À
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)
Coordenação-Geral de Normatização
normatizacao@anpd.gov.br

São Paulo, 31 de maio de 2023

Ref.: Consulta Pública sobre Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais

Prezados senhores,

A **ASSOCIAÇÃO BRASILEIRA DE INTERNET – "ABRANET"**, pessoa jurídica constituída na forma de associação civil sem fins lucrativos, com sede na Rua MMDC, nº 450, cj. 304, São Paulo/SP, é uma entidade de classe que representa empresas de diversos segmentos que desenvolvem atividades prestadas através da Internet e das tecnologias da informação.

A Associação possui abrangência nacional, com mais de 400 (quatrocentas) associadas, atuando nas áreas de meios de pagamento, conectividade de internet, aplicações e conteúdos. Trata-se, portanto, de uma das principais entidades envolvendo agentes de tratamento atuantes na internet no Brasil. Diante disso, enquanto representantes de uma ampla gama de controladores, a ABRANET possui profundo interesse em contribuir com a construção de um mecanismo justo e eficiente que regulamente a comunicação de incidentes de segurança.

Nesta oportunidade, a **ABRANET** vem oferecer suas contribuições à consulta pública sobre o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. Nos tópicos a seguir, a ABRANET resume os principais comentários feitos aos dispositivos do projeto de resolução.

I. DA DELIMITAÇÃO DAS DEFINIÇÕES E COERÊNCIA NORMATIVA:

A ABRANET sustenta que deve haver uma maior precisão e delimitação das definições dos termos e conceitos fundamentais para a regulamentação. Além disso, é essencial que haja uma harmonia e compatibilidade entre a futura Resolução e os normativos já vigentes.

Nesse sentido, entende-se que a **definição de dados de autenticação em sistemas** deve ser mais específica, para contemplar as situações em que determinado incidente de segurança **possua o condão de permitir o acesso indevido a contas e sistemas com base nos dados afetados e, portanto, o potencial de ocasionar um dano relevante ao titular.**

Por fim, a Associação entende que a ANPD não deveria estabelecer conceitualmente o que é dado financeiro, na medida em que o regulador financeiro (Banco Central do Brasil) é o responsável pelo tema e que a própria LGPD, em seu art. 55-J, prevê que haja cooperação entre a autoridade de proteção de dados e outros órgãos e agências reguladoras do Brasil, garantindo uma harmonia e uma colaboração em assuntos transversais.

Ademais, nota-se que a ANPD pretende estabelecer uma analogia entre os dados pessoais sensíveis e os dados financeiros, de modo a conferir a eles uma tutela especial como os daquela natureza. Contudo, é importante salientar que o legislador, ao delimitar os dados sensíveis, optou por não incluir os dados financeiros. Assim, não cabe à ANPD, em sua função de regulamentar a proteção de dados pessoais, extrapolar as funções delegadas pela LGPD.

Por fim, cumpre salientar que seria ideal a extinção da utilização do conceito de "categorias" na regulamentação do incidente de segurança com dados pessoais. Considerando que o legislador, que possui a competência para definir as normas gerais relativas à proteção de dados – e que assim o fez na Lei 13.709/2018 – não as mencionou, ou seja, deliberadamente optou por se omitir sobre qualquer categorização dos dados pessoais que não as relativas à natureza dos dados (se sensíveis ou não), a ABRANET entende que a ANPD não deveria inserir um elemento de tamanha importância e impacto de forma infralegal.

A sugestão da ABRANET, melhor delimitada no Anexo, tem como objetivo a tutela da coesão e a harmonia do sistema normativo de proteção de dados pessoais por meio do respeito às competências e funções da autoridade reguladora e do legislador. Contudo, caso seja do interesse da ANPD manter a utilizaçao do sistema de categorias, sugere-se, alternativamente, a observância dos comentários que justificam a proposição de uma nova redação do art. 3º, III, do regulamento, de forma a evitar problemáticas como o conflito de competências com outras autoridades reguladoras, em linha com os argumentos supra.

II. DOS CRITÉRIOS PARA COMUNICAÇÃO DOS INCIDENTES

Conforme já dito, a ABRANET entende como inadequada a inclusão deste critério de comunicação de incidentes do art. 5, III, relativo a dados financeiros, sugerindo a sua remoção. Em relação ao conceito de "tratamento de dados pessoais em larga escala", a ABRANET sugere que sejam adotados critérios objetivos que delimitem melhor esse conceito, de modo a evitar insegurança jurídica.

Nesse mesmo sentido, sugere-se a inclusão do termo "apenas" na frase "São considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aqueles que possam" para delimitar que se trata de um rol taxativo, de modo a evitar possíveis conflitos de interpretações do parágrafo primeiro do referido art. 5.

Ainda, importante destacar que a ABRANET entende necessário especificar situações em que não será preciso comunicar à ANPD e aos titulares acerca de incidente de segurança, pelo que sugere a adição de um parágrafo ao artigo 4º prevendo essas situações. Caso o controlador já tenha implementado medidas suficientes para mitigação ou reversão dos possíveis riscos ou danos relevantes aos titulares, não há porque se notificar, haja vista que a finalidade da comunicação é justamente a adoção desse tipo de medidas, já implementado. Outra hipótese que dispensa a comunicação diz respeito a dados que já sejam públicos, uma vez que não foi evento adverso que os tornou disponíveis, mas a própria vontade da parte do titular.

III. DOS PRAZOS E PROCEDIMENTOS PARA COMUNICAÇÃO DO INCIDENTE À ANPD

Em relação aos prazos para comunicação do incidente à ANPD, a ABRANET entende que dever haver uma melhor definição da expressão "tomar conhecimento", e também deve haver uma ampliação do prazo previsto na proposta disponibilizada pela ANPD. Quanto ao termo inicial, a ABRANET sugere, inspirando-se em *guidelines* disponibilizadas pelo *European Data Protection Board* ("EDPB"), que seja entendido como o momento a partir do qual o controlador possuir **um grau razoável de certeza de que o incidente ocorreu.**

Além disso, sugere-se, considerando o grau pouco desenvolvido da cultura de proteção de dados no Brasil – que pode ser especialmente problemático em se tratando da comunicação

interna nos agentes de tratamento - que o marco inicial do prazo para comunicação seja o momento a partir do qual o **Encarregado seja efetivamente informado e reconheça o incidente.**

Quanto ao prazo para comunicação à ANPD, entende-se que o período hoje proposto é irrazoavelmente exíguo, de modo que é virtualmente impossível – considerando o cenário e o desenvolvimento da cultura de proteção de dados do Brasil – que os agentes levantem, com qualidade e com grau de precisão necessários – todas as informações requeridas no prazo de 3 dias úteis. Nesse sentido, e para garantir um regime transitório gradual do *enforcement* da ANPD, sugere-se a **adoção de um prazo de 5 dias úteis,** que pode ser revisto futuramente pela autoridade. Por fim, sugere-se a adoção de uma redação mais abrangente para contemplar casos em que não seja possível manifestar-se no prazo estipulado, em linha com as práticas estabelecidas na União Europeia por meio da *General Data Protection Regulation* (GDPR) em seu art. 33 (1).

Sugere-se também que seja adotado um prazo indeterminado para a complementação das informações prestadas no primeiro momento. Considerando que muitas das informações que podem ser úteis à ANPD para a avaliação da extensão do dano e para determinar medidas mitigatórias para preservar os direitos dos titulares podem não estar disponíveis inicialmente e, em alguns casos mais complexos, tampouco em 20 ou 40 dias úteis, entende-se que seria mais útil se houvesse um prazo em aberto para a complementação das informações, sem fixar prazo específico.

No que tange aos elementos essenciais da comunicação inicial a ser feita, entende-se como desnecessário o item "total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente." No atual quadro normativo da ANPD, não há qualquer tipo de previsão ou consideração da larga escala como um elemento comparativo, relacional (i.e., o número de titulares afetados em relação ao total de titulares cujos dados são tratados por um controlador), portanto, não há razão para se exigir tal informação na comunicação do incidente, em um primeiro momento.

Abordando questões mais procedimentais, a **A**BRANET entende importante melhor delimitar a realização de auditorias ou inspeções por parte da ANPD, no contexto do processo de comunicação de incidente de segurança com dados pessoais – art. 18. Nesse sentido, a

Associação busca incorporar referências basilares de processo administrativo ao procedimento, como a delimitação fundamentada de escopo da auditoria ou inspeção que se pretende realizar e a previsão de um prazo para que o controlador possa se manifestar sobre a medida planejada – que, aliás, deve ser de caráter excepcional, respeitando os prazos de comucanicação do incidente de segurança e apenas caso os esclarecimentos prestados pelo controlador sejam insuficientes.

Ainda, no que tange à figura do auditor, a ABRANET vê como necessário que a relação entre este e a auditada seja marcada por um dever de sigilo, preservando documentos recebidos e acessos disponibilizados, mesmo após a conclusão do processo de auditoria. As garantias de sigilo comercial e industrial também devem ser resguardadas – de resto, em todos os processos conduzidos pela ANPD. Por fim, como forma de resguardar a imparcialidade necessária para os deveres do auditor, a ABRANET julga prudente que seja assegurado um direito de oposição ao auditor nomeado, em casos de suspeição ou impedimento. O esforço de detalhamento da ABRANET relativamente ao art. 18 demonstra como o tópico ainda demanda maiores especificações antes que sua implementação possa ser cogitada por parte da ANPD.

IV. DOS PRAZOS E PROCEDIMENTOS PARA COMUNICAÇÃO DO INCIDENTE AO TITULAR

O regulamento proposto pela ANPD estipula que os titulares sejam informados do incidente no mesmo prazo que a Autoridade e, apesar do nível de informações exigidas ser distinto, é notório que não se observam as peculiaridades destes dois tipos de comunicação.

Considerando que há sensibilidade em se tratando de comunicação com titulares – em especial, à luz da já mencionada pouco desenvolvida cultura de proteção de dados brasileira – o prazo exíguo de 3 dias úteis não se verifica suficiente para a elaboração de uma comunicação adequada. Por isso, de modo a preservar o titular e evitar prejuízos reputacionais exacerbados, sugerimos que o prazo inicial para comunicação ao titular seja de 7 dias úteis.

Outro ponto fundamental é uma delimitação mais técnica das hipóteses em que o titular deverá ser comunicado de um incidente. Inspirando-se na experiência internacional e, em especial, na GDPR e nos normativos da ICO/UK, entende-se que deve haver uma diferenciação entre quando se deve comunicar a ANPD e quando se deve comunicar o titular, sendo esta uma

hipótese restrita a **quando o incidente representar alto risco ao titular.** Em relação ao conceito de alto risco, recomenda-se que se adote os critérios que serão definidos a partir da "Tomada de Subsídios sobre tratamento de dados pessoais de alto risco". Provisoriamente, a ABRANET recomenda a utilização dos critérios definidos no art. 4 da Resolução CD/ANDP nº 2.

No que tange ao mérito da comunicação em si, entende-se como desnecessária a obrigação de disponibilizar o contato do Encarregado para dirimir dúvidas dos titulares em relação ao incidente. Apesar da importância de se manter um canal de comunicação com os indivíduos, é do entendimento da Associação que esse dispositivo poderia levar à sobrecarga do Encarregado com manifestações pontuais, de forma que impediria o exercício de suas demais funções. Sugere-se, portanto, que seja disponibilizado aos controladores a opção de **criar um canal de comunicação específico para lidar com questões relativas ao incidente.**

Por fim, importante destacar que a possibilidade de determinação, por parte da ANPD, da ampla divulgação em meios de comunicação de incidente de segurança com dados pessoais deve ocorrer apenas em casos de insuficiência da via eleita pelo controlador para adequadamente notificar os titulares afetados. Na visão da **ABRANET**, além da importância em se harmonizar as redações do inciso I do artgo 19 com o artigo 20 da Resolução, é preciso que a ampla divulgação – realizada para a salvaguarda dos direitos dos titulares – não se confunda com a aplicação de pena de caráter sancionador ao controlador. O cerne que deve orientar a Resolução é compreender que uma divulgação ostensiva é diferente de uma divulgação que adequamente informa o titular de dados, sendo certo que o importante – e que deve ser buscado – é que este seja adequadamente informado dos fatos ocorridos. Nesse sentido, a ampla divulgação deve figurar como medida excepcional, em caso de ineficácia dos caminhos inicialmente adotados pelo controlador para notificar os titulares de dados.

V. DA VIGÊNCIA DAS DISPOSIÇÕES DO REGULAMENTO

A **ABRANET**, enquanto representante de pequenas, médias e grandes empresas no mercado digital, sugere que a ANPD conceda um tempo hábil de 12 meses após a publicação desta Resolução para a necessária adaptação do setor às regras, exigências e procedimentos estipulados, em sua integralidade.

A *vacatio legis* se faz necessária pois, no atual estado da cultura de proteção de dados do Brasil, e levando em consideração que até o presente momento não existiram recomendações ou orientações suficientes para fins de balizar os agentes em relação aos requisitos postos, serão necessárias consideráveis adaptações e alinhamentos (ou mesmo a elaboração) nos procedimentos internos de investigação e averiguação de possíveis incidentes, registro de incidentes não notificáveis, procedimentos de respostas ao titular e à autoridade e até mesmo procedimentos de circulação de informações relevantes dentro das empresas ou organizações.

Essas adaptações se apresentarão como um desafio ainda maior para pequenas e médias empresas e organizações, que precisarão fornecer formações e treinamentos aos seus colaboradores responsáveis (sendo eles Encarregados ou não) para garantir o efetivo cumprimento das disposições. Por isso a importância do prazo de *vacatio* acima sugerido.

CONCLUSÃO

A **ABRANET** reitera seus argumentos trazidos no corpo desta manifestação e na tabela do Anexo I, cumprimentando a Autoridade Nacional de Proteção de Dados pela abertura em discutir o tema e construir uma regulamentação democrática e abrangente e reitera sua disposição para colaborar com o aprimoramento da regulação supracitada.

Sendo o que nos cumpria para o momento, a **ABRANET** coloca-se à disposição da ANPD para qualquer colaboração que esta venha a julgar necessária e apresenta seus protestos de elevada estima e consideração.

Atenciosamente,

ASSOCIAÇÃO BRASILEIRA DE INTERNET – ABRANET

ANEXO I - REGULAMENTO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS		
DISPOSITIVO	**SUGESTÃO**	**COMENTÁRIOS**
CAPÍTULO II - DAS DEFINIÇÕES		
Art. 3º Esta Resolução entra em vigor em 1º de xxxxxx de 2023.	Art. 3º Esta Resolução entra em vigor um ano após a publicação.	A ABRANET propõe que haja prazo sufuciente para a entrada em vigor deste regulamento, dado que há previsão de novos documentos e obrigações que demandarão esforço de adaptação pelos agentes de tratamento.
Art. 3º Para efeitos deste Regulamento são adotadas as seguintes definições:		
I - ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela ANPD ao controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança com dados pessoais, como a publicação no sítio da Internet e nas redes sociais do controlador ou em outros meios de grande alcance;	I - ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela ANPD ao controlador, excepcionalmente e em caso de elevada gravidade do incidente e de necessidade de divulgação para salvaguarda dos direitos de titulares, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança com dados pessoais, como a publicação no sítio da Internet ~~e nas redes sociais~~ do controlador. ~~ou em outros meios de grande alcance.~~	A ABRANET destaca que a determinação de ampla divulgação do incidente em meios de comunicação, tal como previsto na LGPD, deve ser medida aplicada pela ANPD de **forma excepcional,** a partir de critérios e limites objetivos, apenas quando estritamente necessário para a salvaguarda dos direitos dos titulares e no contexto da gravidade do incidente que realmente justifique tal medida. O termo é vago e pode gerar dúvidas. A alteração proposta tem por finalidade adequar o dispositivo ao texto contido no §2º do art. 48, conforme indicado no inciso.
II - autenticidade: propriedade pela qual se assegura que o dado pessoal foi produzido, expedido, modificado ou destruído por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;	**EXCLUSÃO** ~~II - autenticidade: propriedade pela qual se assegura que o dado pessoal foi produzido, expedido, modificado ou destruído por uma determinada pessoa física, equipamento, sistema, órgão ou~~	O conceito de autenticidade não está previsto na LGPD, que se baseia no pilar CID (Confidencialidade, Integridade e Disponibilidade). No mesmo sentido, a ANPD utiliza essa tríade no Formulário de Comunicação de Incidentes, ao avalir o impacto do incidente. Por fim, a ISO 20252:2019 deixa claro que

	~~entidade;~~	o conceito de incidente de segurança, em seu sentido mais amplo, está relacionado à perda de uma das características da segurança da informação: confidencialidade, integridade e disponibilidade, sem incluir autenticidade.
III - categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, como identificação pessoal, autenticação em sistemas, financeiro, saúde, educação e judicial;	III - categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, como identificação pessoal e autenticação em sistemas~~, financeiro, saúde, educação e judicial;~~ Alternativamente: **EXCLUSÃO** ~~III - categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, como identificação pessoal, autenticação em sistemas, financeiro, saúde, educação e judicial;~~	As categorias de dados pessoais trazidas no texto da Consulta Pública não constam na LGPD, que se restringe a diferenciar dados pessoais de dados pessoais sensíveis. Propõe-se a alteração do texto ou, alternativamente, a exclusão do dispositivo.
VI - dado de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, tokens e senhas;	VI - dados de autenticação em sistemas: ~~qualquer~~ conjunto de dados pessoais utilizados como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como login em conjunto com a senha, ou tokens. Não se considera dado de autenticação em sistemas dados que, sozinhos, não concedam acesso a um sistema;	Na atual definição de "dados de autenticação em sistemas" trazida pela referida resolução, há um problema em relação ao escopo almejado, – conforme o contexto no qual a definição é inserida. Nesse sentido, a redação atual não protegeria somente os dados que funcionassem como credenciais, ou seja, que efetivamente permitissem o acesso às contas. Conforme o texto, **bastaria que ocorresse o vazamento de, por exemplo, um endereço de e-mail ou um nome de usuário para que fosse considerado dado** dessa natureza, já que tais dados são amplamente utilizados como um dos componentes das credenciais (especificamente como dados de "login") e, portanto, estariam sujeitos necessariamente à notificação do incidente de segurança à ANPD e a titulares.

		Na visão da ABRANET, dados de autenticação de sistemas **só merecem ser qualificados dessa forma quando o conjunto de dados vazados permitir o acesso a um sistema** (login e senha e token; etc.). Nesses casos, há efetivamente **maiores riscos de danos aos titulares**, na medida em que será possível acessar o sistema com o **conjunto de credenciais vazadas**. Isso não ocorre, contudo, caso apenas o login (como um e-mail) tenha sido alvo de incidente de segurança. Com isso, assegura-se que a qualificação como "dados de autenticação em sistemas" seja reservada a incidentes de segurança que abarquem dados cuja natureza exige maiores cautelas, pois há mais riscos de danos para os titulares e de maior gravidade para os direitos e liberdades dos titulares. Nessas hipóteses, é recomendável que o controlador informe aos titulares a importância de redefinição de senhas ou tokens, tal como ilustram as *Guidelines 9/2022 do European Data Protection Board ("EDPB").* Disponível em: https://edpb.europa.eu/system/files/2022-10/edpb_guidelines_202209_personal_data_breach_notification_targetedupdate_en.pdf
VII - dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;	~~VII – dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;~~ Alternativamente: VII – dado financeiro: dado pessoal qualificado como dado financeiro em leis e normativas do Banco	Em relação ao conceito de dado financeiro, o entendimento da ABRANET é de que, enquanto autoridade de proteção de dados pessoais, **não estaria na competência exclusiva da ANPD definir dado financeiro**, na medida em que o regulador financeiro (Banco Central do Brasil) é o responsável pelo tema. No art. 55-J da Lei Geral de Proteção de Dados Pessoais (LGPD), todas as competências da

	Central do Brasil;	ANPD giram em torno estritamente da proteção de dados pessoais e da privacidade. Por isso, de forma a evitar possíveis conflitos de competência e de forma a harmonizar o *enforcement* das autoridades reguladoras brasileiras, de modo a promover o bom e eficiente ambiente regulatório Eventual definição de dado financeiro envolveria exercer a competência atribuída a outros órgãos, ignorando as previsões do art. 55-J, inciso XXIII da LGPD, que trata sobre a articulação com reguladores de setores específicos, sujeitos à regulação. Ao analisarmos as normativas de outras autoridades de proteção de dados no mundo, em especial as da ICO/UK e as de autoridades da UE, nota-se que não há uma prática de se definir dados financeiros em sede de autoridades de proteção de dados via regulamentos e normativos infralegais. Além disso, nota-se que a ANPD realizou uma **analogia e equiparação de dado financeiro com dado pessoal sensível**, conferindo a ambos o mesmo regime de cautela especial. Todavia**, a LGPD não faz tal equiparação,** sendo que o legislador poderia ter abarcado dado financeiro no conceito taxativo do art. 5º, II da LGPD de dado pessoal sensível. **Como isso não foi feito, entende-se que não cabe essa extensão pela via infralegal, em especial por não se estar diante de rol exemplificativo.** Sugere-se, portanto, que **o conceito de dado financeiro seja excluído** e **não configure critério para determinar a notificação de um incidente de segurança.**

		Ademais, o conceito de dado financeiro é apresentado de **forma significativamente abrangente,** omo consequência desta amplitude, a futura norma promoverá um ambiente regulatório **sobrecarregado em termos de obrigações de comunicação de incidentes**, gerando fadiga informacional a titulares e à ANPD. Alternativamente, a ABRANET sugere que a ANPD faça referência às normativas do Banco Central do Brasil para delimitar o conceito de dado financeiro, articulando de forma coerente com a autoridade do setor específico, **de modo a delimitar de forma mais estrita e menos abrangente o referido conceito.** Nesse sentido, reconhece-se a boa prática de se observar o respeito às competências de outros órgãos e entidades em matérias específicas que são, necessariamente, transversais.
X - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;	X - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e ~~autenticidade~~ da segurança de dados pessoais;	Respeitados os limites da LGPD, a experiência internacional (como o GDPR e ISO) e da tríade CID, deve haver a exclusão do termo autenticidade, conforme já detalhado no inciso II.
XII - medidas de segurança relacionadas a dados pessoais: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação;	XII - medidas de segurança relacionadas a dados pessoais: medidas técnicas e administrativas adotadas para proteger os dados pessoais de tratamentos e/ou acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação;	A ABRANET sugere a inclusão de uma menção ao termo “tratamento” no inciso XII para que a redação esteja alinhada à definição prevista no artigo 5º, inciso X, da LGPD.
XVI - processo de comunicação de incidente de segurança com dados pessoais: processo instaurado	XVI - processo de comunicação de incidente de segurança com dados pessoais: processo	A alteração sugerida para o inciso XVI visa esclarecer que o processo mencionado se refere a um processo

no âmbito da ANPD, com o objetivo de verificar a ocorrência de incidentes de segurança com dados pessoais capazes de acarretar risco ou dano relevante aos titulares de dados, podendo abranger o procedimento de apuração de incidente de segurança e o procedimento de comunicação de incidente de segurança; e	administrativo instaurado no âmbito da ANPD, com o objetivo de verificar a ocorrência de incidentes de segurança com dados pessoais capazes de acarretar risco ou dano relevante aos titulares de dados, podendo abranger o procedimento de apuração de incidente de segurança e o procedimento de comunicação de incidente de segurança; e	administrativo.
XVII - relatório de tratamento de incidente: relatório fornecido pelo controlador que contém cópias, em meio físico ou digital, de documentos, dados e informações relevantes para descrever o incidente e as ações adotadas para o seu tratamento, tais como, evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas.	XVII - relatório de tratamento de incidente: relatório fornecido pelo controlador que contém cópias, em meio físico ou digital, de documentos, dados e informações relevantes para descrever o incidente e as ações adotadas para o seu tratamento, tais como, evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas, de acordo com o modelo a ser estabelecido pela ANPD.	Considerando a função educativa da ANPD, entende-se como necessária a elaboração de um documento orientativo para os controladores de modo a estabelecer as expectativas da ANPD e, ao mesmo tempo, solucionar eventuais dúvidas que possam surgir no momento da elaboração dos relatórios, especialmente considerando que a cultura de proteção de dados do país ainda carece de um desenvolvimento maior. Por isso, a alteração sugerida para o inciso XVII visa a criação, pela ANPD, de um modelo relatório de tratamento de incidente que possa ser usado pelos controladores de forma a padronizar os relatórios, semelhante ao que é disponibilizado pela ANPD em relação ao formulário de comunicação de incidente de segurança com dados pessoais ou mesmo ao modelo de ROPA proposto na Tomada de Subsídios do modelo de registro simplificado das operações de tratamento de dados pessoais
CAPÍTULO III - DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA		
SEÇÃO I - Dos critérios para comunicação de incidentes de segurança		
Art. 4º O controlador deverá comunicar à ANPD e ao titular os incidentes de segurança com dados	**ADICIONAR:** § 1º - Não será necessário comunicar à ANPD e aos	Sugere-se a inclusão de um parágrafo que explicite as hipóteses em que não é necessário comunicar um

pessoais que possam acarretar risco ou dano relevante aos titulares.	titulares a respeito de incidente de segurança nas seguintes hipóteses: a) caso o controlador tenha implementado medidas suficientes para mitigação ou reversão dos possíveis riscos ou danos relevantes identificados; e b) caso os dados afetados ou os dados envolvidos no incidente sejam previamente públicos e o incidente não altere a disponibilidade e publicidade desses dados pessoais.	incidente de segurança à ANPD e aos titulares. Considerando que a finalidade da comunicação do incidente é a implementação de medidas mitigadoras, assecuratórias ou reversíveis cabíveis no caso, quando o controlador já o fez, não é necessária a comunicação. Ademais, dados meramente cadastrais que foram voluntariamente disponibilizados de forma ampla na Internet pelos titulares não geram a necessidade de comunicação, já que não houve um evento adverso que os tornou disponíveis.
Art. 5º Para fins deste Regulamento, considera-se que um incidente de segurança com dados pessoais pode acarretar risco ou dano relevante aos titulares quando tiver potencial de afetar significativamente interesses e direitos fundamentais dos titulares e envolver pelo menos um dos seguintes critérios:		
III - dados financeiros;	~~III - dados financeiros;~~	A ABRANET acredita que o fato de um incidente de segurança abarcar dados financeiros não é critério suficiente para, se realizar, necessariamente, uma notificação de incidente de segurança. Considerando o amplo conceito adotado na atual definição de dado financeiro da ANPD, haveria um volume considerável de incidentes que teriam de ser notificados, sobrecarregando a ANPD de forma desnecessária. Ao avaliarmos o posicionamento de outras autoridades de proteção de dados no mundo, há sempre uma **delimitação bastante estrita dos critérios de notificação de incidentes de segurança**, de modo que sejam direcionados às autoridades

		apenas os incidentes realmente importantes, que acarretem risco ou dano relevante. Desse modo, sugere-se a exclusão do inciso III. Ao contrário dos incisos I e II, que envolvem dados de natureza especial, cuja própria LGPD define como sendo protegidos por um regime diferenciado em relação aos outros dados, os dados financeiros, previstos no inciso III, não recebem a mesma atenção do legislador e, portanto, é possível estabelecer que o legislador optou por não os diferenciar dos demais tipos de dados. Nesse sentido, não compete à ANPD regulamentar em sentido contrário ao que estabeleceu o legislador e, portanto, não compete estabelecer categorias especiais de dados quando o legislador assim não o fez.
V - dados em larga escala.		De modo a tornar a interpretação e aplicação da norma mais objetiva, sugere-se ainda que sejam definidos os critérios objetivos que definirão um determinado tratamento como sendo tratamento de “dados em larga escala” e que contenha um “número significativo de titulares” na prática, conforme mencionado, respectivamente, no inciso V, caput, e no parágrafo 2º do artigo. Desse modo, evita-se a subjetividade e a possibilidade de discricionaridade na função de fiscalização da ANPD evitando, por conseguinte, o aumento do cenário de insegurança jurídica. Essa definição é especialmente importante pois o conceito de tratamento de “dados em larga escala” é proposto em outras resoluções e propostas de

		normativos da ANPD.
§ 1º São considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aqueles que possam:	§ 1º São considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares apenas aqueles que possam:	A alteração na redação do caput do parágrafo primeiro foi sugerida para reforçar que o item abrange um rol taxativo.
§ 2º Para aplicação deste Regulamento, os incidentes de segurança com dados pessoais em larga escala serão assim caracterizados quando abrangerem número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares.	§ 2º Para aplicação deste Regulamento, os incidentes de segurança com dados pessoais em larga escala serão assim caracterizados quando abrangerem, cumulativamente, um número significativo de titulares, um volume significativo de dados envolvidos e uma considerável extensão geográfica de localização dos titulares.	No que tange aos dados de larga escala, a ABRANET sustenta que o **termo "larga escala" não está bem definido e pode gerar interpretações excessivamente subjetivas, causando maior insegurança jurídica para os agentes de tratamento**, conforme já estabelecido no item 5, V. Apesar do §2º trazer alguns critérios para a avaliação da larga escala, a ABRANET sugere alguns ajustes, de forma que haja mais clareza no tema. Ao colocar os parâmetros como cumulativos, gera-se maior segurança jurídica para a aplicabilidade da larga escala. Contudo, entendemos que o cenário ainda sim é preocupante e, portanto, seria mais recomendável que a ANPD definisse critérios objetivos para essa caracterização, de forma a afastar qualquer tipo de subjetividade e discricionariedade.
SEÇÃO II - Da comunicação do incidente à ANPD		
Art. 6º A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e	Art. 6º A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de ~~três até~~ cinco dias úteis, sempre que possível, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar alto risco de dano relevante aos	Com relação ao prazo de comunicação de incidente de segurança à ANPD, a ABRANET entende que, em virtude da grande influência da *General Data Protection Regulation* (GDPR) na LGPD, é pertinente se inspirar no normativo europeu também nesse tema. Nesse sentido, **sugere-se inspiração no art. 33(1), para inserir a expressão de notificar, sempre**

deve conter as seguintes informações:	titulares afetados, e deve conter as seguintes informações:	**que possível, no prazo estabelecido, de forma a ter uma cláusula mais geral que abarque os casos em que não é possível cumprir o prazo, mediante justificativa adequada, de forma a garantir o respeito à capacidade dos agentes e observar as peculiaridades do caso concreto, evitando possíveis injustiças e, por conseguinte, evitando judicializações das decisões da autoridade.** Além disso, levando em consideração a atuação mais educativa e gradual da ANPD em relação à propagação da cultura de proteção de dados, a ABRANET defende que o **prazo seja ampliado para 5 dias úteis,** pelo menos em um primeiro momento de maiores dificuldades de conformidade dos agentes com a nova legislação.
VII - a data e a hora do conhecimento do incidente de segurança;	VII – a data e hora ~~do conhecimento do incidente de segurança~~ em que o controlador determinou o impacto aos titulares.	A ABRANET sugere a alteração do inciso VII, considerando que, muitas vezes, o controlador precisa investigar internamente dados e fatos para determinar o impacto aos titulares de dados pessoais.
XIII - o total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.	~~XIII - o total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.~~	Na visão da ABRANET, a LGPD não exige a indicação do número total de titulares cujos dados são tratados pelo controlador. Ainda, a ABRANET vislumbra que, ao comunicar um incidente de segurança, é excessivo e desnecessário informar à ANPD o volume total de titulares cujos dados são tratados pela organização e na atividade afetada pelo incidente**.** Entende-se que essa informação só seria relevante caso a ANPD viesse a estabelecer um critério comparativo para a definição de larga escala – por exemplo, caso um percentual elevado dos titulares fosse afetado, a escala seria

		necessariamente "larga". A ABRANET, porém, discorda do uso desse critério que, além de extremamente subjetivo, não parece denotar qualquer relevância na definição de severidade do incidente.
§ 1º Excepcionalmente, as informações poderão ser complementadas, no prazo de vinte dias úteis, a contar do momento em que o controlador tomou conhecimento do incidente, prorrogável uma vez, por igual período, mediante solicitação fundamentada a ser avaliada pela ANPD.	§ 1º ~~Excepcionalmente,~~ as informações poderão ser complementadas~~, no prazo de vinte dias úteis,~~ a contar do momento em que o controlador tomou conhecimento do incidente mediante solicitação fundamentada a ser avaliada pela ANPD.	Na visão da ABRANET, a possibilidade de complementação das informações revela-se uma alternativa necessária para que os controladores e não deve ser considerada medida excepcional. Outro ponto é que não parece ser o melhor caminho delimitar um prazo máximo de envio de novas informações pelo agente de tratamento à ANPD. A depender do tipo de informação requerida, pode fazer sentido que ela seja entregue num prazo mais exíguo ou mais longo e retirar da autoridade a flexibilidade na definição desse tema não parece produtivo. Isso porque, conforme a investigação avança, **novas informações podem surgir mesmo após os vinte dias úteis iniciais e ainda serem relevantes para a ANPD após tal prazo**. Enquanto a ANPD ainda analisa o incidente comunicado, **o controlador deve poder trazer informações complementares, exaurindo-se essa oportunidade apenas quando a ANPD deliberar sobre o incidente.** Considerando que muitas das informações que podem ser úteis à ANPD para a avaliação da extensão do dano e para determinar medidas mitigatórias para preservar os direitos dos titulares podem não estar disponíveis em um primeiro momento e, em alguns casos mais complexos, tampouco em 20 ou 40 dias úteis, entendemos que poderia ser mais eficiente prever a possibilidade de

		se conceder um prazo indeterminado para a prestação de informações à autoridade até que seja findo o processo de comunicação pela ANPD, com eventual decisão final. Garantindo que o processo possa ser complementado como um todo a qualquer momento, é possível conferir uma maior segurança e qualidade da atuação da agência e da colaboração do controlador no intuito de garantir e preservar ao máximo os direitos dos titulares e para mitigar os efeitos do incidente.
§ 6º O prazo constante no caput deste artigo conta-se em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.	**ADICIONAR:** §7º Em caso de impossibilidade de comunicar o incidente no prazo estipulado no caput, o agente de tratamento deverá notificá-lo no menor prazo possível, apresentando justificativa suficiente e adequada para o não cumprimento do prazo geral. §8º Considera-se como conhecimento do incidente, nos termos do caput, o momento a partir do qual o controlador tem razoável grau de certeza da ocorrência do incidente de segurança com dados pessoais, materializada com a ciência pelo Encarregado de Dados ou do responsável pelo canal de comunicação nos termos da Resolução CD/ANPD n. 2/2022.	Por fim, a ABRANET, inspirando-se nas *Guidelines 9/2022 do European Data Protection Board ("EDPB"),* sugere que haja delimitação do significado de "tomar conhecimento do incidente", como marco temporal de início do prazo de comunicação à ANPD. Desse modo, propõe-se que seja entendido como **um grau razoável de certeza do controlador de que o incidente ocorreu,** podendo, até mesmo, ir além e referenciar que esse conhecimento ocorre **quando o Encarregado de Dados do controlador é efetivamente informado ou, no caso de pequenos agentes de tratamento que não possuam encarregado, quando o setor ou funcionário responsável pelo canal de comunicação com os titulares e com a autoridade seja informado.** Em virtude da ainda escassa cultura de proteção de dados nas empresas brasileiras, nem sempre há essa consciência dos funcionários, em todas as pontas, da necessidade de informar imediatamente o Encarregado. Muitas vezes, em grupos econômicos

		maiores, há grande demora do envio dessa informação ao Encarregado, que estará efetivamente apto a avaliar a necessidade de comunicação.
Art. 7º Cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.	Art. 7º Será conferido sigilo à tramitação de processo de comunicação de incidente de segurança, cabendo ao controlador solitar à ANPD, de maneira fundamentada, esse sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.	A ABRANET entende que toda a tramitação do processo de comunicação do incidente de segurança deveria ter o sigilo na sua tramitação como premissa, em linha com o que ocorre em outras legislações, como o Código de Processo Civil. Várias são as informações protegidas por sigilo e relacionadas à sua atividade que devem ser fornecidas no processo de comunicação pelo controlador, inclusive documentos internos e sigilosos como o relatório do incidente, registro de atividades de tratamento e relatório de impacto à proteção de dados pessoais, além de informações sobre medidas de segurança e número de titulares que são tratados pela organização, entre outras protegidas por segredo. Assim, sugerimos a alteração deste artigo prevendo expressamente o sigilo de todo o processo de comunicação de incidentes.
Art. 8º A ANPD poderá, a qualquer tempo, solicitar informações adicionais ao controlador, referentes ao incidente de segurança, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente, o relatório de impacto à proteção de dados pessoais (RIPD) e o relatório de tratamento do incidente, estabelecendo prazo para o envio das informações.	Art. 8º Ressalvados os segredos comercial e industrial e as informações sigilosas, a ANPD poderá, até a extinção do processo de investigação do incidente, ~~a qualquer tempo~~ solicitar informações adicionais ao controlador, referentes ao incidente de segurança com dados pessoais, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente, o relatório de impacto à proteção de dados pessoais (RIPD) e o relatório de tratamento do incidente, estabelecendo prazo para o envio das informações, de, no mínimo,	Primeiramente, é importante notar que o ordenamento jurídico nacional salvaguarda o segredo de negócio, bem como que o §3º do artigo 10º e o artigo 38º da LGPD ressalvam os segredos comercial e industrial na elaboração e compartilhamento do relatório de impacto à proteção de dados pessoais. Em adição, o inciso II do artigo 55-J da LGPD estabelece que compete à ANPD zelar pelos segredos comercial e industrial, no mesmo sentido, o §5º do referido artigo dispõe que, no exercício de suas competências, a Autoridade

	20 dias úteis, contados a partir do dia seguinte do recebimento da intimação da solicitação pelo controlador.	deverá zelar pela preservação do segredo empresarial e do sigilo das informações. Desta feita, sugere-se que o artigo 8º reflita tal proteção. O artigo utiliza termos que dão ampla discricionariedade à ANPD, como "a qualquer tempo" e "estabelecendo prazo para envio das informações". Diante disso, recomenda-se que a solicitação de informações adicionais por parte da Autoridade ocorra até a extinção do processo de comunicação. Além disso, para assegurar que a ANPD estabeleça prazos factíveis para que o controlador forneça informações adicionais, recomenda-se que esse prazo possa ser estabelecido com o mínimo de 20 dias úteis (seguindo o paralelismo com os demais prazos da minuta) ou de 15 dias úteis, caso o paralelismo ocorra com os artigos do CPC.

Seção III - Da comunicação do incidente ao titular de dados pessoais		
Art. 9º A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador, no prazo de três dias úteis contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:	Art. 9º A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador, sempre que possível, no prazo de ~~três~~ sete dias úteis, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar alto risco de dano relevante aos titulares afetados, e deve conter as seguintes informações: Alternativamente	Tal como argumentado no art. 6º, com relação ao prazo de comunicação de incidente de segurança à ANPD, a ABRANET entende que, em virtude da grande influência da *General Data Protection Regulation* (GDPR) na LGPD, é pertinente se inspirar no normativo europeu também nesse tema. Nesse sentido, **sugere-se inspiração no art. 33(1) do GDPR, para inserir a expressão de notificar, sempre que possível, no prazo estabelecido, de forma a ter uma cláusula mais geral que abarque os casos em que não é possível cumprir o prazo, mediante**

	Art. 9 A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador em um prazo razoável, sempre que o incidente possa acarretar alto risco de dano relevante aos titulares afetados, e deve conter as seguintes informações:	**justificativa adequada.** Além disso, levando em consideração a atuação mais educativa e gradual da ANPD em relação à propagação da cultura de proteção de dados, a ABRANET defende que o **prazo seja ampliado para 7 dias úteis,** pelo menos em um primeiro momento de maiores dificuldades de conformidade dos agentes com a nova legislação. **Deve-se considerar que notificar toda uma base de titulares, em uma linguagem acessível, é bem mais demorado e sensível do que notificar a ANPD, sendo necessário maior prazo.** A ANPD deve também considerar que, **em mercados digitais, os temas avançam de forma dinâmica e acelerada,** sendo que um prazo de seis meses para manutenção de informe sobre o incidente na sua página **é excessivamente longo. No entendimento da ABRANET, um mês é tempo suficiente e adequado para fins de relações econômicas e sociais pela Internet.**
V - o contato para obtenção de informações e dados do encarregado, quando aplicável.	V - o contato ou canal de atendimento para obtenção de informações e dados ~~do encarregado,~~ quando aplicável.	Acerca do envio do contato do Encarregado de Dados aos titulares, a ABRANET vislumbra que **poderia prejudicar o exercício de suas funções na organização, especialmente quando for uma pessoa física, com um sobrecarregamento de sua caixa para sanar eventuais dúvidas**, que poderiam ser solucionadas em contato próprio para o incidente. Não haveria prejuízo para os titulares que tal contato não seja do Encarregado e, caso seja, pode haver prejuízo à observância da LGPD pelo

		agente de tratamento. Ademais, seria importante que **a ANPD delimitasse critérios objetivos para quando esse contato é aplicável.**
§1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios: II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.	II – ocorrer, preferencialmente, de forma direta e individualizada, caso seja possível identificá-los e contatá-los, salvo se o controlador decidir por outro meio de comunicação mais eficiente.	Considerando que nem sempre quando se identifica um titular é possível contatá-lo, a ABRANET defende a inclusão sugerida. É preciso que essa Autoridade considere que, em certas circunstâncias, existem formas mais eficazes de comunicar os titulares afetados. Nesse sentido, destaca-se que o Working Party 29 pontua que os controladores estão na melhor posição para determinar o canal mais adequado para comunicar os titulares. Em complemento, no mesmo documento, o grupo de trabalho indica que os controladores devem escolher o meio de comunicação que maximize as chances de que as informações necessárias cheguem àqueles afetados pelo ocorrido. Sendo assim, sugere-se que o dispositivo em questão seja reformulado.
§ 3º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis, tais como na sua página na Internet, em aplicativos, em suas mídias sociais e em canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização pelo período de, no mínimo, seis meses.	§ 3º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis, tais como na sua página na Internet, em aplicativos, em suas mídias sociais e em canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização pelo período de, no mínimo, ~~seis meses~~ um mês.	No entendimento da ABRANET, o prazo de 6 meses como prazo mínimo para a divulgação da ocorrência do incidente se mostra extremamente extenso e desproporcional, quando se leva em conta o dinamismo e rapidez da Internet. Considerando-se pesquisas realizadas na legislação do Canadá, Australia, Nova Zelândia, Espanha, Reino Unido, Irlanda e Portugal, não foi identificada abordagem como essa relacionada com o assunto.
§ 5º Poderá ser considerada boa prática para fins do disposto no art. 52, §1º, IX da LGPD, a inclusão na	§ 5º ~~Poderá ser~~ Será considerada boa prática para fins do disposto no art. 52, §1º, IX da LGPD, a	Na linha da regulação responsiva, seria importante a ANPD considerar sempre como boa prática medidas

comunicação ao titular de recomendações aptas a reduzir os efeitos do incidente.	inclusão na comunicação ao titular de recomendações aptas a reduzir os efeitos do incidente de segurança com dados pessoais e circunstância atenuante, nos termos do art. 13, II, da Resolução CD/ANPD nº 4/2023, que institui o Regulamento de Dosimetria e Aplicação de Sanções Administrativas.	proativas adotadas pelos agentes de tratamento de dados que atendam ao previsto na LGPD e mitiguem danos a titulares em caso de eventual incidente de segurança. Desta forma, tal consideração não precisaria ficar sujeita à discricionariedade administrativa, mas, sim ser concedida como um direito do agente de tratamento, representando um estímulo ao desenvolvimento dessas práticas. Ademais, o Regulamento de Dosimetria e Aplicação de Sanções Administrativas prevê em seu artigo 13, II, a redução da sanção pecuniária em 20% (vinte por cento) nos casos de implementação de política de boas práticas e de governança ou de adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar os danos aos titulares. Neste mesmo caso, a comunicação ao titular de recomendações e as ações educativas, para fins deste Regulamento também devem ser consideradas boas práticas e atenuantes a serem consideradas no processo administrativo sancionador.
§ 6º O prazo constante no caput deste artigo conta-se em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.	**ADICIONAR:** §7º Considera-se como alto risco de dano relevante aos titulares a definição da regulamentação própria da ANPD sobre o tema. §8º Em caso de impossibilidade de comunicar o incidente no prazo estipulado no caput, o agente de tratamento deverá notificá-lo no menor prazo possível, apresentando justificativa suficiente e adequada para o não cumprimento do prazo geral. §9º Considera-se como conhecimento do incidente, nos termos do caput, o momento a partir do qual o controlador tem razoável grau de certeza da	Novamente inspirando-se no GDPR, a ABRANET propõe que haja diferenciação dos critérios para notificar a ANPD e os titulares, **colocando uma barra mais alta para a exigência de notificar titulares, tal como ocorre no art. 34(1) do GDPR, que usa o conceito de alto risco para notificar titulares.** Nesse sentido, a ANPD já realizou consulta pública sobre o significado de alto risco, que pode ser aplicado aqui nesse contexto, assegurando-se coerência normativa e proporcionalidade regulatória. Fonte: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach/personal-data-

	ocorrência do incidente de segurança envolvendo dados pessoais, materializada com a ciência pelo Encarregado de Dados ou do responsável pelo canal de comunicação nos termos da Resolução CD/ANPD n. 2/2022.	breaches-a-guide/. Enquanto a consulta pública não definir, em concreto, o que determina um tratamento como sendo de alto risco, a ABRANET recomenda a utilização dos critérios definidos no art. 4 da Resolução CD/ANDP nº 2.
CAPÍTULO V - DO PROCESSO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS		
SEÇÃO I - Das disposições gerais		
Art. 10. O controlador deverá manter o registro de incidentes de segurança com dados pessoais, inclusive daqueles não comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.	Art. 10. O controlador deverá manter o registro de incidentes de segurança significativos com dados pessoais, inclusive daqueles não comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.	Na visão da ABRANET, o registro a ser realizado e mantido acerca de incidentes de segurança deve ser relacionado aos incidentes de segurança que sejam significativos, ainda que não comunicados por não causarem risco ou dano relevante aos titulares, não devendo englobar toda e qualquer ocorrência. Lembramos que o registro de incidentes de segurança, especialmente os não comunicados à ANPD, é uma obrigação de documentação nova, prevista apenas nesta proposta de norma e que demandará esforços de adaptação dos controladores, inclusive para sua guarda pelo tempo aqui indicado.
Art. 14. Em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, sem prévia manifestação do controlador.	Art. 14. Em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, a ANPD, após a avaliação da gravidade do incidente, poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, ~~sem prévia~~ após a manifestação do controlador. Alternativamente:	Em consonância com os princípios constitucionais do contraditório e da ampla defesa, o controlador deverá ser ouvido pela ANPD para esclarecimento dos fatos e sobre a viabilidade de implementação das medidas preventivas antes da sua aplicação pela ANPD, devendo a determinação dessas medidas ocorrer sem prévia manifestação do controlador em casos excepcionais, em linha com a atuação responsiva da ANPD. Minimamente, é essencial garantir ao controlador a oportunidade para se manifestar sobre tais medidas.

	Art. 14. Em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, sem prévia manifestação do controlador, sendo reservado o direito do controlador de recorrer dessa decisão.	Alternativamente, a ABRANET propõe ao menos a inserção do direito de recorrer de uma decisão da ANPD no processo de comunicação de incidente, para fins de observância dos princípios basilares do direito ao contraditório e devido processo legal, nos termos da Lei de Processo Administrativo.
Art. 16. A ANPD determinará ao controlador o envio da comunicação do incidente à Autoridade e aos titulares, quando identificar a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados que não tenha sido comunicado pelo controlador. § 1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no caput.	§1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no caput, após ter notificado o controlador do cometimento de irregularidades que tenham sido praticadas e este deixar, de forma injustificada, de saná-las no prazo assinalado.	A multa diária, em leitura conjunta desta minuta de Regulamento e do Regulamento de Dosimetria e Aplicação de Sanções Administrativas, poderá ser aplicada para assegurar o cumprimento, em prazo certo, de uma sanção não pecuniária ou de uma determinação estabelecida pela ANPD. Contudo, devem ser observadas as hipóteses em que essa multa cominatória se aplicará, conforme disposto no § 3º do art. 16 do Regulamento de Dosimetria e Aplicação de Sanções Administrativos, que dispõe "A sanção de multa diária poderá ser aplicada na hipótese do caput deste artigo ou quando o infrator: I - após notificado do cometimento de irregularidades que tenham sido praticadas, deixar de saná-las no prazo assinalado; II - praticar obstrução à atividade de fiscalização, desde que a aplicação da multa diária seja necessária para desobstrui-la; ou III - praticar infração permanente não cessada até a decisão".
Art. 18. A ANPD poderá, a qualquer momento, realizar auditorias ou inspeções junto aos agentes de tratamento, ou determinar a sua realização, para coletar informações complementares ou validar as informações recebidas, com o objetivo de subsidiar	Art. 18. Respeitados os prazos de comunicação do incidente de segurança com dados pessoais e caso insuficientes os esclarecimentos prestados pelo controlador, ~~A ANPD~~ poderá a ANPD, no âmbito de atividade de fiscalização, ~~a qualquer momento,~~	Conforme o que determina o art. 55-J, XVI da LGPD, a realização de auditorias é admitida apenas no âmbito da atividade de fiscalização. Ainda, recomenda-se que seu procedimento seja desenhado de forma mais restrita, no âmbito do

as decisões no âmbito do processo de comunicação de incidente de segurança com dados pessoais.	excepcionalmente, realizar auditorias ou inspeções junto aos agentes de tratamento, ou determinar a sua realização, para coletar informações complementares ou validar as informações recebidas, com o objetivo de subsidiar as decisões no âmbito do processo de comunicação de incidente de segurança com dados pessoais. § 1º - A Autoridade especificará em sua decisão o objetivo da auditoria ou das inspeções a serem realizadas, de forma fundamentada e delimitada ao escopo do incidente, abrindo prazo de dez dias úteis para a manifestação do controlador; § 2º - Durante todo o processo de auditoria determinado pela ANPD e após sua conclusão, o sigilo profissional deve permanecer entre o auditor e o auditado, sendo confidenciais qualquer informação e/ou documentos recebidos pelo auditor, bem como os acessos autorizados ao auditor. § 3º - O controlador pode, a qualquer momento, opor-se ao auditor nomeado pela Autoridade em casos de suspeição ou impedimento do auditor; §4º - Na realização de auditorias e inspeções ficam expressamente salvaguardados os segredos comercial e industrial.	processo de comunicação do incidente de segurança com dados pessoais, e apenas quando absolutamente necessária para subsidiar as determinações da ANPD sobre a adoção de providências e medidas para reverter ou mitigar os efeitos do incidente para salvaguardar direitos dos titulares (em coerência com o disposto nos arts. 14 e 19 desta minuta). Ademais, devem ser preservados, em quaisquer hipóteses, os segredos comerciais e de negócio, o sigilo profissional do auditor e a possibilidade do controlador opor-se - a qualquer momento - ao auditor nomeado. A manifestação do controlador a respeito do despacho determinando a auditoria também deve ser preservada, de modo que este possa alegar incongruência entre o escopo da auditoria e o incidente reportado, hipóteses de segredo comercial ou industrial, dentre outros questionamentos que se façam pertinentes a partir do caso concreto.
Art. 19. Avaliada a gravidade do incidente, a ANPD poderá determinar ao controlador a adoção das seguintes providências para a salvaguarda dos direitos dos titulares, dentre outras: I - ampla divulgação do incidente em meios de comunicação; ou	I – ampla divulgação do incidente de segurança com dados pessoais em meios de comunicação, como medida excepcional e exclusivamente na hipótese prevista no at. 20 deste Regulamento, e desde que a via eleita pelo controlador tenha se demonstrado ineficaz para fins de comunicação com os titulares afetados.	A ampla divulgação deve ser medida excepcional, aplicada apenas na hipótese prevista no art. 20 e desde que estritamente necessário, de forma a não acarretar ao titular aplicação de medida que possa ser confundida com aplicação de pena com caráter sancionador. Ainda, a depender do conteúdo e extensão das informações divulgadas sobre o incidente, a ampla divulgação do incidente durante

		o processo de comunicação à ANPD poderá acarretar prejuízos para a apuração e/ou investigação do incidente, bem como o aumento da circulação indevida dos dados atingidos em razão da exposição do caso e exploração de vulnerabilidades por terceiros. Ademais, o resultado do processo de comunicação de incidente pode ser a verificação de não ocorrência do incidente ou a ocorrência de incidente sem potencial de dano relevante aos titulares, tal como previsto no art. 25, o que reforça a necessidade de cautela na aplicação desta medida.
§ 3º A ANPD poderá divulgar em sua página na Internet informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial.	"§ 3º A ANPD poderá divulgar, de forma agregada e após extinto ou finalizado o processo de comunicação, em sua página na Internet, informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial e em conformidade com seus poderes previstos no Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador. §4º Tal divulgação referida no parágrafo anterior deverá observar os segredos comercial e industrial, bem como a confidencialidade de informações que identifiquem ou possam identificar os agentes de tratamento envolvidos.	A própria LGPD define como penalidade a publicização da infração após devidamente confirmada e apurada a sua ocorrência, observado o devido processo administrativo. A ocorrência de incidente de segurança não é uma infração por si só, entretanto, tornar o incidente público na página da ANPD, ainda mais sem prazo específico para tal divulgação, pode trazer efeito similar ao agente de tratamento, ainda mais se for imputada a pena de publicização da infração ao controlador eventualmente decorrente do incidente de segurança. Por mais que as propostas sejam distintas, para o homem médio a reputação do controlador poderá estar comprometida, mesmo que o objetivo inicial da medida seja assegurar maior transparência para os titulares. Ademais, tal medida não poderia ser aplicada durante o curso do processo de comunicação de incidente à ANPD, uma vez que o resultado do processo pode ser a verificação de não ocorrência do incidente ou a ocorrência de incidente sem potencial de dano relevante aos titulares, tal como previsto no art. 25.

		Assim, sugere-se que o dispositivo seja ajustado para deixar claro que as informações a serem divulgadas são informações agregadas e gerais sobre incidentes de segurança, sem revelar a identidade do controlador ou especificidades do caso concreto. Tal medida é importante, inclusive, para que não se crie um ambiente de desincentivo às notificações, visto que poderia aumentar o risco de dano aos titulares, além de o controlador ficar sujeito a um dano reputacional sem que tenha passado por um processo administrativo sancionador, com direito à ampla defesa e contraditório
Art. 20. A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação, a ser custeada pelo controlador, para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I da LGPD, quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.	Art. 20. A ANPD poderá determinar ampla divulgação do incidente de segurança com dados pessoais em meios de comunicação, a ser custeada pelo controlador, desde que seja estritamente necessária para a salvaguarda dos direitos dos titulares e nos casos de incidentes de segurança de maior gravidade, nos termos do art. 48, § 2º, I da LGPD, apenas se a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.	A ampla divulgação da ocorrência do incidente deve ser medida excepcional, aplicada apenas na hipótese prevista no art. 20 e se for estritamente necessária em razão da gravidade do incidente e da necessidade de salvaguardar os direitos do titular dos dados, de forma a não acarretar ao controlador a aplicação de medida que possa ser confundida com aplicação de pena com caráter sancionador. Ainda, a depender do conteúdo e extensão das informações divulgadas sobre o incidente, a ampla divulgação do incidente durante o processo de comunicação à ANPD poderá acarretar prejuízos para a apuração e/ou investigação do incidente, bem como o aumento da circulação indevida dos dados atingidos em razão da exposição do caso e exploração de vulnerabilidades por terceiros. Ademais, o resultado do processo de comunicação de incidente pode ser a verificação de não ocorrência do incidente ou a ocorrência de incidente sem potencial de dano relevante aos titulares, tal como previsto no art. 25, o que reforça a necessidade de cautela na aplicação

		desta medida. Por fim, importante destacar se tratar de medida extremamente onerosa, que somente deve ser aplicada em casos que realmente a justifiquem e dentro de parâmetros e critérios claros e razoáveis, inclusive com relação ao prazo e dos meios estritamente necessários, que não estão ainda definidos nesta minuta de regulamento.