar to SCCs, they must be approved by each individual country and sometimes must be modified to comply with different domestic laws. Furthermore, multiple large U.S. companies utilize both BCRs and the CBPR certification, noting that the CBPR System provides them with more flexibility as an instrument with common program requirements recognized across multiple jurisdictions, especially as that company scales and enters new markets that recognize or are considering recognizing the certification. For example, if a new jurisdiction chooses to legally recognize the CBPR certification and participate in the Global CBPR Forum, companies that are already CBPR-certified could instantly apply the certification as an instrument for compliance in that jurisdiction, whereas if they only used BCRs, they likely would first need to submit the BCR for review and approval from the domestic regulator. ","174361":"Rather than adopt an "adequacy determination" model, the United States recommends that the ANPD consider a more flexible approach that protects consumer data while supporting the free flow of information. We emphasize that the European Union (EU) has taken an adequacy-based approach toward regulating the transfer of data to other jurisdictions, but the EU has still only issued 15 adequacy decisions across 14 countries over 24 years, first under the EU Directive and later under the General Data Protection Regulation (GDPR). This demonstrates the considerable time and human resources required for regulators to conduct country-by-country adequacy assessments. Additionally, although numerous countries include the concept of adequacy assessments in their data protection and privacy laws, not all of them utilize the same process and, in some cases, have not actually implemented those provisions. Therefore, we recommend focusing on ensuring that individual companies uphold privacy standards,

regardless of where such data is transferred. Given the great degree of variation among countries' legal frameworks, we invite Brazil to look beyond individual laws and consider the interrelated set of practices, enforcement authorities, and voluntary and enforceable mechanisms that combine to form a privacy protection regime. ","174362":"As opposed to advocating for a specific type of SCC, the United States instead encourages countries to prioritize recognizing data transfer mechanisms that are interoperable with various privacy regulations, provide effective and enforceable data privacy protections, and are flexible to accommodate different legal regimes. We encourage the ANPD, as it considers various instruments to enable companies to transfer data internationally, including SCCs, to prioritize recognizing a broad array of mechanisms under the law for how individual companies can adequately protect personal information, including internationally-recognized privacy certifications and codes of conduct that are consistent and enforceable across jurisdictions. Given that companies vary in size, geographic scope, and financial and operational resources, a data transfer mechanism that works well for a large, multinational company may prove infeasible for a startup with fewer in-country resources. A broad toolkit of data transfer options ensures a flexible approach that will advance data protection and facilitate data transfers. ","174363":" As stated above, the United States does not have a preferred format for instruments like SCCs and instead advocates for data transfer instruments that are interoperable, flexible in implementation, and legally-enforceable across jurisdictions. The CBPR certification serves as a good example of this type of data transfer instrument, in that it is a government-recognized, multilateral, and legally-enforceable system of mutually recognized data privacy best practices and standards and focuses on commercial data processing. We would encourage the ANPD to review the current CBPR program requirements at: https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-ProgramRequirements.pdf The 50 CBPR program requirements cover eight (8) internationally-recognized privacy principles and include a series of assessment criteria and questions for companies to demonstrate how they adhere to these principles. We should note that current CBPR members are interested in reviewing current program requirements and considering updates, particularly as we engage with new jurisdictions about future membership in the Global CBPR Forum. With the upcoming establishment of a Global CBPR System, we have an opportunity to review the program requirements to see how they can be updated to reflect new developments. It is important to emphasize, however, that any program requirements must be enforceable for all Global CBPR Forum members. This is an important foundation of the CBPR certification – that it means the same thing when issued to a company in any participating jurisdiction. The CBPR System was developed with multistakeholder input, and we intend to continue to work with all stakeholders as we undertake this review.
","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373":"In the CBPR program requirements, under the Uses of Personal Information section, the certifying Accountability Agent must verify that, if the company is transferring personal information to other personal information controllers or transferred to processors, such disclosures and/or transfers are undertaken to fulfill the original stated purpose of collection or another compatible or related purpose, unless based upon the express consent of the

individual necessary to provide a service or product requested by the individual, or compelled by law. Also, the company must identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose (e.g. order fulfillment etc.). Lastly, the Accountability Agent must verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes. For companies that have the CBPR certification, they are also required to promptly notify their certifying Accountability Agent, and in some cases the data subject, if material changes are made to their privacy policies and if they modify the originally stated purpose for transferring personal data. For example, the CBPR program requirements obligate all Participants (companies certified by that Accountability Agent) to attest on an annual basis to the continuing adherence of the CBPR program requirements. Additionally, the Accountability Agent conducts regular comprehensive reviews to ensure the integrity of the re-certification process. In cases where the certified company has made material changes to its privacy policy, an immediate review process will be carried out. This re-certification review process includes: a) an assessment of compliance, which will include verification of the contents of the self-assessment forms updated by the company, and which may also include in-person or phone interviews, inspection of the personal data system, Web site scans, or automated security tools; b) A report to the Participant outlining the Accountability Agent's findings regarding the Participant's level of compliance with the program requirements. The report must also list any corrections the Participant needs to make to correct areas of non-compliance and the timeframe within which the corrections must be completed for purposes of obtaining re-certification; c) Verification that required changes have been properly completed by Participant; d) Notice to the Participant that the Participant is in compliance with the Accountability Agent's program requirements and has been re-certified. Additionally, Accountability Agents must have comprehensive written procedures designed to ensure the integrity of the certification process and to monitor certified companies throughout the certification period to ensure compliance with CBPR program requirements. Where there are reasonable grounds for the Accountability Agent to believe that a Participant has engaged in a practice that may constitute a breach of the program requirements, an immediate review process will be triggered whereby verification of compliance will be carried out. Where non-compliance with any of the program requirements is found, the Accountability Agent will notify the certified company outlining the corrections the company needs to make and a reasonable timeframe within which the corrections must be completed. The Accountability Agent must verify that the required changes have been properly completed by the Participant within the stated timeframe. ","174375":"Under the CBPR certification system, Accountability Agents are responsible for receiving and investigating complaints from data subjects and resolving disputes between consumers and certified companies. If disputes cannot be resolved or a certified company's violations of CBPR program requirements or national laws continue, the Accountability Agent can refer complaints to participating economies' enforcement bodies. where there are reasonable grounds for the Accountability Agent to believe that a certified company has engaged in a practice that may constitute a breach of the program requirements, an immediate review

process will be triggered whereby verification of compliance will be carried out. Furthermore, CBPR participating countries are required to designate an independent data protection authority from their respective governments to participate in the CBPR Cross-Border Privacy Enforcement Arrangement (CPEA). For the United States this enforcement body is the Federal Trade Commission. The CPEA creates a framework for regional cooperation in the enforcement of privacy laws and the CBPR certification across jurisdictions. The CPEA facilitates information sharing among data protection authorities in CBPR participating countries and for purposes of consumer privacy investigations and other enforcement matters. ","174376":"","174378":"As noted previously, the U.S. FTC has explained that SCCs often lack strong enforcement mechanisms to ensure compliance from the data importers in a third country. In the CBPR certification system, the program requirements obligate the certifying Accountability Agent to verify that the company notifies individuals that their personal information will or may be made available to third parties, identifies the categories or specific third parties, and explains the purpose for which the personal information will or may be made available. Additionally, the Accountability Agent must verify that, if the company discloses personal information to other personal information controllers or transferred to processors, such disclosures and/or transfers are undertaken to fulfill the original purpose of collection or another compatible or related purpose, unless based upon the express consent of the individual necessary to provide a service or product requested by the individual or compelled by law. The Accountability Agent will require the company to identify: 1) each type of data disclosed or transferred; 2) the corresponding stated purpose of collection for each type of disclosed data; and 3) the manner in which the disclosure fulfills the identified purpose. The Accountability Agent must then verify that the Applicant's disclosures or transfers of all personal information is limited to the purpose(s) of collection, or compatible or related purposes.","174379":"","174380":"The CBPR certification offers a model for providing data subjects with clear and relevant information regarding how a company intends to use their data, including the purposes of any transfers of their information to another country or jurisdiction. The CBPR provides maximum transparency by making public all companies that have the certification, which Accountability Agent certified them, and all program requirements for which the certified companies must comply. The CBPR System also provides a mechanism for regulators to empower independent third parties - Accountability Agents – to certify and monitor companies' compliance with CBPR program requirements, but only after those Accountability Agents have also demonstrated their transparency, independence and proactive procedures to data protection authorities in CBPR participating countries. Lastly, CBPR-certified companies and Accountability Agents must be re-certified on a regular basis, ensuring ongoing transparency into companies' privacy policies and maximum accountability for companies and Accountability Agents.

Contribuinte: Sam Schofield

Número: OP-181906

Data: 23/06/2022 - 15:12

Resumo: :"TOZZINIFREIRE ADVOGADOS: Entende-se que os obstáculos enfrentados por empresas para realização de transferência internacional de dados pessoais para fora do Brasil são a ausência de regulamentação específica sobre o tema e a incerteza sobre a adequação desta operação de tratamento de acordo com a LGPD e outras legislações aplicáveis. Os mesmos obstáculos se aplicam a transferências internacionais realizadas de outros países para o Brasil. Isto porque muitas autoridades consideram que o nível de adequação do Brasil não é equivalente ao nível dos países exportadores, especialmente quando estes estão localizados na União Europeia e quando o Regulamento Europeu de Proteção de Dados (GDPR) é aplicável. Por este motivo, cláusulas padrão da União Europeia são frequentemente impostas de maneira automática a todas as transferências de dados destinadas ao Brasil, de tal maneira que a discussão sobre a necessidade de aplicação de todas as obrigações ali previstas resta impossibilitada por conta da rigidez de tais cláusulas. Assim, a falta de regulamentação específica sobre transferência internacional de dados pessoais corrobora para a incerteza sobre a conformidade desta transferência com as legislações de proteção de dados aplicáveis, bem como para a aplicação automática de instrumentos contratuais de outros países sem que haja qualquer discussão ou análise sobre a viabilidade de sua aplicação ao caso concreto e específico. ","174354":"TOZZINIFREIRE ADVOGADOS: Entende-se que a maneira ideal de promover a convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições é a adoção de decisões de adequação, as quais avaliam o nível de adequação de países para quais dados pessoais possam ser exportados. Não obstante, dada a ausência de um procedimento estruturado sobre de decisões de adequação, instrumentos contratuais devem ser considerados neste primeiro momento de regulação das transferências internacionais. Decisões de adequação são atualmente adotadas pela União Europeia e, se aprovadas, permitem que transferências internacionais sejam realizadas sem necessidade de implementação de outras medidas ou garantias para garantir a conformidade da operação de tratamento. Assim, a ANPD poderia implementar o sistema de decisões de adequação a fim de garantir a conformidade das transferências internacionais com a LGPD e, se necessário, estabelecer a implementação de garantias especificas para aqueles países que possuem grau de adequação inferior ao do Brasil. Todavia, frente à ausência de decisões de adequações e de um procedimento estruturado no Brasil sobre tais decisões, instrumentos contratuais como cláusulas contratuais padrão, cláusulas específicas e normas corporativas globais são as alternativas mais adequadas e viáveis neste momento. Assim, a adoção de cláusulas e normas principiológicas e flexíveis seria positiva nesta primeira fase da regulação sobre transferência internacional até que o procedimento de decisões de adequações seja constituído. Ressalta-se que a opção por cláusulas e normas mais genéricas visa conciliar a aplicação de diferentes leis de proteção de dados que possam ser aplicáveis a uma mesma transferência internacional e evitar possíveis conflitos decorrentes desta dupla incidência. ","174356":"TOZZINIFREIRE ADVOGADOS: Atualmente, os principais instrumentos utilizados pelas autoridades de proteção de dados são cláusulas contratuais padrão e normas corporativas globais, as quais são avaliadas e aprovadas pelas próprias autoridades. Tais instrumentos possuem requisitos básicos que garantem contratualmente a conformidade da transferência os normas de proteção de dados

aplicáveis. Por outro lado, decisões sobre a conformidade de países a leis de proteção de dados aplicáveis também são utilizadas para avaliar se os dados objeto da transferência serão enviados a países com nível igual ou inferior ao país do exportador de dados e se serão necessárias adoção de medidas específicas. A Autoridade de Proteção de Dados da França, por exemplo, disponibilizou em seu site um mapa com o nível de adequação dos países, conforme link. Neste mapa, são indicados, além do nível de adequação, a existência de autoridade de proteção de dados e a necessidade de adoção de garantias específicas para a transferência de dados para tais países. Enquanto isso, a Autoridade de Proteção de Dados do Reino Unido oferece um contrato padrão de transferência internacional de dados aplicável a transferência de dados para fora do Reino Unido, conforme link.
","174359":"TOZZINIFREIRE ADVOGADOS: No âmbito de operações de transferências internacionais, os principais benefícios de sua regulamentação são a possibilidade de interoperabilidade entre os agentes de tratamento espalhados pelo mundo e a garantia de que essa interoperabilidade se dará de acordo com à LGPD e a outras legislações aplicáveis. Assim, a ausência de uma regulamentação específica sobre a realização de transferências internacionais no Brasil leva à incerteza da observância da LGPD e do cumprimento de obrigações essenciais por partes dos agentes de tratamento. Como alternativas para o endereçamento do tema de transferência internacional de dados, vale ressaltar que os instrumentos previstos na LGPD (também refletidos na prática internacional como disposto, dentre outros, no GDPR) já contam com relevantes estratégias para essa discussão ao contarem com benefícios tais como: a. Cláusulas padrão contratuais – Na hipótese de elaboração de cláusulas padrão contratuais, o ônus da ANPD em fiscalizar as operações de transferência internacional é mitigado à medida em que este conjunto de disposições já será apto a refletir as melhores práticas definidas pela Autoridade sobre o tema no âmbito dos acordos de fluxo transfronteiriço dos dados. De todo modo, considerando que este modelo preza por uma padronização mais rígida, vale ressaltar que sua implementação pelos agentes de tratamento pode não ser capaz de contemplar as especificidades da operação de cada grupo de agentes envolvidos na transferência internacional. b. Cláusulas contratuais específicas – Normas contratuais específicas proporcionam a adaptação das obrigações dos agentes de tratamento sobre os casos de transferência internacional específicos que demandam regras particulares a serem acordadas entre as partes pela natureza dos dados pessoais a serem transferidos, pela categoria de titulares envolvidos ou pela relação entre os agentes de tratamento propriamente. Neste sentido, entende-se que as partes podem utilizar cláusulas especiais para melhor adequar suas obrigações à realidade prática, de modo a observar tanto a aplicação da LGPD quanto de outras leis de proteção de dados que possam incidir. c. Normas corporativas globais – Se apresenta no contexto regulatório como mecanismo apto a reduzir os riscos de incerteza jurídica sobre a operacionalização legítima de transferências internacionais de dados ao envolver com uma padronização e assertividade no tema para as empresas de um Grupo Econômico, já podendo inclusive contar com o aval da Autoridade para a implementação deste regime no Grupo. Com a definição destas normas, o fluxo internacional de dados fica facilitado sem a necessidade de revisão constante do status de conformidade das operações em questão no curso das atividades de transferência internacional de dados pessoais (salvo na hipótese de alteração substancial destas normas).

","174360":"TOZZINIFREIRE ADVOGADOS: a. Cláusulas-padrão contratuais Para regulamentação de cláusulas contratuais padrão, entende-se que devem ser estabelecidos parâmetros mínimos, principalmente, os quais devem estar contidos em todos os contratos que se relacionem com transferência internacional de dados pessoais. A ANPD deverá elaborar cláusulas que versem sobre aspectos mais gerais, contendo a parte principiológica, propósitos do tratamento e breve descrição da transferência, contendo a definição de quem será operador e controlador. b. Cláusulas contratuais específicas Para regulamentação de cláusulas contratuais específicas, entende-se que devem ser estabelecidos os limites sobre a liberdade das partes em estipular livremente sobre a transferência internacional a ser realizada. As partes não devem se eximir de suas responsabilidades básicas de agentes de tratamento dispostas na LGPD, por exemplo, manutenção de registros de atividades de tratamento, atendimento de solicitações de titulares e comunicação de incidentes de segurança ocorridos no âmbito da transferência internacional. Isto porque, embora as cláusulas contratuais específicas possam se adequar melhor às situações concretas, as mesmas não devem ser responsáveis por excluir responsabilidades fundamentais de agentes de tratamento, cuja não observância pode afetar negativamente os direitos de titulares de dados. c. Normas corporativas globais Para a regulamentação de normas corporativas globais, entende-se que devem ser estabelecidos limites para a determinação de utilização dos dados para fins legítimos, de acordo com a LGPD, alinhados com o melhor interesse do titular e de forma correlata à finalidade que justificou o tratamento original, pelas partes envolvidas. Por outro lado, caso a empresa do grupo receptora esteja localizada em países com legislação de proteção de dados tanto ou mais protetiva que a LGPD, entende-se ser possível abrandar as normas corporativas, tendo em vista o grau de adequação imposto pelas demais legislações aplicáveis. ","174361":"TOZZINIFREIRE ADVOGADOS: Considerando que se pleiteia aqui maior flexibilidade com relação às cláusulas, o nível de proteção de dados de países ou organismos estrangeiros devem ser considerados para fins de estabelecimento do nível de proteção a ser implementado nos instrumentos contratuais. Isso significa dizer que a ANPD deverá criar níveis de classificação para os países ou organismos estrangeiros avaliados, por exemplo, em uma escala de 0 a 10 em termos de proteção oferecida. Assim, após a classificação das entidades, a ANPD deverá criar uma escala correspondente para as cláusulas, por exemplo, cláusulas a serem aplicadas para países de níveis 4 seriam diferentes e/ou mais robustas do que cláusulas para países de níveis 9.","174362":"TOZZINIFREIRE ADVOGADOS: Entende-se que, por conta do caráter distinto das atividades envolvendo dados pessoais que envolvem transferências internacionais, o ideal seria a permissão de determinada flexibilidade em relação ao texto das cláusulas. Dessa maneira, as alterações poderiam ser realizadas com a inclusão de cláusulas mais ou menos robustas sobre determinado aspecto, a depender da natureza do tratamento. Um exemplo disso é a transferência internacional realizada para fins de armazenamento de dados em servidores localizados fora do país. Este tratamento deve ser considerado distinto de uma atividade de transferência de dados a uma empresa não responsável pelo armazenamento de informações fora do país, por exemplo. Assim como a transferência internacional de dados para a matriz de uma empresa transnacional deve ser tratada de outra forma. É importante a diferenciação entre as cláusulas, para garantir flexibilidade, a depender do caso específico. Além disso, há

grande dificuldade em realizar a negociação de cláusulas-padrão contratuais com empresas transnacionais que utilizam as Standard Contractual Clauses, que são protetivas e deverão ter redação semelhante à proposta no Brasil. Por isso, entende-se que não haveria necessidade de impor cláusulas inflexíveis que muito provavelmente não serão aceitas pela rigidez das grandes companhias. ","174363":"TOZZINIFREIRE ADVOGADOS: Considerando como parâmetro as Standard Contractual Clauses, da União Europeia, seria interessante que a ANPD disponibilizasse um modelo editável, em Word, por exemplo. Isso facilitaria a inclusão das disposições nos contratos, como um anexo, da mesma forma que tem sido feito com as Standard Contractual Clauses. Ademais, seria relevante que a ANPD elaborasse um documento com explicações acerca das cláusulas-padrão, da mesma forma realizada para União Europeia, no documento "The New Standard Contractual Clauses – Questions and Answers", com explicações e orientações, com relação ao papel destas cláusulas, requisitos específicos para a inclusão das cláusulas, possibilidade ou não de alteração dos textos ou de inclusão de outras disposições, entre outros aspectos relevantes.
","174364":"TOZZINIFREIRE ADVOGADOS: Considerando (i) a diferença entre as obrigações legais às quais os controladores e os operadores são sujeitos pela LGPD e (ii) a própria relação entre controlador e operador, entende-se que a adoção de regras diferenciadas a depender do tipo dos agentes de tratamento é positiva. No caso de um operador de dados ser o exportador no âmbito de uma transferência internacional, o primeiro agirá segundo instruções específicas do seu controlador (art. 39, LGPD). Neste sentido, sugere-se que o controlador seja responsável pela transferência internacional. Da mesma forma, caso o operador seja importador de dados, o controlador ainda restará responsável pelo tratamento e o operador, restrito às instruções do controlador. Logo, diferentes responsabilidades e obrigações podem surgir a depender do agente de tratamento que ocupa as posições de exportadores e importadores de dados. Para adoção de regras específicas, União Europeia adota a seguinte classificação: (i) MÓDULO UM: Transferência entre controladores; (ii) MÓDULO DOIS: Transferência de controlador pelo tratamento para operador; (iii) MÓDULO TRÊS: Transferência entre operadores; e (iv) MÓDULO QUATRO: Transferência de operador para controlador. Entre os temas abordados nas regras específicas implementadas estão: (i) instruções dos controladores que devem ser seguidas pelos operadores, caso estes últimos façam parte da transferência internacional; (ii) exercício de direitos por parte dos titulares de dados; e (iii) contratação de sub-operadores.
","174367":"TOZZINIFREIRE ADVOGADOS: Sim. Enquanto cláusulas-padrão contratuais devem se voltar majoritariamente ao tratamento dos dados de acordo com as disposições da LGPD, especialmente ao regime de responsabilidade, qualificação das partes envolvidas enquanto agentes de tratamento, definição de finalidade específica para o tratamento, necessidade de se ater a esta finalidade, dentre outros pontos tratados anteriormente, as Normas Corporativas Globais devem ter um caráter mais atinente aos princípios da LGPD, tendo em vista que nem sempre a transferência intragrupo terá uma finalidade específica e relacionada à finalidade que originou o tratamento dos dados em questão. Na realidade, na maioria dos casos é possível verificar que a transferência de dados intragrupo visa a gestão das atividades do grupo, análise de KPIs, valores das subsidiárias, análise das medidas comerciais adotadas e formas de melhorias nas operações. Estas situações, não raramente não

precisam envolver dados pessoais, mas podem se beneficiar de tais atividades de tratamento. ","174368":"TOZZINIFREIRE ADVOGADOS: Entendemos que os critérios devem ser os mesmos já adotados no ordenamento jurídico para a definição desses entes – a existência de duas ou mais empresas atuando de forma coordenada com objetivos comuns ou com relação de subordinação entre elas. De forma semelhante ao entendimento firmado pelo Tribunal Superior do Trabalho (TST), a simples coincidência de sócios em quadros societários/de acionistas de empresas não é razão suficiente para a caracterização de grupos econômicos. Nestas situações em que não há relação de hierarquia ou coordenação entre as empresas em questão, a utilização de cláusulas padrão seria suficiente. De qualquer maneira, entende-se que a definição de grupo econômico ou empresarial deve ser alinhada com a atual interpretação do ordenamento jurídico e jurisprudência brasileiros, inclusive para viabilizar a execução de eventuais multas aplicadas no contexto de processos administrativos sancionatórios, tendo em vista que o Art. 52 da LGPD determina que o valor da multa será de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil. ","174369":"TOZZINIFREIRE ADVOGADOS: As informações mínimas sobre os dados pessoais necessárias para análise da conformidade pela LGPD das transferências internacionais são: i. Categorias de dados pessoais objeto da transferência (dados pessoais e/ou dados pessoais sensíveis); ii. Categorias de titulares de dados cujos dados são objeto da transferência (crianças, adolescentes, adultos, idosos, empregados, consumidores, alunos, etc...); iii. Tipo de relação entre os titulares de dados, o exportador e o importador (relação consumerista, relação de emprego, etc...); iv. Finalidade específica com a qual os dados pessoais serão transferidos; v. Base legal adequada para a transferência dos dados pessoais; vi. Conhecimento do titular de dados sobre a transferência de dados pessoais e por qual meio este conhecimento se dá (aviso de privacidade, consentimento, etc...); e vii. Meios que os titulares terão para exercer seus direitos. ","174371":"TOZZINIFREIRE ADVOGADOS: Conforme indicado no item 10, é comum que a transferência de dados intragrupo esteja relacionada a atividades não necessariamente ligadas à finalidade que originou e justificou o tratamento original destas informações. Da mesma forma, isto pode ser identificado em transferência entre grupos econômicos distintos, sem ser necessário endereçar especificidades das atividades de tratamento desempenhadas pelas empresas do grupo e das especificidades da própria estrutura das empresas em questão. Por outro lado, caso os grupos envolvidos na transferência tenham suas normas corporativas globais aprovadas pela ANPD, entende-se que, em tese, tratariam os dados de acordo com as disposições da LGPD, tendo em vista os pontos que se entende que as normas corporativas globais devam cobrir. Na medida em que qualquer transferência de dados pessoais é uma atividade de tratamento de dados que precisa obedecer às disposições da LGPD e ser fundamentada em uma base legal válida, a existência de normas corporativas globais não é necessária para que isso ocorra. No entanto, as normas corporativas globais podem ser vistas como um benefício nestes casos, na medida em que existe uma expectativa de tratamento de dados pessoais de maneira segura e de acordo com as disposições da LGPD por empresas que seguem normas corporativas globais aprovadas pela ANPD. De qualquer forma, é preciso garantir que qualquer das medidas facilitadoras de transferências internacionais de dados pessoais editadas pela ANPD (sejam normas corporativas globais, cláusulas padrão

contratuais ou decisões de adequação) não sejam interpretadas como situações excessivamente permissivas para as empresas envolvidas nos tratamentos em questão, além da necessidade de tais instrumentos estabelecerem disposições para situações específicas que exigem maior grau de proteção, como o tratamento de dados sensíveis, de crianças, idosos ou outro grupo de vulneráveis. ","174372":"TOZZINIFREIRE ADVOGADOS: Com relação às cláusulas contratuais específicas, atualmente não há quaisquer experiências sobre a sua verificação e aprovação por autoridades de proteção de dados competentes. A Comissão Europeia, por sua vez, adota módulos de cláusulas a depender do agente de tratamento que ocupa as posições de exportadores e importadores de dados – (i) MÓDULO UM: Transferência entre controladores; (ii) MÓDULO DOIS: Transferência de controlador pelo tratamento para operador; (iii) MÓDULO TRÊS: Transferência entre operadores; e (iv) MÓDULO QUATRO: Transferência de operador para controlador –, mas não por temas, categorias de dados pessoais ou de titulares. Por outro lado, no tangente às normas corporativas globais, a União Europeia verifica e aprova tais normas, as quais devem ser submetidas pelas empresas perante a autoridade de proteção de dados competente. Segundo a Comissão Europeia, tais normais devem incluir todos os princípios de proteção de dados e direitos para assegurar garantias apropriadas para transferência de dados internacional. Assim, entende-se que caminho semelhante poderia ser adotado para a realidade brasileira. ","174373":"TOZZINIFREIRE ADVOGADOS: Considerando que a transferência internacional de dados pessoais também se configura enquanto uma operação de tratamento, é importante assegurar que o rol de direitos dos artigos 18 e seguintes da LGPD seja resguardado. No que diz respeito ao dever de transparência com os titulares, ressaltamos que uma eventual comunicação para os titulares (viabilizando sua potencial intervenção), será necessária tão somente caso: (I) Dados pessoais coletados com base no consentimento dos titulares venham a posteriormente ser sujeitos a uma atividade de transferência internacional, independentemente do meio que legitime esta transferência (como atualmente é feito no âmbito das Políticas de Privacidade, já seguindo a mesma racional exigida no Art. 8, §6º da LGPD); (II) A operação de transferência internacional em questão tenha sido fundamentada no consentimento do titular para legitimar sua ocorrência; ou ainda caso (III) O cenário de transferência internacional (não contemplado pelas hipóteses anteriores) sofra qualquer alteração material em algum dos elementos que configuram essa operação (ex. transferência feita para novos fins) resultando, como consequência em novos riscos para os direitos e liberdades fundamentais dos titulares (em linha com a racional prevista no Art. 49, 1, "a" do GPDR). Com relação à hipótese (III) acima, entende-se por “alteração material” qualquer mudança nos “elementos essenciais” do tratamento definidos no Art. 9 da LGPD e no Guia Orientativo Para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, quais sejam: (i) a finalidade específica do tratamento; (ii) a natureza dos dados pessoais coletados; (iii) a forma e duração do tratamento; (iv) a identificação do Controlador; e (v) as informações acerca do uso compartilhado de dados pelo controlador (com as finalidades para tanto). ","174375":"TOZZINIFREIRE ADVOGADOS: À medida em que a transferência internacional de dados for legitimada com fundamento em instrumentos contratuais (sejam cláusulas padrão ou ainda cláusulas específicas), a resolução de eventuais conflitos que venham a surgir no contexto das relações de agentes de tratamento também deve ser baseada

em instrumentos privados (como acordos bilaterais aptos a endereçar a controvérsia e as medidas necessárias para endereçá-la, por exemplo). De todo modo, reconhecemos que as Autoridades de Proteção de Dados também podem contar com papel relevante nesse processo na hipótese em que os agentes de tratamento envolvidos não obtenham resultados na eventual negociação dos acordos privados. Nesse contexto, é possível que os agentes remetam a controvérsia à consulta das autoridades envolvidas, sem que a decisão das autoridades nacionais tenha efeito vinculante sobre a matéria em questão. Além disso, entendemos que seria salutar as autoridades de países distintos firmarem acordos de cooperação entre si, estabelecendo orientações sobre o tema. Caso haja conflito entre os agentes de tratamento e seus titulares, por sua vez, as mesmas medidas já adotadas para a resolução de controvérsias referentes às operações de tratamento desenvolvidas em território nacional podem ser implementadas. ","174376":"TOZZINIFREIRE ADVOGADOS: A regulamentação de transferência internacional de dados já conta com direta conexão com o texto da LGPD, motivo pelo qual a inclusão de incentivos negativos adicionais não seria necessária para incentivar a conformidade com suas disposições (afinal, uma violação às suas disposições já se ensejaria a possibilidade de aplicação das sanções existentes). Dessa forma, com o intuito de incentivar a conformidade às garantias gerais desse regulamento, é importante que a Autoridade trabalhe com mecanismos de: (i) Padronização e simplificação do processo de transferência internacional legítima de dados pessoais (com o estabelecimento de cláusulas contratuais padrão e ainda com a definição de países tidos como seguros para o fluxo de dados pessoais); (ii) Incentivo à governança e controle interno dos próprios agentes de tratamento, estabelecendo então a possibilidade de realização de Relatório de Impacto com análise de riscos inerentes às atividades de transferência internacional (em linha com o que atualmente é previsto na LGPD no contexto de processos fundados no legítimo interesse – Art. 10, §3º); (iii) Parametrização dos requisitos mínimos de segurança da informação a serem observadas pelos agentes de tratamento no desenho de suas relações com agentes terceiros fora do território nacional (em cláusulas contratuais específicas, por exemplo). ","174378":"TOZZINIFREIRE ADVOGADOS: Com o intuito de resolver questões práticas referente à responsabilização dos atores, é importante que as previsões legais já existentes na LGPD sejam observadas como parâmetros relevantes nesse contexto, em especial no que diz respeito à avaliação sobre se a transferência internacional (seja ela uma transferência ulterior ou não) (i) resultou em uma violação à legislação de proteção de dados pessoais e se (ii) o agente de tratamento exportador em território nacional de fato deixou de adotar as medidas técnicas disponíveis para fornecer a segurança que o titular possa legitimamente esperar (ou seja, sob uma análise subjetiva de sua potencial responsabilização no cenário em análise).","174379":"TOZZINIFREIRE ADVOGADOS: Diante do interesse público que justifica a solicitação de acesso aos dados pessoais por determinação de autoridades públicas estrangeiras, é importante que a legislação brasileira não imponha ônus adicionais para o atendimento destas solicitações pelos agentes de tratamento. De todo modo, em linha com as garantias gerais previstas no ordenamento jurídico brasileiro, é importante ressaltar que compete aos agentes de tratamento uma análise prévia sobre a legitimidade da solicitação recebida a fim de assegurar que a transferência solicitada não resultará na violação de obrigações locais destes agentes de tratamento. Ainda, caberá aos agentes importadores e

exportadores assegurar que as medidas técnicas e administrativas necessárias foram adotadas para viabilizar a transferência segura dos dados pessoais solicitados. Com relação à transparência com os titulares, uma eventual notificação será necessária somente nos limites delineados no Item 15 acima, sendo necessário ainda observar um terceiro quesito, qual seja (III) assegurar que a transparência com o titular não comprometerá a finalidade que justificou a solicitação de compartilhamento de dados da autoridade pública estrangeira em questão (por exemplo, caso o compartilhamento envolva eventual investigação legítima em curso sobre o titular). ","174380":"Com o intuito de fornecer aos titulares informações claras e relevantes sobre a eventual transferência internacional de seus dados pessoais, é possível que haja um complemento aos mecanismos de transparência já adotados atualmente para esse fim nas operações em geral dos agentes de tratamento (tais como com a inclusão de disposições mais robustas a respeito da transferência transfronteiriça de dados nas Políticas de Privacidade apresentadas aos titulares, prezando ainda pelo uso de linguagem simplificada e visual nesse processo). Para assegurar a efetiva proteção de direitos dos titulares, as mesmas premissas acima se aplicam no que diz respeito à possibilidade de os agentes de tratamento aproveitarem dos mecanismos e estratégias já implementadas em suas operações para esse fim. Dessa forma, em linha com o que é feito no âmbito das diferentes Políticas Internas dos agentes (conforme previsto no Art. 50 e seguintes da LGPD), é recomendado que haja uma política específica para dispor sobre as garantias gerais que devem ser observadas pelos colaboradores envolvidos nas atividades de transferência internacional de dados. Este documento passa a ter relevante papel de governança na operação dos agentes de tratamento, visando então resguardar os titulares contexto de transferências transfronteiriças de dados a partir de diferentes estratégias internas de gestão destas atividades (como atualmente é feito em políticas internas de resposta a solicitações de titulares ou de resposta a incidentes de segurança, por exemplo).

Contribuinte: João vitor de Almeida Ramos

Número: OP-182497

Data: 27/06/2022 - 08:19

Resumo:
:"","174354":"","174356":"","174359":"","174360":"","174361":"","174362":"","174363":"","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373":"","174375":"","174376":"","174378":"","174379":"","174380":"

Contribuinte: Maria Ligia da Cunha Gomes

Número: OP-182526

Data: 27/06/2022 - 09:05

Resumo: :"Aqui nos limitaremos a apontar as dificuldades que identificamos diante de nossa realidade como instituição de pesquisa. Considerando que a Lei de Inovação (Lei n.º 10.973/2004) tem como um de seus pilares a construção de parcerias entre universidades e empresas no Brasil, se valendo de instrumentos jurídicos para a viabilização de projetos de pesquisa, desenvolvimento e inovação a partir de parcerias com desenhos diversos, como por meio do intercâmbio entre pesquisadores de Instituições Científica, Tecnológica e de Inovação (ICTs) e empresas privadas para que, juntos, realizem projetos de Pesquisa, Desenvolvimento e Inovação (PD&I), a criação de Parques e Pólos Tecnológicos nas ICTs, foi aberta a possibilidade legal de que a atividade de pesquisa não seja realizada exclusivamente por um Órgão de Pesquisa, segundo a definição do art. 5º XVIII da LGPD, podendo ser realizada a partir de parcerias com empresas privadas, gerando implicações evidentes sobre a discussão de transferência internacional de dados pessoais. Pergunta-se: em um projeto de pesquisa estruturado a partir de uma parceria entre universidade e empresa privada, tendo como escopo a pesquisa básica ou aplicada, qual regime jurídico deve ser aplicado as operações de tratamento de dados pessoais, em participar a transferência internacional de dados, o aplicado aos órgãos de pesquisa ou o aplicável aos controles de dados pessoais de forma geral? A pergunta se insere no contexto em que a Lei de Inovação possibilitou a criação de novo "grupo de pesquisa", formado por pesquisadores de Órgãos de Pesquisa, na forma da LGPD e por Pesquisadores de empresas, incentivadas pela Lei de Inovação a participar do desenvolvimento tecnológico, trazendo uma infinidade de dados consigo, muitos deles eventualmente sensíveis ou que estejam amparados por legislações que "abracem" a nossa legislação de dados pessoais, tais como os que são basilares à Propriedade Intelectual e igualmente embasam os pilares da Pesquisa nacional e internacional. Por não haver ainda uma regulamentação norteadora sobre a égide de tais transferências, a normatização atual deixa dúvida sobre o tratamento que será dado a esse novo "grupo de pesquisa" em eventual transferência internacional de dados pessoais, se serão considerados órgãos de Pesquisa, devido à atividade-fim ou se deverão ter o tratamento direcionado a empresas, conforme seu porte? Imaginemos o seguinte cenário: um centro de pesquisa da universidade X (fundação privada) forma um convênio de cooperação com um centro de pesquisa da universidade Y (universidade pública federal) e com um centro de pesquisa da universidade Z (universidade francesa) para a realização de uma pesquisa conjunta sobre o desenvolvimento de uma nova técnica de processamento de linguagem natural. Os centros de pesquisa passam a realizar atividades em conjunto, construindo bases de dados com contribuições mútuas e promovendo o intercâmbio de professores e pesquisadores por meio de eventos e encontros de trabalho. A iniciativa passa a chamar a atenção da empresa A (multinacional com atuação em 11 países), que oferece financiar a pesquisa do grupo de centros de pesquisa, desde que possa participar do desenvolvimento da técnica de processamento de linguagem natural objeto do estudo. Os coordenadores do projeto de pesquisa propõem para a empresa que o projeto seja apresentado a uma Fundação de Amparo a Pesquisa e que para além dos recursos privados, o projeto também conte com os recursos da Agência de Fomento. Aprovado o projeto com as duas fontes de recurso, cria-se uma rede de troca de dados, muitos deles dados pessoais, entre as diversas entidades, incluindo a universidade francesa, que segue os protocolos de proteção de dados pessoais de sua

autoridade nacional – Commission Nationale Informatique & Libertés (CNIL). Contudo, paira uma dúvida no projeto, para as operações de transferência internacional de dados pessoais Brasil-França, qual o regime jurídico de tratamento de dados pessoais deverá ser observado, o aplicável a empresa A, ou o aplicável as universidades, caracterizadas como órgãos de pesquisa? É essencial a comprovação do fluxo de dados em ambiente seguro, mas sem restrições excessivas, de modo a não dificultar ou impedir, por exemplo o fomento à Pesquisa, Inovação Tecnológica e Intercâmbio Educacional, fontes inesgotáveis para o progresso global, e entendemos que para tanto, seria ideal a criação de uma Regulamentação específica para a matéria pela ANPD, na forma do art. 33, inciso. V, para que pesquisas realizadas sob as bases legais, independente de quem as execute, possam ter o tratamento especial que a LGPD destina à Pesquisa. ","174354":"Acreditamos ser necessário que as Regras estabelecidas para o Brasil sejam flexíveis de forma a poder abarcar as exigências das legislações específicas dos parceiros internacionais. Em se tratando de Pesquisa, em particular, há diversos casos de financiamento internacional em que o financiador não aceita a alteração da lei de regência em matéria de proteção de dados pessoais, pelo que a possibilidade de opção por uma das legislações, também seria de grande auxílio na concretização de financiamentos para a Pesquisa e o Desenvolvimento Nacional. Um exemplo da falta de flexibilidade na negociação dos termos de operações de transferência internacional de dados pessoais são os editais de financiamento de pesquisa de entidades internacionais. Quando um centro de pesquisa propõe um projeto no contexto de um edital internacional (e.g. União Europeia, Estados Unidos da América, etc.) é muito comum que um dos requisitos seja a apresentação de uma parceria com uma universidade local (e.g. na União Europeia, uma universidade de um de seus países membros). Dessa forma, o fluxo de dados entre os pesquisadores brasileiros e os pesquisadores estrangeiros será uma constante na execução do projeto de pesquisa. Contudo, quando o projeto é selecionado e se inicia a discussão contratual do financiamento, a entidade financiadora é pouco flexível na alteração das cláusulas de seu instrumento contratual padrão, não aceitando sugestões de alteração, por exemplo, nas suas regras sobre transferência internacional de dados pessoais. Por essa razão, sugerimos que a Autoridade Nacional de Dados Pessoais (ANPD) crie uma autorização especial para transferência internacional de dados pessoais entre instituições de pesquisa no contexto de financiamentos internacionais, reconhecendo como válidos e adequados os protocolos de proteção de dados pessoais presentes nesses instrumentos. A regra serviria como uma autorização prévia na área de pesquisa, sem obstaculizar a competência fiscalizatória da entidade no exame posterior de quaisquer dos acordos celebrados. Acrescente-se na proposta a possibilidade de a ANPD estipular que a regra de transferência internacional de dados pessoais na área de pesquisa só poderá ser aplicada para operações envolvendo países que possuam um regramento jurídico de proteção de dados pessoais (e.g. Lei geral, leis setoriais, etc.). ","174356":"O instrumento mais efetivo para legitimar a transferência internacional de dados pessoais no âmbito das atividades de ensino e pesquisa são as decisões de adequação da ANPD. Isto porque a decisão de adequação reduz os custos regulatórios do órgão de pesquisa nacional em seus projetos com entidades de outros países. Todavia, reconhecemos que a construção de uma decisão de adequação não é um processo simples e rápido, exigindo do regulador uma análise cuidadosa que poderá tomar alguns anos

até alcançar uma lista extensa de países. Sendo assim, é necessário observar outras alternativas disponíveis. Uma delas é a adoção de cláusulas contratuais-padrão. Uma alternativa interessante do ponto de vista dos custos envolvidos, tendo em vista que é a própria ANPD que apresenta a sua redação. Contudo, deve-se tomar um cuidado para criar formas de flexibilização das cláusulas, de modo a permitir adaptações setoriais e em contextos específicos. Na Fundação Getulio Vargas convivemos com alguns cenários em que a transferência internacional de dados pessoais é parte integrante de diversos programas, como por exemplo nos programas de intercâmbio de estudantes de graduação ou nos programas de duplo doutoramento, com estudantes realizando pesquisas em mais de um país, ou até mesmo nos nossos acordos de cooperação internacional, em que podemos ter professores de nossos programas ofertando cursos em instituições estrangeiras. Assim como a UE, o Japão, a Oceania e outros territórios que possuem compromissos, reconhecidos internacionalmente, em garantir as melhores práticas de governança na tratativa segura, mas ao mesmo tempo dinâmica dos dados pessoais, é recomendável que ANPD delimite as diretrizes norteadoras de tais tratativas, levando em consideração as exceções inerentes ao âmbito da Pesquisa e Inovação. Um exemplo é a utilização de mecanismos e setores internos nas instituições de Pesquisa, tal como é realizado na Fundação Getulio Vargas (FGV), com o Comitê de Ética, que analisa os instrumentos aplicáveis a qualquer Pesquisa em que haja interação com seres humanos, além das medidas adotadas pelo Encarregado de Proteção de Dados Pessoais, que avalia e recomenda ações para mitigar os riscos em Pesquisas, que envolvam dados pessoais para serem desenvolvidas, utilizando técnicas de anonimização e seguindo as melhores práticas em Segurança da Informação por meio de Comitê próprio, havendo, dessa forma, uma dupla análise institucional. A presença de estruturas de governança, com diversas instâncias de checagem e protocolos de proteção de dados pessoais, poderia ser reconhecida pela ANPD como salvaguarda para operações de transferência internacional de dados pessoais no contexto de atividades de ensino e pesquisa. ","174359":"A regulação é essencial para o Brasil integrar, com segurança, todos os fluxos internacionais de dados dos quais participe. Essas tratativas, diante da economia global e tecnológica, necessitam de forma urgente de diretrizes pré-definidas, mas por outro lado flexíveis, de acordo com a previsibilidade de tratamento dos dados em âmbito internacional, podendo usar como inspiração as SSCs da Comissão Europeia (Cláusulas-Padrão Contratuais). As SSCs possuem dificuldade de aplicação a um grande número de dados na transferência, como ocorre com multinacionais, mas tanto as SSCs quanto as Regras Corporativas Vinculantes (Binding Corporate Rules ou BCRs) podem ser uma inspiração para que se desenvolvam guidelines nacionais para as transferências internacionais de dados. Exemplificando, o que verificamos na prática, é a dificuldade em se tratar dados pessoais, definindo quais países possuem regras rígidas e legislação adequada para a tratativa de dados, quando para a efetividade do processo de Pesquisa precisamos de etapas com fluxos tão ágeis quanto seguros, para que não se perca o timing inovador. ","174360":"A presença de um programa interno de governança de dados de uma instituição de pesquisa poderia ser considerado hipótese autorizativa para a transferência internacional de dados pessoais e também que nas transferências internacionais baseadas em editais estrangeiros de financiamento, que as regras previstas pela financiadora sejam reconhecidas como válidas e

possam autorizar a transferência internacional de dados pessoais.","174361":"Entendemos que os elementos listados no art. 34 da LGPD tem o propósito de garantir que a transferência internacional de dados seja o mais segura possível e tais itens devem ser considerados na emissão de um parecer pela ANPD, como um rol exemplificativo, devendo ser consideradas todas as particularidades dos casos levados à análise. Todavia, existem atualmente inúmeras atividades em Pesquisa que estão em desenvolvimento ou prestes a serem iniciadas e, até que seja realizada a edição de resoluções específicas, após a análise de cada um dos parceiros internacionais e dos casos específicos de transferência internacional de dados pessoais, sugerimos a criação de uma regra de transição. Essa regra geral, funcionaria como uma autorização prévia da ANPD, reconhecendo que, no âmbito da Pesquisa Acadêmica e Institucional, seja chancelada a transferência internacional de dados para países com legislação de proteção de dados pessoais vigentes, havendo o compromisso do Importador (país receptor dos dados) de que adotará todos os protocolos e as melhores práticas para a segurança dos dados pessoais transferidos a ele, como destino, e durante todo o fluxo de tais dados. Em hipóteses de acordos já vigentes, continuariam seguindo o que foi determinado anteriormente, e em casos de novos acordos, haveria uma adaptação gradativa, adotando-se, temporariamente, as diretrizes de órgãos como Japão, Oceania e UE. ","174362":"A flexibilidade pontual em consonância com o texto padrão disponibilizado, que permita a incorporação das exigências legais do Brasil e do país do parceiro, traz um melhor equilíbrio contratual e a possibilidade de tratativas ágeis, em especial quando se tratam de dados em ambiente acadêmico e de Pesquisa, que possuem como caraterística principal a constante evolução dos dados tratados, sobre diversas frentes. A grande dificuldade está em não haverem diretrizes orientadoras já firmadas, refletindo na Pesquisa e Inovação, através de negociações, acordos de cooperação em que é necessária a adequação ao regramento do outro país. ","174363":"Os modelos de cláusula-padrão devem ser os mais plurais possíveis, de modo a atender diversos contextos. Formulários podem beneficiar entidades de pequeno porte que poderão já reutilizar o modelo em suas atividades cotidianas a um baixo custo. Árvore de decisão pode beneficiar aqueles que irão utilizar plataformas digitais nas operações de transferência internacional e o formato árvore de decisão pode facilitar a atividade de programação. Checkboxes pode servir para aqueles que já possuem processos internos que se baseiam nesse formato. A sugestão é que elas sejam disponibilizadas em diversos formatos.","174364":"Sim, é necessário ter regras diferenciadas para os casos de controlador, operador e também o reconhecimento da possibilidade de haver co-controladores, a depender de quem é a contraparte. Dentro do campo da Pesquisa, identificamos que, para que a pesquisa seja independente é necessário que os dados a serem tratados sejam despidos de tratamento prévio, para que não haja qualquer imposição de viés à Pesquisa, devendo ser o órgão de Pesquisa o Controlador desses dados, sendo admitida a hipótese de Pesquisas elaboradas dentro de uma Rede de Pesquisa composta por dois ou mais órgãos de Pesquisa, nacionais ou internacionais. Por outro lado, se a contraparte não for outro órgão de Pesquisa e sim um financiador, como uma empresa ou fundação, as atuações serão diferenciadas, assim como o acesso e o controle dos dados pessoais, que estão sendo utilizados no projeto. ","174367":"","174368":"","174369":"","174371":"","174372":"A União Europeia possui cláusulas-padrão contratuais (CPC) a serem utilizadas em contratos onde haja o tratamento de

dados pessoais, cláusulas essas que são norteadoras das garantias e forma de segurança mínimas para os tratamentos de dados, mas que permitem alterações e ajustes para a incorporação de exigências dos demais parceiros. ","174373":"Direitos dos titulares: 1- Serem informados sobre as operações de tratamento; 2- Terem meios eficazes para contatar controladores estrangeiros; 3- Terem acesso às cláusulas padrão que permitiram o tratamento de seus dados; 4- Rever a continuidade do tratamento e ter danos reparados. ","174375":"","174376":"No que tange à área de Pesquisa, entendemos que o ideal seria a regulamentação da matéria de forma geral, garantindo a agilidade na formação de Redes de Pesquisa Globais. Ainda há outro ponto que carece de regulamentação: de acordo com a definição legal brasileira sobre órgão de Pesquisa, diversas Universidades e institutos de Pesquisa renomados mundialmente não são considerados órgãos de Pesquisa, pois as legislações alienígenas possuem requisitos diversos para esse reconhecimento. Desta forma, seria muito profícuo se a ANPD reconhecesse, previamente, que instituições de ensino e Pesquisa do exterior, seriam consideradas órgão de Pesquisa no Brasil, ainda que não preencham os requisitos exigidos para os órgãos de Pesquisa nacionais. ","174378":"","174379":"Comunicação à autoridade de seus territórios e aos titulares que tenham os dados pessoais acessados, bem como as atualizações sobre o deslinde da questão.","174380":"O Princípio da Transparência com a utilização de Visual Law seria uma alternativa ágil e eficaz, trazendo a conscientização para o fluxo contratual, com relevantes e potenciais resultados em ambiente globalizado. A implementação é simples, em especial, no ambiente acadêmico de Pesquisa e Inovação, torna-se muito mais econômico e agrega valores mais sólidos na dinâmica que norteia o Princípio da Autodeterminação Informativa em consonância com o Princípio da Finalidade. Um exemplo de implementação de visual law é o Projeto DaPIS, a criação de uma ontologia iconográfica própria para a proteção de dados pessoais no contexto europeu. A Universidade de Bolonha em colaboração com a Academia de Belas Artes da cidade e a Sociedade Italiana de Informática criaram o Data Protection Icon Set (DaPIS), um conjunto de representações gráficas de operações de tratamento de dados pessoais, finalidades do tratamento, bases legais, direitos do titular e papeis exercidos por agentes de tratamento. O projeto além de servir como uma forma simples de comunicação com titulares de dados pessoais, também funciona como uma forma de comunicação entre máquinas, pois os ícones desenvolvidos são machine-readable, criando processos automatizados de tratamento de dados pessoais a partir das regras europeias de proteção.

Contribuinte: Daniela de Jesus Machado Ribeiro

Número: OP-182675

Data: 27/06/2022 - 14:57

Resumo: :"Pela ANBC - As transferências internacionais de dados são um fator essencial na regulamentação da LGPD, tendo em vista a relevância do tema para as atividades cotidianas de uma série de empresas. Com efeito, as transferências internacionais de dados são uma realidade para a maior parte das empresas, inclusive ao se considerar a infraestrutura das empresas, como serviços de cloud computing (ou computação em nuvem). Ademais, as

transferências internacionais de dados também são frequentes, a título exemplificativo, (i) quando da operação de empresas multinacionais ou que possuem a sua sede ou suas filiais no exterior, bem como (ii) nas situações em que as empresas localizadas no Brasil mantêm relações comerciais com parceiros estrangeiros. Desta maneira, a regulamentação do tema é relevante para que os contornos sobre as transferências internacionais sejam melhor desenhados, inclusive de forma a assegurar mais segurança jurídica às empresas que se valem de transferências internacionais. Tendo isso em vista, a atuação da ANPD é importante, sendo que a tomada de subsídios vem em momento ideal, uma vez que as discussões a respeito de transferências internacionais de dados se intensificaram na União Europeia e também no Reino Unido em razão da divulgação das novas cláusulas contratuais padrão a serem adotadas nessas regiões, além da decisão no conhecido caso Schrems II. Todavia, a despeito do desenvolvimento da matéria no continente europeu, é essencial, a fim de regular o tema no Brasil, que sejam avaliadas as condições próprias do país, especialmente em termos de acesso a tecnologias, infraestrutura e desenvolvimento econômico. No que se refere especificamente a cloud computing, ainda que o mercado brasileiro de data centers esteja em expansão, especialmente se comparado ao restante da América Latina, a presença de servidores que servem de base para o armazenamento em nuvem em países estrangeiros ainda é muito prevalente. Assim, nesse setor, ao que tudo indica, parece ser pouco provável que as empresas nacionais possam se valer apenas de data centers localizados no Brasil. As transferências internacionais de dados já fazem e continuarão fazendo parte da realidade da maioria das empresas que atuam no Brasil, sendo certo, portanto, que eventual regulamentação do tema deve estar atenta para não estabelecer obstáculos desnecessários, prejudicando a inovação em múltiplos setores. Há também de se considerar que a prática de manter e armazenar dados fora do país de origem deles pode ser benéfica quando avaliada em face de questões como privacidade e segurança dos dados. Assim, o armazenamento de dados em jurisdições distintas, além de, em algumas situações, ser necessário, pode apresentar vantagens, reduzindo vulnerabilidades. Além disso, mesmo que a estrutura de data centers na União Europeia seja robusta, região que poderia ser contemplada com decisão de adequação por parte da ANPD em razão de semelhanças entre a Regulation (EU) 2016/679 (General Data Protection Rule ou "GDPR") e a LGPD, é inegável que diversas empresas utilizam data centers que se encontram em outros países e regiões, como os Estados Unidos. Para fins exemplificativos, pode-se citar aqui as empresas Google, com o armazenamento chamado Google Drive, e a Amazon, que disponibiliza os serviços por meio da AWS. O Google não possui nenhum data center localizado no Brasil, mas possui quatorze de seus data centers nos EUA, sendo essa a região com a maior concentração de seus data centers. Por outro lado, a AWS possui um data center em São Paulo, no Brasil, tendo seis outros nos EUA. Há clara desproporcionalidade, como destacado, entre as possibilidades de data centers disponíveis para empresas que desejam manter dados pessoais no Brasil. Ademais, há de se considerar também que, em especial no caso de serviços de infraestrutura, como o cloud computing, há, de maneira geral, grandes players do mercado oferecendo seus serviços a diversas empresas. Em que pese muitas dessas empresas estarem adequadas, principalmente, à GDPR, os contratos firmados costumam seguir o modelo de adesão, abrindo pouco ou nenhum espaço para negociações ou inclusões de novas cláusulas a respeito de transferências internacionais

de dados. Portanto, ainda que os aspectos dispostos acima não sejam propriamente obstáculos à transferência de dados do Brasil para fora ou vice-versa, são pontos que devem ser considerados pela ANPD, já que uma parte expressiva das empresas brasileiras que se valem de armazenamento ou processamento em nuvem no exterior assinam esses contratos de adesão e têm nos serviços de cloud computing uma ferramenta essencial para o desenvolvimento de suas atividades. Com efeito, eventual regulamentação do tema, como já afirmado na presente contribuição, deve situar adequadamente o Brasil no ecossistema da tecnologia, a fim de bem compreender especificidades do país e evitar implementação de normas, cláusulas e demais parâmetros que sejam demasiado rígidos a ponto de impedirem ou mesmo dificultarem substancialmente que as transferências internacionais ocorram. Conjuntamente a pontos já analisados acima, é também relevante que a ANPD leve em consideração a existência de empresas brasileiras com presença internacional e as empresas multinacionais que se encontram no país. Isso porque, para esses modelos de negócio, as transferências internacionais podem ser relevantes para seu funcionamento. Nesse cenário, há diversas atividades que podem requerer as transferências internacionais, como atender as demandas de clientes estrangeiros, comunicações com o exterior (sejam filiais ou não) para fins de controles internos, até compartilhar dados com investidores internacionais e buscar oportunidades de negócio fora do país. Nesse sentido, as transferências internacionais auxiliam inclusive as empresas que estejam em processo de expansão, crescimento e inovação, sendo essencial que esse tipo de ambiente que permite o crescimento nacional exista, especialmente ao se tratar da proteção de dados pessoais, tendo em vista a necessidade, muitas vezes, de seu compartilhamento. Por esses motivos, a regulamentação a respeito das transferências internacionais de dados precisa considerar seus impactos sobre a economia e a inovação, de forma a não prejudicar o papel do Brasil nesse debate, mas sim de criar condições para o desenvolvimento de atividades empresariais com segurança no tratamento de dados e incluindo cada vez mais o país no circuito de transferência internacional de dados. Em outras palavras, deve haver um alinhamento entre a regulamentação e a realidade socioeconômica do país, permitindo a continuidade das empresas e dos negócios aqui desenvolvidos. Ainda, é importante que a ANPD avalie outras regulamentações setoriais, por parte de órgãos e entidades governamentais, que já tratem do tema de transferências internacionais de dados e/ou de questões de localização territorial dos dados, de maneira a não criar conflitos entre a eventual regulamentação da Autoridade com as normas já existentes no país. É possível citar, a título exemplificativo, norma do Banco Central do Brasil ("BCB") (Resolução BCB n.º 85/2021), que estabelece os procedimentos, no âmbito da sua competência de supervisão, para contratação de serviços relevantes de processamento e armazenamento em cloud no exterior pelas instituições reguladas pelo BCB. Além disso, a Resolução n.º 85/2021 do BCB permite a contratação de serviços de nuvem no exterior pelas instituições sujeitas a regulamentação do BCB sem necessidade de aprovação daquela Autarquia quando da existência de convênios para troca de informações entre o BCB e as autoridades supervisoras dos países nos quais os dados poderão ser armazenados (artigo 16, I da Resolução n.º 85/2021 do BCB). Com base no Comunicado n.º 31.999/2018, o BCB divulgou essa relação de convênios. Correspondem, dentre outros, a países aos quais as transferências internacionais de dados pessoais estariam autorizadas pelo BCB: África do Sul,

Alemanha, Argentina, Áustria, Bahamas, Chile, China, Colômbia, Coreia do Sul, Espanha, Estados Unidos, Ilhas Cayman, Índia, Indonésia, Itália, Luxemburgo, México, Panamá, Paraguai, Peru, Portugal, Reino Unido, Suíça, Uruguai e demais países da Europa. Ademais, junto aos EUA, há alguns Memorandos de Entendimento acordados com o Board of Governors of the FED System (FED), Office of the Comtroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC) e Department of Financial Services (DFS) que garantem que ocorram transferências de dados do Brasil aos EUA. Isso significa que, na prática, há diversas instituições reguladas pelo BCB que transferem dados para os países que estão postos acima com base em normas emitidas pela autarquia, aspecto que precisa ser levado em conta pela ANPD a fim, inclusive, de evitar conflito de normas no Brasil. Nesse sentido, poderia ser inclusive interessante que a ANPD, tal como feito pelo BCB, estudasse a possibilidade de eventuais acordos com os EUA a fim de facilitar as transferências de dados para o país, garantindo ainda seu nível de segurança e a proteção dos mesmos. Em paralelo, há a necessidade de verificar se há outras normas nesse sentido que possam afetar setores específicos da economia, especialmente os regulados por autarquias, órgãos e entidades. Destacamos, ainda, a importância de se ter transparência com os agentes de tratamento sobre os critérios utilizados por esta D. Autoridade para determinar o "grau de proteção de dados pessoais adequado" em outras jurisdições, dando-se transparência sobre todo acordo de cooperação firmado pela ANPD. A partir de todo o exposto acima, o objetivo final deve ser elaborar uma regulamentação no tema de transferências internacionais de dados que seja clara e flexível, garantindo sempre a proteção dos dados, mas sem impor entraves ao desenvolvimento econômico dos setores que dependem das transferências internacionais de dados para suas atividades. ","174354":"Como afirmado previamente, as transferências internacionais são essenciais na realidade de diversas empresas, inclusive brasileiras. Assim, é importante que exista um meio de promover, de forma central, a interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os previstos nas outras jurisdições. A ideia de convergência, por sua vez, não necessariamente é a mais adequada, tendo em vista que, tal como já destacado, o ideal é que a ANPD considere essencialmente o cenário brasileiro para a implementação das normas, cláusulas e diretrizes sobre as transferências internacionais. Com efeito, é possível, e desejável, que a Autoridade avalie as práticas internacionais no tema a fim de elaborar a regulamentação nacional, mas deve haver uma análise crítica acerca do contexto brasileiro em relação ao internacional. Por isso, entende-se que a convergência não necessariamente deve ser alcançada, sendo relevante apenas caso contribua para o cenário socioeconômico local, sem dificultar a ocorrência de transferências internacionais. O conceito de interoperabilidade, por sua vez, costuma-se referir à capacidade dos sistemas e organizações em trabalhar de maneira conjunta, garantindo que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente (i). É claro, então, que há uma diferença quando se fala de interoperabilidade entre jurisdições se comparada ao conceito tradicional de interoperabilidade. Em termos de jurisdições, existem, provavelmente, elementos que não poderão ser interoperáveis, tendo em conta as diversas especificidades de cada legislação de proteção de dados pessoais, por exemplo. No entanto, haver uma certa compatibilidade, no que fizer sentido, entre os instrumentos contratuais de diferentes jurisdições que sejam

voltados a transferências internacionais de dados pode ser produtivo. As discussões a respeito da interoperabilidade entre instrumentos contratuais que permitam as transferências internacionais de dados, porém, ainda parecem incipientes. No entanto, há uma experiência internacional recente, no Reino Unido, que pode ser interessante à ANPD e à regulamentação do tema no Brasil, em especial para empresas que tenham contratos que utilizem as cláusulas de proteção de dados previstas na União Europeia a partir da GDPR. É o caso do adendo às cláusulas contratuais padrão do European Data Protection Board (EDPB), que se baseiam na GDPR, elaborado por parte da Information Commissioner's Office (ICO), autoridade de proteção de dados do Reino Unido (ii) . Trata-se de documento que serve como um anexo aos contratos já firmados que utilizem as cláusulas contratuais padrão do EDPB, o que permite mais flexibilidade às empresas e redução de custos. Isso porque organizações que se encontrem adequadas à GDPR a partir das cláusulas contratuais padrão do EDPB não precisam assinar mais um conjunto de cláusulas, que seriam as emitidas pela própria ICO. O adendo em si é recente, então ainda não se sabe propriamente como ele será aplicado ou quais as dificuldades envolvidas em sua aplicação. No entanto, a ANPD pode considerar esse formato a fim de pensar em eventuais modelos semelhantes que sejam aplicáveis à LGPD no contexto de transferências realizadas por empresas que já tenham cláusulas contratuais em seus contratos que sigam modelos como as do EDPB ou ICO. Com essa medida, as empresas não precisariam necessariamente adotar cláusulas contratuais padrão emitidas por parte da ANPD, uma vez que poderiam se valer das que já aplicam normalmente, reduzindo seus custos em alterar contratos vigentes e aumentando a interoperabilidade e a eficiência. (i) Fundação Escola Nacional de Administração Pública (ENAP). Introdução à Interoperabilidade. Módulo 01. p. 5. Disponível em: http://repositorio.enap.gov.br/handle/1/2398. Acesso em: 06.06.2022. (ii) Information Commissioner's Office. International Data Transfer Addendum to the EU Commission Standard Contractual Clauses. Version B1.0. Disponível em: https://ico.org.uk/media/for-organisations/documents/4019539/international-data-transfer-addendum.pdf. Acesso em: 06.06.2022. ","174356":"","174359":"","174360":"a. Cláusulas-padrão contratuais Quanto às cláusulas contratuais padrão, com base na análise de experiências internacionais, um formato interessante parece ser o que apresenta um conteúdo mínimo para as cláusulas com flexibilidade acerca de sua aplicação, permitindo que sejam levadas em consideração os elementos essenciais de uma relação contratual que possam influenciar um acordo quanto à transferência internacional de dados. Nesse sentido, a ANPD pode também considerar maior flexibilidade às cláusulas em si, permitindo modificações a elas, desde que os elementos que são necessários tenham sido abarcados. Além disso, é interessante que a ANPD defina quais as obrigações mínimas das partes por meio das cláusulas contratuais padrão de maneira a se assegurar mais segurança jurídica ao tema das transferências internacionais. Contudo, ainda assim, é essencial que o conteúdo mínimo não dificulte a realização das transferências. Em outras palavras, deve haver uma razoabilidade por parte da ANPD a fim de não criar obstáculos a que os dados pessoais sejam transferidos para fora do Brasil, tendo em vista como as transferências se tornaram parte essencial dos modelos de negócio hoje nos mais diversos setores. Junto a esses pontos, é importante que o documento final e as cláusulas em si não sejam de difícil utilização para micro, pequenas e médias empresas, tendo em vista que

também é um mercado que se vale de transferências internacionais, mas que, em diversos casos, não tem a mesma capacidade de negociação de grandes empresas brasileiras ou multinacionais. Nesse sentido, é importante que os parâmetros para o uso das cláusulas não sejam excessivamente burocráticos, evitando que tornem o uso do documento inviável. Desta forma, ainda que as cláusulas divulgadas por autoridades de proteção de dados de outras jurisdições possam ser analisadas pela ANPD para a regulamentação nacional, é importante que a realidade social e econômica do Brasil seja um elemento essencial para a definição das cláusulas no país. b. Cláusulas contratuais específicas Em primeiro lugar, tendo em vista o art. 33, II, a, da LGPD, de acordo com o que as cláusulas contratuais específicas podem ser utilizadas para "determinada transferência", é importante que a ANPD se debruce sobre as possibilidades nas quais esse mecanismo para transferência internacional poderia ser utilizado de forma a garantir a segurança jurídica de empresas que façam uso dele. Além disso, considerando que cláusulas contratuais padrão já têm parte do seu conteúdo pré-definido, poderia ser interessante permitir que as cláusulas específicas, de fato, sejam flexíveis e determinadas pelas partes envolvidas, sendo que caberia à ANPD mais o papel de definir diretrizes mínimas e princípios a serem observados. Na União Europeia, a partir da GDPR, a aprovação de cláusulas contratuais específicas fica sujeita à autorização pela autoridade nacional de proteção de dados pessoais para, apenas em momento posterior, submetê-la ao mecanismo de consistência pelo EDPB. Assim, parece que o fluxo excessivamente burocrático de aprovação contribui para a perda de efetividade do mecanismo em si. Por esse motivo, é importante que a ANPD pense em formas a fim de flexibilizar esse modelo a partir de recomendações próprias ou viabilize um processo para tal aprovação que seja extremamente célere, de modo a não atravancar negociações por conta da não-aprovação ou aprovação com atraso das cláusulas. Pode haver, inclusive, fiscalização e/ou aprovação baseada em risco, ou seja, algumas situações específicas podem demandar a aprovação a depender de critérios previamente definidos pela ANPD (ex.: transferência de dados de forma massiva). Para os outros casos, as cláusulas poderiam seguir sem que haja a aprovação expressa da ANPD, podendo a Autoridade exercer a fiscalização dos instrumentos para transferências internacionais, se entender ser necessário. c. Normas corporativas globais As normas corporativas globais estão previstas no art. 33, II, c, da LGPD e encontram a sua correspondência nas binding corporate rules europeias, estabelecidas para multinacionais, joint ventures e grupos de franquia. Além disso, no cenário europeu, referidos documentos devem ser aprovados previamente pela autoridade de proteção de dados correspondente (i). Em termos de normas corporativas globais, parece ser relevante que a ANPD permita que a conformidade de um grupo econômico possa ser comprovada a partir de diversos tipos de documentos, como políticas internas, políticas de privacidade, contratos com fornecedores, informações a colaboradores, dentre outros. Nesse sentido, é importante a flexibilidade em relação aos instrumentos e mecanismos que podem ser utilizados, levando em consideração as diferentes estruturas de governança em proteção de dados implementadas no mercado e em setores econômicos variados. Além disso, seria interessante que a ANPD esclarecesse em que contextos as empresas podem adotar as normas corporativas globais para transferência internacional de dados, visando à segurança jurídica daquelas que as utilizarem. Em relação ao conteúdo, entende-se que o papel da ANPD deveria ser no sentido de divulgar diretrizes e

recomendações mínimas sobre o que se espera das normas corporativas globais a fim de que estejam adequadas à LGPD. Já em relação à necessidade de sua aprovação pela ANPD, pode-se pensar na possibilidade de aprovação baseada em risco, ou seja, grupos que forem vistos como de maior risco em razão dos tratamentos realizados ou do setor em que atuam teriam de passar por um escrutínio maior, com a aprovação mais célere para negócios ou atividades de baixo risco. No mais, para empresas cuja sede se encontra no exterior e que já tenham em vigor normas corporativas globais, espera-se que o papel da ANDP seja o de validar o documento para ser implementado no âmbito do Brasil, de modo que a organização não tenha que produzir um procedimento novo para a mesma função, especialmente se tais normas já forem aprovadas na União Europeia. Assim, sugerimos endereçamento deste ponto também pela ANPD. d. Códigos de conduta Na GDPR, são documentos (validados pela autoridade europeia) elaborados pelas empresas para garantir que estão adequadas e possuem salvaguardas suficientes para atuarem em transferências internacionais. Este documento pode ser muito bem utilizado no Brasil e bem-visto pela comunidade internacional, garantindo eficácia nos negócios. (i) BLUM, R. O.; MALDONADO, V. N. (coordenação). Lei Geral de Proteção de Dados Comentada. São Paulo: Thomson Reuters Brasil, 2020 ","174361":"","174362":"Considerando as experiências internacionais no tema e o contexto brasileiro, o modelo ideal caminha no sentido de demandar uma mescla entre conteúdo pré-definido e a flexibilidade quanto ao texto das cláusulas. De fato, esta prática confere segurança jurídica às empresas em relação ao conteúdo mínimo necessário das cláusulas contratuais padrão ao mesmo tempo em que abre o espaço para adequações que devam ser feitas por empresas a fim de adaptar as cláusulas aos seus modelos negociais e aos próprios contratos e/ou acordos que já foram assinados a respeito da proteção de dados pessoais. Além disso, é importante que o documento que traz as diretrizes sobre as cláusulas contratuais padrão seja acompanhado de explicações a respeito das mesmas, de modo a garantir que exista uma interpretação clara sobre como as utilizar e as inserir em determinada relação contratual. Recomenda-se, portanto, que o documento final a ser elaborado pela ANPD seja intuitivo e de fácil utilização pelas empresas que se valham dele para alterar suas políticas e cláusulas sobre transferências internacionais de dados. Nesse sentido, é bem-vindo que a Autoridade aproveite recursos visuais, como tabelas ou diagramas de decisão, que guiem a aplicação das cláusulas e a compreensão sobre como elas devem ser aplicadas à relação contratual que se encontre sob análise. Um exemplo importante sobre como as tabelas podem auxiliar nesse processo são as cláusulas contratuais padrão divulgadas, no início deste ano, por parte da Information Commissioner’s Office (ICO), autoridade de proteção de dados do Reino Unido (i). É necessário, também, que a ANPD leve em consideração os elementos que são peculiares ao Brasil em termos de proteção de dados, a maturidade das empresas brasileiras no tema e a realidade socioeconômica vigente no país. Ao mesmo tempo, é igualmente útil levar em consideração a experiência internacional sobre as cláusulas contratuais padrão. As cláusulas da ICO, assim, apresentam um aspecto relevante, na medida em que demonstram uma preocupação em torná-las mais acessíveis e ‘user-friendly’ (ii), permitindo que as empresas compreendam bem as cláusulas e, consequentemente, reduzindo dúvidas sobre sua aplicação que possam vir a dificultar a implementação das mesmas no dia a dia. Especificamente quanto às tabelas disponibilizadas pela ICO (correspondentes à

primeira parte do documento contendo as cláusulas contratuais padrão da ICO), o objetivo central dessas é guiar a aplicação das cláusulas a partir do preenchimento de suas células, que contêm certas perguntas como quem seria o controlador ou o operador, qual a relação contratual existente entre as partes, dentre outros questionamentos. Por essa razão, tais tabelas e suas questões fornecem um panorama amplo quanto à relação entre as partes, normalmente chamadas de importador e exportador de dados, que auxiliam a entender em que medida essas cláusulas são aplicáveis a elas. Assim, as tabelas deixam mais explícitos os pressupostos das transferências internacionais de dados, dando transparência às cláusulas. Trata-se de um modelo específico que pode ser adaptado à realidade e às necessidades em termos de LGPD pela ANPD, sem que isso signifique necessariamente utilizar o conteúdo em si das tabelas e perguntas, mas sim o formato delas. Além desses pontos, é importante que a ANPD elabore cláusulas que permitam seu uso por diversas das partes que estão envolvidas em transferências internacionais de dados, sejam elas as controladoras ou operadoras. Por conseguinte, idealmente, as cláusulas contratuais padrão devem ser utilizadas em relações de transferência de dados entre: (i) controlador e controlador; (ii) controlador e operador; e (iii) operador e operador, sendo essas empresas distintas ou do mesmo grupo econômico. Por fim, pode-se pensar também no uso das cláusulas em relações entre as partes acima e o suboperador (iii) de dados ou mesmo com partes que não participem da relação contratual como agentes de tratamento. Isso é importante para que não existam lacunas em relação a que partes estão, de fato, abarcadas pelas cláusulas contratuais padrão, evitando dificuldades na aplicação das mesmas ou a necessidade de ajustes posteriores às cláusulas elaboradas. Essa aplicação abrangente, inclusive, é essencial para fins da proteção de dados pessoais, tendo em vista a diversidade de acordos de transferências internacionais que podem existir. (i) Information Commissioner's Office. Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018. Version A1.0. p. 9-32. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. Acesso em: 30.05.2022. (ii) SPEECHLYS, Charles Russell. ICO's final version of the UK international data transfer agreement (i.e. the new 'UK SCCs') published and will enter into force from 21 March 2022. Lexology. Disponível em: https://www.lexology.com/library/detail.aspx?g=3ac291b5-da66-4c4f-939e-822606d8ae5a. Acesso em: 27.05.2022. (ii) Afigura do suboperador de dados não está prevista expressamente na LGPD, mas foi reconhecida por parte da Autoridade Nacional de Proteção de Dados em seu documento chamado de "Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado" de maio de 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 30.05.2022. ","174363":"Não há necessariamente um formato mais adequado para que a ANPD disponibilize modelos de cláusulas contratuais padrão. Com base na análise da experiência internacional no tema de transferências internacionais de dados, é possível que o ideal seja, na verdade, permitir a coexistência de mais de uma forma de formato a fim de aumentar a compreensão quanto às cláusulas contratuais padrão em si. Assim, por exemplo, pode-se combinar o uso de tabelas com um texto explicativo acerca das cláusulas que guie a

aplicação. Nesse sentido, cita-se as tabelas utilizadas pela Information Commissioner's Office (ICO), autoridade de proteção de dados do Reino Unido (i), disponibilizadas em conjunto com as cláusulas contratuais padrão a serem aplicáveis na região. Note-se que a inspiração aqui encontra-se em um contexto formal, de visualização, e não necessariamente do conteúdo das cláusulas, na medida em que, como já destacado, as cláusulas e os parâmetros eventualmente elaborados pela ANPD devem levar em consideração as particularidades do contexto brasileiro.. Quanto às tabelas elaboradas pela ICO (correspondentes ao primeiro item do documento contendo as cláusulas contratuais padrão), seu propósito é guiar a aplicação das cláusulas a partir do preenchimento de suas células, que contêm certas perguntas como quem seria o controlador ou o operador, qual a relação contratual existente entre as partes, dentre outros questionamentos. As tabelas, portanto, auxiliam as partes a compreenderem a aplicação das cláusulas contratuais padrão, sendo modelo que a ANPD pode considerar para os fins de sua regulamentação acerca de transferências internacionais. Trata-se de modelo específico que pode ser adaptado à realidade e necessidades em termos de LGPD pela ANPD, sem que isso signifique necessariamente utilizar o conteúdo em si das tabelas e das perguntas, mas sim o formato delas. Em conjunto, outros formatos para disponibilização e auxílio no entendimento das cláusulas, como uma árvore de decisões, formulários e checkboxes, podem ser igualmente úteis. Uma possibilidade seria elaborar esquema em formato de árvore de decisões e/ou checkboxes que possam auxiliar agentes de tratamento a identificarem se precisam ou não de cláusulas contratuais padrão, se há necessidade de cláusulas adicionais e demais pontos necessários à matéria. Ademais, um modelo muito interessante é o Model Clause Agreement Builder, previsto pela autoridade de proteção de dados da Nova Zelândia (ii), o qual permite que as partes de certo acordo de transferência de dados ajustem as cláusulas necessárias à atividade por meio do preenchimento de formulário online. Ao longo do preenchimento, são indicados os campos obrigatórios e os opcionais. Trata-se de formato que pode estimular as partes a utilizarem as cláusulas adequadas, tendo em vista que há maior facilidade no próprio momento de definir o acordo de transferência de dados. (i) Information Commissioner's Office. Standard Data Protection Clauses to be issued by the Commissioner under S119A(1) Data Protection Act 2018. Version A1.0. p. 9-32. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-data-transfer-agreement-and-guidance/. Acesso em: 30.05.2022 (ii) Privacy Commissioner. Model Clause Agreement Builder. Disponível em: https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/model-clause-agreement-builder/. Acesso em: 06.06.2022.
","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373":"Co
nsiderando que, em muitos dos casos, as transferências internacionais de dados não irão depender do consentimento como base legal, parece pouco provável que haja uma situação em que a comunicação direta seja imprescindível. Nesse sentido, o mais relevante seria dar a devida transparência a eventuais alterações na configuração original da transferência. Para isso, o ideal seria a ANPD estabelecer aspectos mínimos que devem ser informados para que as empresas saibam exatamente os pontos mais importantes a fim de informar alterações. A nosso ver, as modificações que precisam ser informadas podem ser divulgadas com base nos

mecanismos de transparência já normalmente utilizados e implementados pelas empresas a partir da adequação à LGPD, como políticas de privacidade, termos de uso ou contratos. Em última medida, especialmente nos casos em que a transferência não tiver como sua base legal o consentimento, o mais indicado seria deixar a transparência aos titulares de dados a cargo das próprias empresas, a fim de que elas compreendam qual o melhor formato para a informação a ser dada a partir de seus modelos de negócio e especificidades. Além disso, há de se considerar que diversas mudanças nas transferências internacionais podem ser apenas de ordem procedimental, sem que tenham um impacto ao que já foi previamente informado aos titulares. De toda forma, a comunicação direta, além de mais onerosa, pode gerar mais incômodo ao próprio titular se excessiva ou desnecessária. Além disso, os documentos citados já são frequentemente utilizados, o que facilita e permite que eventuais alterações sejam feitas de forma facilitada, evitando ônus às empresas que têm as suas atividades adequadas à LGPD. A medida é relevante para mercados e empresas que funcionam pela lógica business to business (B2B), tendo em vista que, nesses casos, há pouco ou nenhum contato com o titular de dados envolvido nos tratamentos que requeiram transferências internacionais. Por esse motivo, poderia ser impraticável, além de oneroso, se essas empresas tivessem de informar por meio de comunicação direta cada titular de dados afetado por alterações nas transferências internacionais. Assim, deve haver uma flexibilidade para que se possa informar sobre modificações às transferências internacionais de dados.","174375":"","174376":"","174378":"","174379":" Entendemos que impor obrigações adicionais para fins de transferência aos agentes de tratamento (importador ou exportador de dados) quando forem obrigados a se sujeitar a uma determinação das autoridades públicas, a depender do conteúdo, poderia inviabilizar o fluxo de dados, prejudicar de forma excessiva as negociações a fim de transferir dados internacionalmente e tornar a adequação à possível regulamentação da ANPD demasiado onerosa. Inclusive, na União Europeia, em que há obrigações extensivas no tema, a onerosidade de tais cláusulas foi apontada por profissionais da área de proteção de dados como uma questão. Nesse sentido, se a ANPD compreender serem necessárias obrigações ou orientações ao importador e mesmo ao exportador (tendo em vista que as obrigações normalmente recaem sobre o importador de dados), é importante que elas sejam viáveis, tenham cumprimento facilitado e não sejam excessivas. Seria recomendável que a ANPD analisasse de forma mais profunda o nível de proteção de dados estabelecido entre países e mapeasse os países em que há a possibilidade de acesso às informações pelas autoridades públicas locais. Eventuais orientações adicionais atribuídas ao importador e ao exportador em caso de acesso aos dados por determinação de autoridades públicas estrangeiras deveriam ser discutidas previamente com o mercado, factíveis do ponto de vista operacional e jurídico e poderiam ser recomendadas somente quando a transferência for feita a países específicos que representem um grau de risco elevado no tema.
","174380":"Os meios que parecem mais adequados para fornecer aos titulares de dados informações claras e relevantes sobre a eventual transferência de seus dados pessoais para fora do Brasil seriam mecanismos de transparência já normalmente adotados pelas empresas por conta da necessidade de adequação à LGPD, tais como as políticas de privacidade, termos de uso ou os contratos. A título exemplificativo, as políticas de privacidade possuem disponibilização facilitada por canais acessíveis a titulares, seja em meios físicos ou digitais,

assegurando o acesso gratuito e facilitado, cumprindo com o pressuposto da LGPD a respeito da transparência sobre as atividades de tratamento, sendo plenamente compatível o seu uso a fim de informar sobre transferências internacionais de dados que ocorram. São documentos já frequentemente utilizados e implementados, o que facilita e permite que eventuais alterações sejam feitas de forma facilitada, evitando ônus às empresas que têm as suas atividades adequadas à LGPD, tendo em vista a desnecessidade de adoção de um novo mecanismo específico para informar sobre a ocorrência de transferências internacionais. A medida é especialmente relevante para os mercados e empresas que funcionam pela lógica business to business (B2B), tendo em vista que, nesses casos, há pouco ou nenhum contato com o titular de dados envolvido nos tratamentos em questão que requeiram transferências internacionais. Ou seja, seria demasiado oneroso exigir desse tipo de negócio contato direto e específico com cada titular de dados. Assim, deve haver flexibilidade a fim de que se possa informar a respeito das transferências internacionais de dados da forma que se encontre em conformidade com a realidade das empresas e dos diferentes setores da economia. Portanto, a menos em casos específicos, como quando a transferência usar o consentimento enquanto base legal, não parece haver um motivo para utilizar mecanismos de transparência que não sejam os já adotados pelo mercado.

Contribuinte: Luciane Helena Vieira Pinheiro Pedro

Número: OP-182923

Data: 28/06/2022 - 13:29

Resumo:
:"","174354":"","174356":"","174359":"","174360":"","174361":"","174362":"","174363":"","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373":"","174375":"","174376":"","174378":"","174379":"","174380":"

Contribuinte: Jaqueline Simas Claveland de Oliveira

Número: OP-182975

Data: 28/06/2022 - 19:54

Resumo: :"Os principais motivos para a transferência de dados pessoais do Brasil para outros países são: - Falta de segurança; - Falta de decisões de adequação; - Ausência de uma orientação específica da ANPD acerca de países considerados adequados/seguros para a transferência internacional de dados pessoais. Os principais motivos para a transferência de dados pessoais de outros países para o Brasil: - Insegurança jurídica em razão do grau regulatório do Brasil que se encontra em construção; - Falta de decisão de adequação.","174354":"Seria necessária a realização de um estudo para levantamento das principais práticas adotadas internacionalmente objetivando a verificação de convergência destas práticas para a criação de instrumentos que garantam a convergência e a

interoperabilidade. A ANPD deve realizar tratativas com os órgãos internacionais de privacidade e proteção de dados para criar acordos/convênios que garantam essa convergência bem como os mecanismos de interoperabilidade que garantam a fluidez e a segurança da transferência.","174356":"Os instrumentos mais efetivos para a transferência internacional no caso de pequenas e grandes organizações são as cláusulas contratuais padrão, haja vista que são mecanismos de efeito imediato, de fácil aplicação e sem custo adicional, e dessa forma, são aplicáveis a todos os tipos de organização.","174359":"Os principais benefícios e impactos são a possibilidade de adoção de mecanismos para armazenamento, transferência, e guarda de dados pessoais mais robustos, baratos, dinâmicos e seguros. A melhor alternativa para o endereçamento nos instrumentos contratuais é a criação de cláusulas padrão que se adequem aos principais modelos de negócio que demandam a transferência.","174360":"Considerando que esses padrões já existem em outros países e, em muitos casos, encontram-se consolidados pela prática de mercado, o ideal em todas as três hipóteses seria a adoção de critérios e ou requisitos baseados nesses padrões existentes, de modo a criar tais mecanismos de forma mais aderente ao mercado mundial. Isso porque o principal norteador dessas cláusulas seriam as práticas mercadológicas e os modelos de negócio, que no caso do Brasil, não se diferenciam do resto do mundo de modo considerável.","174361":"Entendemos que tanto a adoção de medidas de segurança previstas em regulamento quanto a natureza dos dados pessoais devam ser levados em consideração tanto na avaliação de países ou organismos estrangeiros quanto no estabelecimento de regras para instrumentos contratuais, já que se tratam de elementos presentes em ambas as situações e que podem impactar na avaliação.","174362":"Entendemos que o ideal seria adotar um padrão maduro com possibilidade de flexibilização, mantendo-se o núcleo da cláusula em relação ao texto padrão, que nesse caso seria apenas exemplificativo. Assim, também seria importante definir os temas obrigatórios a serem enfrentados no contrato em cada ramo de negócio.","174363":"Qualquer possibilidade deve ser avaliada pela ANPD e se possível e viável, implementada, inclusive observadas as soluções já adotadas por outros organismos internacionais, como por exemplo o ICO.","174364":"Sim. A adoção de padrões de acordo com a posição do agente de tratamento e com o ramo de negócio, a exemplo do que já ocorre em outros países, é fundamental para viabilizar a transferência internacional de dados pessoais com um padrão de segurança razoável e um nível de flexibilização e adaptação compatíveis com a realidade de mercado. Vide exemplos adotados pelo ICO.","174367":"Não necessariamente haveria a necessidade de requisitos específicos, no entanto, considerando que as Normas Corporativas Globais se aproximam de uma modelagem de política, haveria a necessidade de maior detalhamento nesta última, principalmente considerando a volumetria dos dados, estrutura de transferência, e tipo de dados envolvidos, que vão demandar uma estruturação mais complexa.","174368":"Os mesmos critérios já utilizados no direito para a definição jurídica de grupo econômico, grupo societário e grupo de fato. Além disso, outros aspectos devem ser levados em consideração, tais como: - Possibilidade de indicação de um mesmo DPO para todo o grupo; - Políticas de privacidade, proteção de dados e segurança da informação comuns; - Existência de diretrizes, regras e entendimentos comuns em relação ao tratamento de dados pessoais; - Existência de operações de tratamento de dados pessoais realizadas em conjunto por mais de uma

organização do Grupo.","174369":"Esse detalhamento deveria considerar os tipos de dados (sensíveis e de menores de idade) bem como a volumetria, contudo, garantindo um grau de detalhamento que não engesse a operação e proteja o titular. ","174371":"Os benefícios seriam a facilitação do fluxo de dados em decorrência da desburocratização, considerando que os dois grupos econômicos já possuiriam um grau de maturidade elevado em relação à transferência internacional de dados por conta de já possuírem normas corporativas globais aprovadas pela ANPD. Os riscos estariam associados ao fato de que os parâmetros que possam ter sido considerados para aprovação das Normas Corporativas Globais sejam de natureza interna ou relacionados ao volume e tipos de dados o que poderia não conferir a mesma segurança em relação à uma transferência para outra organização.","174372":"Sim. Vide exemplos adotados pelo ICO.","174373":"O direito de oposição caso o titular julgue que a alteração configura alguma ilegalidade ou mesmo o direito de informação caso entenda que as informações não foram suficientes para compreender os riscos e impactos. Sempre que essa alteração demandar uma ação específica do titular como no caso do consentimento.","174375":"Entendemos que as melhores alternativas seriam os acordos multilaterais e a cooperação internacional, haja vista que estas hipóteses trariam soluções mais estruturadas e aderentes à dinamicidade que a matéria demanda. A criação de um fórum internacional que tenha como objetivo discutir e equacionar interesses divergentes na transferência internacional de dados pessoais, inclusive uniformizando a interpretação sobre as respectivas legislações domésticas, pode constituir um passo importante para a geração de acordos multilaterais ou para o início da cooperação entre Autoridades.","174376":"As melhores alternativas seriam a homologação de políticas e/ou cláusulas contratuais padrão.","174378":"Entendemos que as melhores alternativas também nessa hipótese seriam os acordos multilaterais e a cooperação internacional, haja vista que estas hipóteses trariam soluções mais estruturadas para a resolução de questões envolvendo a exequibilidade de decisões quanto a agentes de tratamento não alcançados jurisdicionalmente com base na legislação vigente.","174379":"Em relação às determinações administrativas de autoridades e/ou organismos internacionais, considerando as outras competências já estabelecidas para a ANPD (vide art. 55, XX), entendemos que uma solução para essas hipóteses seria a alteração da LGPD para incluir a competência para a ANPD homologar tais determinações.","174380":"Seriam os mecanismos comumente adotados para dar transparência sobre as atividades de tratamento de dados pessoais realizadas pelo controlador, tais como, o próprio contrato (nas relações de consumo), as políticas e avisos de privacidade ou similares e as mensagens prévias ao fornecimento de dados cadastrais no próprio sitio eletrônico. Essas comunicações devem ser atualizadas junto ao titular toda vez que houver alguma modificação dos parâmetros inicialmente informados relacionados à transferência internacional. Como mecanismos para garantir a proteção dos direitos dos titulares podemos citar aqueles inerentes à Prestação de Contas e à Transparência.

Contribuinte: Marcos Roberto Oliveira de Souza

Número: OP-183072

Data: 29/06/2022 - 12:50

Resumo: :"Breve introdução: A INTERFARMA é uma entidade sem fins lucrativos fundada em 1990, que congrega as indústrias farmacêuticas de pesquisa instaladas no Brasil, dedicadas à atividade da indústria de produtos de pesquisa para fins farmacêuticos (insumos, matérias primas, medicamentos e correlatos). Reúne cerca de 50 associadas que representam quase 50% (cinquenta por cento) do mercado brasileiro varejista de medicamentos e são responsáveis por promover o ciclo virtuoso de pesquisa e desenvolvimento de medicamentos inovadores. Dado que nossas associadas operam em diversos outros países (localizados na Europa, América do Norte, Ásia, dentre outros), a regulamentação de transferência internacional de dados pessoais é de extrema importância para a indústria. Nesse sentido, a harmonização internacional da matéria é essencial para adequação, transparência e maior eficiência aos agentes de tratamento. Resposta ao item 1: Os atuais obstáculos são o atraso e a falta de regulamentação no Brasil. Para que o tema seja regulamentado, todavia, é essencial a harmonização com as regras já adotadas por outros países, com destaque para a Comissão Europeia. Cumpre destacar, como exemplo, que a falta de convergência entre as legislações de proteção de dados levou à invalidação dos acordos para o tratamento transfronteiriço de dados entre os EUA e a EU, do Safe Harbour e Privacy Shield, pelo Tribunal de Justiça da União Europeia, respectivamente, nos processos conhecidos como 'Schrems', em 2015 e 'Schrems II', em 2020. Essa compatibilidade com mecanismos amplamente utilizados por outros países, como é o caso das Standard Contractual Clauses (SCCs), adotadas pela Comissão Europeia em atenção ao GDPR, visam garantir a efetividade dos instrumentos de transferência internacional e evitar impactos injustificados à operação das empresas. O modelo adotado pelo Reino Unido através do adendo às SCCs da Comissão Europeia (International data transfer addendum to the European Commission's standard contractual clauses for international data transfers) pode ser uma referência interessante a ser considerada pela ANPD. O mesmo se aplica para a definição dos países considerados seguros nos termos do artigo 33, I da LGPD. Considerando a similaridade de princípios da Lei brasileira com a GDPR, é importante que a ANPD considere os mesmos critérios adotados na definição da lista de países sancionados pela União Europeia. Por fim, importante salientar a necessidade de que seja conferido aos agentes de tratamento um período adequado de transição para conformidade com o novo regramento, para que as empresas tenham tempo necessário para ajustar seus mecanismos internos de transferências internacionais de dados pessoais e implementar as cláusulas publicadas pela ANPD, sem prejudicar suas operações.","174354":"A adoção de critérios semelhantes aos já adotados em outras legislações internacionais similares à LGPD, como o GDPR, se mostra como a maneira mais prática de encontrar uma interoperabilidade e convergência de requisitos e padrões de regras. A falta de harmonização com as SCCs europeias pode complicar e prejudicar, inclusive, a aprovação do Brasil como um país adequado. Importante que o processo de definição de Cláusulas Contratuais Padrão passe por um processo amplo e participativo, com a disponibilização do conteúdo para consulta pública. O recebimento de contribuições focadas para setores específicos poderia se mostrar bastante efetivo, principalmente diante da experiência de algumas empresas nesse contexto.","174356":"A ANPD precisa levar em consideração o caráter globalizado da economia atual, principalmente no que se refere ao uso

de serviços de armazenamento em nuvem. Nesse sentido, é preciso que a regulamentação a ser editada pela ANPD não inviabilize ou crie obstáculos desnecessários para as empresas, em especial aquelas que tenham atuação internacional. Os instrumentos mais efetivos são (i) cláusulas-padrão contratuais (art. 33, II, "b", LGPD); garantem níveis adequados de segurança aos agentes de tratamento e aos titulares dos dados pessoais, e estabelecem certo nível de uniformidade/interoperabilidade com relação aos critérios exigidos dos receptores de dados localizados em outras jurisdições; e (ii) normas corporativas globais (art. 33, II, "b", LGPD), como as utilizadas por países sob a jurisdição do GDPR (Binding Corporate Rules - BCRs), que estabelecem um conjunto de princípios que regem a transferência internacional de dados pessoais da União Europeia para afiliadas de uma organização localizadas em outros países em conformidade com leis de proteção de dados pessoais da União Europeia. ","174359":"Cada vez mais operações de negócios exigem o uso de sistemas globais de administração de dados e modelos de serviço compartilhados, bem como o uso de novas tecnologias para atuar com eficiência. Esse desenvolvimento levou ao aumento da mobilidade e acessibilidade de informações pessoais globalmente. O Brasil hospeda diversas empresas multinacionais que precisam transferir um alto volume de dados pessoais dentro de seus grupos para viabilizar a operacionalização de seus negócios, portanto, a transferência de dados pessoais intra grupo por meio de normas corporativas globais apresenta um papel relevante.","174360":"Para as cláusulas-padrão contratuais, é preciso que a ANPD leve em consideração requisitos e modelos já amplamente adotados pelos demais países, evitando-se a criação de um modelo muito particular, com condições operacionais específicas, que não se assemelhe com outras legislações e dificulte a implementação/negociação. As regras previstas nas cláusulas devem buscar a proteção do titular e de seus dados, sem que isso implique em um fardo desproporcional e injustificado nas empresas, o que poderia desestimular a inovação e desenvolvimento de novas tecnologias e modelos de negócio, em benefício dos titulares. No que se refere as cláusulas contratuais específicas, devem ser elaboradas de forma a cobrir os principais riscos operacionais de um tratamento de dados específico, conforme riscos identificados no mapeamento da atividade. Para as normas corporativas globais, deveriam ser definidos critérios mínimos, tais como: obrigações das entidades do grupo que forem atuar como controladoras de dados pessoais, obrigações das entidades do grupo que forem atuar como operadoras de dados pessoais, compromisso do grupo em fornecer treinamentos internos sobre privacidade e proteção de dados pessoais, criar um grupo independente / comitê que será responsável por fornecer orientações, incentivar os treinamentos e promover conscientização sobre privacidade e proteção de dados pessoais dentro do grupo de empresas, ter um programa de monitoria e auditoria dos processos relacionados ao programa de privacidade e proteção de dados pessoais, para garantir o cumprimento dos mesmos pelo grupo e como serão executados os direitos dos titulares de dados pessoais e dada a devida transparência aos titulares.","174361":"Ambos devem ser analisados e considerados com base em uma análise principiológica. Ou seja, com foco nos objetivos principais e sem se ater a detalhes ou condições de ordem muito operacional. Ademais, não deve haver uma diferenciação de cláusulas contratuais padrão em função do país de destino dos dados.","174362":"A regulamentação deve permitir certa flexibilidade em relação ao texto das cláusulas para que as partes possam realizar eventuais

ajustes necessários em vista do caso concreto, desde que tais alterações não comprometam o nível de proteção garantido pelo texto original. Desse modo, é possível eliminar eventuais entraves comerciais e restrições à inovação.","174363":"Para facilitar a adoção, a publicação das cláusulas deve ser acompanhada de material de orientação, que guie os agentes de tratamento na sua aplicação. Nesse sentido, as empresas deverão ter liberdade na adoção das ferramentas que melhor lhes atendam para a implementação das cláusulas. Arvores de decisão estipulando o instrumento que pode ser mais adequado para cada tipo de transferência, aliado a cláusulas padrões mínimos, também podem ser eficazes nesse momento. Por exemplo, para transferências internacionais entre empresas do mesmo grupo econômico, o uso de normas corporativas globais (BCRs); caso a transferência seja feita para um país já estipulado como seguro pela ANPD, o uso de cláusula simples exigindo o cumprimento dos requisitos locais de proteção de dados para os dados pessoais a serem transacionados; e, caso a transferência seja feita para um país não seguro, a utilização de normas padrão pré-aprovadas que garantam os princípios básicos da LGPD (segurança, necessidade, finalidade, adequação, transparência, não discriminação, etc.). É importante que essas ferramentas sejam válidas por um prazo transicional razoável, para que as empresas tenham tempo necessário para ajustar seus mecanismos internos de transferências internacionais de dados pessoais e implementar as cláusulas publicadas pela ANPD, sem prejudicar suas operações. Da mesma forma, a Information Commissioner's Office - ICO e a Comissão Europeia já concederam prazos transicionais para que os agentes de tratamento pudessem rever seus arranjos contratuais e seus mecanismos de transferência internacional, sem incorrer em desconformidade com as leis de proteção de dados pessoais aplicáveis. Outro exemplo que pode ser citado é a UK Addendum que determina os mecanismos de dados pessoais transfronteiriços. (fonte: New UK Standard Contractual Clauses for Personal Data Transfer: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/whats-new/)","174364":"Com relação ao modelo de cláusulas-padrão contratuais para transferências internacionais de dados, entendemos que a ANPD poderia se valer de uma divisão em módulos, conforme proposto pela Comissão Europeia, acomodando diferentes cenários de transferências internacionais de dados pessoais, quais sejam: (i) controlador para controlador; (ii) controlador para operador; (iii) operador para operador; e (iv) operador para controlador. Ainda, a utilização de ferramentas como árvores de decisão, formulários e checkboxes pode ser interessante para que os agentes de tratamento verifiquem a necessidade de aplicação de mecanismos de transferência internacional de dados pessoais – incluindo, neste ponto, a eventual adoção de cláusulas-padrão contratuais como mecanismo aplicável. ","174367":"Sim. Algumas sugestões de requisitos a serem incluídos são: • Previsão de que Normas Corporativas já assinadas por empresas podem ser acatadas para fins da legislação brasileira, desde que consoantes aos requisitos mínimos exigidos pelas normas corporativas brasileiras e que devidamente traduzidas em idioma português e publicadas localmente. •Descrição da estrutura de Proteção de Dados capaz de garantir o cumprimento dos requisitos estipulados nas normas nos diversos países; • Condições mínimas para a contratação de processadores de dados nas diferentes entidades da organização; • Protocolo de Auditoria nas diferentes entidades da organização; e • Processo de Requisição para cobrir solicitações de titulares de dados

nas diferentes entidades da organização.","174368":"Empresas controladas, controladoras (direta ou indiretamente) ou sob controle comum.","174369":"Para permitir a análise da conformidade pela ANPD das informações mínimas sobre os dados pessoais para transferências internacionais, a UK GDPR traz uma lista de requerimentos documentais que poderiam servir de base para análise (disponível no site da autoridade do Reino Unido (ICO): https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/documentation/). Além disto há formulários para coleta dos dados pessoais por parte dos controladores e processadores (Vide, por exemplo, os modelos disponibilizados pelo ICO: https://ico.org.uk/media/for-organisations/documents/2172936/gdpr-documentation-processor-template.xlsx; https://ico.org.uk/media/for-organisations/documents/2172936/gdpr-documentation-processor-template.xlsx).","174371":"Como benefícios da transferência internacional de dados entre grupos econômicos distintos com normas corporativas globais aprovada pela ANPD, destaca-se a Garantia de nível adequado e agilidade das transações e negociação. O risco seria a falta de controle quanto ao uso dos mesmos padrões no que diz respeito ao tratamento de dados pessoais.","174372":"Sim. A Comissão Europeia de Proteção de Dados disponibiliza, em seu site, todas as normas corporativas globais aprovadas e as respectivas empresas (disponível em: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_en), bem como as cláusulas-padrão contratuais (Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en).","174373":"Seguindo o princípio da transparência, os titulares devem ter direito a informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados, inclusive no que diz respeito a transferências internacionais. Para tanto, os controladores devem manter as informações a respeito da transferência internacional sempre atualizadas e facilmente acessíveis (na política de privacidade, por exemplo) aos titulares. Entendemos que os controladores deverão comunicar os titulares nos casos em que alterações impactem substancialmente o exercício de seus direitos ou, ainda, caso algum dos países constantes das normas corporativas seja sancionado pela ANPD.","174375":"As partes (agente exportador e agente importador) devem ter liberdade em relação à escolha para a forma de resolução de conflitos, sendo permitida, inclusive, a adoção de arbitragem, caso assim entendam adequado.","174376":"","174378":"","174379":"Deve ser atribuída ao importador e ao exportador o dever de comprovar o respeito a condições mínimas de proteção aos dados pessoas, condizentes àquelas predispostas na LGPD, incluindo: • estar em um país que contém o mesmo nível de proteção de dados pessoais (conforme designação da ANPD); ou • assinar cláusulas padrão para transferência internacional, conforme cláusulas padrão emitidas pela ANPD.","174380":"Por meio de informação constante de Aviso de Privacidade, bem como do website das instituições que realizam tais transferências de dados pessoais. Na notificação ao titular, deverá ser informado como funcionará a árvore de decisão para o caso de transferências internacionais, incluindo: • Se haverá transferência internacional; • Se sim, para quais países; • Se a transferência se der para um país classificado como seguro pela ANPD, informar isso na referida notificação de titular de dados; • Se houver transferência entre empresas do mesmo grupo econômico, informar se há normas

corporativas em vigor e onde encontrá-las e/ou se estes países são considerados seguros pela ANPD; • Se a transferência se der com outros agentes, informar que serão assinadas as cláusulas padrão de proteção de dados com esses parceiros/fornecedores.

Contribuinte: JESSICA RIBEIRO FERREIRA

Número: OP-183076

Data: 29/06/2022 - 13:16

Resumo: :"A Associação Brasileira de Crédito Digital (“ABCD”), com sede na cidade de São Paulo, representa as principais fintechs de crédito em funcionamento no Brasil. A ABCD e seus membros buscam impactar positivamente a economia e a sociedade brasileira por intermédio do desenvolvimento sustentável do setor de crédito, utilizando o poder de novas tecnologias e permitindo produtos mais adequados à realidade dos consumidores brasileiros, incluindo ofertas melhores e variadas de serviços e preços. Os membros da ABCD acreditam em um ambiente de crédito mais inclusivo e eficiente no Brasil. Por meio desta Tomada de Subsídios n. 2/2022, a ABCD vem apresentar suas contribuições ao tema da transferência internacional de dados pessoais. 1. Principais obstáculos atualmente para que as empresas transfiram dados de outros países para o Brasil Em relação à primeira pergunta, os principais obstáculos atualmente para que as empresas transfiram dados de outros países para o Brasil envolvem, majoritariamente, custos de transferência, falta de condições operacionais para a implementação, e a existência de sistemas de proteção de dados lacunosos ou com disposições desproporcionais, obrigatórias e pouco flexíveis para a transferência internacional de dados pessoais, imputando a qualquer agente econômico, independentemente do seu porte e da natureza do tratamento realizado pelo importador, as mesmas obrigações regulatórias. Tais regulações acabam por não equalizar a proteção de dados com o desenvolvimento econômico, incentivos à inovação no país e acesso à tecnologia independentemente do seu local de origem, impondo barreiras ao fluxo de dados e ao desenvolvimento tecnológico dos países, especialmente para empresas entrantes. No cenário atual, há a exigência de cláusulas muito gravosas para todos os agentes de tratamentos, impondo obrigações de difícil aplicabilidade prática, especialmente quando avaliados os diferentes portes de agentes de tratamento. Por exemplo, as cláusulas-padrão contratuais europeias (“SCCs”) estabelecem um conjunto tão amplo de termos de proteção de dados que é quase inevitável que, entre as partes, haja conflito entre os termos das cláusulas-padrão contratuais com alguns dos termos de proteção de dados acordados comercialmente. Ainda, quando surgem conflitos, as cláusulas-padrão estabelecem que elas prevalecerão sobre o contrato das partes, o que na prática pode ser difícil de ser realizado (vide Cláusula 5 da Decisão de Execução (UE) 2021-914 da Comissão de 4 de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016-679 do Parlamento Europeu e do Conselho). Ademais, as cláusulas-padrão contratuais incluem requisitos para que um exportador de dados notifique sua autoridade competente caso um importador de dados informe que pode não ser capaz de cumprir com o referido mecanismo (vide Considerando 21 - Decisão de Execução (UE) 2021-914 da Comissão de 4

de junho de 2021, relativa às cláusulas contratuais-tipo aplicáveis à transferência de dados pessoais para países terceiros nos termos do Regulamento (UE) 2016-679 do Parlamento Europeu e do Conselho). Esta exigência de que o exportador informe a autoridade competente se aplica tanto se (i) o exportador decidir continuar a transferência após ter tomado as medidas apropriadas com o importador de dados para remediar a questão; quanto se (ii) o exportador decidir suspender a transferência - o que provavelmente desencorajará os importadores de informar aos exportadores sobre quaisquer problemas. Há, ainda, uma evidente desproporcionalidade regulatória quando é observada a indistinguibilidade de aplicação normativa apesar das diferenças entre porte/tamanho de empresas, bem como da natureza do tratamento realizado pelo importador. Além disso, a não-participação do Brasil em organismos internacionais, como a Organização para a Cooperação e Desenvolvimento Econômico ("OCDE") (seguindo recomendações sobre transferência internacional de dados pessoais, como a disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188), bem como a falta de acordos internacionais do Brasil com outras jurisdições, por exemplo, também acaba afetando a possibilidade de transferência de dados de outros países para o Brasil. No cenário atual, o Brasil acaba por não fornecer segurança jurídica para outros países, mesmo que o país estrangeiro possua regime de proteção de dados adequado à LGPD. Por fim, a duplicidade de obrigações em caso de transferência internacional de dados pessoais. Isso porque, tomando o exemplo do Brasil, a depender da definição de transferência internacional de dados pessoais, o agente de tratamento importador estaria obrigado a cumprir a LGPD (aplicação extraterritorial da lei prevista no art. 3º) e estaria sujeito a obrigações adicionais previstas em mecanismos de transferência internacional. Um bom exemplo onde essa duplicidade não acontece é a Nova Zelândia, que não incluiu na sua definição de transferência internacional de dados, os casos nos quais a lei se aplica de maneira extraterritorial. 2. Principais obstáculos atualmente para que as empresas transfiram dados pessoais do Brasil para outros países Já na transferência de dados pessoais do Brasil para outros países, os principais obstáculos, além dos já mencionados acima, são: (i) a ausência de reconhecimento do Brasil como um país considerado adequado para a transferência internacional dados por outras jurisdições; bem como (ii) a insegurança jurídica trazida pela ausência de perspectiva sobre qual será a abordagem regulatória a ser adotada pela r. ANPD. A ausência de perspectiva sobre qual será a abordagem regulatória a ser adotada pela r. ANPD traz insegurança jurídica em relação à adoção de regulamentação porque poderia ser um entrave ao desenvolvimento econômico e ao acesso à inovação e tecnologia. Importante reforçar que o art. 2º da LGPD estabelece que a disciplina da proteção de dados pessoais tem como fundamentos o desenvolvimento econômico e tecnológico e a inovação (inciso V), bem como a livre iniciativa e a livre concorrência (inciso VI). O atual cenário brasileiro, especialmente devida à ausência de reconhecimento do Brasil como país adequado para a transferência internacional dado por outras jurisdições, coloca as empresas brasileiras na condição inevitável de assinarem os termos adequados a outras jurisdições, impostos em modelos pré-determinados à legislação de países estrangeiros. Majoritariamente, tal assinatura ocorre sem a possibilidade de negociar os termos contratuais – especialmente quando se trata de prestadores de serviço estrangeiros que disponibilizam apenas contrato por adesão. Inclusive, muitos desses prestadores de serviço internacionais imputam às empresas

brasileiras quaisquer obrigações regulatórias. Por isso, é importante que a ANPD traga salvaguardas para equilibrar essas relações contratuais. Sob o aspecto concorrencial, seria importante a existência de instruções da ANPD, para fomentar a negociação contratual e uma viabilização concreta para negociação de cláusulas contratuais. Uma vez que considerada a diversidade de porte/tamanho dos entes regulados, deveria ser reconhecida a necessidade de haver tratamento diferenciado entre os entes, ainda que tais entes não se enquadrem na classificação de agentes de tratamento de pequeno porte determinada pela ANPD. Há também a perspectiva de entes já regulados por setores específicos, como o setor financeiro, em que a transferência internacional de dados pessoais (representada por processamento relevante de dados) já está regulamentada nas Resoluções n. 4.983/2021 do Conselho Monetário Nacional (aplicável a instituições financeiras) e n. 85/2021 do Banco Central do Brasil ("BACEN") (aplicável a instituições de pagamento). Tais regulamentações exigem que, no caso de os dados serem processados em outro país que não o Brasil, deve-se verificar se o país importador possui convênio com o BACEN e, em caso negativo, requerer a autorização do BACEN. Em setores não regulados (mercados digitais em geral) que não possuem quaisquer regulações ou supervisão por autoridades reguladoras, seria importante que a ANPD informasse diretrizes para empresas que contratam nesses mercados em posição de desvantagem comercial, como já ressaltado. O Código Civil e a Lei de Liberdade Econômica, por exemplo, preconizam a liberdade das partes em contratar sempre que as disposições contratuais não violem a legislação brasileira. Ou seja, os agentes de tratamento deveriam possuir liberdade contratual, desde que os direitos e obrigações contratados não violem as disposições da LGPD. Lembramos que os principais desafios e barreiras enfrentados pelas fintechs na adequação de suas atividades à LGPD são justamente os já citados (i) elevado investimento em recursos temporais, humanos e financeiros para a adequação aos padrões legais; e (ii) a possível concorrência entre a LGPD e demais regulações, em especial as regulações impostas às Instituições Financeiras, Instituições de Pagamento e demais entidades reguladas pelo Banco Central do Brasil. Portanto, quando se exige, de fintechs o mesmo rigor, celeridade e investimento de recursos (mesmo em termos proporcionais) que se exige de grandes atores já consolidados no mercado, o resultado é a imposição de barreiras para o crescimento e desenvolvimento das fintechs. Como mencionado, as fintechs almejam democratizar o acesso a serviços financeiros, levando produtos e serviços àqueles que, em regra, não fazem (ou não faziam) parte do público-alvo das grandes instituições. Dessa maneira, criar barreiras e obstáculos cujo nível de rigor impossibilita o surgimento e desenvolvimento de fintechs é, de maneira indireta, privar determinados consumidores de produtos e serviços inovadores aos quais eles não teriam acesso em outras circunstâncias.","174354":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] A melhor maneira atualmente de promover convergência e interoperabilidade entre os instrumentos contratuais de transferências internacionais de dados com os de outras jurisdições vêm se mostrando por meio de: (i) reconhecimento de adequação de outras jurisdições emitido pela autoridade de proteção de dados do país ("Decisões de Adequação") - conforme melhor descrito na resposta à pergunta 3; (ii) acordos de cooperação internacionais; (iii) observação a requisitos de proteção de dados e segurança da informação normalmente exigidos por certificações com validade internacional; e (iv)

ações informativas/educativas realizadas pela autoridade. (i) Decisões de Adequação As Decisões de Adequação, como mais bem explicado na resposta à pergunta 3, possibilitam a convergência e interoperabilidade da transferência uma vez que a própria autoridade reconhece a proteção de dados existente no país do importador. (ii) Acordos de cooperação internacionais. Internacionalmente, as autoridades poderiam caminhar para a identificação de melhores práticas adotadas em comum, ao redor do mundo, bem como para a identificação de princípios aplicáveis à proteção dados. Isto favoreceria a publicação de guias exemplificativos (e não-vinculantes) para orientação dos regulados. Por exemplo, o Office of the Privacy Commissioner da Nova Zelândia, emitiu documento comentado, por cláusula, sobre o direito que busca ser protegido pelo modelo fornecido pela autoridade (vide IPP 12 - Model Clauses with OPC Commentary - disponível em: https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/#TEMPLATE). Com este tipo de orientação, é mais factível que as autoridades reconheçam o racional comum que possuem em relação à proteção de dados pessoais. Ressalta-se que devem ser observadas, no diálogo internacional de autoridades, as diferenças entre governança/exigências regulatórias, especialmente os diferentes graus de maturidade dos sistemas de proteção de dados, como também os custos envolvidos (custo humano e financeiro) por cada uma (e, como consequência, os custos relativos à adequação a ambas as jurisdições envolvidas na transferência). (iii) Certificação Os requisitos normalmente exigidos por certificações, ainda que sem a concessão da certificação em si, podem ser um bom indicativo de convergência e interoperabilidade entre jurisdições. Ou seja, as certificações podem ser uma boa maneira de auxiliar o diálogo para estabelecimento de uniformização de padrões e princípios de proteção de dados. É importante notar que a certificação em si poderia ser demasiadamente custosa para determinados players. Isso porque a concessão de certificação, por se basear na padronização de medidas independentemente do segmento e porte da empresa, também pode vir a ser um entrave a determinados players dado o alto investimento à sua contratação por players de diferentes maturidades. Por isso que os requisitos para a concessão da certificação (e não a concessão da certificação, em si) podem ser um bom indicativo de exigências de segurança e proteção de dados que são comuns a nível internacional. (iv) Ações informativas educativas A r. ANPD pode auxiliar na interoperabilidade e convergência dos mecanismos internacionais emitindo publicações com orientações, modelos e guias (não-vinculativos) – conforme função da r. ANPF estabelecida no art. 55-J, especialmente no inciso XVIII, da LGPD. Dessa maneira, poderiam ser informados princípios de proteção de dados, permitindo a adequação ao racional da legislação em si. Como já mencionado no item (ii), esta prática facilita a formação de acordos de cooperação internacional. ","174356":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] Internacionalmente, observa-se que os mecanismos mais utilizados são: (i) o reconhecimento de adequação de outras jurisdições emitido pela autoridade de proteção de dados do país (“Decisões de Adequação”); bem como (ii) a utilização de modelos de cláusulas-padrão contratuais. (i) Decisões de Adequação As Decisões de Adequação ainda não foram especificamente regulamentadas pela r. ANPD, de modo que até o presente momento são inaplicáveis no Brasil. De toda forma, elas possibilitariam a transferência sem que existissem maiores custos e burocracias impostos aos

agentes regulados, já que a própria autoridade reconhece que os dados estarão suficientemente resguardados no país do importador. Por isso, esse mecanismo é eficiente para todos os portes de empresas, bem como para organizações internacionais. (ii) Modelos de cláusulas-padrão contratuais flexíveis Já os modelos das cláusulas-padrão contratuais flexíveis (que diferem das SCCs mencionadas na resposta à pergunta 1), por serem documentos que legitimam a transferência internacional de dados, ainda que entre agentes de tratamento localizados em países considerados não adequados, são amplamente utilizadas em jurisdições nas quais já foram definidas. Em tais jurisdições, as cláusulas-padrão contratuais parecem direcionar de maneira bastante efetiva os agentes de tratamento a como realizar a transferência nos limites da lei. Uma vez que flexíveis e acessíveis, os modelos de cláusulas-padrão contratuais, podem atender empresas e organizações de qualquer porte ao proporcionar grau de segurança jurídica elevado a um baixo custo, bem como ao permitir um maior grau de adaptação da empresa a esses modelos a depender da atividade, porte e uso dos dados da empresa. Demais instrumentos, como normas corporativas globais, por exemplo, não foram amplamente adotados por todos os entes regulados por diversas razões, dentre elas a inacessibilidade envolvendo custos financeiros, recursos humanos, capacidade técnica e inviabilidade de implementação considerando o tempo de análise da autoridade para aprovação do documento que regulamenta as normas corporativas globais. Como melhor mencionado na resposta à pergunta 13, por exemplo, apenas 30 grupos conseguiram a aprovação de suas Binding Corporate Rules (“BCRs”) após a promulgação da GDPR (informações disponíveis no link: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_el?page=2). ","174359":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] Dentre os principais benefícios trazidos relacionados ao tema das transferências internacionais de dados destacam-se, por meio da facilitação na comunicação entre diferentes jurisdições: (i) aumento do nível de integração do mercado global; (ii) aumento da integração de diferentes mercados, trazendo benefícios econômicos a cada um dos envolvidos; (iii) diversificação nos modelos de negócio, facilitando a prestação de serviços a nível internacional; e (iv) fomento à inovação e a novas tecnologias. Dentre os impactos e possíveis pontos de risco nos quais a regulação poderia se tornar excessivamente onerosa, elencamos os seguintes: (i) convergência e interoperabilidade com regulações já existentes; (ii) criação de novas obrigações que impliquem em elevados custos; e (iii) imposição de normas inflexíveis que inviabilizem a negociação contratual e impactem aspetos concorrenciais como competição no mercado e acesso ao mercado global. Os impactos podem significar uma barreira à entrada de novos participantes no mercado – especialmente startups e empresas emergentes, como as fintechs, que, em regra, operam com número limitado de recursos durante os primeiros anos de existência (ainda que tais startups e empresas emergentes, como as fintechs, não estejam enquadradas nas definições de agentes de tratamento de pequeno porte da ANPD), como já abordado na resposta à pergunta 1. As melhores alternativas para o endereçamento desses impactos são a adoção de critérios e/ou requisitos para a regulação de cada mecanismo de transferência internacional, conforme mencionado e mais bem explicado nas respostas à pergunta 5, quais sejam: (i) proporcionalidade do mecanismo ao porte do agente de tratamento, e à natureza do tratamento realizado pelo importador; (ii) flexibilidade por meio de modelos opcionais de

mecanismos; (iii) aplicação de mecanismos apenas quando exportador e importador atuarem ambos como controladores na relação (ou seja, desnecessidade da implementação de mecanismos de transferência internacional no caso de exportação de dados a um operador); e (iv) aplicação de mecanismos apenas quando o importador não estiver sujeito à LGPD. Por fim, uma vez que atualmente não há regulações em matéria de transferência internacional de dados no Brasil, seria fundamental que a r. ANPD desenvolvesse um regime de transição para que as empresas que já realizam transferências internacionais se adequarem à nova regulação. ","174360":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] No contexto de aplicação das associadas da ABCD, serão mencionados os critérios e/ou requisitos para: I. Mecanismos gerais (i.e., que poderiam ser aplicáveis a todos os mecanismos); e II. Normas corporativas globais. I. Mecanismos gerais (i) Proporcionalidade do mecanismo ao porte do agente de tratamento e à natureza do tratamento realizado pelo importador. Os critérios e requisitos que devem ser considerados na regulamentação dos mecanismos de transferência internacional de dados pessoais são, principalmente, o porte da empresa contratante/exportadora (principalmente para considerar o leverage de negociação que as partes possuem, mesmo que a empresa não se enquadre no conceito de agente de pequeno porte estabelecido pela r. ANPD) e o volume e natureza do serviço/de uso do dado pessoal que está envolvido na contratação - como explicado abaixo em nos tópicos I(iii) e I(iv). Por exemplo, a autoridade nacional de proteção de dados da Singapura disponibilizou em seu site documento sobre: (i) framework de gerenciamento de dados (disponível no link: https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf); e (ii) "Model-Contractual-Clauses" (modelos de cláusulas contratuais, em tradução livre) para transferência internacional de dados (disponível no link: https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf). Ambos os documentos são não-vinculantes e aplicáveis a quaisquer agentes regulados, mas estão direcionados especialmente para as pequenas e médias empresas visando à adequação de mecanismos de proteção de dados para players que são menores no mercado. Da mesma forma, os mecanismos deverão ser proporcionais de acordo com os fundamentos da LGPD – e não necessariamente de acordo com regras rígidas -, destacando-se aqui os fundamentos do desenvolvimento econômico e tecnológico e a inovação, bem como da livre iniciativa e da livre concorrência. (ii) Flexibilidade por meio de modelos opcionais de mecanismos Considerando a proporcionalidade, é fundamental que esses critérios e requisitos permitam uma regulação flexível, que pontue os princípios essenciais que devem estar presentes no contrato ao invés de estabelecer de maneira rigorosa e inegociável o que deve estar previsto em cada mecanismo. Como exemplo, a autoridade nacional de proteção de dados da Nova Zelândia disponibilizou em seu site um formulário de construção de cláusula modelo ("model clause agreement builder" em tradução livre) para servir de modelo não vinculativo para os agentes de tratamento (link disponível em https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/model-clause-agreement-builder/). Além disso, a liberdade das partes em contratar é prescrita por normas brasileiras (como o Código Civil e a Lei de Liberdade Econômica) sempre que as disposições contratuais não violem a legislação brasileira. Ou seja, os agentes de tratamento devem possuir liberdade contratual, desde que os direitos e obrigações

contratados não violem as disposições da LGPD. (iii) Aplicação de mecanismos quando exportador e importador atuarem ambos como controladores na relação O Office of the Privacy Commissioner da Nova Zelândia, em guia referente aos mecanismos de transferência internacional, estabeleceu que a transferência de dados pessoais para operadores localizados em outras jurisdições não precisaria se submeter a mecanismos de transferência internacional (Principle 12, página 3, disponível no link: https://www.privacy.org.nz/assets/New-order/Your-responsibilities/Sending-information-overseas/1.-Principle-12-Guidance-web.pdf). Isso porque o operador-importador deve agir de acordo com as instruções do controlador-exportador; ou seja, o operador-importador, por meio de sua relação contratual com o controlador-exportador, já estará sujeito às regras de proteção de dados pessoais da legislação imposta ao controlador. Em outras palavras, neste caso haveria duplicidade de regulação caso fossem exigidos mecanismos de transferência internacional de dados pessoais, visto que tais mecanismos buscariam assegurar algo que já estaria assegurado pela própria relação controlador-exportador e operador-importador. Da mesma forma, no Brasil seria possível firmar o entendimento de que, por exemplo, empresa de servidor de cloud que atue única e exclusivamente como operadora de dados para controlador situado no Brasil e sujeito à LGPD não necessitaria celebrar, adicionalmente, mecanismo de transferência internacional de dados pessoais. Isso porque o controlador será o responsável por instruir o operador em seu tratamento dos dados pessoais. Assim, uma vez que o controlador esteja sujeito à LGPD, já deverá cumprir as obrigações e deveres da LGPD e exigirá do operador o cumprimento à LGPD. (iv) Aplicação de mecanismos apenas quando o importador não estiver sujeito à LGPD O Office of the Privacy Commissioner da Nova Zelândia, em guia referente aos mecanismos de transferência internacional, estabeleceu que a transferência de dados pessoais para controladores localizados em outras jurisdições que já estivessem sujeitos à legislação de proteção de dados do exportador não precisaria se submeter a mecanismos de transferência internacional (Principle 12, página 2, disponível no link: https://www.privacy.org.nz/assets/New-order/Your-responsibilities/Sending-information-overseas/1.-Principle-12-Guidance-web.pdf). Isso porque o importador já está sujeito às regras de proteção de dados pessoais da legislação do país do exportador. Em outras palavras, neste caso haveria duplicidade de regulação caso fossem exigidos mecanismos de transferência internacional de dados pessoais, visto que tais mecanismos buscariam assegurar algo que já seria cumprido pelo importador. Da mesma forma, no Brasil seria possível firmar o entendimento de que o controlador-importador situado fora do Brasil, porém sujeito à LGPD dada a extraterritorialidade da aplicação da lei, não necessitaria celebrar, adicionalmente, mecanismo de transferência internacional de dados pessoais. (v) Verificação e/ou aprovação da ANPD provocada pelo agente de tratamento. Visando o desenvolvimento econômico e fomento à inovação e à economia brasileira, a r. ANPD poderia emitir nota informando que os agentes de tratamento que realizem transferência internacional de dados pessoais podem, desde já, celebrar os mecanismos estabelecidos no art. 33 da LGPD, sem prejuízo de que um futuro modelo não-vinculativo e/ou guia com indicação de requisitos mínimos a serem observados pelas partes seja publicado pela ANPD. Conforme disposto no artigo 35, caput e artigo 35, §2º, as normas corporativas globais quando verificadas e aprovadas, terão esses procedimentos realizados pela r. ANPD. Isso porque a redação do

artigo versa sobre a competência da ANPD em realizar tal verificação, porém não sobre a obrigatoriedade e tampouco sobre o momento em que tal verificação/aprovação seria realizada. Entendemos que um agente de tratamento poderia adotar um mecanismo de transferência e, caso tivesse interesse em verificar a sua adequação, teria a opção de submeter, à ANPD, a verificação desse mecanismo (por meio de formulário específico para a coordenação de fiscalização, por exemplo). Dessa forma, o agente poderia obter aprovação da ANPD como uma maneira de reconhecimento formal da autoridade da adequação do referido mecanismo de transferência. Caso tal verificação e/ou aprovação fosse estabelecida como procedimento prévio e necessário para a realização de transferência internacional de dados pessoais, corre-se o risco de que a proposta de regulação responsiva da ANPD se encontre prejudicada. Além disso, a necessidade de procedimento prévio não somente sobrecarrega a atividade fiscalizatória da própria r. autoridade, como também atua desfavoravelmente para o grupo de agentes que realiza o compartilhamento, funcionando como entrave à atividade econômica e atuação do grupo. II. Normas corporativas globais Para a regulamentação das normas corporativas globais, deveria ser levado em consideração as categorias de agentes aos quais tal mecanismo é aplicável, o porte do agente e a natureza do tratamento realizado pelo importador, o que poderia ser definido pela r. ANPD por meio de rol exemplificativo - vide resposta à pergunta 11). ","174361":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] Entre os elementos indicados nos incisos do art. 34 da LGPD como alternativas a serem levadas em consideração para avaliação do nível de proteção de país estrangeiro ou de organismo internacional, entendemos que nas relações privadas a r. ANPD deveria considerar o inciso III, V e VI. Em relação ao inciso III, toda a atividade de tratamento de dados pessoais deve levar em consideração a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos na LGPD. Já o inciso V também deveria ser considerado para se garantir meios institucionais de proteção aos dados pessoais. Por fim, o inciso VI abre a possibilidade de outras circunstâncias específicas serem consideradas, tais como a natureza do tratamento realizado pelo importador e a existência de regulação setorial específica aplicável como fator mitigador de risco. Uma vez que os incisos I e IV do art. 34 da LGPD são relativos à avaliação do nível de proteção de dados do país estrangeiro ou do organismo internacional, entendemos que para os instrumentos contratuais os demais incisos não seriam aplicáveis uma vez que interfeririam de forma demasiada em relações privadas – impondo, inclusive, entraves às integrações de atividades econômicas quando ocorrem em diferentes países. Apenas a título exemplificativo: (i) o inciso IV estabelece a adoção de medidas de segurança a serem previstas em regulamento, no entanto, a determinação de medidas de segurança exata em um regulamento pode rapidamente ficar desatualizada em vista das tecnologias que estão em constante desenvolvimento. Por isso, estabelecer uma determinada medida de segurança poderia, ao contrário do que se espera, vir de encontro à proteção de dados ao invés de garantir maior segurança ao titular de dados. Como já mencionado na resposta à pergunta 1, o Código Civil e a Lei de Liberdade Econômica, por exemplo, preconizam a liberdade das partes em contratar sempre que as disposições contratuais não violem a legislação brasileira. Dessa forma, a avaliação do nível de proteção de dados em instrumentos contratuais deve preservar a liberdade contratual e garantir que os direitos e obrigações contratados não violem os fundamentos e princípios da

LGPD. ","174362":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] É preferível que a regulamentação das cláusulas-padrão contratuais permita flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com o texto padrão disponibilizado. Como exemplo, citamos o modelo adotado pela autoridade de proteção de dados da Nova Zelândia (conforme apontado nas respostas às perguntas 2, 3, 5, 8 e 17), que: (i) comenta sobre quais são os princípios assegurados nos modelos de cláusulas contratuais (a autoridade comenta cláusula por cláusula sobre o direito que busca proteger); (ii) estabelece que a transferência de dados pessoais para operadores localizados em outras jurisdições não precisaria se submeter a mecanismos de transferência internacional; (iii) disponibiliza em seu site um formulário de construção de modelo de cláusula contratual, “model clause agreement builder” em tradução livre; e (iv) publica um guia determinando que a transferência de dados pessoais para agentes de tratamento localizados em outras jurisdições que já estivessem sujeitos à legislação de proteção de dados do exportador não precisariam se submeter a mecanismos de transferência internacional. Também, citamos o exemplo da Singapura (conforme mencionado na resposta à pergunta 17), que aponta, no modelo de cláusula contratual, quais cláusulas possuem conteúdo que (i) precisa estar presente em contrato; (ii) é opcional (i.e., não precisa estar presente em contrato); (iii) possui redação modular, ou seja, que pode ser adaptada pelos agentes de tratamento. O modelo de cláusula contratual, além de não-vinculante, volta-se especialmente para as pequenas e médias empresas, possuindo linguagem acessível e não mais do que um total de 9 (nove) modelos de cláusulas, as quais estão dispostas em apenas 3 (três) folhas. Um modelo muito rígido de cláusulas dificultaria a transferência de dados pelos agentes, especialmente os entrantes, gerando barreiras comerciais e restringindo a inovação, concorrência e a geração de conhecimento no Brasil. Isso porque, em um modelo rígido, qualquer alteração na cláusula-padrão contratual poderia tornar o mecanismo, para a autoridade, inefetivo. Por essa razão, entendemos que as cláusulas-padrões contratuais que impliquem em inflexibilidade não deveriam ser adotadas pela r. ANPD. Estes termos rígidos, não flexíveis, não são favoráveis aos negócios, especialmente de pequenos players, como as fintechs, que possuem um papel fundamental na democratização do crédito no Brasil e um papel de impacto e transformação no setor financeiro como um todo. Isso porque a rigidez implica em um processo mais oneroso para transferência de dados, assim como responsabilidades não equitativas para as partes. Além disso, podem até mesmo impedir que as fintechs (empresas de menor porte) não consigam contratar prestadores de serviço e/ou empresas fora do país por não aceitarem determinadas redações de cláusulas (as quais, neste modelo de termos rígidos, seriam proibidas de serem alteradas), incorrendo em todos os desafios mencionados na resposta à pergunta 1. ","174363":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] O formato mais adequado seria a disponibilização de modelos de cláusulas contratuais seguindo os critérios e/ou requisitos mencionados na resposta à pergunta 5, dentre eles o requisito e/ou critério da flexibilidade por meio de modelos opcionais de mecanismos. Um exemplo da disponibilização de modelos flexíveis foi o seguido pela autoridade nacional de proteção de dados da Singapura, que, por meio de publicação em seu próprio site oficial, providenciou guias orientativos não-vinculativos, de fácil acesso, para os agentes regulados – quais sejam, o (i) framework de gerenciamento de

dados (disponível no link: https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf); e (ii) modelos de cláusulas contratuais para transferência internacional de dados (disponível no link: https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf). Na Nova Zelândia, a autoridade nacional de proteção de dados fornece modelos de clausulas-padrão contratuais, disponibilizando um gerador de cláusulas-padrão que auxiliam aos interessados na transferência de dados, de forma personalizada, o qual disponibiliza cláusulas conforme o tipo de transferência e o tipo de tratamento. Tal modelo, acessível por meio do site da autoridade, segue formato de um formulário online de construção de cláusula-padrão contratual, "model clause agreement builder" em tradução livre (link disponível em https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/model-clause-agreement-builder/). Este tipo de modelo (formulário) poderia ser adotado pela ANPD, levando em conta que permite alguma flexibilidade nas cláusulas, mas ainda garante o cumprimento adequado dos costumes e regulamentações internacionais na matéria. Da mesma forma, árvores de decisão, como a publicada na versão n. 2 do Guia Orientativo para Definições de Agentes de Tratamento de Dados Pessoais e do Encarregado, publicado pela r. ANPD, fornecem autonomia e maturidade ao agente de tratamento para tomar ações de adequação. Além disso, estariam de acordo com a abordagem de risco regulatório adotada pela r. ANPD.
","174364":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] Inicialmente, entendemos que haveria a necessidade de se estabelecer que os mecanismos de transferência internacional de dados não precisam ser aplicáveis quando: (i) a LGPD já se aplicar ao controlador-importador; ou (ii) quando o importador atua como operador de dados pessoais. Isso porque poderia haver duplicidade de regulação caso fossem exigidos mecanismos de transferência internacional de dados pessoais nessas situações. No item (i) acima, o controlador-importador situado fora do Brasil, porém sujeito à LGPD dada a extraterritorialidade da aplicação da lei, não necessitaria celebrar, adicionalmente, mecanismo de transferência internacional de dados pessoais. Já em relação ao item (ii) acima, uma vez que o controlador já esteja sujeito às obrigações e deveres da LGPD, exigirá do operador o cumprimento à LGPD e o operador deverá agir de acordo com as instruções do controlador (isto é, de acordo com a LGPD). Tal interpretação já é adotada pelo Office of the Privacy Commissioner da Nova Zelândia, por exemplo, conforme explicado na resposta à pergunta 5. Em adição aos comentários acima, entendemos que a r. ANPD deveria estabelecer cláusulas flexíveis que sejam passíveis de serem adaptadas pelos agentes de tratamento de acordo com o porte das empresas (e consequentemente, com o poder de negociação em contratos dessas empresas) – conforme expostos na resposta à pergunta 5.","174367":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] As Normas Corporativas Globais são diferentes das cláusulas-padrão contratuais por serem mais específicas, demonstrando, além dos dados transferidos, informações sobre o grupo que compartilha dados regularmente entre si, fluxo de dados e local de decisões sobre dados. Além disso, essas Normas apenas são cabíveis para os casos de transferência internacional de dados pessoais dentro de um mesmo grupo que compartilha dados entre si (definido conforme sugestão à pergunta 11), não sendo possível a sua utilização para contratos com terceiros independentes. Por outro lado, as

cláusulas-padrão acabam por ser necessárias em relações de contratações independentes, que podem ser iniciadas e terminadas a qualquer momento e, portanto, são mais dinâmicas do que a relação de compartilhamento de dados em um grupo que compartilha dados regularmente entre si. Portanto, impõe-se a necessidade de maior flexibilidade nas cláusulas-padrão contratuais como forma de fomento aos negócios internacionais. A despeito dessa diferença, as Normas Corporativas Globais e os modelos de cláusulas contratuais deverão ter requisitos comuns que configuram informações gerais sobre o tratamento, conforme comentado na resposta à pergunta 5, quais sejam: (i) proporcionalidade do mecanismo ao porte do agente de tratamento, bem como à natureza do tratamento realizado pelo importador; (ii) flexibilidade por meio de modelos opcionais de mecanismos; (iii) aplicação de mecanismos quando exportador e importador atuarem ambos como controladores na relação; e (iv) aplicação de mecanismos apenas quando o importador não estiver sujeito à LGPD. ","174368":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] Não entendemos que deveriam ser considerados quaisquer critérios na definição de grupo econômico ou empresarial. O texto da LGPD em nenhum momento cita, tampouco define, a expressão grupo econômico ou empresarial. A LGPD também não utiliza tal conceito como condicionante à aplicação de normas corporativas globais. Por isso, entendemos que não é necessário definir conceito de grupo econômico ou empresarial para regulamentar as normas corporativas globais. Isso porque para que um agente de tratamento esteja sujeito às normas corporativas globais é necessário que tal agente tenha se manifestado formalmente para aderir ao conteúdo das normas corporativas globais. Ou seja, não cabe afirmar que as normas corporativa globais seriam aplicáveis de forma automática a todas as empresas de um grupo econômico. Pelo contrário: cabe às empresas aderentes às normas corporativas globais determinarem se estão sujeitas ou não, de maneira expressa e formal, às referidas normas através do documento escrito próprio. Por outro lado, entendemos como bastante aconselhável que a r. ANPD estabeleça rol exemplificativo das hipóteses de agentes aos quais as normas corporativas globais seriam aplicáveis, citando, por exemplo, empresas controladas, empresas controladoras, joint-ventures, dentre outros. ","174369":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] Entendemos que as informações mínimas que devem ser exigidas são relacionadas a: (i) o tipo de uso/atividade que está sendo realizada com o dado; (ii) os princípios de proteção que estão sendo cumpridos; e (iii) o devido atendimento aos direitos do titular por meio dos mecanismos respondidos na pergunta 20 – política de privacidade e canal de atendimento ao titular. A fim de se preservar os segredos comercial e industrial (conforme estabelecido no art. 55-J, inciso II, da LGPD, como competência da r. ANPD), entendemos que não deveriam ser requeridas informações que divulguem aspectos sigilosos ou que, se acessíveis a concorrente, possam gerar impactos na vantagem competitiva do detentor da informação. ","174371":"[Contribuição da Associação Brasileira de Crédito Digital (“ABCD”)] 1. Riscos O primeiro ponto sobre os riscos diz respeito a questões práticas relativas às normas corporativas globais, visto que, caso sejam reguladas de maneira rígida, poderiam se tornar inacessíveis envolvendo custos financeiros, recursos humanos, capacidade técnica e inviabilidade de implementação considerando o tempo de análise da autoridade para aprovação do documento que regulamenta as normas corporativas globais. Na União Europeia, por exemplo, de acordo

com o European Data Protection Board, apenas 30 grupos conseguiram a aprovação de suas Binding Corporate Rules ("BCRs") após a promulgação da GDPR (informações disponíveis no link: https://edpb.europa.eu/our-work-tools/accountability-tools/bcr_el?page=2), dado fatores como alto custo e backlog das autoridades. No Brasil, caso seja implementado processo como o das BCRs, tal processo corre o risco de ser custoso e demorado – a título exemplificativo, o processo das BCRs na União Europeia leva uma média de 18 (dezoito) a 24 (vinte e quatro) meses, conforme informação disponível em: https://www.arthurcox.com/knowledge/what-are-bcrs/). Há jurisdições que, neste processo, chegam a exigir um programa detalhado de conformidade e auditoria que inclui auditorias regulares ("Binding Corporate Rules: Corporate rules for data transfers within multinational companies", disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en). Outras jurisdições estabelecem que, caso haja o compartilhamento de dados de uma empresa que faz parte de um grupo para operadores que estão fora desse grupo, além da celebração da BCR precisar-se-ia celebrar cláusula-padrão contratual com esse operador (informação disponível em: https://www.technologylawdispatch.com/2022/03/global-data-transfers/so-you-have-got-bcrs-you-may-still-need-to-use-the-new-eu-sccs/). No final, caso fosse adotado esse entendimento no Brasil, ele levaria ao descrédito do uso das BCRs, uma vez que ela não resolveria a transferência internacional entre os agentes do grupo e seus operadores/suboperadores. Vale ressaltar o entendimento da ABCD de que, em caso de transferência internacional realizada com operador/suboperador, não seria necessária a celebração de instrumento contratual adicional, conforme fundamentado na resposta à pergunta 5. Por fim, o escopo das normas corporativas globais poderia não garantir transferências para terceiros que estivessem fora do grupo beneficiado pelo mecanismo. Dessa forma, transferências para terceiros teriam que ser feitas por meios alternativos às normas corporativas globais. Logo, mesmo após um processo demorado e com alto investimento, a empresa ainda teria que investir em outra ferramenta de transferência (o que pode se mostrar ainda mais custoso para todos os agentes, mas em especial para players menores, como as fintechs, ainda que não tenham sido abarcadas pela definição de agentes de pequeno porte pela r. ANPD). 2. Benefícios As normas corporativas globais possuem como benefício a possibilidade de, em vez de diversos documentos relacionados com os seus métodos de transferência de dados, utilizar apenas um único instrumento contratual para cobrir a totalidade das suas atividades de partilha de dados entre um mesmo grupo. Ou seja, as normas corporativas globais facilitam a estruturação de empresas (principalmente as de maior porte) que realizam a transferência internacional de dados pessoais ao proporcionarem clareza, consistência e segurança jurídica, bem como flexibilidade, redução de custos de conformidade e até mesmo vantagem competitiva. Ademais, harmonização interna da governança de dados poderia simplificar a relação com grupo de empresas distinto. Uma vez que, internamente, um grupo já teria simplificado a governança interna de dados e a facilitação de negociação de acordos dentro da própria empresa, haveria maior disposição de recursos (humanos, financeiros, temporais, técnicos etc.) para investir na transferência de dados com grupo composto por terceiros independentes. Ou seja, essa possibilidade beneficiaria, em uma primeira análise, para a redução dos custos para as empresas em relação

a transferências de dados. Esse fator, por sua vez, poderia levar a uma maior interação entre empresas de grupos distintos, bem como a outros benefícios indicados na resposta à pergunta 4, a saber: (i) aumento do nível de integração do mercado global; (ii) aumento da integração de diferentes mercados, trazendo benefícios econômicos a cada um dos envolvidos; (iii) diversificação nos modelos de negócio, facilitando a prestação de serviços a nível internacional; e (iv) fomento à inovação e a novas tecnologias. ","174372":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] A experiência internacional que pode servir de exemplo é a autoridade nacional da Singapura. A lei de proteção de dados da Singapura ("PDPA") estabelece que a autoridade de proteção de dados apenas precisará conceder autorização formal e escrita no caso em que excepcionar a aplicação dos requisitos legais a um agente de tratamento – Part. 7.26(2) do PDPA. Ou seja, caso o agente de tratamento cumpra com os requisitos previstos em lei, seguindo as orientações não vinculativas da autoridade que foram e emitidas por meio de guias, como comentado na resposta à pergunta 17, não seria necessária uma autorização adicional por parte da autoridade de proteção de dados. Da mesma forma, a r. ANPD poderia adotar o entendimento de que a verificação e aprovação prévia e por escrito da autoridade apenas será necessária em casos excepcionais, nos quais o cumprimento das obrigações de proteção de dados pessoais não estaria garantido nos termos da lei. Isto é, caso sejam adotados os mecanismos para transferência internacional estabelecidos pela LGPD, o nível de proteção exigido pela legislação já estaria sendo adotado e não seria necessária dupla aprovação (uma aprovação legal e outra aprovação concedida pela r. ANPD) para a realização da transferência internacional de dados pessoais. ","174373":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] Independentemente da situação, ou seja, havendo ou não alteração no formato original da transferência, os direitos do titular conforme previstos na LGPD, principalmente no art. 18, precisam ser garantidos pelo controlador (controladoria conjunta e/ou singular) – por exemplo, o direito de solicitar alterações, pedir exclusão de seus dados ou se opor à alteração da nova forma de tratamento. Os direitos do titular podem ser efetivados como citado na resposta à pergunta de n. 20, quais sejam: por meio da disponibilização (i) da política de privacidade e (ii) de canal específico para atendimento de solicitação de titular de dados. Ambas as opções estão de acordo com o princípio da transparência e do livre acesso, assegurando ao titular informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento. Por essa razão, a comunicação direta deverá ocorrer apenas em casos que a transferência for autorizada por consentimento, de acordo com o art. 33 da LGPD. Vale ressaltar que o controlador, na medida do aplicável por lei, poderá se encontrar impossibilitado de cumprir com o requisitado pelo titular como, por exemplo, situação na qual o agente de tratamento não pode eliminar os dados conforme requisitado pelo titular por conta do cumprimento de obrigação legal ou regulatória. ","174375":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] I. Entre agentes de tratamento As principais alternativas para a resolução de conflitos no caso de litígios entre agentes de tratamento seriam: a previsão contratual de (i) cláusula de eleição de foro; (ii) cláusula expressa que preveja a sujeição do importador à Autoridade Nacional de Dados ou ao Judiciário do país que está exportando os dados; ou de (iii) cláusula arbitral. II. Entre titulares e agentes de tratamento No que diz

respeito às resoluções de conflito dos titulares de dados aos agentes de tratamento, prezando pelo princípio da transparência no tratamento dos dados, é necessário que haja a disponibilização de canal de atendimento de solicitações de titulares de dados, conforme resposta à pergunta 20. Este deve ser um canal eficiente de comunicação, com informações de fácil acesso sobre o contato do agente de tratamento - e, se aplicável, de seu Encarregado de Dados. Caso a solicitação do titular perante o controlador de dados não seja atendida, o titular de dados pode ainda buscar resolução pela via administrativa, apresentando Petição de Titular perante a ANPD. III. Acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados A integração do Brasil em acordos bilaterais e multilaterais, assim como o fomento à cooperação internacional entre autoridades de proteção de dados, pode ser de grande auxílio na resolução de conflitos. Na experiência internacional, é possível haver seções específicas desses acordos que prevejam mecanismos de resolução de conflitos específicos. ","174376":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] As melhores alternativas para promover a conformidade com a regulamentação se baseiam em dois pontos: (i) elaboração de materiais educativos; e (ii) estabelecimento de período de transição. I. Materiais educativos Considerando a dificuldade de adequação às leis de proteção de dados, especialmente por parte de players menores do mercado, algumas autoridades vêm investindo em materiais educativos, voltados para pequenas e médias empresas, como é o exemplo das autoridades de proteção de dados da Nova Zelândia e da Singapura. A autoridade nacional de proteção de dados da Nova Zelândia disponibilizou em seu site um formulário de construção de cláusula-padrão contratual, "model clause agreement builder" em tradução livre, para servir de modelo não vinculativo para os agentes de tratamento (link disponível em https://www.privacy.org.nz/responsibilities/disclosing-personal-information-outside-new-zealand/model-clause-agreement-builder/). A autoridade nacional de proteção de dados da Singapura disponibilizou em seu site documento sobre: (i) framework de gerenciamento de dados (disponível no link: https://asean.org/wp-content/uploads/2021/08/ASEAN-Data-Management-Framework.pdf); e (ii) modelos de cláusulas contratuais para transferência internacional de dados (disponível no link: https://asean.org/wp-content/uploads/2021/08/ASEAN-Model-Contractual-Clauses-for-Cross-Border-Data-Flows.pdf). Ambos os documentos são não-vinculantes e aplicáveis a quaisquer agentes regulados, mas voltaram-se especialmente para as pequenas e médias empresas. II. Período de transição Como já mencionado na resposta à pergunta 4, uma vez que atualmente não há regulações em matéria de transferência internacional de dados no Brasil, seria fundamental que a r. ANPD desenvolvesse um regime de transição para que as empresas que já realizam transferências internacionais se adequarem à nova regulação. Como exemplo, temos o Information Comissioner's Office, autoridade de proteção de dados do Reino Unido, que estabeleceu um período de transição para adequação dos agentes regulados após a saída do Reino Unido do Brexit (informações disponíveis no link: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/). No caso, as cláusulas-padrão contratuais da união europeira ("SCCs") foram atualizadas e, para membros da União Europeia, poderão continuar sendo utilizadas até 2024. No Brasil, considerando o período de vacatio legis de 2 anos ao qual a LGPD foi submetida para promover uma maior

possibilidade de adequação dos agentes regulados às disposições da lei, poderia ser estabelecido igual período de duração – ou seja, período de transição de 24 (vinte e quatro) meses, para adequação dos agentes à regulamentação de transferências internacionais de dados pessoais. Isso porque os agentes de tratamento de dados não puderam se valer do período de 2 (dois) anos da vacatio legis para implementar os mecanismos de transferência internacional de dados, pois estes mecanismos ainda não haviam sido regulamentados pela r. ANPD. Dessa forma, igual período deveria ser agora concedido aos agentes de tratamento para que, com a regulamentação da r. ANPD, possam adaptar as suas atividades às novas regras. ","174378":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] Neste caso, corre-se o risco de tornar as questões práticas relacionadas à responsabilização dos atores que transferem dados internacionalmente em uma matéria que provoque não apenas o conflito de normas nacionais. A responsabilização de agentes já está regulamentada, no caso do Brasil, pelo Código Civil (título IX, arts., 927 e ss.), Código de Processo Civil, pela própria LGPD (Seção III, arts. 42 e ss.) bem como por regulações setoriais, a exemplo de regulações voltadas para o setor financeiro – que atingem as fintechs. ","174379":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] Em caso de acesso aos dados por determinação de autoridades públicas estrangeiras, há uma extrapolação da matéria estabelecida e regulada pelos mecanismos de transferência internacional de dados pessoais. Para evitar tais situações, devem ser firmadas responsabilidades entre os Estados e suas respectivas autoridades públicas por meio de, por exemplo, acordos de cooperação internacionais entre os Estados. Caso tais alternativas não sejam observadas, corre-se o risco de responsabilizar agentes de tratamento por conta de conflitos entre legislações de diferentes jurisdições, o que foge ao controle dos agentes de tratamento em si. Dessa forma, busca-se evitar a criação de uma nova esfera capaz de causar discussões entre Estados e eventualmente materializar um conflito internacional de maiores proporções. ","174380":"[Contribuição da Associação Brasileira de Crédito Digital ("ABCD")] A disponibilização, por parte do agente de tratamento, da política de privacidade é o mecanismo mais adequado para fornecer aos titulares a informação clara e relevante sobre transferência de seus dados pessoais para fora do Brasil. É importante considerar que a adoção dos mecanismos de transferências internacionais previstos na LGPD respeitará os direitos dos titulares, independentemente dos mecanismos escolhidos para realizar as transferências, uma vez que tais direitos, previstos principalmente no art. 18 da LGPD, são uma obrigação do controlador. Assim, para assegurar a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais, são mais adequados: (i) a disponibilização de canal de atendimento de solicitações de titulares de dados; (ii) o reconhecimento, da ANPD, de adequação de países ou organismos internacionais ao grau de proteção da LGPD; e (iii) cláusula no instrumento celebrado entre agentes de tratamento. I. Política de privacidade Por meio da política de privacidade, o controlador de dados pessoais fornece ao titular, em cumprimento ao art. 9º da LGPD, o acesso facilitado às informações sobre o tratamento de seus dados. Visto que a transferência dados pessoais é uma forma de tratamento, ela deve estar prevista na política de privacidade, o que é suficiente para fornecer aos titulares informação clara e relevante sobre tal tratamento. Uma vez que essa informação deve ser veiculada "forma clara, adequada e ostensiva" (art. 6º, inciso VI, da LGPD), a

disponibilização da política de privacidade no site do controlador de dados pessoais é um bom exemplo do cumprimento da LGPD, especialmente em relação ao atendimento do princípio do livre acesso. II. Canal de atendimento de solicitações de titulares de dados Por meio de um canal de atendimento específico para solicitações de titulares de dados, os princípios de transparência e de livre acesso elencados no art. 6º da LGPD asseguram a efetiva proteção de direitos dos titulares nas transferências internacionais de dados pessoais. Da mesma forma que a política de privacidade, a disponibilização do canal de atendimento no site do controlador de dados pessoais é um bom exemplo do cumprimento da LGPD, especialmente em relação ao atendimento do princípio do livre acesso. III. Reconhecimento, da ANPD, de adequação de países ou organismos internacionais ao grau de proteção da LGPD Como mencionado na resposta à pergunta 3, a decisão de adequação é o mecanismo menos burocrático, mais abrangente e acessível para a transferência internacional de dados, assegurando a efetiva proteção dos direitos dos titulares por meio do reconhecimento de que o país ou organismo internacional possui as condições necessárias para garantir tal proteção. IV. Cláusula no instrumento celebrado entre os agentes de tratamento Caso a r. ANPD não tenha reconhecido o país ou organismo internacional como adequado ao nível de proteção de dados da LGPD, os agentes de tratamento, por meio do instrumento celebrado entre si, poderiam inserir cláusula que garanta que as partes que realizem transferência internacional de dados pessoais atenderão às solicitações dos titulares.

Contribuinte: MARA REGINA GELSI DOS SANTOS

Número: OP-183087

Data: 29/06/2022 - 14:24

Resumo: :"Contribuição DPO - ABRAMGE/SINOG: Ressaltamos, em especial, a insegurança jurídica e impossibilidade de aplicação de bases legais trazidas pelo art. 33, I e II, geradas pela ausência de diretrizes quanto aos artigos 34 (definição dos países com nível de proteção adequado) e 35 (definição das SCCs, BCRs, organismos de certificação, etc). Em suma, os principais mecanismos de transferência internacional dependem de um posicionamento da ANPD, que vem se mantendo silente. Isso restringe a aplicabilidade de todas as bases legais do artigo 33, restringindo-as apenas ao (i.) consentimento, cuja aplicação prática é complexa, (ii.) autorização da ANPD, que pode prejudicar a celeridade do tratamento, (iii.) proteção à vida, hipótese menos frequentemente verificada na prática, (iv.) execução de contrato/procedimentos preliminares, desde que a pedido do titular, condicionante que prejudica a aplicação da base legal e (v.) exercício regular de direitos. A limitação prática parece dificultar a adequação das transferências internacionais e, em último grau, prejudica a operacionalização dos negócios, haja vista que a atividade não possui bases legais suficientes capazes de serem aplicadas no cenário atual. Acreditamos ser importante destacar que a transferência internacional de dados, como disposto no Art. 5º, XVI, da LGPD, resulta no uso compartilhado de dados. ","174354":"Contribuição DPO - ABRAMGE/SINOG: ainda que o GDPR exerça uma grande influência, ainda não há consenso global quanto ao assunto. Nesse contexto, a flexibilidade para lidar contratualmente

é medida que se impõe à realidade. Sugerimos que a ANPD, além de definir os países com padrão considerado adequado, disponibilize recomendações e/ou padrões mínimos a serem aplicados para transferências a países considerados não adequados, mas garantindo a discricionariedade das partes na estipulação de condições contratuais no âmbito privado. A ANPD poderia fazer um compilado mínimo de normas aceitas internacionalmente para que possamos observar / exigir ao contratar tais transferências. Entendemos que a ANPD pode atuar orientando as cláusulas contratuais aos princípios legais, sobretudo de necessidade, prevenção, segurança e finalidade. A ideia seria enxergar situações padrão e requisitos de adequação dos contratos àqueles que garantam, minimamente, a segurança das informações, a existência de finalidade para o tratamento e a transparência, sem afastar a possibilidade de que as partes acrescentem outras cláusulas ou garantias adicionais, desde que não colidam, direta ou indiretamente, com as cláusulas contratuais-padrão, e sem prejuízo dos direitos ou das liberdades fundamentais dos titulares dos dados. ","174356":"Contribuição DPO - ABRAMGE/SINOG: Tratados, pactos e contratos Internacionais estruturados que tragam maior segurança. (i.) Mais efetivos, de acordo com os trazidos pela Lei, cláusulas-padrão, definição de países que possuam nível adequado de proteção de dados, normas corporativas globais e acordos de cooperação internacional; (ii) Mais utilizados frente à impossibilidade de utilização de outros instrumentos, para os fins previstos no art. 7º, II e V. ","174359":"Contribuição DPO - ABRAMGE/SINOG: Os contratos devem ser considerados um mecanismo suficiente e adequado de proteção da privacidade, desde que exijam o cumprimento dos padrões esperados. Isto é particularmente verdadeiro quando o risco associado à transferência é baixo (ou seja, não se classificam no capítulo III da RESOLUÇÃO CD/ANPD Nº 2, DE 27 DE JANEIRO DE 2022). Os principais benefícios das transferências internacionais são a viabilização de negócios jurídicos internacionais que, por si, exigem a transferência de dados pessoais não somente de seus subscritores, como também a facilitação das operações de negócio das empresas que utilizam fornecedores estrangeiros, ampliando o rol de prestadores. Em último grau, a transferência internacional de dados viabiliza progressos na economia digital, com a utilização adequada e ampla de operações de tratamento complexas, das quais participem múltiplos importadores e exportadores de dados e que conte com cadeias de tratamento longas. ","174360":"Contribuição DPO - ABRAMGE/SINOG: A segunda opção é a mais desejável (flexibilidade em relação ao texto das cláusulas, especificando os resultados desejados e permitindo alterações desde que não conflitem com os guidelines da ANPD e da LGPD). Todavia, dentre as possibilidades de endereçamento dos mecanismos contratuais, entendemos que se destacariam: (i.) incluir a necessidade de fornecimento de informações aos titulares acerca da transferência internacional que se pretende, com referência aos direitos que lhes assistem; (ii.) incluir medidas mínimas de garantia da segurança física e digital dos dados; (iii.) incluir medidas mínimas de mitigação de incidentes; (iv.) descrição das finalidades; (v.) imposição de limite de retenção e dever de expurgo quando terminada a finalidade; (v.) possibilidade de a outra parte exigir demonstração de conformidade com os requisitos contratuais, respeitados os limites do segredo comercial. ","174361":"Contribuição DPO - ABRAMGE/SINOG: A padronização dos acordos contratuais leva a uma maior eficiência, um entendimento comum e uma adesão mais ampla. A sugestão, por parte da ANPD, para

cláusulas contratuais é útil, mas é necessária alguma flexibilidade para que as organizações negociem um acordo apropriado, com base nas distintas realidades operacionais. Ao menos os elementos principiológicos mínimos mencionados acima deveriam ser considerados para considerar o país adequado para transferências internacionais de dados.
","174362":"Contribuição DPO - ABRAMGE/SINOG: Devem permitir flexibilidade, a fim de promover a inclusão das mais diferentes realidades de negócios presentes no Brasil, em linhas das políticas de medidas de fomento ao ambiente de negócios e ao aumento da oferta de capital para investimento em empreendedorismo inovador - tais como a LEI COMPLEMENTAR Nº 182, DE 1º DE JUNHO DE 2021, o principio constitucional garantido de liberdade econômica (presente na lei federal nº 13.874/19) e o próprio fundamento da LGPD de desenvolvimento econômico e tecnológico e inovação (art. 2º, inciso V).","174363":"Contribuição DPO - ABRAMGE/SINOG: Formulários, pois é o modelo majoritamente adotado quando falamos das Standard Contractual Clauses (SCC) no âmbito da GDPR.","174364":"","174367":"","174368":"Contribuição DPO - ABRAMGE/SINOG: Segundo o CADE, a definição de grupo econômico envolve “as empresas que estejam sob controle comum, interno ou externo”. ","174369":"Contribuição DPO - ABRAMGE/SINOG: As disposições que regulam a transferência de dados pessoais precisam estar alinhadas com os princípios gerais de outros regimes internacionais de proteção de dados (como o GDPR). Além disso, as organizações precisam de flexibilidade para atender aos padrões mínimos impostos por várias jurisdições. Em termos de detalhamento mínimo, sugerimos o da natureza dos dados pessoais transferidos.
","174371":"Contribuição DPO - ABRAMGE/SINOG: Os dados pessoais devem poder fluir livremente através das fronteiras internacionais para fins comerciais, desde que sejam alcançados os princípios legais para a proteção de dados. Os riscos seriam de as necessidades específicas de negócios distintos não serem cobertas pelas normas corporativas globais, levando a um descumprimento da LGPD. ","174372":"","174373":"Contribuição DPO - ABRAMGE/SINOG: O direito de ser informado pelo controlador das mudanças na configuração da transferência global, para a reconsideração do atendimento aos seus interesses ou a remoção do consentimento, caso essa seja a base legal utilizada. A comunicação direta deve ser realizada após uma análise de riscos sobre a operação de tratamento, caso o risco seja elevado na mudança da configuração original, o titular deverá ser comunicado.","174375":"Contribuição DPO - ABRAMGE/SINOG: No que tange a relação entre os agentes de tratamento, as definições de jurisdição para resolução de conflitos seriam melhor definidas conforme conveniência das partes.","174376":"","174378":"","174379":"","174380":"Contribuição DPO - ABRAMGE/SINOG: Uma legislação clara e precisa, com transparência, que trate especificamente sobre a transferencia internacional de dados, pactos firmados com outros países que tragam maior segurança. Conscientização e divulgação sobre dados pessoais, com o objetivo de promover uma cultura de maior responsabilidade e proteção de dados.

Contribuinte: Camila Castioni Secundino

Número: OP-183096

Data: 29/06/2022 - 14:55

Resumo: :"/","174354":"/","174356":"/","174359":"/","174360":":Contribuição enviada em nome de ADP Brasil e complementada por documento enviado por email para normatizacao@anpd.gov.br: CRITÉRIOS PARA AVALIAÇÃO DAS BCRs 21. A Comissão Europeia indica que os seguintes elementos devem ser avaliados quando da aprovação ou rejeição de BCRs pela autoridade de proteção de dados: Critério Explicação Direito de petição BCRs devem prever que o titular dos dados pessoais possa peticionar contra o agente do tratamento ou seu grupo empresarial perante a autoridade de proteção de dados de seu país. Transparência Grupo empresarial deve garantir transparência aos titulares dos dados compartilhados — informando, inclusive, sobre a circulação destes dados nas afiliadas. Direitos dos titulares devem ser garantidos e informados aos titulares. Escopo de aplicação BCRs devem especificar o escopo da transferência de dados, incluindo as categorias de dados pessoais, o tipo de tratamento e suas finalidades, os titulares afetados e a identificação do(s) país(es) terceiro(s). Além disso, os canais de contato devem se facilmente acessíveis aos titulares de dados. Princípios de proteção de dados BCR analisada deve conter princípios para o tratamento de dados pessoais que reflitam os princípios presentes no GDPR (e.g. finalidade, transparência, adequação, não-discriminação, etc). Accountability Todas as filiais que recebem dados pessoais e atuam como controladoras dos dados devem ser capazes de demonstrar o cumprimento das BCRs. Solicitações de acesso por autoridades do país importador BCRs devem conter provisões sobre solicitações de acesso a dados pessoais recebidas de autoridades governamentais de países terceiros, incluindo obrigações de notificação a titulares dos dados pessoais. 22. Assim como em relação às decisões de adequação, os critérios da Comissão Europeia podem servir de base para o desenvolvimento dos critérios da ANPD — reforçando, novamente, a importância da participação multissetorial na regulamentação do mecanismo. 23. Uma recomendação adicional, fundamental no cenário brasileiro, seria associar a aprovação de BCRs às decisões de adequação de determinado país (art. 33, I) proferidas pela ANPD. Entendemos que a ANPD deve reconhecer a aprovação (ou facilitar a aprovação rápida) de BCRs que já tenham sido aprovadas por autoridades de proteção de dados de países que receberem decisão de adequação da ANPD. Isto garantiria mais dinamicidade na utilização do mecanismo e evitaria sobrecarregar a própria ANPD. 24. Por exemplo, caso a ANPD viesse a reconhecer o bloco de países da União Europeia como devidamente adequado, isso significaria que as BCRs aprovadas pela Comissão Europeia teriam trâmite acelerado na análise pela Autoridade. ","174361":"/","174362":"/","174363":"/","174364":"/","174367":":Contribuição enviada em nome de ADP Brasil e complementada por documento enviado por email para normatizacao@anpd.gov.br: A empresa deve comprovar que as políticas internas de proteção de dados resguardam todos os direitos previstos na LGPD e que contêm expressamente os princípios gerais previstos na lei. Ao lado disso, a avaliação das BCRs a partir dos critérios apresentados na resposta à pergunta 5 será suficiente.","174368":":Contribuição enviada em nome de ADP Brasil e complementada por documento enviado por email para normatizacao@anpd.gov.br: Recomendamos que a definição de grupo econômico reflita aquela presente no Art. 4(19) do GDPR: um grupo composto pela empresa que exerce o controle e pelas empresas controladas.","174369":"/","174371":":Contribuição enviada em

nome de ADP Brasil e complementada por documento enviado por email para normatizacao@anpd.gov.br: Ao aprovar as normas corporativas globais, a ANPD reconhece que as políticas internas dos grupos econômicos são adequadas e suficientes para garantir os direitos dos titulares de dados, previstos na legislação nacional. Dessa forma, ao permitir a transferência de grupos distintos, mas ambos com as normas corporativas globais aprovadas, cria-se uma melhora no ambiente de negócios, facilitando a troca de informações e dados entre as empresas, ao mesmo tempo em que se resguardam os direitos dos titulares. Quanto ao risco, este pode ser considerado minimizado ao constatar-se que há uma preocupação mútua entre os grupos de que ambos estejam atuando em conformidade com a lei.","174372":":Contribuição enviada em nome de ADP Brasil e complementada por documento enviado por email para normatizacao@anpd.gov.br: A Comissa~o Europeia de Protec¸a~o de Dados disponibiliza, em seu site, todas as normas corporativas globais aprovadas e as respectivas empresas, bem como as cla´usulas-padra~o contratuais. Tendo em vista a forte influe^ncia da legislac¸a~o europeia sobre a brasileira, elas podem servir como exemplo para a ANPD.","174373":"/","174375":"/","174376":"/","174378":"/","174379":"/","174380":"/

Contribuinte: Marcel Leonardi

Número: OP-183098

Data: 29/06/2022 - 15:32

Resumo: :"Um ponto importante a ser considerado é a definição do que pode ser considerado como transferência internacional de dados. Em determinados casos, a simples redundância dos dados para garantir sua segurança fará com que os dados transitem por diversas regiões. É necessário estabelecer casos e critérios de aplicação das normas, que devem ser genericamente estabelecidas para todos os casos, ou diferenciadas para cada caso específico a que se aplicam, de forma clara. Atualmente, as hipóteses previstas na LGPD que autorizam a transferência de dados do Brasil para outros países são limitadas. Ou dependem da manifestação da ANPD, em alguma medida; ou da existência de situação excepcional – tal como cooperação jurídica internacional entre órgãos públicos de inteligência; para a proteção da vida ou da incolumidade física do titular ou de terceiro. Para situações cotidianas, a única alternativa existente é obtenção do consentimento do titular. O Brasil ainda não está inserido e reconhecido como um destino seguro para dados. Esse reconhecimento faria com que mais empresas estivessem dispostas a transferir dados para o Brasil. A falta de regulamentação sobre transferência internacional no Brasil, atualmente se apresenta como um dos principais obstáculos tanto para transferências (i) de outros países para o Brasil; quanto (ii) do Brasil para outros países. A falta de regulamentação específica desencadeia incerteza quanto às medidas/garantias a serem adotadas para garantir a conformidade da transferência com leis de proteção de dados aplicáveis. Como consequência, é comum que cláusulas padrões gerais adotadas por autoridade de outros países sejam aplicadas de modo automático e, por vezes, que obrigações não essenciais recaiam sobre agentes de tratamento localizados no Brasil. Contribuição apresentada em nome do Comitê de Proteção de Dados da

Associação Brasileira Online to Offline (ABO2O) ","174354":"A regulação a ser elaborada pela ANPD deve seguir condições principiológicas, sem definição de cláusulas obrigatórias com textos rígidos a serem adotados amplamente por todos os participantes da cadeia de tratamento de dados. Situações específicas devem ser endereçadas de forma correspondente. A previsão principiológica de proteções e responsabilidades será favorável inclusive para aceitar os modelos mais rígidos estabelecidos por outras autoridades de proteção de dados. E também poderá ser utilizada de base para desenvolvimento de redações que sejam aceitas em diversas regiões, sem que decorra a necessidade de revisar as normas a serem estabelecidas pela ANPD. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174356":"No Brasil, o artigo 33, inciso II, da LGPD prevê a transferência de dados quando subsidiada por cláusulas contratuais específicas, cláusulas-padrão contratuais, normas corporativas globais, e selos, certificados e códigos de conduta regularmente emitidos. Dentre esses, entendemos que uma das estratégias concretas para garantir a conformidade de uma transferência internacional mais efetiva atualmente é a implementação de decisões sobre a conformidade de países a leis de proteção de dados aplicáveis, uma vez que tais decisões avaliam se o país a receber os dados pessoais possuem nível igual ou inferior ao país do exportador de dados e se serão necessárias adoção de medidas específicas. Em complemento a esta abordagem, reconhecemos que adoção de selos e certificações também será subsidiariamente relevante nesse contexto, afinal, estas estratégias facilitam a análise sobre a necessidade de cláusulas contratuais específicas mais ou menos robustas de proteção de dados, a depender (i) se a empresa possui selos e certificados ou (ii) do nível de proteção atestado por tais instrumentos . Através dos selos e certificações o próprio mercado acaba reconhecendo a qualidade de determinados selos e certificados que passam a ser mais adotados pelas empresas para demonstrar adequação com as normas de proteção de dados. Além dos selos e certificados, empresas têm adotado normas corporativas globais que abarcam o tratamento de dados respeitando diversas regras locais de onde estabeleceram suas atividades. Essas normas acabam sendo compartilhadas com fornecedores e prestadores de serviços, que assumem o compromisso de também respeitá-las. Para isso, as cláusulas contratuais são as ferramentas normalmente utilizadas para que se estabeleçam declarações, garantias e obrigações entre os contratantes. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174359":"Transferências internacionais de dados pessoais são tema de suma importância atualmente tendo em vista que o rápido desenvolvimento das tecnologias nos últimos decênios conduziu a economia global a um modelo baseado na ampla coleta e processamento de informações e dados, incluindo-se dados pessoais. Nesse sentido, tornou-se impossível restringir a criação e o processamento de dados a apenas um país, considerando-se também a escala na qual se procede o fluxo de processamento e as necessidades impostas pelo modelo atual. Com isso, mecanismos que visam a garantir a proteção de dados pessoais em transferências internacionais não apenas impactam positivamente os titulares – protegendo-lhes seus direitos básicos – como também criam salvaguardas e garantias para os diferentes atores que dependem do fluxo global de informações. Além disso, o estabelecimento de padrões para a transferência garante o fluxo seguro de dados, evitando que aspectos políticos, econômicos e/ou culturais de países ou

regiões diferentes influenciem no nível de garantias aos titulares dos dados. Especificamente no caso brasileiro, o estabelecimento de parâmetros mínimos, pela ANPD, dos instrumentos elencados no artigo 33, significaria convergência com as melhores práticas internacionais em termos de proteção de dados. Com isso, o Brasil se alinharia a países que detêm altos padrões e as empresas que aqui atuam e se utilizarem dos mecanismos previstos na LGPD (cláusulas contratuais, normas corporativas globais) e validados pela ANPD se beneficiariam. Isto porque, uma vez inserido no fluxo global de informações e dados com parâmetros robustos de proteção em transferência de dados, os atores econômicos brasileiros teriam maior acesso às tecnologias, serviços, inovações e investimentos disponíveis. Diante desse cenário apresentado, tem-se que limitações e entraves à transferência internacional de dados pela Autoridade Nacional constituiria um entrave à economia e à inovação brasileira, em si consideradas. Nesse sentido, entendemos que as regras a serem estabelecidas pela ANPD devem ser gerais e principiológicas, de forma a não conflitar com as normas de outras regiões e não inviabilizar o fluxo de informações. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174360":"a. cláusulas-padrão contratuais; As cláusulas-padrão contratuais devem conter requisitos mínimos que assegurem a proteção adequada dos dados em transferências internacionais. Considera-se que devem ser previstos conteúdos essenciais como os dados do Exportador e do Importador, a relação de dados pessoais a serem transferidos e as finalidades para tanto, as medidas de segurança a serem tomadas no âmbito da transferência (de modo específico), a relação de encarregados pelo tratamento – conteúdos que podem ser passíveis de fiscalização pela ANPD. A adoção de um documento padrão de cláusulas, sem a possibilidade de edição do conteúdo, pode ser prejudicial tanto para exportadores quanto para importadores. Por isso, sugere-se que a ANPD estabeleça meramente o conteúdo mínimo, para que as partes possam editar e adaptar as redações conforme as necessidades das transferências se impuserem, de modo que a alocação de recursos seja mais eficiente. b. cláusulas contratuais específicas; e Cláusulas contratuais específicas requerem autorização prévia da ANPD à transferência internacional de dados e devem ser utilizadas em transações específicas. Assim, sugere-se que a ANPD forneça aos Controladores e Operadores um checklist do conteúdo mínimo que deve constar nas cláusulas anteriormente à submissão para aprovação, bem como cenários e fatores a serem considerados pelos agentes para a utilização desse mecanismo antes de procederem à sua redação e submissão à Autoridade – como uma página de orientações anterior ao checklist do conteúdo. c. normas corporativas globais. Normas corporativas globais são geralmente aplicáveis a transferências internacionais de dados entre empresas pertencentes ao mesmo grupo econômico. Considerando-se que empresas que possuem políticas de privacidade e proteção de dados e governança detêm recursos humanos e financeiros, as normas corporativas globais são comumente utilizadas por organizações maiores e que, muitas vezes, têm participação em outros países. Tratando-se de transferência de dados intra-corporação, entende-se que as garantias prestadas não precisariam ser tão rígidas caso se trate de grupo econômico em conformidade com as normas corporativas globais. A fiscalização e regulamentação da ANPD, neste caso, incidiria sobre a empresa baseada no Brasil, que assumiria a responsabilidade de atender aos titulares e aos eventuais questionamentos da ANPD. Ademais, sugere-se que a ANPD apoie as práticas de

governança de dados a fim de fortalecê-las e expandi-las também para pequenas e médias empresas. Ademais, sugere-se a publicação de guias de boas práticas para agentes de tratamento que ainda não adotem boas práticas corporativas, além de recomendações específicas para a transferência de dados submetida a tais normas entre mesmo grupo econômico. Não se olvida também a competência fiscalizatória da ANPD para vigiar o cumprimento das normas e das boas práticas nas transferências de dados. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174361":"Os instrumentos contratuais são utilizados por empresas e organizações para realizarem transferências internacionais de dados pessoais para outras empresas e organizações localizadas em países que não possuem o mesmo nível de proteção de dados, como forma de manter a equivalência na proteção dos dados transferidos. Dado que são instrumentos que devem ser adequados a cada caso e cada fluxo particular, a imposição de regras restritivas poderia impor dificuldades às empresas. Isto porque as regras a serem editadas pela ANPD levaria em consideração o nível de proteção oferecido pelo país, porém os instrumentos contratuais visam a constituir um arcabouço de adequação a nível da empresa que receberá os dados – sendo dois âmbitos distintos, portanto. Assim, eventual regulamentação e fiscalização da ANPD dos instrumentos contratuais utilizados para transferências internacionais por empresas e organizações devem ser baseados meramente em recomendações. De qualquer maneira, o diálogo entre estes dois contextos pode ser benéfico para atingir os objetivos de maior flexibilidade com relação às cláusulas contratuais elaboradas e, portanto, sem a necessidade de regras tão restritivas. É importante que a definição de cláusulas contratuais considere o contexto concreto das partes envolvidas para avaliar se devem ser redigidas com maior ou menor grau de complexidade e garantias. Para tanto, é possível considerar não apenas se a contraparte conta com algum selo ou certificação, mas ainda se este agente se encontra em um país tido como mais seguro para a gestão de dados pessoais a partir da avaliação da ANPD. Em ambos os casos, quando for identificado que o nível de proteção de dados do agente estrangeiro é maior, será possível a inclusão de instrumentos contratuais menos robustos (e vice-versa). Para tanto, por exemplo, é possível que seja desenvolvido pela ANPD um conjunto de níveis de classificação para os países ou organismos estrangeiros em uma escala determinada em termos de proteção oferecida. Com essa classificação definida, a ANPD pode ainda estabelecer uma escala correspondente para as cláusulas, por exemplo, cláusulas a serem aplicadas para países de níveis mais baixos seriam diferentes e/ou mais robustas do que cláusulas para países de níveis mais altos. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174362":"Texto a ser disponibilizado deve permitir flexibilidade para adequação às transferências a serem realizadas, desde que sejam observados os critérios mínimos e as orientações de conteúdo das cláusulas. Exemplos a serem observados: cláusulas-padrão da União Europeia e da Rede Ibero-Americana de Proteção de Dados. Cláusulas-padrão formuladas pela Comissão Europeia – com a assistência do Grupo de Trabalho do Artigo 29 – são rígidas (transferências entre controlador e receptor dos dados localizado em país terceiro). Entretanto, a existência de tais cláusulas não impede que agentes de tratamento, sobretudo controladores, formulem cláusulas próprias – desde que a Autoridade de dados as aprove previamente e exista o mesmo nível de proteção que aquele

conferido pelas cláusulas padrão fornecidas pela Autoridade de Dados (Handbook on European Data Protection Law – p. 260). Contudo, essa aprovação pode demorar e burocratizar uma contratação. Assim, entendemos que não seja o melhor modelo, por mais que ele busque manter a consistência e homogeneidade regulatória. Entendemos que o mesmo poderá ser obtido pelo estabelecimento de regras gerais a serem seguidas pelas empresas para a elaboração de cláusulas próprias, que poderão evoluir ao longo do tempo. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174363":"Sugere-se que a ANPD disponibilize ferramenta de orientação geral que, inicialmente, auxilie os agentes de tratamento a entender o que são as cláusulas-padrão, como devem ser utilizadas, exemplos de situações de transferências de dados em que podem ser utilizadas e demais informações que podem ser úteis, como, por exemplo, um checklist de cláusulas que podem ser aplicáveis a um contrato (por exemplo, como realizado pelo ICO – Autoridade Reino Unido – Checklist). (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/) Após as orientações iniciais, recomenda-se que a ANPD disponibilize um modelo geral de cláusulas-padrão elaborado para servir meramente como norte aos agentes de tratamento – que não contenha cláusulas padronizadas a serem utilizadas e executadas em sua redação fiel como disponibilizada pela ANPD, mas que possa ser adaptada às necessidades das transferências realizadas e dos agentes de tratamento envolvidos. Ainda, pode ser útil a publicação de um guia com recomendações para a utilização das cláusulas-padrão (como as Recomendações emitidas pela EDPB (de medidas que suplementam ferramentas de transferência como as cláusulas-padrão da UE). (https://edpb.europa.eu/system/files/2021-06/edpb_recommendations_202001vo.2.0_supplementarymeasurestransferstools_en.pdf) (https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc/standard-contractual-clauses-international-transfers_en) Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174364":"Sim. Entre agentes de tratamento, é necessário estabelecer cenários distintos para a transferência de dados. A transferência poderá ocorrer (i) de um Operador (localizado no Brasil) para um Controlador (localizado no exterior), (ii) de um Controlador (localizado no Brasil) para um Operador (localizado no exterior), ou (iii) de um Controlador (localizado no Brasil) para outro Controlador (localizado no exterior). Nas três situações, podem se referir a agentes que são empresas partes do mesmo grupo econômico ou empresas completamente distintas. Quando (i), (ii) e (iii) se referirem a empresas integrantes do mesmo grupo econômico, independentemente de atuarem como Controlador ou Operador, entende-se que estarão sujeitas à regulamentação e fiscalização da ANPD, assumindo completamente a responsabilidade para responder aos titulares de dados, inclusive. Portanto, as regras poderão ser uniformes para esse grupo. Contudo, quando o cenário for de empresas de diferentes grupos econômicos, entende-se que: (i) quando o Controlador estiver localizado no Brasil, ele será responsável pela operação de tratamento de dados, que deverá estar adequada com a LGPD. Bastará esclarecer que mesmo nesses casos o Controlador deverá estabelecer regras para a contratação do serviço que respeitem a LGPD; (ii) quando o Controlador estiver fora

do território brasileiro, se a transferência for realizada por um Operador, caberá ao Operador determinar, na melhor medida possível, que a operação está adequada com a LGPD. Entendemos que apenas no caso do Operador ser responsável pela coleta ou produção do dado existirá uma situação de atenção especial a ser regulada pela ANPD; e (iii) quando o Controlador estiver fora do território brasileiro, se a transferência for realizada por um outro Controlador no território brasileiro, caberá ao Controlador local estabelecer cláusulas contratuais e condições que resguardem o dado e eventual competência da ANPD para fiscalização do tratamento desse dado, devendo haver coordenação entre autoridades para o estabelecimento de regras de competência territorial. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174367":"Sim. Tendo em vista que as Normas Corporativas Globais são códigos de conduta a serem seguidos por empresas de um mesmo grupo econômico ou conglomerado, elas são – em essência – políticas de privacidade e compliance com a lei de dados nacional e do país para o qual será realizada a transferência de dados. Portanto, diferem das cláusulas-padrão contratuais, visto que estas impõem obrigações específicas ao controlador e ao importador de dados pessoais, em contraste com as Normas Corporativas Globais que têm escopo de aplicação muito mais amplo em termos de "conformidade" e "adequação" à lei de dados em geral. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174368":"Normas Corporativas Globais são códigos de conduta a serem seguidos por empresas de um mesmo grupo econômico ou conglomerado, elas são – em essência – políticas de privacidade e compliance com a lei de dados nacional e do país para o qual será realizada a transferência de dados. Para a aplicação das Normas Corporativas Globais são necessários investimentos significativos de tempo e de recursos humanos e financeiros. Deste modo, entendemos que existem empresas que podem decidir se organizar em verdadeiros grupos setoriais aderentes ao mesmo conjunto de normas corporativas globais. Portanto, o critério a ser adotado deveria ser a declaração da própria empresa de que deseja aderir a determinada norma corporativa global. De qualquer maneira, pensando em uma maior integração do ordenamento jurídico e na facilidade de controle e aplicação de eventuais sanções, se o caso, é recomendável que a definição de grupo econômico/empresarial siga a definição presente em outras normas do ordenamento, como por exemplo, a existência de duas ou mais empresas atuando de forma coordenada com objetivos comuns ou com relação de subordinação entre elas. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174369":"Defende-se que, a nível de conglomerados e grupos empresariais que atendam a normas corporativas globais, estes agentes já atenderiam a níveis mínimos de conformidade para transferências internacionais que se realizarem entre as empresas do próprio grupo – portanto, não seria necessária a formalização por contratos adicionais. A empresa agente de tratamento que estiver no Brasil será a responsável por atender aos eventuais questionamentos da ANPD e manter o nível de proteção de dados ao titular (como, por exemplo, realizar a transferência com base no consentimento dele ou informá-lo da transferência, etc). Nesse contexto, entendemos que a diferenciação entre categorias de dados – dado pessoal; dado pessoal sensível; dado anonimizado, bem como informações adicionais, tais como a indicação de (i) Categorias de titulares de dados cujos dados são objeto da

transferência (crianças, adolescentes, adultos, idosos, empregados, consumidores, alunos, etc.); (ii) Tipos de relação entre os titulares de dados, o exportador e o importador (relação consumerista, relação de emprego, etc.); e da (iii) Finalidade específica com a qual os dados pessoais serão transferidos – sejam suficientes para permitir a aplicação de normas específicas e condizentes com cada espécie de dado que poderá ser compartilhado internacionalmente. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174371":"Por um lado, a aplicação de normas corporativas globais seria reforçada e encorajada a ser adotada por um maior número de empresas. Ainda, as empresas agentes de tratamento que transferirem dados com base em normas globais teriam um nível de confiança maior uma na outra para realizarem o fluxo de dados, beneficiando-se mutuamente e criando também um ambiente saudável de proteção de dados para os titulares. Em contrapartida, o principal risco relacionado à utilização de normas corporativas globais é a permissividade que tais normas podem oferecer aos agentes de tratamento, de tal modo a possibilitar transferências internacionais possivelmente excessivas. Por este motivo, é necessário garantir que as normas aprovadas sejam utilizadas de maneira moderada e sempre em observância aos requisitos necessários para a sua conformidade com a LGPD. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174372":"Quanto às normas corporativas globais, tem-se o exemplo da experiência da União Europeia, cujo modelo de adoção de normas corporativas é considerado lento e custoso – além de demandar uma excessiva quantidade de recursos por parte da própria Autoridade de Dados. Para que não haja a mesma morosidade na ANPD, sugere-se que a ANPD considere A elaboração de "padrões de análise" (por meio do desenho de "modelos de avaliação de cláusulas/normas corporativas" ou ainda com "checklists de exigências que devem ser observadas pelos agentes de tratamento"). a partir de mecanismos que prezam por uma avaliação mais direta e objetiva da Autoridade sobre os documentos que são apresentados, entende-se ser viável o desenvolvimento de análises mais céleres por parte da ANPD Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174373":"De acordo com o artigo 6º da LGPD, para que haja a transferência de dados dos titulares, os agentes de tratamento devem respeitar os princípios de finalidade, adequação, necessidade, qualidade dos dados e segurança, e demonstrarem a adoção de medidas eficazes para tanto e prestarem contas. Considerando que a LGPD não define o que seja alteração na configuração original da transferência, a transferência de dados deve assegurar que os princípios tratados no artigo 6º sejam garantidos e efetivados, e o artigo 33 da LGPD especificamente elenca as hipóteses nas quais é possível a realização de transferência de dados sem que haja a violação dos direitos dos titulares. Portanto, entendemos que o mesmo se aplique para o caso de transferência internacional de dados, ou seja, em tese, os direitos dos titulares não se alteram com a alteração da configuração original da transferência internacional. Para além destes casos, entendemos que uma eventual comunicação para os titulares (viabilizando sua eventual intervenção) a respeito de alterações na configuração original da transferência, seria necessária na hipótese em que o consentimento do titular tenha sido necessário no contexto dessa operação, seguindo a mesma racional exigida no Art. 8, §6º da LGPD). Ou seja, caso: (i) A operação de transferência internacional em si tenha sido

fundamentada no consentimento do titular; ou se (ii) Os dados pessoais coletados com base no consentimento dos titulares venham a posteriormente ser sujeitos a uma atividade de transferência internacional, independentemente do meio que legitime esta transferência Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174375":"Entre agentes de tratamento, é necessário estabelecer cenários distintos para a transferência de dados. A transferência poderá ocorrer (i) de um Operador (localizado no Brasil) para um Controlador (localizado no exterior), (ii) de um Controlador (localizado no Brasil) para um Operador (localizado no exterior), ou (iii) de um Controlador (localizado no Brasil) para outro Controlador (localizado no exterior). Nas três situações, podem se referir a agentes que são empresas partes do mesmo grupo econômico ou empresas completamente distintas. Quando (i), (ii) e (iii) se referirem a empresas integrantes do mesmo grupo econômico, independentemente de atuarem como Controlador ou Operador, entende-se que não existirá conflito entre si e que a empresa localizada no Brasil terá condições de atender os titulares de dados. Contudo, quando o cenário for de empresas de diferentes grupos econômicos, entende-se que: no cenário (i) descrito acima, o Operador será responsável por direcionar a demanda ao Controlador, que também será o responsável por atender a ANPD; no cenário (ii) o Controlador será responsável pelo atendimento de titulares e eventuais questionamentos da ANPD; e no cenário (iii) o Controlador local estará sujeito localmente à LGPD e à fiscalização da ANPD, bem como por informar o Controlador estrangeiro sobre eventual resultado desfavorável em disputa com o titular ou com a ANPD sobre tratamento de dados transferidos; porém a responsabilização do Controlador estrangeiro deverá ser estabelecida por meio de coordenação entre autoridades para o estabelecimento de regras de competência territorial. Portanto, ao se distinguir os cenários dos possíveis conflitos, as alternativas de resolução de conflitos podem ser distintas, a depender da complexidade do cenário. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174376":"Os mecanismos que legitimam a transferência internacional de dados é a melhor alternativa para promover a conformidade, e consiste na normas corporativas globais, cláusulas-padrão contratuais, cláusulas contratuais específicas, selos, certificações ou códigos de conduta, que respeitem os direitos dos titulares e assegurem o cumprimento das diretrizes e princípios estabelecidos pela LGPD. É importante que a ANPD, por meio de suas orientações, conceda prazo razoável para que os agentes de tratamento possam adequar suas relações contratuais no âmbito das transferências internacionais. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O) ","174378":"Em caso de transferências ulteriores para outras jurisdições ou em que os dados, mesmo que na mesma jurisdição, são processados por outros agentes de tratamento distintos do importador, nos parece ser adequado que tais situações sejam contempladas contratualmente entre as partes, sem, contudo, afastar o regime de responsabilidade previsto na LGPD. Novamente invocamos o exemplo da que as standard contractual clauses da União Europeia permitem essas modalidades de transferências ulteriores, sempre que o terceiro esteja sujeito às obrigações contratuais pactuadas que suportam a legitimidade da transferência internacional de dados. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline

(ABO2O) ","174379":"Entendemos que o acesso aos dados por determinação de autoridades públicas estrangeiras deve ser condicionado à existência de acordos de cooperação internacional e/ou sujeitos às regras do direito internacional. Isto porque tais situações encontram limitações relacionadas à soberania estatal cujos efeitos jurídicos da legislação nacional de um país, assim como a efetividade de sua jurisdição (ordens do Poder Judiciário) estão limitadas ao território nacional respectivo da autoridade que a proferiu. Como forma de extensão da soberania, e o consequente cumprimento da ordem fora do território nacional que a proferiu, é necessário a utilização mecanismos de cooperação internacional para produção de efeitos em países terceiros (como por exemplo, acordos internacionais, carta rogatória etc. - no Brasil, vide artigos 26 a 41 do nosso Código de Processo Civil, ou o Decreto 3.810/2001, conhecido como MLAT), ou se normas de direito internacional admitirem a aplicação extraterritorial das leis (no Brasil, vide Lei de Introdução às Normas do Direito Brasileiro). Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O)","174380":"A comunicação transparente, clara e objetiva é a melhor forma de manter os titulares de dados informados sobre a transferência internacional de seus dados pessoais para fora do Brasil. Existem diversos mecanismos por meio dos quais os agentes de tratamento podem se comunicar com os titulares, como, por exemplo, os avisos e declarações de privacidade, sem prejuízo do estabelecimento de contratos de prestação de serviços, canais de atendimento e o próprio site do agente de tratamento. Estes documentos devem conter informações claras sobre o tratamento dos dados pessoais como determina a LGPD, em especial o conteúdo de seu artigo 9, e ser aplicável tanto ao importador quanto ao exportador. Contribuição apresentada em nome do Comitê de Proteção de Dados da Associação Brasileira Online to Offline (ABO2O)

Contribuinte: Samanta Santos de Oliveira

Número: OP-183119

Data: 29/06/2022 - 18:44

Resumo: :"Ao nosso ver, o maior obstáculo hoje é a própria inexistência de regras mais específicas sobre a transferência internacional de dados, resultando em uma relação mais cautelosa/receosa do Grupo perante seus Clientes em realizar tais transferências, na medida em que desconhecem os mecanismos para tanto validados pela ANPD. Empresas estrangeiras e Clientes Nacionais que tendem a questionar o regramento brasileiro para transferência internacional, bem como as regras para armazenamento de dados fora do país. Além disso, o Brasil hoje não faz parte da lista de países adequados para importação de dados pessoais pela legislação europeia, o que também é um obstáculo para o Grupo, tornando necessária a existência de uma cláusula contratual especifica onde o Cliente afirma estar ciente e autoriza o compartilhamento de dados pessoais com as empresas integrantes do Grupo Michelin. ","174354":"Acreditamos que, como já vem sendo feito em outros casos por esta Autoridade, a ANPD deve se espelhar em outros modelos já existentes em outras jurisdições, sem necessariamente inovar na interpretação e consolidação das regras de transferência internacional, bem como utilizar da experiência das empresas que já atuam no

ramo e lidam com a situação diariamente.","174356":"Em nossa opinião, os instrumentos de maior efetividade e adoção para legitimar as transferências de dados internacionalmente hoje são as cláusulas-padrão contratuais (CPCs), dada a sua maior capacidade de uniformizar regras de proteção de dados de legislações e países diversos. Como já mencionado acima, o Grupo Michelin já utiliza esse modelo para legitimar a transferência internacional, uma vez que possui cláusula contratual com seus clientes para ciência e autorização para compartilhamento de dados pessoais com as empresas integrantes do Grupo. ","174359":"Os benefícios vão desde a inclusão do Brasil no ecossistema de transferência internacional de dados pessoais até a necessária segurança jurídica para operar e tratar dados pessoais no país. A ausência de regramento torna o Brasil um país inseguro para ser o receptor ou exportador de dados pessoais perante os demais países dentro do Grupo Michelin e seus clientes. Sendo assim, se faz necessária a utilização de modelos já existentes em outras jurisdições como base para prosseguirmos com nossos serviços. ","174360":"a. cláusulas-padrão contratuais; R: Importante definir a lei de regência do contrato (a qual, preferencialmente, deve ser a brasileira), o conceito e o conteúdo das CPCs, bem como o procedimento para elaboração e divulgação de tais cláusulas pela ANPD. b. cláusulas contratuais específicas; e R: Diferenciação entre o conceito das cláusulas contratuais específicas e as padrão, estabelecer o procedimento para aprovação de tais cláusulas pela ANPD, bem como o estabelecimento do prazo para deliberação da autoridade, o qual não deveria exceder 30 dias. c. normas corporativas globais. R: Requisitos mínimos para a formulação das normas corporativas globais, bem como o estabelecimento do prazo para deliberação da autoridade, o qual não deveria exceder 30 dias.","174361":"A Autoridade deve levar em conta todos os elementos presentes no artigo 34, com especial ênfase para os incisos: I, no sentido de exigir que o país de destino possua normas gerais e/ou setoriais na legislação em vigor que proporcionem mínima segurança ao tratamento dos dados; III, para exigir que sejam observados os princípios gerais de proteção de dados e os direitos dos titulares previstos na LGPD; IV, no sentido estabelecer medidas de segurança mínimas a serem adotadas pelo importador; e V, no sentido de exigir que o importador declare a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais.","174362":"Verifica-se a necessidade de encontrar um equilíbrio, uma vez que as cláusulas devem ser instrumentos dinâmicos e adaptáveis conforme a necessidade Além disso, entendemos pela necessidade de abertura para a indicação do objeto e da duração do tratamento de dados, bem como da sua natureza e da sua finalidade, visto que dentro do nosso Grupo existem diversas atividades que envolvem a transferência de dados e, para ser feita de uma forma segura é necessário que seja desenvolvida cláusulas específicas para regulação de cada uma delas.","174363":"A ANPD deve disponibilizar os modelos editáveis (word) de forma facilmente acessível em seu site, já preparados para cada circunstância de transferência. ","174364":"Sim, entendemos que as responsabilidades aplicáveis ao importador devem ser compatíveis com o seu papel de controlador ou operador, nos termos da LGPD, mantendo os níveis de segurança mais rígidos no caso do país importador não possuir normas para a recepção de dados no caso de uma transferência internacional.","174367":"Sim. Normas Corporativas Globais deveriam ser usados por conglomerados internacionais, e organizações menores, pelo grau de complexidade, devem continuar usando as cláusulas-padrão contratuais. Para BCRs, deve

haver toda uma auditoria de documentos e procedimentos adotados dentro de um grupo econômico para a proteção de dados. Para SCCs, há um conjunto de cláusulas pré-aprovadas pela ANPD, que é um processo muito menos complexo e mais cabível para empresas que fazem a transferências simples e bilaterais. Por outro lado, BCRs são feitas e aprovadas uma só vez. Assim, seria inviável para um grupo econômico que pratica volumosa atividade de transferências internacionais ter SCCs para cada uma delas. SCCs são self-assessment das empresas que aplicam. BCRs são aprovadas pela autoridade com base no que verifica na prática do grupo. BCRs já aprovadas em outro lugar: facilitaria caminho da ANPD. ","174368":"A existência de duas ou mais empresas, atuando de forma coordenada, com uma convenção comum, cujos objetivos e atividades estejam alinhados ou desde que haja uma relação de subordinação entre elas, inclusive em relação as empresas adquiridas posteriormente que precisam ser inseridas dentro dos mesmos preceitos. Sendo que no caso de empresas adquiridas, é possível realizar auditorias para atestar ou não o alinhamento de acordo com as normas e procedimentos. ","174369":"A Políticas de proteção de dados da empresa, o programa de governança, a lista de entidades, as diretrizes definidas para o tratamento de dados de empregados, documento de responsabilidade da matriz sobre todas as empresas do grupo, contrato intragrupo sobre o assunto. Além disso, há de se exigir a base legal em que se apoia a transferência, cláusulas contratuais específicas, cláusulas-padrão contratuais, bem como a informação do propósito/necessidade da transferência. Importante que sejam observados os princípios de proteção de dados pessoais em conformidade com o previsto na LGPD pelo país ou organismo envolvido na transferência. Cumpre evidenciar que a transferência em tela precisa ser realizada para uma finalidade específica, não se admitindo a indicação de finalidade genérica.","174371":"Temos como benefícios: a possibilidade de compartilhamento de base de dados entre Grupos Econômicos, não sendo necessário SCCs ou outro mecanismo. Como risco, podemos citar a ausência de contratos entre eles. Para BCRs, intragroup agreement é necessário. A ausência de contrato entre os Grupos Econômicos e falta de uniformização e procedimento pode gerar descomprometimento, pois o acordado por um pode não ser cumprido pelo outro. Isso pode acarretar na possibilidade de violação do direito e liberdade dos titulares de dados pessoais, uma vez que caso não sejam entregues medidas adequadas e satisfatórias, aumentam as chances de incidentes de segurança e por consequência eventual responsabilização por danos recorrentes da referida violação. Além disso, existe o risco de perda de reputação das Companhias envolvidas, em razão de estarem associadas a possível falha de segurança, quando da transferência de dados pessoais. Da mesma forma, podemos mencionar o risco de violação da privacidade dos dados do titular, considerando que seus dados foram expostos.","174372":"Temos um referencial Grupo sobre proteção de dados(Política de Privacidade), além de um treinamento para os empregados sobre a conscientização sobre dados pessoais. Atualmente todos os contratos novos possuem cláusulas-padrão sobre proteção de dados. Os contratos anteriores a LGPD estão sendo aditados com a inclusão da cláusula padrão de proteção de dados pessoais. Atualmente, na Europa, o processo é bastante burocrático, especialmente porque envolve aprovação das demais DPAs. Se possível, precisamos evitar esse nível de burocracia no Brasil.","174373":"Para os mecanismos de transferências internacionais, assim como todos os princípios da LGPD, devem ser garantidos os mesmos direitos dos artigos 18 a 20 aos

titulares. Por exemplo, o titular deve estar informado sobre a transferência internacional com transparência e tal atividade deve estar dentro dos propósitos legítimos (finalidade), assim como deve conseguir obter informações sobre o compartilhamento de seus dados pessoais e revogar seu consentimento quanto à transferência internacional de dados, se essa foi a base legal que justificou a atividade. Ademais, é imprescindível a comunicação direta aos titulares de dados pessoais em caso de qualquer incidente de vazamento.","174375":"Nesses casos é possível a execução de instrumentos contratuais de transferência internacional / tratamento de dados pessoais, celebração de composição onde as partes comprometem-se a adotarem mecanismos previstos na LGPD (acordos extrajudiciais, podendo ser através da criação de um núcleo específico junto à ANPD) e como última medida, em caso de impossibilidade de resolução amigável do conflito, o ajuizamento de Ação Judicial. Ex: Prática adotada pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), que instituiu, em 30 de setembro de 2010, o Sistema Administrativo de Conflitos de Internet (SACI-Adm), que nada mais é do que um procedimento conduzido por instituições previamente aprovadas pelo NIC.br. Segundo modelo atualmente adotado pelo NIC.br há três instituições credenciadas pelo NIC.br para processar e decidir controvérsias do SACI-Adm: a Associação Brasileira da Propriedade Intelectual (ABPI), a Câmara de Comércio Brasil Canadá (CCBC) e a Organização Mundial da Propriedade Intelectual (OMPI ou WIPO), que, na qualidade de provedoras do serviço de resolução administrativa de disputas, devem aplicar seus respectivos regulamentos aprovados pelo NIC.br, que estarão sempre em consonância com o regulamento geral próprio do SACI-Adm. Acredita-se que a adoção de tal mecanismo se mostrará bastante útil na resolução de conflitos envolvendo instrumentos contratuais de transferência internacional de dados. Além disso, em razão do tema, acordos bilaterais, multilaterais ou a cooperação internacional entre autoridades de proteção de dados podem auxiliar na resolução de tais conflitos, em especial com autoridades que já possuem reconhecida experiência na matéria, visto que poderiam contribuir com exemplos e casos práticos já enfrentados, para a resolução dos conflitos.","174376":"Para promover a conformidade com a regulamentação, algumas medidas podem ser tomadas : Do ponto de vista contratual, possuir Termos de Cooperação, cláusulas-padrão contratuais robustas e cláusulas contratuais específicas. Do ponto de vista operacional, implementar medidas de segurança e procedimentos técnicos para garantir a proteção de dados pessoais contra qualquer tipo de violação. Inclusive, com base em experiências já adotadas na União Europeia –, é possível promover: Pedidos de informação: o importador de dados deve responder, rápida e adequadamente, aos pedidos de informação do exportador de dados relacionados com o tratamento objeto da transferência. Cumprimento do contrato: as partes devem poder demonstrar o cumprimento das presentes cláusulas contratuais. Em particular, o importador de dados deve conservar documentação adequada sobre as atividades de tratamento realizadas por conta do exportador de dados. Disponibilização de informações e auditoria: o importador de dados deve disponibilizar ao exportador de dados todas as informações necessárias para demonstrar o cumprimento das obrigações previstas nas presentes cláusulas e, a pedido deste último, facilitar e contribuir para as auditorias das operações de tratamento abrangidas pelas presentes cláusulas, a intervalos razoáveis ou se houver indícios de incumprimento. Ao decidir sobre uma revisão ou auditoria, o exportador

de dados pode ter em conta as certificações pertinentes detidas pelo importador de dados. Auditorias: o exportador de dados pode optar por realizar a auditoria ou contratar um auditor independente. As auditorias podem incluir inspeções nos edifícios ou nas instalações físicas do importador de dados, devendo, se for caso disso, ser realizadas com uma antecedência razoável. Comunicação à autoridade: as partes devem disponibilizar as informações necessárias, incluindo os resultados de quaisquer auditorias, à autoridade de controle competente, mediante pedido.","174378":"Algumas alternativas seriam a aplicação de multas e outras penalidades com previsão expressas nos contratos e termos de cooperação, além da legislação cabível nos países envolvidos, podendo ainda os contratos contemplarem lucros cessantes, danos indiretos e outros de mesma natureza. Além disso, como a LGPD foi ampla e fortemente inspirada na legislação europeia, algumas práticas já utilizadas sob o contexto do GDPR podem ser úteis, inclusive com o intuito de trazer certa harmonização entre as práticas, dado que o Brasil possui grande relação comercial com o bloco europeu. Assim, seguem alguns exemplos: Instruções do exportador: O importador de dados só deve divulgar os dados pessoais a terceiros mediante instruções documentadas do exportador de dados. Divulgação dos dados: os dados só podem ser divulgados a terceiros localizados fora do Brasil (no mesmo país que o importador de dados ou em outro país terceiro, a seguir designado como "transferência ulterior") se o terceiro estiver ou aceitar estar vinculado as respectivas cláusulas contratuais das quais o importador se obrigou, ao abrigo do módulo adequado, ou, ainda, se: ¿ o destino da transferência ulterior for um país que beneficie de uma decisão de adequação (quando a ANPD emitir as decisões) que abranja tal transferência ulterior; ¿ o terceiro assegurar, de qualquer outra forma, as garantias adequadas nos termos dos artigos 33 a 36 da LGPD, no que diz respeito ao tratamento em questão, ¿ a transferência ulterior for necessária à declaração, ao exercício ou à defesa de um direito do importador num processo judicial no contexto de processos administrativos, regulamentares ou judiciais específicos, ou ¿ a transferência ulterior for necessária para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular. Cumprimento de garantias: Qualquer transferência ulterior está sujeita ao cumprimento, pelo importador de dados, de todas as outras garantias previstas nas respectivas cláusulas contratuais, em particular a limitação da finalidade.","174379":"O exportador somente poderá enviar os dados em casos previstos em lei/instrumentos de direito internacional ou autorizados pela ANPD. Ademais, deve garantir o envio dos dados criptografados ou anonimizados, a fim de manter o nível de proteção dos mesmos. Da mesma forma, o importador deve garantir o mesmo grau de proteção adequado, conforme previsto na LGPD. Além disso, algumas práticas já adotadas no contexto do bloco europeu podem ser adotadas no Brasil, para fins de harmonização dos dois sistemas, em razão das relações comerciais/negócio existentes entre Brasil e União Europeia, tais como: •

Notificação (solicitação): Sempre que possível, o importador de dados deve notificar o exportador de dados e o titular dos dados se receber um pedido juridicamente vinculativo de uma autoridade pública (incluindo judiciária) ao abrigo da legislação do país de destino para a divulgação dos dados pessoais transferidos nos termos das cláusulas contratuais. •

Notificação (acesso): Do mesmo modo, o importador de dados deve notificar o exportador de dados e o titular dos dados se tomar conhecimento de qualquer acesso direto das autoridades públicas a tais dados pessoais, em conformidade com a legislação do

país terceiro de destino. • Impossibilidade de notificação: Se, não obstante todos os seus esforços, o importador de dados não estiver em condições de notificar o exportador de dados e/ou o titular dos dados de pedidos específicos de divulgação, deve fornecer ao exportador de dados o máximo possível de informações pertinentes sobre os pedidos. • Documentação dos pedidos: O importador de dados deve igualmente ser obrigado a documentar qualquer pedido de divulgação recebido e a resposta fornecida, e a disponibilizar essa informação ao exportador de dados ou à autoridade de controle competente, ou a ambos, mediante pedido. •Fiscalização: Se, na sequência de uma fiscalização da legalidade de tal pedido, de acordo com a legislação do país de destino, o importador de dados concluir que existem motivos razoáveis para considerar que o pedido é ilegal nos termos da legislação do país terceiro de destino, deve contestá-lo, nomeadamente, quando adequado, esgotando todas as possibilidades de recurso disponíveis. • Não cumprimento das cláusulas contratuais: Em todo o caso, se o importador de dados deixar de ter capacidade de cumprir com o quanto disposto nas cláusulas contratuais, deve informar o exportador de dados em conformidade, inclusivamente quando tal for consequência de um pedido de divulgação.","174380":"Dar publicidade sobre a natureza dos dados a serem transferidos, a finalidade e os agentes de tratamento, garantindo a criptografia ou anonimização dos dados, solicitando seu consentimento expresso e inequívoco sempre que necessário. Como instrumento para auxiliar nesse mecanismo, sugerimos a criação de formulário padrão para requerimento do consentimento, contendo todos os dados necessários ao conhecimento do titular dos dados. Um caminho possível seria trazer os requisitos mínimos que devem conter em tal comunicação, assim como o é feito no art. 9º da LGPD, para que os agentes de tratamento responsáveis escolham o melhor mecanismo, seja uma política de privacidade, um aviso de privacidade, um vídeo explicativo, etc. No que diz respeito às formas de assegurar a efetiva proteção de direitos dos titulares, entende-se que o próprio mecanismo que autoriza a transferência deve prever isso, por meio de menção explícita sobre o tema. Por fim, para implementação dos instrumentos, tudo vai depender da relação existente entre o exportador e a pessoa titular de dados em questão. Por exemplo, se for no âmbito de utilização de um aplicativo/software, por meio de pop-up's banner; se for no âmbito de uma relação de emprego, por meio de uma política ou aviso de privacidade específicos.

Contribuinte: andreia marques de almeida barbosa

Número: OP-183128

Data: 30/06/2022 - 03:12

Contribuinte: FERNANDO BOUSSO

Número: OP-183135

Data: 30/06/2022 - 05:33

Resumo: :"Confederação Nacional das Seguradoras – CNseg: Atualmente, o principal obstáculo para a realização da transferência de dados do Brasil para outros países é a ausência de regulamentação dos requisitos previstos na LGPD que devem ser atendidos para que se proceda à transferência. Com isso as empresas realizam, por conta e riscos próprios o que é necessário ser atendido para que a transferência seja realizada, gerando insegurança jurídica para todo o setor de seguros, pois não é possível aferir o grau de adequação ou inadequação ao se executar tal processo. É preciso que a ANPD estabeleça, por exemplo, (i) o procedimento para que seja requerida a avaliação do nível de proteção de dados pessoais conferido por país estrangeiro ou organismo internacional, tendo em vista que a existência de diversas normas estrangeiras sobre o tema, com peculiaridades que não são de domínio de todos, principalmente porque o controlador pode não ter segurança em saber se ao exportar dados para outro território, continuará tendo o mesmo nível de proteção que teria em território nacional; (ii) a definição do conteúdo das cláusulas-padrão contratuais; e (iii) o procedimento de verificação das cláusulas contratuais específicas para uma determinada transferência, das normas corporativas globais, dos selos, certificados e dos códigos de conduta. Além disso, a partir da experiência do setor de seguros, é primordial que a ANPD deixe claro que a transferência internacional se dá entre agentes de tratamento e não, por exemplo, entre um titular de dados e uma empresa sediada em território estrangeiro. Outra dificuldade é a falta de uniformidade do tratamento legal, que ocasiona um conflito de jurisdições e de autoridades competentes em matéria de proteção de dados pessoais. É importante que a ANPD envide esforços para estreitar relacionamento com outras autoridades de dados em outros países e observe as melhores práticas para transferência internacional. Por outro lado, os requisitos para aplicação da lei brasileira e da lei europeia, por exemplo, são coincidentes, o que implica a atração das suas legislações às mesmas situações. No entanto, gera dúvidas sobre o motivo pelo qual no Brasil, precisam ser avaliadas cláusulas contratuais ou normas corporativas aprovadas pelas autoridades europeias e não brasileiras, quando os dados saem do Brasil para serem tratados na Europa e retornam ao Brasil.
","174354":"Confederação Nacional das Seguradoras – CNseg: A maneira mais eficaz de promover a convergência e interoperabilidade entre os instrumentos contratuais de transferência internacional de dados de distintas jurisdições é torná-los similares em sua essência. Em outras palavras, para que o Brasil esteja inserido na cadeia global de fluxo de dados, deve, sem abdicar do que estabelece o seu direito interno, regulamentar a questão de transferência internacional de dados observando as melhores práticas internacionais. A ANPD poderia, por exemplo, valer-se das diretrizes da comissão europeia, que possui uma sólida expertise no estabelecimento e verificação de mecanismos alternativos de transferência de dados, notadamente os de natureza contratual. Outras fontes que poderiam nortear a atuação da ANPD na regulamentação dos instrumentos contratuais de transferência internacional de dados são as “Guidelines on the Protection of Privacy and Transborder Flows of Personal Data” da OCDE (Organização para Cooperação e Desenvolvimento Econômico). Contudo, cumpre destacar a necessidade de adaptar a experiência internacional à realidade brasileira, tendo em vista que o grau de maturidade das empresas nacionais não é o mesmo que o das empresas multinacionais, levando-se em consideração tanto porte quanto utilização de tecnologia. Neste sentido, uma sugestão de ordem prática é a realização pela

ANPD de benchmark internacional, que possibilitará conhecer os instrumentos utilizados por outras jurisdições para a adoção dos princípios nos nossos instrumentos contratuais, compatíveis com nossa legislação. A ANPD também poderia ter uma agenda com as autoridades de outros países, inclusive celebrando convênios com essas autoridades, de modo que requisitos mínimos relacionados aos princípios de privacidade e proteção de dados estejam contemplados nos instrumentos contratuais independentemente de particularidades das legislações locais, como mecanismos de transparência, garantia de atendimento dos titulares, boas práticas de segurança e requisitos relacionados a incidentes de segurança com dados pessoais. Importante, também, que a ANPD reconheça os países e organismos internacionais que possuem níveis de proteção de dados compatíveis com a LGPD, devendo considerar, inclusive, as boas práticas adotadas em outros países. Sugere-se ainda a disponibilização de lista de países em seu site para consulta dos interessados, assim como o BACEN fez em relação à norma de Segurança Cibernética (resolução nº 4.893/21). No caso do setor de seguros, experiências com incidentes em outros países poderá auxiliar na melhor gestão de dados pessoais, inclusive tendo em vista que a Circular Susep nº 638/2021, que dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais, sempre observando a confidencialidade da entidade, determina a observância na adoção de tratamentos e controles para os riscos cibernéticos, as boas práticas internacionais de segurança cibernética. Além disso, considerando a convergência da LGPD com determinadas legislações estrangeiras, como o GDPR, outra sugestão a ser avaliada é que instrumentos contratuais devidamente aprovados por autoridades com legislações convergentes com a LGPD sejam considerados pré-aprovados pela ANPD, e as Partes possuam a liberdade de realizar ajustes pontuais para considerar características regionais, sem que as condições mínimas previstas no documento aprovado pela autoridade estrangeira sejam alteradas. São convergentes com a LGPD, por exemplo, as legislações dos países da União Europeia, da Zona Econômica Europeia e daqueles que já foram objeto de uma decisão de adequação por parte da Comissão Europeia, como Andorra, Argentina, Canadá, Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido e Uruguai. ","174356":"Confederação Nacional das Seguradoras – CNseg: Na falta de uma orientação de adequação, as cláusulas-padrão contratuais têm sido o meio mais simples e utilizado para respaldar a transferência internacional de dados pessoais entre agentes privados, especialmente envolvendo empresas de menor porte. Nas transferências internacionais entre grandes empresas e grupos empresariais, também é frequente a utilização de normas corporativas globais, códigos de conduta, a realização de pactos internacionais e a adoção de decisões de adequação da legislação.","174359":"Confederação Nacional das Seguradoras – CNseg: Os principais benefícios, na experiência do setor de seguros, relacionados com a transferência internacional de dados, são: i. ganhos operacionais e de custo, na medida em que os fornecedores que apresentam os melhores serviços, considerando-se aspectos técnicos e financeiros, prestam serviços no exterior ou possuem servidores no exterior; ii. segurança jurídica, que promove um ambiente favorável ao desenvolvimento econômico; iii. segurança quanto ao nível de proteção de dados, independente do local de tratamento e garantia ao titular dos dados de

que seus dados permanecerão seguros; iv. economia com infraestrutura tecnológica interna, escalabilidade e alta disponibilidade, trazendo impactos positivos para o processamento dos dados; v. uniformidade de tratamento de forma similar entre os concorrentes, garantindo a viabilização de negócios com mais segurança; vi. armazenamento de forma segura certamente é um diferencial que agrega valor ao produto ou serviço, na medida em que o titular tem a garantia de que os seus dados estão protegidos na forma da lei; vii. disseminação dos reais direitos e benefícios do titular de dados; e viii. a transferência de dados deve ser para um país atrativo em termos de legislação de proteção de dados, para viabilizar parcerias com empresas que possuam melhores níveis de segurança. Os principais impactos são as dificuldades nas negociações de contratos com partes estrangeiras, em virtude da ausência de regulamentação nacional sobre o assunto. São alternativas para os instrumentos contratuais de transferências de dados: as cláusulas-padrão-contratuais, as normas corporativas globais, os códigos de conduta, a realização de pactos internacionais e a adoção de decisões de adequação, conforme resposta à pergunta 3. ","174360":"Confederação Nacional das Seguradoras – CNseg: Extrai-se do artigo 35, § 1º, da LGPD, que os mecanismos de transferência internacional de dados objetivam assegurar que os dados pessoais estarão protegidos no exterior de acordo com os direitos, as garantias e os princípios estabelecidos pela legislação nacional. Portanto, na regulamentação desses mecanismos, são esses critérios que devem nortear a atuação da ANPD. Um aspecto importante que precisa ser também previsto nestes instrumentos são as regras de lei e jurisdição aplicável em caso de conflito. Para sinergia entre as legislações, em especial aquelas que conferem ao titular a proteção de dados como direito fundamental, é importante que as empresas garantam como padrão as melhores práticas internacionais de proteção de dados e segurança da informação, adequadas à realidade da empresa e/ou do seu setor de atuação. Além desses critérios gerais, recomenda-se que sejam considerados os seguintes requisitos na regulamentação desses mecanismos: a. cláusulas-padrão contratuais: As cláusulas-padrão devem estabelecer salvaguardas de proteção dos dados pessoais transferidos, que garantam aos titulares desses dados o exercício dos direitos previstos na LGPD. Recomenda-se que as cláusulas-padrão contemplem, pelo menos, o seguinte: (i) as obrigações e as responsabilidades dos agentes de tratamento envolvidos na transferência; (ii) os direitos dos titulares dos dados e os meios pelos quais poderão exercê-los; (iii) o direito aplicável ao contrato; (iv) a finalidade, o destino, os tipos de dados que serão transferidos; (v) os tipos de agentes de tratamento envolvidos; (vi) disposições mínimas acerca do atendimento aos princípios e direitos dos titulares previstos na LGPD; (vii) ordem de prevalência de normas internacionais x LGPD; (viii) territorialidade; (ix) medidas técnicas mínimas de proteção de dados; (x) ações a serem observadas em caso de requerimentos advindos de autoridades competentes; (xi) limitação de uso e devolução de dados; e (xii) regras específicas para transferência de dados entre controladores x controladores, controladores x operadores e operadores x operadores. Por vincular apenas as partes, o controlador deve avaliar se as cláusulas-padrão terão efetividade (se o importador será impedido de cumpri-la por determinação legal ou das autoridades públicas locais). Se não forem efetivas, poderá adotar medidas adicionais para se salvaguardar. Deve-se considerar ainda o porte das empresas e a classificação dos agentes de tratamento, dado que controlador

e operador possuem papéis distintos do ponto de vista da LGPD. b. cláusulas contratuais específicas: Na avaliação das cláusulas contratuais específicas, deve-se levar em consideração, casuisticamente, os aspectos envolvidos na transferência (tipo de dados, bases legais do tratamento, finalidade etc.), assim como os aspectos indicados para as cláusulas contratuais- padrão, dando-se às partes liberdade para disporem livremente sobre particularidades na transferência internacional de dados. A sua aplicação deveria ocorrer para transferência internacional de dados pessoais esporádicos, em que as organizações estipulem cláusulas específicas para a transferência, mediante aprovação pela ANPD. A ANPD deveria editar um guia orientativo sobre a transferência de dados, contemplando particularidades de certos negócios, especialmente dos mercados regulados (Banco, Seguro, Saúde, Energia, por exemplo). O ponto negativo é que poderá haver entraves nos processos de transferência internacional de dados, enquanto não esclarecido como será realizado e em que tempo ocorrerá o processo, aprovação e/ou reavaliação. É importante que os critérios não sejam muito restritivos, o que dificultaria a aprovação das cláusulas e a consequente adoção desse mecanismo. c. normas corporativas globais: Essas normas precisam: (i) ser juridicamente vinculantes aos agentes envolvidos na transferência internacional de dados; (ii) descrever as empresas e os grupos empresariais aos quais se aplica; (iii) informar as finalidades, os destinos e os tipos de dados das transferências abrangidas pelas normas; (iv) estabelecer as regras de responsabilização e as obrigações dos agentes de tratamento; (v) ser públicas, para dar conhecimento de seu conteúdo aos titulares dos dados; e (vi) informar requisitos básicos e essenciais que devem constar nas cláusulas, para que as empresas tenham um direcionamento na construção das cláusulas, mas também tenham liberdade de criação, evitando-se ingerências. ","174361":"Confederação Nacional das Seguradoras – CNseg: Entende-se que os assuntos são complementares. O fato de um país ser reconhecido por proporcionar grau de proteção de dados adequado ao previsto na LGPD não exime as Partes de realizarem as suas diligências e avaliações e estabelecerem as regras necessárias para garantirem, uma perante a outra, os preceitos previstos na lei. Isso porque uma empresa pode estar localizada em um país que é reconhecido por proporcionar grau de proteção de dados pessoais adequado ao previsto na LGPD, e ela, por si só, não adotar internamente as medidas necessárias para estar adequada aos preceitos da lei. Não obstante, além da aprovação do nível de adequação e das cláusulas contratuais pelas autoridades, a existência de tratados internacionais entre países prevendo condições mínimas a serem previstas em contratos entre empresas sediadas neles, pode, também, ser uma medida eficaz. Outra sugestão é que os países que forem classificados pela ANPD com alto risco de proteção de dados, não poderão ser contratados pelos operadores e controladores de dados, sem oferecimento de garantias contratuais e/ou planos de ação para mitigação de riscos. Também não deve haver lista de países proibidos, mas sim lista de países pré-aprovados pela ANPD e critérios básicos que devem ser observados pelo controlador caso seja necessário transferir dados para outros países. ","174362":"Confederação Nacional das Seguradoras – CNseg: As cláusulas-padrão contratuais devem ter conteúdo pré-definido, como por exemplo, para prever situações de vulnerabilidade de incidentes, sempre observando as bases legais locais, a fim de conferir maior segurança jurídica para os agentes de tratamento de dados e, ao mesmo tempo, melhor preservar o regime de proteção de dados estabelecido pela LGPD. A utilização das

cláusulas-padrão contratuais deve permitir a flexibilização e não impedir que os agentes de tratamento de dados se valham de disposições contratuais mais abrangentes, sendo que em caso de conflito deve prevalecer o disposto no conteúdo pré-definido. Deve ser permitido, e na medida do possível estimulado, que os agentes de tratamento acrescentem outras disposições contratuais que tenham por finalidade robustecer as garantias de proteção de dados contidas nas cláusulas-padrão contratuais. Ressalta-se que diante da pluralidade de legislações que tratam do tema entre os países, a flexibilidade em relação ao texto torna-se viável para favorecer as negociações. Por outro lado, eventuais restrições excessivas podem impactar negativamente exportadores e importadores de informações, dificultando o fluxo informacional. Deve-se observar ainda como flexibilização as características regionais e relacionadas à atividade das partes, como, por exemplo, envolvendo empresas reguladas pelo setor público, sem que as condições mínimas previstas no documento aprovado pela autoridade estrangeira sejam alteradas. ","174363":"Confederação Nacional das Seguradoras – CNseg: A solução que se mostra mais utilizada e prática é a adoção de um bloco de cláusulas sobre transferência internacional de dados a serem incluídas como anexos dos contratos a serem celebrados entres os controladores e operadores, levando-se em consideração os tipos de agentes de tratamento envolvidos em cada caso (p.ex. controlador-controlador, controlador-operador, operador-suboperador). Sugere-se disponibilizar as cláusulas-padrão no próprio site da ANPD e publicar um guia orientativo, a exemplo do que foi feito em relação aos agentes de tratamento, bem como utilizar de formulários, porém é necessário que exista uma recomendação da ANPD com os níveis aceitáveis de acordo com cada resposta do formulário, quais critérios são seguros e aceitáveis para prosseguir. ","174364":"Confederação Nacional das Seguradoras – CNseg: Seria interessante ter modelos de cláusulas-padrão considerando se a troca de dados ocorre entre controlador x controlador, controlador x operador, ou operador x suboperador, mas que guardem espaço para flexibilizações, conforme necessidade/peculiaridade do modelo de negócios do agente de tratamento, como por exemplo o setor de seguros, que é regulado. Outra sugestão seria seguir o padrão adotado pelas autoridades europeias (modelos específicos para controladores e operadores, enquadrados nas posições de exportadores e importadores de dados), já que a legislação europeia guarda semelhança com a brasileira. Além disso, a legislação europeia neste quesito já vem sendo executada por empresas que operam em outros países, o que facilita a negociação dos contratos com partes estrangeiras. ","174367":"Confederação Nacional das Seguradoras – CNseg: Apesar de juridicamente distintas, tanto as normas corporativas globais quanto as cláusulas-padrão contratuais destinam-se à mesma finalidade, que é assegurar que os dados pessoais transferidos para o exterior estarão protegidos em grau compatível (não necessariamente idêntico) com a proteção conferida pela LGPD. Portanto, na essência, os requisitos devem ser os mesmos. Porém, como as normas corporativas globais são elaboradas pelos próprios agentes interessados na transferência, é preciso que a ANPD estabeleça o procedimento e as informações que deverão ser apresentadas para a aprovação dessas normas, tais como a definição do papel de agente de tratamento de quem envia e de quem recebe os dados, assim como obrigações e responsabilidades de cada parte. As empresas devem ter espaço para escreverem suas cláusulas conforme suas necessidades/modelo de negócios, apenas observando recomendações necessárias da ANPD.

Deve ficar a critério da empresa a aplicação ou não das normas para todas as empresas do seu grupo econômico. ","174368":"Confederação Nacional das Seguradoras – CNseg: Interessante avaliar as definições trazidas pelo Information Commissioner's Office ("ICO") sobre o tema, além de compatibilizar com a Lei nº 6.404/1976.","174369":"Confederação Nacional das Seguradoras – CNseg: Para a análise a ser realizada pela ANPD, é necessário que sejam consideradas, no mínimo, as seguintes informações: (i) categoria do dado; (ii) a finalidade da transferência; (iii) existência de políticas sobre privacidade e proteção de dados pessoais (corporativas e avisos de privacidade aos titulares), com adesão aos princípios gerais sobre o tema (que se aplicam independente da jurisdição); (iv) categoria de titular; (v) o país ou organismo internacional de destino; (vi) a identificação dos agentes de tratamento envolvidos na transferência; (vii) os mecanismos de segurança adotados e a sua conformidade com as boas práticas sobre o assunto e (viii) as ferramentas disponíveis para o atendimento dos direitos dos titulares. Excepcionalmente, a depender dos riscos associados à transferência, a ANPD poderá, fundamentadamente, solicitar informações adicionais, preservando-se, entretanto, os segredos comerciais e industriais dos agentes de tratamento de dados envolvidos na operação. ","174371":"Confederação Nacional das Seguradoras – CNseg: Riscos: (i) desvirtuar a finalidade do tratamento informada ao titular dos dados; (ii) redução da transparência da operação para o titular dos dados; (iii) vazamento de dados; e (iv) descumprimento de determinação de autoridade competente do país de origem dos dados. Benefícios: (i) agilizar o processo de verificação e de tomada de decisão da ANPD; (ii) reduzir custos para os agentes de tratamento de dados; (iii) fomentar o fluxo transfronteiriço de dados; (iv) aumento de insumo para estudos de perfil de consumo, para incremento das atividades desenvolvidas pelo grupo econômico; e (v) aprimoramento dos produtos e serviços. Ressalta-se que, atualmente, em que tudo praticamente é digitalizado, as empresas dependem de transferência de dados para parte significativa de suas operações. Por isso é imperioso ter definido claramente como poderá a transferência de dados ocorrer entre as empresas, garantindo também aos titulares de dados maior acesso a bens e serviços a um custo menor, por exemplo. Cumpre salientar que com a aprovação das normas e/ou utilização de critérios mínimos que garantam a proteção de dados, tanto os agentes de tratamento quanto o próprio titular do dado serão beneficiados. ","174372":"Confederação Nacional das Seguradoras – CNseg: Sim. O Comitê Europeu de Proteção de Dados, por exemplo, disponibiliza alguns documentos que descrevem o procedimento de aprovação e os requisitos das Binding Corporate Rules (BCR), que são, na Europa, as equivalentes às normas corporativas globais previstas na LGPD, assim como para cláusulas contratuais-padrão. A experiência de algumas autoridades europeias na aprovação de cláusulas contratuais específicas também pode servir de inspiração para a ANPD. Além disso, a ANPD pode se valer de benchmark com outros países, além da União Europeia, focando em modelos que não sejam engessados. ","174373":"Confederação Nacional das Seguradoras – CNseg: Os direitos são os mesmos garantidos a todos os titulares em virtude do tratamento dos seus dados. No entanto, entende-se que, a depender da alteração realizada, não seria necessário nenhum tipo de comunicação específica ou direcionada, por exemplo, uma alteração meramente técnica/operacional, que muitas vezes foge, inclusive, da possibilidade de definição ou interferência do exportador dos dados. Porém, em hipóteses excepcionais, como

ocorre, por exemplo, nas situações envolvendo incidente de segurança (artigo 48, LGPD) o titular deve ser comunicado. No caso de transferência internacional, entende-se que os direitos mínimos que precisam ser garantidos aos titulares são os direitos de transparência no tratamento dos dados e de bloqueio, quando aplicável, em caso de não concordância com o tratamento. Assim, não é necessária a comunicação direta dos titulares nestes casos, pois isso não traz benefícios para a operação (os titulares já reclamam, atualmente, da quantidade de contatos realizados pelas empresas), além deste procedimento trazer ônus financeiros relevantes para as operações. Uma política de privacidade bem estruturada, contemplando todas as informações sobre o tratamento dos dados, inclusive sobre eventual transferência internacional de dados, seria suficiente para garantir a transparência ao titular. Além disso, mediante o direito de acesso, o titular pode obter informações específicas sobre os tratamentos realizados pelo controlador, o que viabiliza, uma vez mais, a possibilidade de bloqueio, se aplicável. ","174375":"Confederação Nacional das Seguradoras – CNseg: Sem prejuízo da adoção de mecanismos de cooperação internacional entre autoridades de proteção de dados - o que seria muito importante -, entende-se que nas hipóteses em que o exportador e o titular dos dados estiverem no Brasil, os conflitos entre agentes de tratamento e entre estes e os titulares dos dados devem estar submetidos à legislação e jurisdição brasileiras. Desse modo, ficará à disposição dos agentes de tratamento e dos titulares dos dados, todos os mecanismos de resolução de conflitos (inclusive os chamados alternativos, como mediação e arbitragem), talvez até utilizando plataformas online que facilitem o processo de solução de litígios, deixando para discussão no judiciário temas com mais complexidade e/ou valores envolvidos, a depender do dano causado. Os conflitos envolvendo apenas agentes de tratamento (sem o titular dos dados), poderiam ser resolvidos (i) conforme regra de jurisdição prevista em contrato, privilegiando o acordo entre as Partes; (ii) por mediação (com definição de mediador em contrato ou recomendação das autoridades de proteção de dados competentes pelo contrato) ou (iii) por arbitragem (conforme regras definidas em contrato ou acordo posterior entre as Partes). Em caso de silêncio quanto a esta previsão, deve-se privilegiar a lei do local de origem do dado referente ao conflito, desde que a jurisdição seja competente e observando-se o art. 21 do CPC, ou a regra prevista em tratados e acordos internacionais celebrados com os Estados das partes envolvidas, em vigor quando da propositura da ação, desde que aplicáveis e não conflitarem com a legislação. Além disso, seria conveniente que os conflitos envolvendo os titulares fossem facilitados por entidade pública com conhecimento técnico no assunto, como a própria ANPD, o que poderia ser aplicado a todo e qualquer conflito envolvendo tratamento de dados e não apenas a transferência internacional de dados pessoais. ","174376":"Confederação Nacional das Seguradoras – CNseg: Inicialmente, entende-se que uma alternativa seria a celebração de acordos de cooperação internacional pela ANPD com autoridades estrangeiras, fixando-se parâmetros mínimos de conformidade, de modo a evitar que o conflito de jurisdições possa acarretar problemas na prática das transferências internacionais. Na medida em que, em regra, os importadores somente garantem conformidade com as legislações do seu local de atuação, o estabelecimento de parâmetros mínimos de conformidade em âmbito internacional já facilitaria as negociações com partes estrangeiras. Além disso, também seria interessante o estabelecimento de diretrizes regulatórias sobre as práticas que seriam minimamente

necessárias para se considerar a adequação das empresas de acordo com a natureza dos dados tratados, as finalidades de tratamento e eventuais decisões de conformidade emitidas por autoridades estrangeiras. A ANPD poderia, por exemplo, elaborar um guia orientativo, à semelhança do “Data sharing code of practice”, editado pelo Information Commissioner’s Office do Reino Unido, além de criar selos e certificados, que sejam aceitos internacionalmente. Sem prejuízo das sugestões acima, entende-se que nas hipóteses em que o exportador e o titular dos dados estiverem no Brasil, os conflitos entre agentes de tratamentos e entre estes e os titulares dos dados devem estar submetidos à legislação e jurisdição brasileiras. ","174378":"Confederação Nacional das Seguradoras – CNseg: No caso do importador e do exportador serem controladores independentes, só haverá a responsabilização solidária das Partes quando ambos contribuírem para a violação à LGPD e às disposições contratuais. Nos demais casos, ficará garantida a possibilidade de o titular dos dados acionar a jurisdição de seu país, com a responsabilidade atribuída apenas ao agente que tiver efetivamente causado o dano. Já para as hipóteses nas quais o exportador seja o controlador e o importador seja operador, aplica-se o disposto no artigo 42, §1º, I da LGDP. A responsabilização do operador na forma do artigo 42, §1º, I da LGDP ocorrerá, também, nas hipóteses em que ele contratar suboperador para o tratamento dos dados sem a autorização prévia e expressa do controlador. ","174379":"Confederação Nacional das Seguradoras – CNseg: Em caso de determinação de acesso aos dados por autoridades públicas estrangeiras, a ANPD deve estabelecer procedimentos para que o importador seja obrigado a: (i) notificar imediatamente ao exportador da existência da determinação da autoridade estrangeira, a não ser que haja proibição expressa neste sentido, de forma a possibilitar à Parte adotar ou requerer qualquer medida cabível para evitar ou mitigar danos decorrentes da revelação de dados pessoais; (ii) cooperar com o exportador, tanto quanto possível, na adoção de qualquer medida lícita, judicial ou não, que objetive garantir tratamento sigiloso aos dados pessoais; (iii) disponibilizar acesso apenas aos dados mínimos necessários para o atendimento da determinação da autoridade estrangeira; e (iv) observar se a solicitação está de fato pautada em legislação aplicável e seguir critérios de segurança que garantam a proteção dos dados.","174380":"Confederação Nacional das Seguradoras – CNseg: O documento mais apropriado para prever a possibilidade de transferência internacional de dados é a política de privacidade do agente de tratamento que envia dados para agente localizado em território internacional. Do ponto de vista operacional torna-se inviável informar o titular a cada transferência realizada, não havendo condições nem necessidade de fornecer informações detalhadas sobre a transferência. Dessa forma, prever na política de privacidade e/ou outro documento que o controlador firme com o titular já atenderia os princípios da LGPD, em especial o princípio da transparência.

Contribuinte: Mariana Coelho de Mendonça

Número: OP-183186

Data: 30/06/2022 - 07:46

Resumo: :"Iniciam-se com a falta de conscientização sobre a cultura e hábito da proteção de dados pela maioria das empresas brasileiras, principalmente, pelo desconhecimento da própria Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e a sua aplicação na prática. Diante da recente vigência da Lei, com menos de dois anos, e a falta de uma regulamentação específica da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) sobre o tema, as transferências internacionais de dados pessoais vêm sendo feitas, sobretudo, com o amparo de cláusulas contratuais, obedecendo aos requisitos legais e com a implementação de medidas técnicas e administrativas para a proteção destes dados de acordo com os princípios da Lei e os direitos dos titulares. Não há, por enquanto, definição pelo Órgão de controle de quais países ou organismos internacionais proporcionam grau de proteção de dados pessoais adequados. Certamente, com a definição da chamada decisão de adequação pela ANPD, relacionada a estes países e organismos com grau de proteção elevado, propiciará maior facilidade à transferência para os contemplados. Garantir-se-á, assim, melhor coordenação entre todos os atores envolvidos – incluindo a supervisão por parte das autoridades competentes. Ressalta-se, por oportuno, que não só as grandes empresas transferem dados pessoais internacionalmente, mas as médias e pequenas também. Isso dificulta o cumprimento de todas as medidas exigidas nos demais casos previstos na Lei, inclusive dado ao próprio tratamento diferenciado dispensado a tais agentes. Outro obstáculo surge quando não há um país ou organismo internacional previamente definido como apto para a transferência, pois se torna necessária a realização de contratos específicos, padrões ou com normas corporativas globais. De igual forma, o inverso, transferência de dados pessoais de outros países para o Brasil, também encontra obstáculos pela falta de cultura, conhecimento e aplicação da LGPD, fazendo com que o Brasil não seja um país reconhecido ainda como adequado para a decisão de adequação de nível internacional. No que se refere às cláusulas contratuais específicas, padrão ou corporativa, o Brasil na grande maioria das empresas ainda não possuem sequer a adequação completa da LGPD, sendo difícil exigir a adoção das medidas necessárias e cláusulas efetivas que protejam os dados pessoais, pois na sua essência é necessário atender os princípios e outras regras da Legislação, em especial as bases legais próprias para a transferência internacional de dados. A regulamentação dos instrumentos contratuais, obedecendo a critérios e padrões internacionais de transferência de dados, certamente, ajudará o Brasil não só a exportar os seus dados, como, também, na importação, porquanto harmonizar-se-á nossa legislação e a respectiva regulamentação com o que é exigido pelos outros países. ","174354":"A ANPD deve orientar e divulgar materiais em seu site para ajudar os agentes de tratamento a elaborarem cláusulas contratuais específicas para determinadas situações de transferência, em consonância com a LGPD, e outras legislações sobre proteção de dados de outros países, para que com uma proximidade maior destas regras voltadas para a salvaguarda apropriada para a transferência internacional, o Brasil possa se inserir no mesmo ritmo de proteção e interoperabilidade nas transferências, atendendo também às exigências de outras jurisdições. Na LGPD, não havendo o reconhecimento pela ANPD de países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado, a transferência somente poderá ser feita nas hipóteses do art. 33, incisos II a IX e, no que se refere aos instrumentos contratuais, somente as alíneas “a”, “b” e “c” do inciso II, tratam deste assunto ao disciplinar que: Art. 33 A

transferência internacional de dados pessoais somente é permitida nos seguintes casos: (...) II quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) Cláusulas contratuais específicas para determinada transferência; b) Cláusulas-padrão contratuais; c) Normas corporativas globais; (...) De igual modo, as cláusulas contratuais padrões devem ser elaboradas pela própria ANPD, com a posterior divulgação em seu site, para que os controladores possam se valer do material no caso da realização de uma transferência internacional de dados. A ANPD assume, desde a vigência da Lei, papel de suma relevância na conscientização e propagação da cultura da proteção de dados pessoais e à privacidade. Regulamentar a transferência internacional é mais uma das relevantes missões que a (agora autarquia especial, vide Medida Provisória nº 1.124/2022) enfrentará – no ponto, de se elogiar o caráter dialético e democrático com o qual a (então) Autoridade vem conduzindo seus trabalhos, reunindo perspectivas das mais distintas e plurais em tomadas de subsídios como essa, buscando o melhor resultado aos sujeitos tutelados pela LGPD. Quanto às normas corporativas globais, por envolver estatutos internos, regras de governança e administração de cada empresa, apenas as diretrizes essenciais devem ser divulgadas pela ANPD, para que as empresas que tenham atuação internacional possam, além de manter as suas próprias regras, se adequarem também às exigências legais e regulamentadas por aquela. Conclui-se, portanto, que compete à ANPD quanto aos 03 tipos de instrumentos contratuais, facilitar a utilização, dispondo de orientações, modelos, exigências mínimas e outras medidas de salvaguarda para a proteção dos dados pessoais e transferência internacional, a fim de colocar o Brasil como reconhecidamente um país de nível adequado de proteção.
","174356":"De forma simples e objetiva, aquele que, em um primeiro momento se mostra o mecanismo mais efetivo para transferências internacionais seguras, e que garantem o cumprimento e a efetivação dos direitos e liberdades dos titulares é o mecanismo estampado no artigo 33, inciso I do caput da lei 13.709, abaixo transcrito: “I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei”1 Para que se possa avaliar qual o grau de proteção de uma proteção de dados pessoais de um país, não basta apenas olhar se tal país possui uma legislação geral de proteção de dados pessoais, uma autoridade independente ou normas setoriais que possuam algum grau de proteção de dados pessoais. Não necessariamente será exigido de um país terceiro que possua leis e proteções idênticas àquelas trazidas pela LGPD;, nas palavras de Leonardi: “Dada a influência Europeia, é de se esperar que a ANPD utilize como referência o conceito europeu de ‘nível adequado de proteção’, por meio do qual se entende que um país não precisa assegurar nível de proteção idêntico, mas ‘substancialmente equivalente’.”2 O próprio artigo 34 da LGPD enumera fatores que deverão ser considerados no momento em que a ANPD decidir por analisar o grau de proteção de dados pessoais de um país terceiro para que possa definir o grau de proteção de dados de um país, que será uma ampla análise ampla e geral, que deverá levar em conta: normas de proteção de dados gerais e setoriais, observância dos princípios e dos direitos dos titulares presentes na LGPD pelo país terceiro ou organismo internacional que receba transferências de dados com aplicação da LGPD, adoção de medidas de segurança previstas em regulamento (que, até o momento, ainda não foi feito), garantias judiciais e institucionais para respeito dos titulares de dados, dentre

outros. A decisão de adequação é um método muito mais efetivo do que os demais, pelo fato de que para que possa ter uma decisão de adequação em relação a país terceiro ou mesmo a organismo internacional, deverá ser feito um longo processo de análise de todo o ordenamento jurídico relativo a proteção de dados de país terceiro ou órgão internacional relativo a proteção de dados pessoais, sua jurisprudência sobre tema e até mesmo as práticas de proteção de dados para se saber sobre a possibilidade ou não de o referido terceiro dar aos titulares garantias "substancialmente equivalentes" àquelas trazidas pela LGPD e pelo ordenamento jurídico brasileiro com relação a proteção de dados pessoais. Com uma decisão de adequação em relação a um país ou um organismo internacional, este estará comprovadamente com as adequações da ANPD, garantindo o cumprimento de requisitos necessários para garantir os direitos dos titulares e princípios da LGPD – ocorrendo também, em tese, profunda análise do sistema jurídico regulatório do país terceiro. Apesar de não existir uma hierarquia entre os mecanismos de transferência internacional de dados pessoais na LGPD, nos resta claro que uma decisão de adequação é o principal meio para realização de transferências internacionais seguras. Inclusive, esse é o posicionamento da doutrina: "Os demais mecanismos de transferência mencionados a seguir podem ser utilizados quando o nível de proteção do país estrangeiro envolvido na transferência de dados pessoais não é considerado adequado pela ANPD."3 No entanto, apesar de as decisões de adequação serem o meio de transferência internacional mais efetivo para garantir proteção aos direitos e liberdades dos titulares, não é um método simples, pois, como já explicitado, exige ampla análise das normas, jurisprudências e práticas relativas a proteção de dados pessoais do país terceiro para ser emitida. Ainda, deve ser tomada uma decisão de adequação individual com relação a cada país terceiro ou organismo internacional com o qual se pretenda realizar transferências internacionais de dados pessoais, o que pode não ser uma medida tão efetiva ao curto prazo. As transferências internacionais de dados são cada vez mais comuns, em especial nos dias de hoje, em razão da globalização e da nova era digital, na qual a grande maioria das empresas possui contratos com prestadores de serviços para armazenamento de dados em nuvem ou com prestadores de serviços de marketing, gestão de clientes ou mesmo gestão de recursos humanos, que utilizam serviços em nuvem, cujo servidor está localizado fora do território nacional. "A Nuvem oferece suporte à escalabilidade e à composição que as tecnologias e aplicações avançadas exigem, ao mesmo tempo em que permite que as empresas atendam às necessidades emergentes, como soberania, integração de dados e experiência aprimorada do cliente." Tendo em conta referida fala, bem como o nosso contexto atual, é evidente que as transferências internacionais de dados pessoais acontecem com enorme frequência e devem ocorrer com frequência cada vez maior nos próximos anos, é de suma importância que se busque uma solução rápida para que as transferências internacionais continuem a ocorrer, de forma a garantir o desenvolvimento econômico e tecnológico e a inovação e também a autodeterminação informativa e o direito fundamental à proteção de dados pessoais dos titulares. Por tal razão, e pelo fato de que a ANPD e a proteção de dados pessoais no Brasil ainda estão em seus primeiros passos, imperioso é, buscarmos por uma solução mais amplas para garantir que as transferências internacionais possam ser feitas segundo os moldes da LGPD e para garantir a segurança dos dados dos titulares de dados pessoais. O artigo 33 da LGPD traz, além das decisões de adequação,

enorme lista com outras 11 hipóteses para legitimar uma transferência internacional de dados pessoais. Tendo em vista a natureza do presente parecer, e a sua busca por uma solução que visa a criação de uma solução, em um curto espaço de tempo, que possa auxiliar na realização de transferências internacionais e garantir a proteção de dados pessoais exigida pelo sistema brasileiro, ou ao menos uma proteção "substancialmente equivalente", iremos focar, a partir de agora nas cláusulas-padrão contratuais, do inciso II, alínea b, do caput do artigo 33 da LGPD. Não se discorre, no presente ensaio, sobre as derrogações, que são, nas palavras de Angelo Gamba Prata de Carvalho5, "que se caracteriza, em verdade, pelo afastamento do manto da proteção de dados do diploma, porém, sempre em homenagem a outros objetivos de interesse público previstos de maneira taxativa pelos incisos III a VII do art. 33 da LGPD..." Em verdade, as situações previstas nos incisos III a IX, constituem situações específicas, são passíveis de ocorrer no mundo real, sem a necessidade da criação de um instrumento específico, como o cumprimento de um contrato ou o consentimento do titular, ou então situações restritas a órgãos públicos ou que dependem de autorização específica da ANPD. O que se pretende no presente ensaio, mais uma vez, é auxiliar na criação de um mecanismo efetivo para uma transferência internacional de dados segura, com aplicação ampla e que possa ser colocado em circulação pela autoridade o mais rápido possível. II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de: a) cláusulas contratuais específicas para determinada transferência;b) cláusulas-padrão contratuais;c) normas corporativas globais;d) selos, certificados e códigos de conduta regularmente emitidos; Com relação aos elementos acima citados, as cláusulas contratuais específicas não se mostram, salvo melhor juízo, o melhor instrumento ao presente momento, pois tais cláusulas deverão ser elaboradas para uma determinada transferência e ainda deverão ser verificadas e aprovadas pela ANPD, segundo o próprio caput do artigo 35 da LGPD. Com isso, pode haver morosidade no processo de aprovação de cada conjunto de cláusulas contratuais especificas enviados para a ANPD por diversos controladores do Brasil, o que vai contra uma ideia inicial de um meio que vise facilitar as transferências internacionais de dados pessoais. Com relação às normas corporativas globais, as palavras de Leonardi6 rapidamente nos mostram seu significado, e a não aplicabilidade das mesmas no presente caso: "As chamadas 'normas corporativas globais' são outra opção disponível para casos de transferência internacional de dados pessoais entre empresas do mesmo Grupo Econômico." Ainda nas palavras do autor, apesar de a LGPD ser silente, espera-se que, assim como no modelo europeu, as normas corporativas globais tenham que ser também aprovadas pela ANPD, o que, somado ao fato de que cada conjunto de normas corporativas globais seja específico para um grupo econômico, mostra que o referido mecanismo também não seja uma solução geral a ser adotada. Quanto aos selos, certificados e códigos regularmente emitidos, a ANPD ainda não criou sequer procedimentos que deverão ser adotados, ou mesmo critérios utilizados para sua aprovação, o que mostra que também não são uma solução para o presente momento. Por fim, temos as cláusulas-padrão contratuais, que nada mais são do que "cláusulas-modelo elaboradas pela ANPD, contendo obrigações das partes envolvidas na transferência e os direitos dos titulares dos dados a serem transferidos".7 Tais cláusulas contratuais, diferentemente de cláusulas específicas ou de normas corporativas globais,

possuem um conteúdo mais geral, o que dispensa aprovação de seu conteúdo pela ANPD a todo momento, possibilitando a criação de um único documento aprovado pela ANPD, e assim, trazendo maior segurança jurídica para as transferências internacionais. Podemos, inclusive, nos espelhar no modelo europeu, no qual os órgãos competentes disponibilizam referidas cláusulas online. No entanto, apesar de as Cláusulas-padrão contratuais serem, inicialmente ...Continua no arquivo enviado por e-mail.","174359":"","174360":"","174361":"","174362":"As cláusulas-padrão contratuais devem sim ser rígidas para possibilitarem uma real proteção aos direitos dos titulares e dos princípios da legislação de proteção de dados pessoais em países terceiros, mas devem também possui um conteúdo pré-definido, pois o nome “cláusulas-padrão” nos leva a entender que seu conteúdo será padrão, igual para todos os casos e com um conteúdo previamente definido pela ANPD. Caso o conteúdo de uma cláusula-padrão contratuais fosse demasiado flexibilizado pela ANPD e agentes de tratamento pudessem alterar o seu conteúdo a todo e qualquer momento, as cláusulas-padrão contratuais perderiam a sua natureza e seriam semelhantes às cláusulas trazidas na alínea a, do inciso II do caput do artigo 33 da LGPD, as cláusulas contratuais específicas para cada transação. O que deve ser ponderado nos casos de cláusulas-padrão contratuais é a possibilidade de incrementação de seu conteúdo conforme o caso concreto, de ocorrer adaptação do conteúdo das cláusulas-padrão ao caso concreto, desde que os direitos dos titulares e os princípios das normas de proteção de dados do Brasil continuem sendo respeitados. Assim mostra, inclusive, o Considerando 109 do GDPR, lei que inspirou e ainda serve de referência para o sistema de proteção de dados nacional: “A possibilidade de o responsável pelo tratamento ou o subcontratante utilizarem cláusulas-tipo de proteção de dados adotadas pela Comissão ou por uma autoridade de controlo não os deverá impedir de incluírem estas cláusulas num contrato mais abrangente, como um contrato entre o subcontratante e outro subcontratante, nem de acrescentarem outras cláusulas ou garantias adicionais desde que não entrem, direta ou indiretamente, em contradição com as cláusulas contratuais-tipo adotadas pela Comissão ou por uma autoridade de controlo, e sem prejuízo dos direitos ou liberdades fundamentais dos titulares dos dados. Os responsáveis pelo tratamento e os subcontratantes deverão ser encorajados a apresentar garantias suplementares através de compromissos contratuais que complementem as cláusulas-tipo de proteção.” Ou seja: a depender do caso concreto, deverão ser adicionadas cláusulas mais detalhadas aos contratos que envolvam as cláusulas-padrão contratuais, para que o contrato seja adequado à realidade jurídico/normativa de cada país que venha a receber os dados pessoais. Para se saber quais cláusulas ou mesmo quais medidas deverão ser incluídas no contrato, o EDPB sugere, na já mencionada Guideline 01/2020, uma sequência de passos para análise do cenário fático/jurídico de país terceiro, para saber se a transferência é viável com as cláusulas&#2;padrão pré-elaboradas pela ANPD, se para possibilitar a transferência serão necessárias alterações/adições de cláusulas contratuais e/ou medidas de segurança adicionais ou se as transferências deverão ser interrompidas em razão de falta de possibilidade de se garantir padrão similar de proteção aos da LGPD. Referido passo a passo é descrito da seguinte forma: Etapa 1: Conhecer as transferências Para saber o que lhe poderá ser exigido para poder prosseguir as suas transferências ou para realizar novas transferências de dados pessoais, o exportador (aquele

que envia os dados pessoais para o exterior) de dados deve começar por se assegurar de que tem pleno conhecimento das suas transferências. O registo (mapeamento de dados/processos) e o levantamento de todas as transferências podem constituir um exercício complexo para as entidades envolvidas em transferências múltiplas, diversas e regulares com países terceiros e que utilizam diversos subcontratantes e subcontratantes ulteriores. Conhecer as suas transferências é uma primeira etapa essencial para cumprir as obrigações que incumbem ao exportador de dados por força do princípio da responsabilidade. Etapa 2: Identificar os instrumentos de transferências utilizados Independentemente do instrumento de transferência do artigo 46.º do RGPD (na LGPD, seria o artigo 33) escolhido, o exportador deve assegurar-se de que, em termos gerais, os dados pessoais transferidos beneficiam de um nível de proteção essencialmente equivalente. Os instrumentos de transferência do artigo 46.º do RGPD contêm principalmente garantias adequadas de natureza contratual que podem ser aplicadas a transferências para todos os países terceiros. A situação existente no país terceiro para o qual o exportador transfere dados pode ainda exigir que este complemente os referidos instrumentos de transferência e as garantias aí contidas com medidas adicionais («medidas complementares») para assegurar um nível de proteção essencialmente equivalente. Se a transferência não puder basear-se legalmente numa decisão de adequação, nem uma derrogação do artigo 49.º, é necessário prosseguir para a etapa 3. (Traduzindo para a LGPD, se a transferência de dados for pautada em alguma das hipóteses do inciso II do caput do artigo 33, deverá o agente de tratamento prosseguir para a próxima etapa do teste). Etapa 3: Avaliar se o instrumento de transferência do artigo 46.º do RGPD utilizado é eficaz tendo em conta todas as circunstâncias da transferência (No caso da LGPD, instrumentos do artigo 33, inciso II) O instrumento de transferência do artigo 46.º do RGPD selecionado deve ser eficaz, assegurando que o nível de proteção garantido pelo RGPD não é comprometido pela transferência. Em especial, a proteção conferida aos dados pessoais transferidos para o país terceiro deve ser essencialmente equivalente à que é garantida no EEE pelo RGPD, lido à luz da Carta dos Direitos Fundamentais da EU. (Onde se lê RGPD, substituir por LGPD e Carta de Direitos substituir por Constituição Federal). Por conseguinte, o exportador deve, se necessário, em colaboração com o importador (aquele que recebe os dados pessoais), avaliar se existe algo no direito ou na prática do país terceiro que possa afetar a eficácia das garantias adequadas (das garantias que criam a possibilidade de cumprimento dos princípios da LGPD e da garantia de exercício de direitos dos titulares naquela transferência) do instrumento de transferência do artigo 46.º do RGPD que utilizou, no contexto da transferência específica. Esta avaliação deve conter elementos relativos ao acesso aos dados das autoridades públicas do país terceiro do importador, tais como: - elementos que indiquem se as autoridades públicas do país terceiro do importador podem procurar aceder aos dados com ou sem o conhecimento do importador de dados, à luz da legislação, prática e precedentes comunicados; - elementos que indiquem se as autoridades públicas do país terceiro do importador poderão ter acesso aos dados através do importador de dados ou através dos fornecedores de telecomunicações ou canais de comunicação, à luz da legislação, dos poderes legais, dos recursos técnicos, financeiros e humanos de que dispõem e dos precedentes comunicados. Para auxiliar na investigação do contexto jurídico de país terceiro ou organismo internacional que irá receber os dados pessoais, o parecer em análise insere os

seguintes tópicos, como um guia: O contexto jurídico e/ou as práticas aplicáveis dependerão das circunstâncias específicas da transferência, nomeadamente: - as finalidades para as quais os dados são transferidos e tratados (por ex., marketing, RH, armazenamento, apoio informático, ensaios clínicos); - os tipos de entidade envolvidos no tratamento (pública/privada; responsável pelo tratamento/subcontratante); - o setor no qual a transferência ocorre (por ex., adtech, telecomunicações, financeiro, etc.); - as categorias de dados pessoais transferidos (por ex., os dados pessoais relativos a crianças podem ser abrangidos pelo âmbito de aplicação de uma legislação específica do país terceiro)42; - se os dados serão armazenados no país terceiro ou se existe acesso remoto aos dados armazenados na UE ou no EEE; - o formato dos dados a transferir (ou seja, texto corrido/pseudonimizado ou encriptado); - a possibilidade de ocorrência de transferências ulteriores dos dados do país terceiro em causa para outro país terceiro Etapa 4: Adotar medidas complementares Se resultar da avaliação efetuada pelo exportador na etapa 3 que o instrumento de transferência do artigo 46.º do RGPD escolhido não é eficaz, o exportador deverá determinar, caso necessário em colaboração com o importador, se existem medidas complementares que, em combinação com as garantias contidas nos instrumentos de transferência, possam assegurar que os dados transferidos beneficiem no país terceiro de um nível de proteção essencialmente equivalente ao que é garantido na UE. As «medidas complementares» são, por definição, complementares das garantias já previstas no instrumento de transferência do artigo 46.º do RGPD e de quaisquer outros requisitos de segurança aplicáveis (por ex., medidas técnicas de segurança) estabelecidos no RGPD. O exportador deve identificar, caso a caso, as medidas complementares que podem ser eficazes para um conjunto de transferências para um país terceiro específico quando utiliza um instrumento de transferência específico do artigo 46.º do RGPD. O exportador não precisa de repetir a avaliação sempre que efetuar a mesma transferência de um tipo específico de dados para o mesmo país terceiro. Alguns dos dados previstos para transferência podem exigir medidas complementares, ao passo que outros podem não exigir essas medidas (tendo em conta a aplicação formal e/ou prática da legislação do país terceiro). O exportador poderá basear-se nas suas avaliações e conclusões anteriores nas etapas 1, 2 e 3 supra e verificar, com base nas suas conclusões, a potencial eficácia das medidas complementares para garantir o nível de proteção exigido. Em princípio, as medidas complementares podem ter um caráter contratual, técnico ou organizativo. Etapa 5: Etapas do processo a seguir quando o exportador ...Continua no documento enviado por e-mail. ","174363":"Acredita-se que o formato mais adequado para disponibilização dos modelos de cláusulas&#2;padrão seria através da ferramenta do Word. Pois, é totalmente acessível e popular no Brasil. Sugere-se também que os documentos estejam em modo editável, adaptáveis pelos agentes, caso queiram acrescentar outras cláusulas ou garantias adicionais, desde que não choquem, direta ou indiretamente, com as cláusulas contratuais sugeridas pela ANPD (sem prejuízo de nenhum dos direitos ou das liberdades fundamentais dos titulares dos dados). Sugere-se ainda que a ANPD disponibilize uma página exclusiva para o tema de Transferência Internacional de Dados. Abaixo, indicações de alguns mecanismos de ajuda aos agentes de tratamento para esclarecimento e direcionamento sobre qual modelo adotar: • Resumo da matéria em passo a passo (como perguntas e respostas): São elaboradas perguntas estratégicas, e suas respostas levarão

conhecimento aos agentes de tratamento. Após os esclarecimentos (inclusive com exemplos práticos hipotéticos) os mesmos conseguirão avaliar a necessidade da utilização das cláusulas-padrão: Com base nas boas práticas adotadas pela Autoridade do Reino Unido – ICO1, temos que ela descreve perguntas chaves sobre o tema. Exemplo: Quais são as restrições às transferências internacionais? Existe outra possibilidade de realização do seu negócio sem que ocorra a transferência internacional? A cada pergunta respondida poderá existir links de direcionamento para modelos de cláusula-padrão ou demais conteúdo. • Checkboxes com avaliação de caso concreto: Com perguntas básicas sobre o tratamento de dados, e sobre os agentes para quem se pretende transferir as informações. À medida que o agente de tratamento vai respondendo as perguntas (com sim ou não), ao final o resultado demostra o tipo de cláusula que ele deverá utilizar. Estará também descrito informações sobre o modelo de contrato que deverá ser aplicado e um link para o modelo em Word editável. • Mapa mundial de adequação: Seguindo as boas práticas da Autoridade Francesa – CNIL2, deve-se elaborar um mapa mundial com descrição dos países adequados, países parcialmente adequados, países com Autoridade instituída, países com leis de proteção de dados e países sem lei específica. Cada país terá sua cor de referência na legenda. Ao clicar no país que deseja transferir os dados, abre-se uma caixa ao lado trazendo informações relevantes e links de mais conteúdo e/ou modelo de contrato&#2;padrão sugerido. • Infográfico ilustrativo: Poderia ser elaborado um infográfico ilustrativo e simplificado com perguntas. A resposta do agente indicará qual a seta e caminho o agente deverá seguir (mecanismo de perguntas e resposta se sim ou não). Sempre nos resultados poderá ser apresentado ainda mais conteúdo e o link do respectivo contrato aplicável. Segue um exemplo encontrado no site Eden Legal. Referências 1 ICO - https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the&#2;general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/#arewemaking (acessado em junho de 2022). 2 CNIL - https://www.cnil.fr/en/data-protection-around-the-world (acessado em junho de 2022). 3 EDEN LEGAL - https://www.edenlegal.com/blog/post.php?s=2016-07-20-infographic&#2;international-data-transfers-from-the-eu (acessado em junho de 2022).","174364":"","174367":"","174368":"","174369":"","174371":"","174372":"","174373":"","174375":"Sugere-se a criação e a constituição de organismo intergovernamental ou órgão no âmbito de entidade intergovernamental já existente, competente para a resolução administrativa de tais conflitos. A entidade pode ser debatida e estruturada a partir de acordo multilateral inspirado nos tratados e convenções internacionais afetas à propriedade intelectual. Exemplificativamente, assim como os escritórios de propriedade intelectual em cada País signatário do Acordo e do Protocolo de Madrid, Acordo de Haia e ou Tratado de Cooperação em Matéria de Patentes têm e exercem interface direta com o Escritório Internacional da Organização Mundial da Propriedade Intelectual sito em Genebra, as respectivas autoridades nacionais de proteção de dados nutririam, nessa proposta, o fluxo e o intercâmbio de procedimentos – coordenando sua atuação conforme parâmetros de referido órgão ou entidade intergovernamental. O fomento e a receita poderiam surgir de fundos solidários e compulsórios entre agentes que transfiram internacionalmente dados pessoais, compostos de contribuições proporcionais às especificidades do agente, do volume de dados pessoais, de avaliação econômica, patrimonial e financeira da empresa, conglomerado ou

grupo econômico e a classe e espécies de dados pessoais transferidos. Isso, sem prejuízo de contribuição também por parte dos países e/ou blocos regionais signatários. O fundo mútuo destinar-se-ia à operacionalização da entidade/órgão intergovernamental, incumbida de mediar, conciliar e dirimir conflitos entre agentes de tratamento e entre estes e titulares de dados. Quando entre agentes de tratamento, a competência para a resolução do conflito verificar-se-ia conforme disposição em contrato. Nada dispondo esse e se tratando de contrato por adesão, da jurisdição da parte aderente ou da parte que não redigiu o contrato, se identificável. Tratando-se de contrato paritário, a competência seria verificada nos termos do foro eleito contratualmente e, no silêncio do contrato, no país em que sediado o proponente (em paralelo ao §2º do art. 9º da Lei de Introdução às Normas do Direito Brasileiro). No que toca a conflitos envolvendo titulares, dada a hipossuficiência das pessoas naturais, faz-se necessário franquear a estas o acesso a tal entidade no país em que domiciliada, facilitando o acesso à jurisdição administrativa. Ainda, há de se pensar em mecanismos que garantam a acessibilidade e proteção adequada às partes hipossuficientes, garantindo o devido processo legal e o contraditório, assim como assegurando que as partes estão em simetria técnica e informacional com a disponibilização de pessoal competente e qualificado para orientação e esclarecimento, mitigando vantagens sistêmicas em prol de grandes litigantes. Sugere-se, ainda, sejam disponibilizados profissionais que orientem os titulares a serem mais práticos, eficientes e com uma boa ideia sobre os procedimentos. O procedimento deve ocorrer eletronicamente em sua íntegra, permitindo apresentação de alegações, postulações e documentos. Sugere-se que a instância final seja órgão da Autoridade Nacional de Proteção de Dados Pessoais no Brasil e congêneres nos demais países signatários dos eventuais acordos multilaterais. O procedimento poderia se dar no formato de resolução de disputas online (também conhecidas como ODR – Online Dispute Resolution). Há, no Brasil, exemplo de sucesso na seara do Direito do Consumidor; trata-se da plataforma www.consumigor.gov.br, lançada pelo Ministério da Justiça e Segurança Pública, em 2015. Na plataforma, partes (consumidores e empresas) dialogam e tentam resolver o conflito antes de uma solução heterocompositiva. Nas questões afetas à proteção de dados pessoais em nível internacional e às transferências nesse particular, agentes de tratamento e pessoas naturais poderiam tentar solucionar o conflito, antes de uma decisão heterocompositiva pela entidade intergovernamental. Vantagem desse modelo seria a otimização na gestão do tempo. Por meio de interações assíncronas, em detrimento de audiências, reuniões ou ligações, abrevia-se o procedimento e logra-se maior controle do momento voltado a essa atividade compositiva. Assim como na plataforma www.consumidor.gov.br, a reclamação é apresentada contra a parte supostamente infratora ou ofensora, tendo essa até prazo razoável para analisar a reclamação e respondê-la. A parte solicitante pode avaliar o atendimento, encerrá-lo dando-se por satisfeita contrapropor medida diversa ou solicitar o encaminhamento do caso a órgão decisório, que conhecerá e apreciará a demanda, podendo determinar medidas cautelares ou satisfativas, providências, sanções, recomendações ou requisições. Como os dados são públicos, viabilizaria pesquisa e criação de índices de solução, índices de satisfação, índices de prazo médio de resposta por fornecedor, propiciando sistema de monitoramento efetivo, que premia e propaga boas práticas na solução de demandas. Os agentes que transferem internacionalmente dados pessoais se cadastrariam obrigatoriamente

perante a plataforma, mediante portal operado e disponibilizado junto a cada autoridade dos respectivos países signatários. O arranjo, execução e coordenação de tal sistema poderiam ser capitaneados pela Autoridade Nacional de Proteção de Dados (ANPD) no exercício da competência disposta no inciso IX do art. 55-J da Lei Geral de Proteção de Dados Pessoais (LGPD). Referências 1. HUSEK, Carlos Roberto. Curso de direito internacional público. — 14ª. ed. — São Paulo: LTr, 2017; 2. ÓPICE BLUM, Renato; MALDONADO, Viviane Nóbrega (coords). LGPD: Lei Geral de Proteção de Dados Comentada 2ª. ed. rev., atual. e ampl. – São Paulo: Thomson Reuters Brasil, 2020.","174376":"","174378":"","174379":"","174380":"A necessidade de transferência internacional deve ser suficiente e claramente esclarecida ao titular, assim como quais dados estão envolvidos em tais transferências. Além das bases legais sob as quais são tratados os dados pessoais, objeto da transferência internacional, deve se garantir informação clara e transparente acerca da observância aos requisitos do art. 33 da LGPD. Sugere-se que esses pontos sejam objeto de destaque nas políticas de privacidade, em contratos, termos de uso e, acaso autorizados pela via do consentimento, seja esse formalizado em estrita observância ao inciso VIII do art. 33 da LGPD. Para que a informação seja útil a quem dela precisa ou para que surta os efeitos desejados, o destinatário das informações precisa ser o ponto focal, parte ativamente considerada na elaboração desses documentos de cunho jurídico ou técnico. O foco no usuário destinatário (em especial a pessoa natural) dá, atualmente, a tônica nos modelos de negócio, nos comportamentos e no mercado. No caso dos contratos e demais documentos em que o receptor das informações é o cidadão-médio, leigo, mais importante se faz o emprego de medidas que facilitem a compreensão do conteúdo dos instrumentos. Medidas como fluxogramas, diagramas, exemplos, ilustrações, gráficos, tabelas, vídeos, animações, inteirações, gamificação e outras formas eficazes de comunicação são recomendáveis. A adoção de medidas tais concretiza, inclusive, a transparência – obrigação que se reflete em vários aspectos do Direito, notadamente nas relações de consumo e no âmbito da privacidade e da proteção de dados pessoais. Outro aspecto de grande importância é a extensão do documento: documentos muito extensos tendem a não comunicar de forma eficaz o que se pretende. A capacidade de síntese e a noção do resultado pretendido são reflexos da empatia e do foco no leitor. Naturalmente, não se deve pretender suprimir informações, mas ter em mente que o contato do leitor com o documento de forma amigável e produtiva é o que vai viabilizar a produção do resultado pretendido. Tais esclarecimentos, cláusulas, termos ou políticas devem privilegiar sempre frases curtas e na ordem direta. Além de auxiliarem na agilidade da análise do documento, apoiam o processo de compreensão, considerando que existem tantas interpretações possíveis quanto há leitores. Quanto mais objetiva for a exposição, menos margem para interpretações diversas daquela objetivada. Linguagem acessível também está intimamente ligada à transparência, a qual, como dito, é privilegiada em vários aspectos da vida cotidiana e da ordem jurídica, seja no Brasil, seja em outros países. Partes em uma relação precisam compreender a extensão de seus direitos e deveres para que possam exercitar sua vontade e seus direitos da personalidade de forma livre e inequívoca. A falta de transparência tem consequências jurídicas indesejadas, e pode macular a própria relação contratual, pelo que são necessários os cuidados devidos com a apresentação e explicação do escopo, finalidade e necessidade da

transferência internacional. Também se faz pertinente a atuação educacional da ANPD, em continuidade às publicações, guias orientativos e fascículos já expedidos, no exercício da atribuição do art. 55-J, inciso VI da LGPD, promovendo à população orientação sobre questões pertinentes à transferência internacional de dados. Assim, municia-se a população para que esta também passe a fiscalizar tais operações internacionais de seu interesse. Referências 1. FRANCO, Isabel (org). Guia Prático de Compliance. – 1ª ed. – Rio de Janeiro: Forense, 2020;

Contribuinte: Poliane Almeida Silva Dias

Número: OP-183203

Data: 30/06/2022 - 08:53

Resumo: :"(Contribuição ABES) Transferência de dados do Brasil para outros países. O Congresso Nacional acertou ao incluir vários mecanismos para viabilizar a transferência de dados para outros países no artigo artigo 33 da LGPD. A possibilidade de uso do mecanismo mais apropriado para cada situação é primordial para o desenvolvimento econômico do Brasil, impulsionado pelo avanço da economia digital, sua competitividade internacional e inserção nas cadeias globais de valor cada vez mais digitalizadas. Entretanto, a regulamentação sobre os mecanismos internacionais de transferência de dados (artigo 33) ainda não está disponível. Isso gera insegurança jurídica para as empresas que precisam de tratamentos de dados realizados fora do Brasil. Nesse sentido, seria importante que a ANPD emitisse uma orientação formal reconhecendo que as cláusulas contratuais, desde que compatíveis com a legislação vigente e as melhores práticas internacionais, são aceitáveis. Transferência de dados de outros países para o Brasil. Infelizmente, alguns países têm adotado ou estão considerando políticas públicas que impedem ou dificultam a transferência internacional de dados para o Brasil, prejudicando a exportação de serviços por organizações brasileiras ou sua inserção em cadeias globais de valor. Assim, a liderança do Brasil contra tendências restritivas ao fluxo de dados entre fronteiras é de suma importância, já que as políticas que exijam a localização de dados ou limitem de forma desnecessária o seu fluxo transfronteiriço, vão em direção contrária à própria arquitetura da internet e podem prejudicar o crescimento econômico do Brasil. Uma das formas de se buscar soluções condizentes às melhores práticas de mercado seria, por exemplo, através da participação em discussões multilaterais como a OCDE, para a elaboração de princípios e diretrizes que fomentem a transferência internacional de dados. Conceito de Transferência Internacional de Dados : Nem todo o envio de dados pessoais do Brasil para outro país pode ser considerado como uma transferência internacional de dados. Uma interpretação sistemática da LGPD indica que "tratamento internacional de dados" e "transferência internacional de dados" não são sinônimos. Cabe ressaltar que nos termos do art. 5, inciso X, a "transferência" é apenas uma das espécies de tratamento de dados pessoais. Nesse sentido, apesar da definição trazida pelo inciso XV do art.5 não deixar claro o conceito de transferência internacional de dados, é possível inferir pela análise de outros dispositivos da LGPD, (arts, 13, §2º, 16, III, 5, XVI, 26, §1º, I, IV e V) que o termo "transferência" utilizado nesses dispositivos faz alusão ao

envio de dados de um agente de tratamento a outro.","174354":"(Contribuição ABES) Instrumentos contratuais são importantes mecanismos para transferência internacional de dados. A ANPD pode promover a interoperabilidade destes mecanismos com aqueles adotados internacionalmente através do reconhecimento de que contratos já celebrados por empresas para embasar transferências internacionais de dados podem ser utilizados e serão suficientes, contanto que incluam proteções similares àquelas exigidas pela LGPD. Fatores como sistemas jurídicos e outras peculiaridades de cada país podem ser considerados na construção de marcos legais para garantir a privacidade e proteção de dados. No entanto, a análise de adequação é apenas uma das alternativas elencadas no artigo 33 da LGPD para garantir a apropriada transferência internacional de dados. Nessa direção, considerando os aspectos globais da economia digital, é essencial que haja interoperabilidade dos mecanismos para a transferência internacional de dados, de forma a possibilitar o crescimento da economia dos países que os adotam. Além disso, o dinamismo dos modelos de negócio e das tecnologias que impulsionam a economia digital dependem de mecanismos para transferência internacional de dados que sejam flexíveis e baseados em níveis de risco. A ABES recomenda fortemente que a ANPD reconheça que contratos já existentes são mecanismos apropriados para embasar a transferência internacional de dados desde que estabeleçam proteções similares àquelas exigidas pela LGPD. Através desta abordagem, a ANPD obteria os resultados desejados, ou seja, a proteção dos dados de acordo com a LGPD, sem exigir a reformulação dos contratos já firmados para que adotem formato específico ou linguagem pré-aprovada. Além da interoperabilidade de instrumentos contratuais, como explicado nas respostas às próximas perguntas, a participação do Brasil em sistemas de certificação internacionais também contribuiria para avançar a convergência e interoperabilidade de mecanismos para transferência internacional de dados. Nesse sentido, poderia ser de grande valia para a nossa competitividade, uma eventual aproximação do Brasil ao arranjo de certificação e boas práticas elaborado pelos países da Cooperação Econômica da Ásia e do Pacífico (APEC).","174356":"(Contribuição ABES) É importante ressaltar que o mecanismo a ser utilizado por uma determinada organização para legitimar suas atividades de transferência internacional de dados pessoais pode variar e deve ser escolhido pelo exportador e importador de dados como aquele que melhor se adapta a cada modelo de negócios. Por exemplo, um controlador de dados pessoais no Brasil poderá escolher a utilização de um contrato para legitimar a transferência internacional de dados para uma empresa operadora localizada em outro país. Outro exemplo: a mesma empresa controladora de dados no Brasil poderá optar pelo uso de normas corporativas globais ("binding corporate rules") para transferir dados para uma de suas empresas subsidiárias sediada no Reino Unido. Em suma, a efetividade do mecanismo a ser utilizado para a transferência internacional de dados vai depender das especificidades de cada caso. Levando em consideração os pontos acima descritos, o instrumento utilizado mais frequentemente por empresas para legitimar a transferência responsável de dados ao redor do mundo é o instrumentos contratual, pois seu o uso não depende de autorização prévia por autoridades de proteção de dados, o que facilita a sua implementação por empresas globais. Exemplos de instrumentos contratuais utilizados por empresas que participam em transações que envolvem transferência internacional de dados constantemente incluem as cláusulas contratuais padrão da União Europeia (EU SCCs)

e Acordos para Transferência Internacionais de Dados do Reino Unido (UK IDTAs). Mecanismos como o reconhecimento do nível de proteção de dados de outros países e uso de certificações internacionais também devem ser utilizados para legitimar a transferência internacional de dados. Cabe ressaltar que a LGPD não prevê relação hierárquica entre os mecanismos de transferência, diferente do que ocorre no GDPR. A escolha pelos agentes de tratamento dependerá de critérios como finalidade, contexto da transferência e natureza dos dados, entre outros.","174359":"(Contribuição ABES) Entidades governamentais e organizações privadas em todos os setores produtivos e de todos os portes (incluindo micro, pequenas e médias empresas) utilizam tecnologias que dependem da transferência internacional de dados para aumentar a produtividade e eficiência de suas atividades, gerando empregos e outros benefícios para a sociedade. Alguns exemplos de atividades que são desenvolvidas através de tecnologias que dependem da transferência internacional de dados pessoais incluem: utilização de diversos serviços em nuvem, fornecimento de produtos e serviços para clientes internacionais, serviços de educação à distância, treinamento e capacitação virtual de colaboradores, análise de informações para detecção de fraude e ameaças cibernética, entre outros. Para que o Brasil continue usufruindo dos benefícios da economia global digital é importante que a ANPD promova o uso de mecanismos interoperáveis, conforme discutido nas respostas às perguntas 2 e 3 acima. ","174360":"(Contribuição ABES) cláusulas-padrão contratuais : Reconhecemos muitas vantagens no campo da padronização, mas elas podem dificultar a adoção entre Prestadores e Tomadores de serviços. cláusulas contratuais específicas : poderia ser prático e viável desde que a regulação estabeleça diretrizes para a construção de cláusulas, sem fixar (“engessar”) sua redação, tal como ocorre no modelo adotado pela Nova Zelândia. normas corporativas globais : são efetivas mas aplicam-se apenas às grandes empresas com atuação global. Recomendamos que as empresas que possuam BCRs (Binding Corporate Rules) já aprovadas em outras jurisdições com legislação equivalente à LGPD (como nos casos da União Européia, Reino Unido e EU), tenham o processo de aprovação de suas cláusulas corporativas abreviado, tal como já ocorre no Reino Unido.","174361":"(Contribuição ABES) É importante ressaltar que a avaliação do nível de proteção de dados de países ou organismos estrangeiros feita pela ANPD e o uso de instrumentos contratuais, são dois mecanismos distintos, podendo cada um deles ser usado individualmente para legitimar a transferência internacional de dados pessoais. Não há, portanto, hierarquia entre os mecanismos previstos no artigo 33 da LGPD, sendo todos, individual e igualmente qualificados para essa finalidade. A ABES recomenda fortemente que a ANPD não exija que as empresas optantes pela adoção de instrumentos contratuais, sejam também obrigadas a realizar uma avaliação do nível de proteção de dados de países ou organismos estrangeiros para os quais os dados serão transferidos. Conforme exposto anteriormente, os instrumentos contratuais por si só, são suficientes para legitimar as transferências internacionais de dados. Muitas empresas, principalmente as de pequeno e médio porte, não estão preparadas para realizar o tipo de análise detalhada e complexa do ordenamento jurídico e ambiente regulatório de países estrangeiros nos termos do artigo 34 da LGPD. A exigência de tal análise impossibilitaria o uso de instrumentos contratuais por grande parte das empresas, criaria insegurança jurídica e não traria benefícios adicionais significativos para os titulares

de dados. Entendemos que as cláusulas padrão contratuais constituem instrumento de salvaguarda e proteção adequado para a transferência internacional, inclusive para países em que não houve determinação de nível de adequação para fins do art. 34 da LGPD. Desta forma, entendemos, complementarmente, que a adoção de cláusulas padrão contratuais deve ser feita de forma apartada e independente da análise de determinação do nível de adequação de um país ou organismo estrangeiro.","174362":"(Contribuição ABES) A ABES sugere que a ANPD adote uma posição flexível quanto ao uso de mecanismos contratuais utilizados como forma de legitimar transferências internacionais de dados. Além disso, conforme explicado em nossa resposta à pergunta 2 acima, recomendamos fortemente que a ANPD reconheça que contratos já existentes e que contenham proteções substancialmente similares àquelas exigidas pela LGPD, são mecanismos apropriados para embasar a transferência internacional de dados. O não conflito com cláusulas-padrão contratuais já adotadas no padrão europeu, por exemplo, permitirá que o agente continue a utilizar tais cláusulas, sem necessidade de alterá-las. Através desta abordagem, a ANPD definiria os requisitos mínimos desejados, sem demandar do agente de tratamento a necessidade de alterá-las para o texto base a ser proposto pela Autoridade. Cabe destacar que muitas empresas já utilizam contratos baseados em legislações de outros países que possuem proteções análogas àquelas exigidas pela LGPD. Deste modo, tais contratos são capazes de oferecer proteção substancialmente similar e o seria extremamente importante, e vantajoso, que o uso de tais contratos fosse autorizado pela ANPD. Caso as cláusulas contratuais modelo sejam adotadas, é necessária alguma flexibilidade para compensar as diferenças nas estruturas organizacionais ou nos ecossistemas de tratamento de dados únicos. Nesse sentido, a Autoridade poderia especificar um conteúdo mínimo para as cláusulas contratuais, permitindo que sejam modificadas desde que mantidas as proteções necessárias.","174363":"(Contribuição ABES) Conforme explicado nas respostas às perguntas 2 e 7 deste documento, a ABES recomenda que ANPD adote uma posição flexível quanto ao uso de mecanismos contratuais utilizados como forma de legitimar as transferências internacionais de dados. As partes devem permanecer livres para negociar os aspectos comerciais de seus contratos, incluindo detalhes sobre os direitos de auditoria (por exemplo, quem é o responsável financeiro pela auditoria, quando a auditoria pode ocorrer, o aviso prévio necessário, os efeitos sobre o preço, etc.), nível de cooperação em relação ao exercício dos direitos de proteção de dados, definição de níveis de serviço e limites de responsabilidade, entre outros. Sugerimos também, conforme já mencionado anteriormente neste documento, que a ANPD reconheça como válidos os contratos já existentes que contenham proteções similares àquelas exigidas pela LGPD. A ANPD pode também preparar cláusulas modelo de contratos para ajudar as empresas que ainda não utilizam instrumentos contratuais, mas que desejem fazê-lo. Esta foi a posição adotada, por exemplo, pela Nova Zelândia, um dos países reconhecidos pela União Européia como um país que oferece um nível de proteção de dados semelhante ao oferecido pela União Européia. Cabe ressaltar que as cláusulas modelo neozelandesas são de uso opcional e, como o nome indica, servem apenas de modelo. A autoridade de proteção de dados daquele país permite que as organizações modifiquem as cláusulas modelo para formar os seus próprios contratos, desde que as proteções básicas estabelecidas nas cláusulas estejam presentes (detalhes disponíveis em: https://privacy.org.nz/publications/statements-media-releases/new-

principle-for-disclosing-personal-information-overseas/ . Acesso em 13 de junho de 2022) Caso a ANPD decida adotar cláusulas contratuais padrão, recomendamos que seja avaliada a posição recentemente adotada pelo Reino Unido que, a despeito de ter estabelecido cláusulas contratuais padrão próprias, também permitiu que as empresas que já utilizam as cláusulas contratuais da União Europeia adotem um adendo mais curto ao seu contrato, contendo apenas algumas cláusulas adicionais. Com isso, o contrato original é reconhecido, sendo suplementado pelas disposições do adendo. A ANPD poderia considerar a adoção de adendos, se necessário, mas caso o contrato original já ofereça os mesmos níveis de proteção da ANPD, seu uso poderia ser dispensado. ","174364":"(Contribuição ABES) Sugerimos a adoção de contratos diferentes, dependendo da relação jurídica entre as partes. Se a ANPD adota cláusulas-padrão, é importante levar em conta os diferentes tipos de transferências (Controlador/Controlador, Controlador/Operador, Operador/Controlador e Operador/Operador). Cada um destes tipos de transferências tem suas peculiaridades e necessita de cláusulas contratuais que reflitam as suas características próprias. Por exemplo, a UE adotou recentemente uma abordagem modular para suas cláusulas-padrões, no qual módulos podem ser utilizados para compor um contrato dependendo do tipo de transferência. Qualquer que seja a abordagem de contratação da ANPD (modular ou não), deve haver flexibilidade suficiente para contemplar os diferentes tipos de transferências de dados.","174367":"(Contribuição ABES) Conforme o exposto na resposta à pergunta 9, as cláusulas-padrão devem incluir quatro cenários de transferência diferentes (Controlador/Controlador, Controlador/Operador, Operador/Controlador e Operador/Operador), enquanto as Normas Corporativas Globais devem se concentrar em duas situações de transferência (grupo de empresas como controlador ou grupo de empresas como operador). Os quatro cenários de transferência nas cláusulas-padrão detalham a complexidade das situações de transferência aplicáveis que não fazem tanto sentido em um contexto de Normas Corporativas Globais. ","174368":"Sem sugestões para esta questão.","174369":"Sem sugestões para esta questão.","174371":"(Contribuição ABES) Vivemos em um mundo onde os fluxos de dados internacionais se tornaram indispensáveis ao funcionamento da economia global. Sem fluxos de dados internacionais, tecnologias transformacionais como inteligência artificial, Internet das Coisas e blockchain, todas alimentadas por grandes quantidades de dados e atendendo a uma variedade de mercados e usuários, não prosperarão. Indivíduos dependem de fluxos de dados para acessar saúde, educação e outros serviços essenciais e vêm fazendo isso mais do que nunca desde o início da pandemia de COVID-19. Os fluxos de dados internacionais fortalecem a segurança cibernética. Os ataques cibernéticos são geralmente internacionais. Portanto, a segurança cibernética exige o compartilhamento de dados, rápido e eficaz, em uma base global. Impedir tal compartilhamento dificultaria a necessária coordenação internacional.","174372":"(Contribuição ABES) Entendemos que esta pergunta se refere à aprovação de cláusulas contratuais específicas. Entretanto, para que não reste dúvidas, é importante que a ANPD esclareça que, caso autorizados pela ANPD como solicitamos aqui, o uso de cláusulas contratuais modelo ou de outros arranjos contratuais que contenham proteções substancialmente similares àquelas exigidas pela LGPD não requer a autorização prévia da ANPD. Nestes casos, bastaria à ANPD especificar os resultados desejados, ou seja

a proteção dos dados de acordo com a LGPD, ao invés de exigir contratos em formato específico ou linguagem pré-aprovada. No que tange à aprovação de cláusulas corporativas globais, recomendamos que as empresas que possuam BCRs (Binding Corporate Rules) já aprovadas em outras jurisdições com legislação equivalente à LGPD (União Europeia e Reino Unido e EU, por exemplo), tenham o processo de aprovação de suas cláusulas corporativas abreviado, tal como já ocorre no Reino Unido.","174373":"(Contribuição ABES) Entendemos que o Titular não é parte da relação contratual e, portanto, a aprovação dos titulares dos dados não deve ser exigida em acordos contratuais entre exportador e importador de dados, desde que o mecanismo utilizado esteja em conformidade com a LGPD e mantenha todas as garantias dos direitos deste titular de dados independentemente de alterações em sua configuração.","174375":"Sem sugestões para esta questão. ","174376":"(Contribuição ABES) Uma ótima alternativa seria a emissão pela ANPD de um Guia e Diretrizes e/ou um guia educativo com orientações para as empresas sobre como os mecanismos de transferência devem ser implementados de acordo com as normas da LGPD e melhores práticas. Esse guia, bem como todas as informações adicionais, poderiam ser divulgados através do site da ANPD. Alguns exemplos de jurisdições que reúnem informações sobre a transferência internacional de dados em seus websites incluem: Reino Unido: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/international-transfers-after-uk-exit/). Nova Zelândia : https://privacy.org.nz/publications/statements-media-releases/new-principle-for-disclosing-personal-information-overseas/ Apoiamos as iniciativas da ANPD no sentido de continuar trabalhando com a cooperação das partes interessadas à medida em que desenvolve seus regulamentos de modo a promover trocas de experiências já vividas pelas empresas. ","174378":"Sem sugestões para esta questão. ","174379":"(Contribuição ABES) Quando uma autoridade pública de um país estrangeiro requerer acesso aos dados pessoais, a obrigação do importador de dados deve ser notificar o exportador de dados o quanto antes. Entretanto, esta obrigação não deve ser absoluta, devendo reconhecer que a lei do país no qual o importador se encontra pode proibir a notificação imediata ao exportador de dados ou limitar as informações que podem ser incluídas na notificação. Neste caso, a obrigação do importador de dados deve ser comunicar ao importador de dados que a ordem foi recebida assim que ele for autorizado a fazê-lo. Esta notificação deve incluir uma quantidade razoável de detalhes de acordo com o permitido pela legislação do país do importador de dados. As obrigações de acesso aos dados por determinação de autoridades públicas estrangeiras devem ser globalmente harmonizadas para que as obrigações para importadores e exportadores sejam consistentes e interoperáveis ¿¿com estruturas internacionalmente reconhecidas, como aquelas que estão sendo desenvolvidas pelo grupo de trabalho da OCDE sobre acesso governamental confiável. Nesse sentido, se um Estado soberano ordena a disponibilização dos dados que se encontrem sob controle de entidade sob jurisdição de outro Estado soberano, não há outra opção senão recorrer ao instituto jurídico da cooperação internacional, de modo a conciliar a soberania brasileira e a soberania dos Estados estrangeiros. Essa é a resposta que clama o art. 4º, incisos VII e IV, da CF, que privilegia o dever de cooperação entre os povos para o progresso da humanidade, assim como o da solução pacífica dos conflitos. Ademais, no mesmo sentido da regra constitucional, o Código de Processo Civil

Contributions on International Transfers

Proposal of answering the Question 06 from Brazilian Data Protection Authority (ANPD) call for contributions

Disclaimer:

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design, and manufacturing. OneTrust LLC shall have no liability for any error or damage of any kind resulting from the use of this document.

OneTrust products, content and materials are for informational purposes only and not for the purpose of providing legal advice. You should contact your attorney to obtain advice with respect to any particular issue. OneTrust materials do not guarantee compliance with applicable laws and regulations.

OneTrust Privacy
PRIVACY MANAGEMENT SOFTWARE

Executive Summary

The document intends to indicate a technical methodology to produce a "Guideline for Recommendations for Assessment of Adequacy" by Brazilian Data Protection Authority (ANPD). The technical research and the Guideline proposed to intend to answer Question 06 from the public call for contributions indicating four core aspects the DPA must follow to produce the Guideline:

(i) Existing European Data Protection Principles and Guidelines.

(ii) Technical and Organisational Measures applied to the data transfers to avoid or minimize the level of intrusion and unauthorized access of personal data from public governmental agencies.

(iii) Principles of private international law within the context of contractual provisions interpretation on an international data transfer also emphasizing the relevant covenants ratified by the Brazilian Government.

(iv) Operational requirements on SCCs implementations.

Finally, the document explains why a normative resolution like the Guideline suggested should be mandatory based on Brazilian Legislation provisions (Federal Law 13.655/2018, Law-Decree 4657/1942, and Presidential Decree 9830/2019).

Answering Question 06

6) To what extent should the elements be considered by ANPD in assessing the level of data protection of foreign countries or international bodies for adequacy purposes (article 34 of the LGPD) also be considered within the scope of the rules for contractual instruments?

The suggestive approach is creating a "Guideline for Recommendations for Assessment of Adequacy". The document would be the leading methodology for two specific situations:

(i) ANPD official procedure to qualify a foreign country or an international body as adequate.

(ii) A recommendation of methodology to organizations to build internal procedures regarding how companies in Brazil will produce their Transfer Impact Assessments (TIA), how they will operate in future negotiations with their Standard Contractual Clauses (SCCs) or Binding Corporate Rules, what kind of specific clauses would be necessary to modify ad-hoc contracts in terms of privacy and data protection, and what minimum baseline should be assessed when it's essential to define supplementary technical measures for troubleshot transfers (e.g. the current scenario of transfers between EEA and the US).

Considering Brazil as a country also inserted on the global economy and with an intense data flow considering variables regions in the World, the recommendations for an internal assessment of adequacy should consider not only the European positions (e.g. EDPB Guidelines or European DPAs opinions such as CNIL or AEPD) regarding the European level of assurance, but also a qualitative approach on technical measures adopted (e.g. IT Infrastructure on the firewall, proxy, antivirus or encryption) to consider localized opinions and patterns (e.g. from Asia-Pacific, Africa, and the United States) as well adequate.

Regarding the global perspectives mentioned, ANPD must consider the possibility of deeming data transfer contracts of other jurisdictions (EU SCCs, UK IDTA etc.) valid under the Brazilian regime, with the caveat of a national addendum capturing the necessary amendments under LGPD.

This might function in reference to the jurisdictions ANPD will consider appropriate under Articles 33(I) and 34 LGPD giving to the transfers two necessary safeguards: (i) providing organisations operating globally with the ability to adapt

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

more quickly to the new regime and (ii) demonstrating the fact that the ANPD considers international data transfer standards and principles when addressing a topic that is naturally cross-border.

Considering the previous introduction, furthering we explain the main aspects ANPD must integrate into this Guideline to provide clear parameters to the adequacy assessment and viability of the global interoperability desire regarding the SCCs: (i) technical aspects for the assessment methodology and for the SCCs clauses content and (ii) operational aspects regarding the scope of application and transfers scenarios ANPD will qualify as feasible to use SCCs to safeguard an international data transfer in light of LGPD.

Technical and Organisational Aspects

The technical aspects to be considered in the production of this Guideline could be grouped as follows:

- **Encompassing European Data Protection Principles and Guidelines[i] into an international data transfer tool with contract provisions describing at least:**
    1. The transfer must have an adequate legal instrument to define the baseline for rules and obligations. The instruments adopted should be understood in a broad way and the best transfer tool must be assessed individually following one of these recommendations:
        - Legally binding and enforceable instrument between public authorities or bodies.
        - Binding corporate rules.
        - Standard Contractual Clauses adopted by the DPA from the data exporter country and recognized as adequate in the data importer country.
        - Code of Conduct approved in the data exporter country and with enforceable commitments (e.g. implementation of shared safeguards or combined procedures to guarantee data subject rights) valid in the data importer country.
        - Certification Scheme approved in the data exporter country and with enforceable commitments (e.g. implementation of shared safeguards or combined procedures to guarantee data subject rights) valid in the data importer country.
        - Ad-hoc contractual clauses approved in the data exporter country and with enforceable commitments (e.g. implementation of shared safeguards or combined procedures to guarantee data subject rights) valid in the data importer country.
    2. The transfer must indicate a clear purpose limitation as the data cannot be subsequently used for secondary purposes not described on the legal instrument (e.g. SCCs or Binding Corporate Rules) as well the presence of strict rules and prohibitions considering onward transfers.
    3. The contracting parties must assure practical measures to guarantee in all data lifecycle the safeguard of data quality, the respect to minimization in the collection and usage as well clear criteria to define what's understood an acceptable level of proportionality to use data.
    4. The contracting parties must assure measures of transparency describing:
        - To whom and why data is being transferred.
        - What kind of security and technical measures are used to safeguard transfer to unauthorized access both from third-party organizations as well as public authorities.
        - Adoption of the less restrictive and most protective framework regarding data subject rights as well as indicating the list of data subject rights.
    5. Consideration of the legal and regulatory scenario of the importer country with these minimum qualitative characteristics:
        - The overall compliance system has a good level of enforcement considering: (i) the Existence of special legislation as a baseline to enforce privacy and data protection norms; (ii) The existence of dissuasive sanctions of any level to enforce the privacy and data protection obligations and (iii) The existence of a Data Protection Authority or any correlated Regulatory Governmental Agency with sufficient legal powers to independently monitor and enforce the rules regarding privacy and data protection.

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

- An appropriate adjudicatory system where the data subject can file claims and exercise an appropriate level of redress. Considering the differences in constitutionalism tradition development, an appropriate adjudicatory system must be considered in a broad way and not always related to traditional judicial courts. An efficient baseline to consider if an adjudicatory system has the probability to produce a fair decision is adopting Michael Asimow analytical methodology presented in his paper "Five Models of Administrative Adjudication[ii]". There are no hindrances to judicial activity outside the strict Judicial Courts if the following characteristics can be recognized in the administrative model: (i) Impartiality in the adjudicatory system, (ii) Competency determined by law or Constitution to adjudicate special claims; (iii) Independency of the adjudicatory body' (iv) Separation by technical criteria the investigatory function from the decisional competency even inside the same adjudicatory body; (v) Adversarial characteristics on the procedure; (vi) Mandatory double degree of jurisdiction for review of decisions even in the same adjudicatory body; (vii) respect to human rights ensuring unrestricted access for harmed individuals and (viii) practical mechanisms to enforce the sanctions imposed and allows compensation's paying when it's appropriate.

- **Identifiable IT technical and organisational measures[iii] applied on the data transfer to avoid or minimize the level of intrusion, unauthorized access of personal data from public governmental agencies and guarantee at least a minimum assurance of confidentiality, integrity, and availability preservation on data processed and transferred:**
  1. Clear identification of the technical transmission tool used (e.g. e-mail, dedicated mobile apps, or shared file storage).
  2. If the application is in-house developed, identify what measures were used to address privacy safeguards on a development environment, SDKs, and system software.
  3. How the IT infrastructure used for data processing and transferring can contribute to guaranteeing the desired level of data protection and preservation of the confidentiality, availability, and integrity of personal data. Several measures can be quoted here with the desired purpose to calibrate a high level of data protection and privacy compliance. An exemplificative list could be:
     - Encryption
     - Network Analysis tools
     - Anti-virus tools
     - Firewalls
     - Security patches regularly
     - Reverse proxy techniques
     - Localization options for database and application servers[iv]
     - Possibility to adopt a virtualization system
  4. What kind of rules do both data importer and exporter adopts to create reasonable practical measures to generally safeguard privacy and data protection in the companies:
     - Privacy and Security internal policies
     - Well-designed procedures to conduct Privacy Impact Assessments
     - Well-designed procedures to conduct Threat Risk Assessments
     - Authentication and access control on corporate systems and applications considering information access privileges
     - Logging and monitoring for future auditing
     - Strong password policy
     - Incident and Disaster Recovery Plans and Procedures
     - International privacy and security standards such as:
       i) ISO 27701
       ii) ISO 27001
       iii) ISO 27002
       iv) ISO 29100
       v) ISO 29134
       vi) ISO 29151
       vii) ISO 29184
       viii) ISO 29190
       ix) NIST Privacy Framework

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

x) SOC Reports
xi) Specific compliance reports depending on the economic activity such as the PCI DSS Report.

5. How can collateral data processing activities on both data exporter and importer organizations could affect directly or indirectly the privacy and data protection safeguards applied. As collateral data processing activities we could list:
    - Processing carried out with the intent of social networks and advertising activities (e.g. use of cookies or data mining).
    - Associated transfers with possible software that can be installed by company employees. Here an IT Information Security Policy with admin restrictions could minimize the risk of associated undesired transfers.
    - Online services subscribed and used by employees to identify other sources of possible data transfers that could affect indirectly the main transfer regulated in the data processing agreement.

- **Application of the principles of private international law (such as treaties or conventions) within the context of contractual provisions interpretation**
    1. Taking into consideration the different approaches national privacy legislation can have when drafted (e.g. as Global Comprehensive laws like GDPR or LGPD, Sectoral regulations like United States, Co-regulatory model like Australia, or State Centric Model like China and Russia), it's necessary to use a common standard framework based on private international law to define the extent of obligations and rules.
    2. Principles of private international law are necessary to be applicable in the situation to avoid undesired blockage on data transfer or to not guarantee a certain data subject right of a special jurisdiction in the instrument. A brief commentary relating the mentioned principles with privacy-related situations can be the following:
        - Avoidance to apply on international data transfers the **principle of non-transactivity or non-negotiation of laws** to avoid the understanding of only one privacy legislation or jurisdiction as valid.
        - The **principle of extraterritoriality** must be applied to an international data transfer to guarantee equally valid the transfer by both data importer and exporter legislation due to the guarantee of interoperability and enforcement of the importer and exporter legislation.
        - **Good faith in the performance of international obligations** to not create unreasonable obstacles to promoting international data transfers or unnoticed changes in positions of the understanding about the international transfer tools that are legally valid.
    3. The adequacy assessment needs to model the transfer tool considering both hard law and soft law instruments from private international legislation to define what's considered acceptable privacy-centric behaviors from data exporter and data importer, what's the limitation of controller and processor responsibility in the activity, and in what extent national privacy legislation from exporter and importer countries will be applied.
    4. Considering Treaties and Conventions as legally binding enforcement instruments, in this case, the relevance is highlighted by the treaties and conventions already ratified by the Brazilian Government. In this situation, those documents must be respected equally as national law. For data protection and privacy, the following treaties and conventions could be relevant when understanding the adequacy of a country or enforcing contractual provisions:
        - **International Covenant on Economic, Social, and Cultural Rights** adopted by the UN General Assembly on 19 December 1966 and ratified by the Brazilian Government on 06 July 1992 by the Legislative Decree 591/92[v]. The interoperability of an international data transfer tool and the necessity to openness in the interpretation of the data flow can be understood as an obligation derived from Article 02[vi] regarding the obligation of the countries to guarantee in maximum the assistance and international cooperation on economic and technical field.
        - **International Covenant on Civil and Political Rights** adopted by the UN General Assembly on 16 December 1966 and ratified by the Brazilian Government on 06 July 1992 by the Legislative Decree 592/92[vii]. The necessity to create an international transfer tool that encompasses different types of privacy legislation and also guarantees in a legal biding

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

instrument (e.g. the contract) data subject rights from different jurisdictions can be understood as an obligation derived from Article 2 (1) (2) and (3)[viii].

- **San José da Costa Rica Covenant also nominated The American Convention on Human Rights** adopted under the approval of the Organization of American States (OAS) in 22 November 1969 and ratified by the Brazilian Government on 06 November 1992 by Legislative Decree 678/92[ix]. This instrument enforces the necessity to not only recognize global human rights (e.g. freedom speech, privacy, non-discrimination or integrity) but also regarding the obligation of the Brazilian State to recognize Court access, the possibility of litigation and redress, and the same constitutional judicial guarantees to non-national. Also, the instrument imposes to the Brazilian National State the right to compensation on the national territory to all human being. These provisions can be understood by the application of Articles 24 and 25[x].
- **Convention on the Rights of the Child** adopted by the UN General Assembly on 20 November 1989 and ratified by the Brazilian Government on 21 November 1990 by the Legislative Decree 99.710/90[xi]. This international document highlights the necessity to incorporate the adequacy analysis and contractual dispositions protections related to children against arbitrary or unlawful interference with their privacy.

5. Other international law instruments[xii] are understood generally as soft law, but in specific situations can be turned out into hard law (e.g. if legally enforced by an international court such as the European Court of Justice or the Inter-American Commission on Human Rights). These instruments are essential to be a baseline for a common analysis framework when understanding the permissible situations to process personal data in different countries:
   - **Universal Declaration of Human Rights**
   - **The Guidelines for the Regulation of Computerized Personal Data Files**
   - **The Special Rapporteur on the Right to Privacy (United Nations Report)**
   - **The Personal Data Protection and Privacy Principles (United Nations Memorandum)**
   - **The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Privacy Guidelines)**
   - **The Revised OECD Privacy Framework**
   - **APEC Privacy Framework**
   - **Madrid Resolution**
   - **ASEAN Human Rights Declaration**

Operational Aspects

ANPD must consider a flexible approach that would encompass a wide range of data transfers use cases, especially considering the different roles of the exporters and importers (controller, processor, sub-processor), like what done by the EU SCCs[xiii]. In addition, explore the possibility of also addressing the applicability of the SCCs to the following use cases, if deemed necessary:

1. Transfer to a non-Brazilian importer that is subject to the LGPD according to Art. 3 (I) and (II) of the LGPD.
2. Subprocessor-2P transfers, by subprocessors subject to LGPD *back* to processors not subject to LGPD.
3. A controller outside Brazil whose processing is subject to LGPD due to Article 3 (II) or (III) to a controller or processor outside Brazil processing data on whose behalf transferred it (e.g. providing security features or organizing administrative and financial aspects of the activity) and not subject to LGPD regarding the following scenarios:
   i) Article 3 (II) first part: the processing activity aims to offer or supply goods or services located in the national territory – This scenario is applied to any foreign company, with or without physical presence in Brazil, that targets the Brazilian market and offers products or services even if the headquarters or data is not located in Brazil. **The company here may be a data exporter or importer depending on the contextual flowchart of further transfers as the company is subject to LGPD by the economic aspect due to the offering of products and services in Brazilian territory.**
   ii) Article 3 (II) second part: the processing activity aims the processing of data of individuals located in the national territory – This scenario is applied to any foreign company, with or without physical presence in Brazil, that uses personal data collected from data subjects located in Brazilian territory

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

(not necessarily Brazilian citizen as it can be any individual) in its processing activity and the processing activity. **In this case, the company subject to LGPD can be a data importer because the processing activity will use data collected from individuals that are physically located in Brazil in the moment of data collection and the data can be used outside Brazilian territory if we have a transfer operation.**

iii) Article 3 (III): the personal data related to the processing activity has been collected in the national territory. This scenario is applied to any foreign company, with or without physical presence in Brazil, that collects personal data from individuals outside Brazil (as the individuals located in Brazil is subject to the Article 3 (II) LGPD) and the collection activity occurs inside Brazilian territory. This legal provision was probably established to avoid 'data protection tax havens', a situation in which a foreign company (e.g. a data broker or a data miner) can establish its data collection activity in a territory that has a legal loophole for not applying data protection rules with reference to data collection. **The company here will be always a data importer as it is subject to LGPD by the fact that the personal data collection stage occurs inside Brazilian territory due the arrangement of its operations, regardless: (i) personal data collected has its origin outside Brazilian territory and (ii) personal data collected will be used in processing activities outside Brazil. If the company do not proceed with further processing activities operations inside Brazilian territory (avoiding the application of Article 3 (I) LGPD) the company will be also a data exporter as it will occur a transfer to where the processing activity will be carried.**

4. Situations where it will be possible for third parties to join the SCCs (docking clause) and, when doing so, establish a clear mechanism for new parties to join, avoiding legal uncertainties and burdensome negotiations for organizations. In special, considering the docking clause, the guidance must specify the following concepts and applicability:
    i) Permitted purposes to use the docking clause.
    ii) Formal requirements to allow third-parties integrations on the docking clause (e.g. how pre-existing parties can formalize the consent or if one party can agree on behalf of all pre-existing parties to the engagement of a new party).
    iii) Consequences for the third party who engages in a docking clause.
5. Situations where it will be possible to provide specific clauses and/or guidance to address in a flexible way the liability of the parties (importer/exporter) under the data transfer contract, eventually leaving some limited space for negotiations, with the aim of avoiding a situation where organizations refrain from entering the SCCs given the risks related to liability.
6. Consider providing a flexible timeframe/deadline to enable organizations to practically implement the transfer contracts, once approved.
7. Detailed explanation about what measures will be considered to qualify a third country or international entity as adequate based on Article 34 LGPD. Regarding the legal requirements addressed in Article 34, it's necessary for a special clarification about Article 34 (II), the nature of data, taking into consideration how it will be implemented in a third country assessment, or if it's a requirement to be analyzed only *case-by-case* depending on the transfer operation. China has a similar approach considering the nature of data when assessing an international data transfer[xiv]. Regardless of the situation where the nature of data will be assessed, we could follow some technical criteria to define classifications considering the nature of data on a transfer based on the following elements:
    i) The amount of data collected.
    ii) The type of data collected.
    iii) If the data has some level of sensitivity based on legal classifications considering both LGPD and the third-country legislation.
    iv) National security impacts.
    v) Economic development relation.
    vi) Social or public interests regarding the transfer.

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

Conclusion

The purpose of the Guideline is to demonstrate a position that more important than the adequate transfer tool used to enforce the data transfer as lawful is to identify the specific technical and organizational supplementary measures that your data are being safeguarded from undesired surveillance. A Guideline indicating an initial framework as a baseline for the Transfer Impact Assessment would permit better interoperability between the different jurisdictions and requirements regarding international data transfers.

Also important, a Guideline expressing the three main points exposed can be also understood as a regulatory instrument obligated by the Brazilian Law when we consider the general provisions on legal certainty and efficiency in the creation and enforcement of public law designed by Federal Law 13.655/2018 and topographic added into the Introductory Law to Brazilian Legislation (Law-Decree 4657/1942)[xv]:

- Prohibition of administrative entities from take decisions on abstract values (Article 20 from Law-Decree 4657/1942)
- The necessity to indicate the consequences of act or contract invalidation by an administrative entity (Article 21 from Law-Decree 4657/1942)
- The obligation the public authorities and administrative entities have to always demonstrate in a public manner the general technical orientations of some subject before taking any decision regarding the invalidation of a contract, act, or administrative rule (Article 24 from Law-Decree 4657/1942).
- The obligation of public authorities and administrative entities to publish complementary norms and guidelines to increase legal certainty regarding the application of national legislation (Article 19 from Presidential Decree 9830/2019 regulating the Article 20 from Law-Decree 4657/1942).

---

[i] Here we are making a clear reference considering the GDPR as our main legal baseline. However, several technical opinions from governmental bodies and DPAs were considered to build the European approach like the following:

- EDPS Position Paper "The transfer of personal data to third countries and international organisations by EU and bodies": https://edps.europa.eu/sites/edp/files/publication/14-07-14_transfer_third_countries_en.pdf
- AEPD General Recommendations: https://www.aepd.es/es/preguntas-frecuentes/6-transferencias-internacionales-bcr-codigos-de-conducta/1-transferencias-internacionales/FAQ-0601-supuestos-rgpd-para-transferencias-internacionales

[ii] Asimow mentioned paper can be accessed here: https://www.jstor.org/stable/26386647

[iii] Creating a list of technical measures to safeguard data subject privacy and guarantee a considerable level of data protection is not easy and it's impossible to create a closed list. However, the following recommendations can be useful to create a methodology on how to assess the state-of-the-art considering IT technological features:

- CNIL international data transfers assessments: https://www.cnil.fr/fr/responsables-de-traitement-comment-identifier-et-traiter-des-transferts-de-donnees-hors-ue
- Ontario Privacy Commissioner Recommendations: https://www.ipc.on.ca/part-x-cyfsa/safeguarding-and-managing-personal-information/
- ICO IT Recommendations: https://ico.org.uk/for-organisations/sme-web-hub/whats-new/blogs/11-practical-ways-to-keep-your-it-systems-safe-and-secure/
- Province of Manitoba (Canada) commonly used security safeguards: https://www.gov.mb.ca/health/phia/docs/security_safeguards.pdf

[iv] Not only for European customers localization possibility is important. Countries such as China are adopting more restrictive approaches to require localization. See for example the PIPL: https://www.dlapiperdataprotection.com/index.html?t=transfer&c=CN or special guidance note on China Data Transfers: https://www.dataguidance.com/notes/china-data-transfers

[v] Access to the legislation: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0591.htm

[vi] Legal quotation (non-official translation from Portuguese):

> ARTICLE 2
>
> 1. Each State Party to the present Covenant undertakes to take steps, individually and through international assistance and co-operation, especially economic and technical, to the maximum of its available resources, with a view to achieving progressively the full realization of the rights recognized in the present Covenant by all appropriate means, including particularly the adoption of legislative measures.
>
> 2. The States Parties to the present Covenant undertake to guarantee that the rights enunciated in the present Covenant will be exercised without discrimination of any kind as to race, color, sex, language, religion, political or other opinion, national or social origin, economic situation, birth or other status.
>
> 3. 3. Developing countries, with due regard to human rights and their national economic situation, may determine to what extent they will guarantee the economic rights recognized in the present Covenant to those who are not their nationals.

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

[vii] Access to the legislation: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm
[viii] Legal quotation (non-official translation from Portuguese):

ARTICLE 2

1. The States Parties to the present Covenant undertake to respect and to ensure to everyone within their territories subject to their jurisdiction the rights recognized in the present Covenant, without discrimination of any kind as to race, color, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.

2. In the absence of legislative or other measures designed to give effect to the rights recognized in the present Covenant, the States Parties to the present Covenant undertake to take the necessary steps with a view to their adoption, considering their respective constitutional procedures and the provisions of the present Covenant.

3. The States Parties to the present Covenant undertake to:

(a) To ensure that every person whose rights and freedoms recognized in the present Covenant have been violated has an effective remedy, even if the violence has been perpetrated by persons acting in an official capacity;

(b) Guarantee that every person who lodges such an appeal shall have his right thereto determined by the competent judicial, administrative or legislative authority, or by any other competent authority provided for by the legal system of the State concerned; and to develop the possibilities of judicial review;

[ix] Access to legislation: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm
[x] Legal quotation (non-official translation from Portuguese):

ARTICLE 24

Equality before the Law

All people are equal before the law. Consequently, they are entitled, without discrimination, to equal protection of the law.

ARTICLE 25

Judicial Protection

(1) Everyone has the right to a simple and prompt remedy or other effective remedy before competent judges or tribunals to protect him against acts violating the fundamental rights recognized in his constitution, by law, or by this Convention, even when such violation is committed by persons acting in an official capacity.

2. The States Parties undertake:

(a) to ensure that the competent authority provided for by the legal system of the State decides on the rights of every person who lodges such an appeal;

(b) To develop possibilities of judicial review; and

(c) To ensure the enforcement by the competent authorities of any decision on the merits of the appeal.

[xi] Access to the legislation: http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d99710.htm
[xii] A list with an historical overview of international instruments on international privacy law regarding principles and guidelines can be accessed here: https://www.nyulawglobal.org/globalex/Right_To_Privacy_International_Perspective.html
[xiii] For this approach, it's recommended the consultation of the recently SCCs Q&A published by European Commission in this link: https://ec.europa.eu/info/sites/default/files/questions_answers_on_sccs_en.pdf
[xiv] You can read technical details about the security assessment conducted by CAC in this article: https://iapp.org/news/a/top-5-operational-impacts-of-the-pipl-part-5-international-data-transfers/
[xv] Access to legislation: http://www.planalto.gov.br/ccivil_03/decreto-lei/del4657compilado.htm

Copyright © 2022 OneTrust LLC. All rights reserved. Proprietary & Confidential.

PRESIDÊNCIA DA REPÚBLICA
PRESIDÊNCIA DA REPÚBLICA
Protocolo da Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização

Memória de Reunião Nº 58/2022/CGN/ANPD/PR

Data: 26/07/2022

Horário: 14h30

Local: Microsoft Teams

Participantes: Fernando Maciel, Isabela Maiolino, Natalia Ives, Virginia de Melo e Davi Teofilo. Externos: Gabriel Cohen (Abipag), Caroline Maciel (Abipag) e Nathália Menezes (Abipag).

Pauta: Reunião com Abipag para discutir sobre a (i) Transferência Internacional de Dados e (ii) Premissas para o Tratamento de Alto Risco.

Memória

O Sr. Gabriel Cohen fez uma apresentação institucional da ABIPAG, contextualizando o trabalho realizado pela Associação, e apresentou contribuições sobre (i) Transferência Internacional de Dados e (ii) Premissas para o Tratamento de Alto Risco.
A Sra. Caroline Maciel pontuou que a regulação de transferências internacionais de dados deve ser proporcional ao risco da atividade, devendo haver proporcionalidade regulatória ao risco da operação, e propôs normas mais rígidas para agentes de alto risco.

Pontuou-se os possíveis seguintes critérios de alto risco (i) tratamento massivo de dados, 45 milhões de titulares - digital market act; (ii) decisões baseadas unicamente em tratamento automatizado; (iii) tratamento de dados sensíveis em volume superior a 20 miilhões de titulares; (iv) transferência para nações sem uma estrutura legal de privacidade reconhecida pela ANPD; (v) tratamento realizado por instituição transnacional sem sede no Brasil, e (vi) inexistência de regulação setorial aplicável à transferência ou a outros tratamentos.

Foram apontados alguns direitos que deveriam ser aplicados àqueles que tratam dados de alto risco, bem como a necessidade de maior transparência. Ressaltou-se a necessidade de aproximação com o Digital Market Acts da U.E.

Encaminhamentos

Nada mais havendo a tratar, a reunião se deu por encerrada, das quais, para constar, eu, Davi Teofilo Nunes Oliveira, lavrei a presente memória.

DAVI TEOFILO NUNES OLIVEIRA

Assistente Técnico

Coordenação-Geral de Normatização

Documento assinado eletronicamente por **Lucas Borges de Carvalho**, **Gerente de Projeto**, em 20/04/2023, às 13:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Virgínia de Melo Dantas Trinks**, **Assessor(a) Técnico(a)**, em 20/04/2023, às 13:39, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Ailana Linhares de Sousa Medeiros**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 20/04/2023, às 14:40, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Davi Teófilo Nunes Oliveira**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 20/04/2023, às 16:55, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

[redacted]

A autenticidade do documento pode ser conferida informando o código verificador [redacted] no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0

CUESTIONARIO ANPD-BRASIL

1. What are the current obstacles for companies to transfer data from Brazil to other countries? And from other countries to Brazil?

In a transfer, regardless of the instrument used, the greatest risk is to violate the principle of continuity. So, normally, the obstacles for companies to transfer data from Brazil or to Brazil will be related to barriers put in place to safeguard the principle of continuity.

2. What is the best way to promote convergence and interoperability between contractual instruments for international data transfers with instruments from other jurisdictions? And how can ANPD act in this regard?

Different countries have different systems, different approaches to privacy, often rooted in very different cultural, constitutional setups and legal traditions. To promote convergence, DPAs should focus on the standards that we are protecting, rather than the specific way in which other jurisdiction(s) are doing so. Hence, focus on the end result rather than irrespective of the way in which things are designed.

3. What are the most effective and the most used instruments to enable international data transfers by large and small companies or organizations?

In Colombia, the most common method used by companies is the transfer of personal data to countries that have been considered by the Colombian DPA to have an adequate level of protection. Additionally, the Colombian authority has made efforts to insist on the implementation of proven accountability measures in each transfer.

4. What are the main benefits and impacts of international data transfers, and what are the best alternatives for addressing them in each of the contractual instruments for data transfers included in the LGPD and in international practice?

Regulations on international data transfer or "transborder data flow" seek to ensure that the level of protection of a country's citizens' personal data does not diminish or disappear when said information is exported to one or more other countries. This rule is known as the principle of continuity of data protection, which is based on the fact that "*the international transfer of data should not affect the protection of data subjects, and therefore the protection of data subjects with regard to the processing of their personal data*"[1].

Hence, the main benefit and impact of well-done international transfers is the continuity the level of protection that Data subjects information has.

[1] De Frutos, José Manuel. 2008. Globalización de la privacidad: hacía unos estándares comunes. Conferencia realizada en el VI Encuentro Iberoamericano de Protección de Datos, 27-30 de mayo del 2008, Cartagena, Colombia.

5. Which criteria and/or requirements should be considered in regulating each of the following international data transfer mechanisms and why?
    a. standard contractual clauses;
    b. specific contractual clauses; and
    c. binding corporate rules.

Contractual Clauses. We refer to the text of the guide approved by the Ibero-American Data Protection Network of which you are aware.

Binding Corporate Rules. The text of are regulation may be found at: https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043921

6. To what extent should the elements to be considered by ANPD in assessing the level of data protection of foreign countries or international bodies for adequacy purposes (article 34 of the LGPD) also be taken into account within the scope of the rules for contractual instruments?

7. Should the standard contractual clauses be rigid and with predefined content, or should their regulation allow certain flexibility concerning the text of the clauses, specifying the desired results and allowing changes as long as they do not conflict with the standard text made available?

We refer to the text of the guide approved by the Ibero-American Data Protection Network of which you are aware.

8. What would be the most appropriate format for ANPD to make availiable models of standard contractual clauses for international data transfers? Are there any relevant 1 For the purposes of the Brazilian General Data Protection Law, the definition of processing agent refers to controllers or processors. tools that could be used to this end (e.g., decision tree, forms, checkboxes)? Are there any experiences on the theme that could serve as an example for ANPD?

We refer to the text of the guide approved by the Ibero-American Data Protection Network of which you are aware.

9. Is it necessary to have different rules depending on the type of processing agents (e.g., specific modules for controllers or processors) as data exporters or importers in international data transfers based on contractual clauses? If so, what would they be?

In Colombia, the instrument by which information is transferred is not differentiated depending on the subject who performs it. Each instrument that enables the regulation can be used by all data Controllers.

10. Are there requirements that need to be different for Binding Corporate Rules from those usually required for Standard Contractual Clauses? If so, what would they be?

We refer to our regulation regarding Binding Corporate Rules. The text of are regulation may be found at: https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043921

11. How should a corporate group be defined for the purpose of application of Binding Corporate Rules?

In Colombia, the decree that regulates BCR states the following:

> "*The Binding Corporate Rules are mandatory for the corporate group, in the terms defined by article 28 of Law 222 of 1995, that carry out transfer or set of transfer of personal data to a responsible of such group, outside the Colombian territory, unless the corporate group applies other mechanisms of data transfer established in the Colombian legislation*"**.**

Therefore, in Colombia the corporate group for purposes of the application of the Binding Corporate Rules is the same as that established in the commercial law of our nation.

12. What is the minimum information (level of detail) on personal data needed to allow proper compliance analysis by ANPD of the international transfers of data carried out by contractual instruments, in order to minimize negative impacts on business activities and preserve a high degree of protection for the data subject?

We refer to the text of the guide approved by the Ibero-American Data Protection Network of which you are aware.

13. What are the risks and benefits of allowing transfers between different economic groups whose binding corporate rules have been approved by ANPD?

In a transfer, regardless of the instrument used, the greatest risk is to violate the principle of continuity.

In this hypothetical case we would be facing a case of transfer as if the Binding Corporate Rules were not in place (a transfer from Controller to Controller). In such a situation, the Colombian authority has emphasized the adoption of *Accountability* measures to prevent the identifies risks.

14. Are there any experiences with the verification and approval of specific contractual clauses and binding corporate rules that could serve as an example for ANPD?

Binding corporate standards were regulated in Colombia in February of this year. Likewise, the only instrument in our legal system on model contractual clauses is the guide of the Ibero-American Network. Therefore, so far, we have no experience in verifying or approving such instruments.

15. What are the data subject's rights in case of changes in the original configuration of the transfer? In which situations is it essential to communicate directly with the data subjects or to enable some type of intervention by them?

In Colombia, in case of changes in the original configuration of the transfer, the Controller does not have the legal duty to communicate said change to Data subjects.

However, in Privacy Policies we have a different approach.

Decree 1377 of 2013 states the following:

> "*In the event of substantial changes in the content of the Privacy Policy referred to in Chapter III of this Decree, the identification of the Controller and the purpose of the Processing of the personal data, which may affect the content of the authorization, the Data Controller must communicate these changes to the Data Subject before or at the latest at the time of implementing the new policies*".

16. What are the best alternatives for resolving conflicts between processing agents and/or between those agents and data subjects involving contractual instruments for international data transfers? Could bilateral, multilateral or international cooperation between data protection authorities assist in conflict resolution? If so, how?

The Colombian DPA strongly believes in the benefits of cooperation between DPAs. That can be one alternative.

Another alternative could be creating a safe zone for agents to talk. For our internal regulation matter, the Colombian DPA has put in place SIC Facilita https://sicfacilita.sic.gov.co/SICFacilita/index.xhtml We invite you to check the website to see how it works.

17. What are the best alternatives to promote regulatory compliance (including concerning the importer) regarding international data transfers?

From a DPA standpoint.

Promote the proactive and preventive measures.

- Administrative orders before a regulation breach.
- Publishing guidelines.
- Personnel training.
- Emphasize the importance of confidence in the market when an adequate Processing is carried out.

18. What are the best alternatives to resolve practical issues related to the accountability of stakeholders who transfer data overseas, especially in cases where onward transfers to other jurisdictions occur or when data is processed by other data processing agents in the same jurisdiction?

In these hypotheses, the ideal would be to have a suitable and direct communication channel with the DPA. In this way, a safe and trustworthy space can be generated in favor of the rights of the Data subjects.

19. What obligations should be assigned to the importer and exporter in case of access to data by foreign public authorities?

Colombian regulation does not have any special requirements for these situations. Therefore, in these situations as a DPA we refer to the rules established on the access of data by authorities established in our general regulation.

20. What are the most appropriate mechanisms to provide data subjects with clear and relevant information about the possible transfer of their personal data outside of Brazil as well as to ensure the adequate protection of data subjects' rights in international data transfers? How should these instruments be implemented?

Through mechanisms of Accountability put the principle of transparency into practice. A transparent organization can generate greater confidence in its clients and data subjects.

To achieve this, the following is suggested:

- Maintain open channels of communication and disclosure of the use of personal data in international data transfer processes. It is important that this is done in very clear and simple terms, using simple language that can be understood by any person.
- Implement an effective system of due and timely attention to complaints and claims.
- Complying in practice with what is stated or promised in the Privacy Policy.