PA-LGPD-AGU

Plano de Ação para adequação da Advocacia-Geral da União (AGU) à Lei Geral de Proteção de Dados Pessoais (LGPD)

FICHA TÉCNICA

ADVOCACIA-GERAL DA UNIÃO

Advogado-Geral da União
Ministro André Luiz de Almeida Mendonça

Coordenação
Vládia Pompeu Silva - ADJ/AGU

Colaboradores
Francis Christian Alves Scherer Bicca – OGAGU
Mário Gleick Aguiar Guimarães – OGAGU
Geraldo Cardoso Moitinho – OGAGU
Claudinyze Maria Feydit Ferreira Avelar – OGAGU
José Luiz Solheiro - OGAGU
Caio Castelliano de Vasconcelos – DGE
Eduardo Watanabe Oliveira - DGE
Sandro de Oliveira Araújo – DTI
Marcelo Fenoll Ramal - DTI

Revisão e texto
Mário Gleick Aguiar Guimarães – OGAGU
Eduardo Watanabe Oliveira - DGE
Marcelo Fenoll Ramal - DTI

Projeto Gráfico
Renato Caetano Menezes - ASCOM

Artes
Walbert kuhne- EAGU

O uso de dados pessoais tem se tornado a cada dia mais frequente, como decorrência lógica da globalização da economia e do avanço tecnológico.

Nesse contexto, um cenário desafiador se apresenta: incentivar a utilização de ferramentas virtuais - as quais podem contribuir sobremaneira para a otimização de tempo e para o melhor uso de recursos -, sem, contudo, descuidar das formalidades legais e dos direitos assegurados aos titulares de dados.

Diante desse cenário, entrou em vigor, em maio de 2018, na União Europeia, o Regulamento Geral sobre Proteção de Dados (também conhecido como GDPR), norma que inspirou a edição de outras análogas, mundo afora, tal como ocorreu no Brasil, com a edição da Lei n.º 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).

A Lei Geral de Proteção de Dados Pessoais dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, sendo que as normas gerais contidas na aludida Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios.

Logo, urge que os entes federativos e seus respectivos órgãos adotem providências para adequar-se à Lei n.º 13.709/18.

Nesse sentido, surge o presente Plano de Ação para adequação da Advocacia-Geral da União à LGPD (PA-LGPD-AGU), o qual se propõe a ser o instrumento orientador de adequação da AGU à Lei Geral de Proteção de Dados Pessoais.

O Plano de Ação para adequação da Advocacia-Geral da União (AGU) à Lei Geral de Proteção de Dados Pessoais (PA-LGPD-AGU), é o documento que norteia a implementação da Lei n.º 13.709, de 14 de agosto de 2018, no âmbito da AGU.

Ao estruturar o planejamento da implementação da Lei Geral de Proteção de Dados na AGU, o PA-LGPD-AGU tem por parâmetro, além da própria LGPD, normas correlatas no plano nacional e internacional, guardando consonância com o arcabouço jurídico pátrio atinente à proteção de dados pessoais e com os compromissos assumidos pelo Brasil relativos ao tema, a exemplo da Parceria para Governo Aberto (Open Government Partnership – OGP) - iniciativa internacional que pretende difundir e incentivar globalmente práticas governamentais relacionadas à transparência dos governos, ao acesso à informação pública e à participação social.

O PA-LGPD-AGU reúne diretrizes para que a AGU, por meio de um esforço conjunto e sinérgico, adote as medidas necessárias para assegurar a observância dos princípios estatuídos na LGPD referentes aos direitos dos titulares de dados pessoais.

Um dos referenciais teóricos utilizados para a elaboração do PA-LGPD-AGU foi o Guia de Boas Práticas da LGPD, o qual visa fornecer orientações aos órgãos e entidades da administração pública federal, autárquica e fundacional, para as operações de tratamento de dados pessoais, conforme previsto no art. 50 da Lei nº 13.709/18, além de detalhar métodos e formas de diferenciação das mais diversas situações com as quais irão deparar os servidores públicos responsáveis por operar ou controlar a aplicação da aludida lei.

Ainda como referenciais teóricos adotados para constituir o PA-LGPD-AGU, citem-se os Marcos de Conformidade com a LGPD, materializados por Guias Operacionais para adequação à LGPD, os quais fazem parte do conjunto de ações preparadas pela Secretaria de Governo Digital do Ministério da Economia (SGD-ME) para fomentar a cultura de proteção de dados e apoiar a evolução da maturidade necessária às adequações da lei nos órgãos do Governo Federal (alinhando-se com os objetivos 10 e 11 do princípio Governo Confiável da Estratégia de Governo Digital – EGD, que prevê a entrega de importantes Marcos de Conformidade com a LGPD, com o objetivo de auxiliar os órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (Sisp) no processo de adequação à Lei Geral de Proteção de Dados Pessoais).

Na construção do PA-LGPD-AGU foram considerados, à luz dos dispositivos pertinentes da LGPD, aspectos atinentes ao Contexto Organizacional, à Liderança, à Capacitação, à Conformidade do Tratamento, aos Direitos do Titular, ao Compartilhamento de Dados Pessoais, à Violação de Dados Pessoais e às Medidas de Proteção, por meio uma abordagem atinente a aspectos de Governança, de Conformidade Legal e Respeito aos Princípios, de Transparência e Direitos do Titular, de Rastreabilidade, de Adequação de Contratos e Relações com Parceiros, de Segurança da Informação, e de Violação de Dados.

É válido destacar que o PA-LGPD-AGU será atualizado, sempre que necessário, para adequar-se às determinações da Autoridade Nacional de Proteção de Dados (ANPD) e dos órgãos de controle interno e de controle externo, bem como para melhor esclarecer algum trecho específico, ou diante de eventuais atualizações legislativas ou de novos entendimentos preponderantes sobre a matéria.

Na elaboração do PA-LGPD-AGU, considerou-se o seguinte escopo de normas que contêm previsões que autorizam o tratamento de dados:

- Lei n° 9.507/1997, que regula o direito de acesso a informações e disciplina o rito processual do habeas data.

- Lei n° 9.784/1999, que regula o processo administrativo no âmbito da Administração Pública Federal.

- Lei n° 12.527/2011 (Lei de Acesso à Informação), que regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

- Decreto n° 7.724/2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

- Lei n° 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Bras

- Lei n° 12.965/2014 (Marco Civil da Internet), que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

- Decreto n° 8.771/2016, que regulamenta a Lei nº 12.965, de 23 de abril de 2014, (Marco Civil da Internet), para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

- Decreto n° 8.936/2016, que institui a Plataforma de Cidadania Digital e dispõe sobre a oferta dos serviços públicos digitais, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

- Lei n° 13.444/2017, que dispõe sobre a Identificação Civil Nacional (ICN).

- Lei n° 13.460/2017, que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública.

- Decreto n° 9.278/2018, que regulamenta a Lei nº 7.116, de 29 de agosto de 1983, que assegura validade nacional às Carteiras de Identidade e regula sua expedição.

- Lei n° 13.709/2018, Lei Geral de Proteção dos Dados – LGPD.

- Decreto n° 9.492/2018, que regulamenta a Lei nº 13.460, de 26 de junho de 2017 , que dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública federal, institui o Sistema de Ouvidoria do Poder Executivo federal, e altera o Decreto nº 8.910, de 22 de novembro de 2016, que aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança do Ministério da Transparência, Fiscalização e Controladoria-Geral da União.

- Decreto n° 9.723/2019, que altera o Decreto nº 9.094, de 17 de julho de 2017, o Decreto nº 8.936, de 19 de dezembro de 2016, e o Decreto nº 9.492, de 5 setembro de 2018, para instituir o Cadastro de Pessoas Físicas - CPF como instrumento suficiente e substitutivo da apresentação de outros documentos do cidadão no exercício de obrigações e direitos ou na obtenção de benefícios e regulamentar dispositivos da Lei nº 13.460, de 26 de junho de 2017.
- Lei n° 13.853/2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.
- Decreto n° 10.046/2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal e institui o Cadastro Base do Cidadão e o Comitê Central de Governança de Dados.
- Lei n° 13.853/2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

Objetivo geral do PA-LGPD-AGU

Nortear a implementação da Lei n.º 13.709/18 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito da Advocacia-Geral da União.

Objetivos específicos do PA-LGPD-AGU

Identificar as atividades prioritárias a serem desenvolvidas para o atendimento das disposições da LGPD

Indicar medidas necessárias para a adequação da AGU à Lei Geral de Proteção de Dados Pessoais

Fixar parâmetros para assegurar a transparência e o respeito aos direitos dos titulares de Dados Pessoais nos serviços prestados pela Advocacia-Geral da União

Fomentar a cultura de Proteção de Dados Pessoais na AGU

Promover o engajamento intersetorial da AGU no atendimento aos marcos de conformidade atinentes à LGPD

II – Tratamento de Dados Pessoais

Conceitos

Nos termos do inciso X do art. 5º da LGPD, considera-se tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

É imperioso destacar ainda os conceitos de dado pessoal e de dado pessoal sensível, assim trazidos pela Lei Geral de Proteção de Dados Pessoais:

- dado pessoal: informação relacionada a pessoa natural identificada ou identificável (LGPD, art. 5º, I)
- dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (LGPD, art. 5º, II)

PRINCÍPIOS

Nesse aspecto, é imperioso destacar os princípios elencados no art. 6º da LGPD, os quais devem orientar o tratamento de dados pessoais:

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS

Nesse sentido, destacam-se as hipóteses de tratamento de dados pessoais trazidas pelo art. 7º da LGPD:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019) Vigência

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

HIPÓTESES DE TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS

No mesmo sentido, é necessário transcrever as hipóteses de tratamentos de dados pessoais sensíveis referidas no art. 11 da LGPD:

Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo controlador;

b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

e) proteção da vida ou da incolumidade física do titular ou de terceiro;

f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou (Redação dada pela Lei nº 13.853, de 2019) Vigência

g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

DIREITOS DO TITULAR

A Lei Geral de Proteção de Dados Pessoais empodera os titulares de dados, fornecendo-lhes direitos a serem exercidos perante os controladores de dados, como se pode verificar na tabela abaixo:

Tabela 1 Direitos garantidos aos titulares de dados

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	PRINCÍPIO CORRESPONDENTE	REFERÊNCIA LEGISLATIVA (LGPD)
Direito ao tratamento adstrito aos propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades	Princípio da finalidade	Art. 6º, I
Direito ao tratamento adequado, compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento	Princípio da adequação	Art. 6º, II
Direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento	Princípio da necessidade	Art. 6º, III
Direito à consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais	Princípio do livre acesso	Art. 6º, IV
Direito à exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade para o cumprimento da finalidade de seu tratamento	Princípio da qualidade dos dados	Art. 6º, V

DIREITOS DO TITULAR

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	PRINCÍPIO CORRESPONDENTE	REFERÊNCIA LEGISLATIVA (LGPD)
Direito a informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial	Princípio da transparência	Art. 6º, VI
Direito à segurança dos dados, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão	Princípio da segurança	Art. 6º, VII
Direito à adequada prevenção de danos, ao qual se contrapõe o dever, por parte dos agentes de tratamento, de adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais	Princípio da prevenção	Art. 6º, VIII
Direito de não ser discriminado de forma ilícita ou abusiva	Princípio da não discriminação	Art. 6º, IX
Direito de exigir a adequada responsabilização e a prestação de contas por parte dos agentes de tratamento, ao qual se contrapõe o dever, por parte destes, de adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais	Princípio da responsabilização e prestação de contas	Art. 6º, X

DIREITOS DO TITULAR

Nessa esteira, a LGPD não só assegura aos titulares de dados os direitos decorrentes dos princípios (art. 6º), mas também outros direitos específicos, conforme referidos na seguinte tabela:

Tabela 2 Diretos específicos dos titulares de dados

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	REFERÊNCIA LEGISLATIVA (LGPD)
Direito de condicionar o tratamento de dados ao prévio consentimento expresso, inequívoco e informado do titular, salvo as exceções legais	Arts. 7º, I, e 8º
Direito de exigir o cumprimento de todas as obrigações de tratamento previstas na lei, mesmo para os casos de dispensa de exigência de consentimento	Art. 7º, § 6º
Direito à inversão do ônus da prova quanto ao consentimento	Art. 8º, § 2º
Direito de requerer a nulidade de autorizações genéricas para o tratamento de dados pessoais	Art. 8º, § 4º
Direito de requerer a nulidade do consentimento caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou, ainda, não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca	Art. 9º, § 1º
Direito de requerer a revogação do consentimento a qualquer tempo, mediante manifestação expressa do titular, por procedimento gratuito e facilitado	Art. 8º, § 5º
Direito de revogar o consentimento caso o titular discorde das alterações quanto ao tratamento de dados, seja na finalidade, forma e duração do tratamento, alteração do controlador ou compartilhamento	Arts. 8º, § 6º e 9º, § 2º
Direito de acesso facilitado ao tratamento de dados, cujas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de (entre outras): finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador; finalidade, responsabilidades dos agentes que realizarão o tratamento e direitos do titular, com menção explícita aos direitos contidos no art. 18	Art. 9º

DIREITOS DO TITULAR

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	REFERÊNCIA LEGISLATIVA (LGPD)
Direito de ser informado sobre aspectos essenciais do tratamento de dados, com destaque específico sobre o teor das alterações supervenientes no tratamento	Art. 8º, § 6º
Direito de ser informado, com destaque, sempre que o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço, ou, ainda, para o exercício de direito, o que se estende à informação sobre os meios pelos quais o titular poderá exercer seus direitos	Art. 9º, § 3º
Direito de ser informado sobre a utilização dos dados pela administração pública para os fins autorizados pela lei e para a realização de estudos por órgão de pesquisa	Art. 7º, III e IV c/c art. 7º, § 1º
Direito de que o tratamento de dados pessoais cujo acesso é público esteja adstrito à finalidade, à boa-fé e ao interesse público que justificaram sua disponibilização	Art. 7º, § 3º
Direito de condicionar o compartilhamento de dados por determinado controlador que já obteve consentimento a novo e específico consentimento. No caso da Administração Pública Federal (APF), em que o tratamento é embasado nas hipóteses de dispensa de consentimento original, o compartilhamento demandará uma nova justificativa de tratamento	Art. 7º, § 5º
Direito de ter o tratamento de dados limitado ao estritamente necessário para a finalidade pretendida quando o tratamento for baseado no legítimo interesse do controlador	Art. 10, § 1º
Direito à transparência do tratamento de dados baseado no legítimo interesse do controlador	Art. 10, § 2º
Direito à anonimização dos dados pessoais sensíveis, sempre que possível, na realização de estudos por órgão de pesquisa	Art. 11, II, c

DIREITOS DO TITULAR

DIREITOS DOS TITULARES DE DADOS QUE DECORREM DOS PRINCÍPIOS	REFERÊNCIA LEGISLATIVA (LGPD)
Direito de ter a devida publicidade em relação às hipóteses de dispensa de consentimento para: tratamento de dados sensíveis no cumprimento de obrigação legal ou regulatória pelo controlador; ou tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos	Art. 11, § 2º
Direito de impedir a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde, com o objetivo de obter vantagem econômica (exceto nos casos de portabilidade de dados quando consentido pelo titular)	Art. 11, § 4º
Direito de que os dados pessoais sensíveis utilizados em estudos de saúde pública sejam tratados exclusivamente dentro do órgão de pesquisa e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas	Art. 13
Direito de não ter dados pessoais revelados na divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa sobre saúde pública	Art. 13, § 1º
Direito de não ter dados pessoais utilizados em pesquisa sobre saúde pública transferidos a terceiros pelo órgão de pesquisa	Art. 13, § 2º
Direito ao término do tratamento, quando verificado que: (i) a finalidade foi alcançada ou que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada; (ii) houve o fim do período de tratamento; (iii) houve comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento, conforme disposto no § 5º do art. 8º da Lei e resguardado o interesse público; ou (iv) por determinação da autoridade nacional, quando houver violação ao disposto na Le	Art. 15
Direito à eliminação ou ao apagamento dos dados, no âmbito e nos limites técnicos das atividades, sendo autorizada a conservação somente nas exceções legais	Art. 16

De modo resumido, temos, na tabela a seguir, as hipóteses de tratamento autorizadas pela LGPD e respectiva base legal:

Tabela 3 Hipóteses de tratamento de dados pessoais

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 1: Mediante consentimento do titular	LGPD, art. 7º, I	LGPD, art. 11, I
Hipótese 2: Para o cumprimento de obrigação legal ou regulatória	LGPD, art. 7º, II	LGPD, art. 11, II, “a”
Hipótese 3: Para a execução de políticas públicas	LGPD, art. 7º, inciso III	LGPD, art. 11, II, “b”
Hipótese 4: Para a realização de estudos e pesquisas	LGPD, art. 7º, inciso IV	LGPD, art. 11, II, “c”
Hipótese 5: Para a execução ou preparação de contrato	LGPD, art. 7º, inciso V	Não se aplica
Hipótese 6: Para o exercício de direitos em processo judicial, administrativo ou arbitral	LGPD, art. 7º, inciso VI	LGPD, art. 11, II, “d”
Hipótese 7: Para a proteção da vida ou da incolumidade física do titular ou de terceiro	LGPD, art. 7º, inciso VII	LGPD, art. 11, II, “e”

DIREITOS DO TITULAR

HIPÓTESE DE TRATAMENTO	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS	DISPOSITIVO LEGAL PARA O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS
Hipótese 8: Para a tutela da saúde do titular	LGPD, art. 7º, inciso VIII	LGPD, art. 11, II, “f”
Hipótese 9: Para atender interesses legítimos do controlador ou de terceiro	LGPD, art. 7º, inciso IX	Não se aplica
Hipótese 10: Para proteção do crédito	LGPD, art. 7º, inciso X	Não se aplica
Hipótese 11: Para a garantia da prevenção à fraude e à segurança do titular	Não se aplica	LGPD, art. 11, II, “g”

“Fonte: Guia de boas práticas (LGPD), 2020. pág. 23”

III – Marcos de Conformidade com a LGPD

1. Programa de Governança e Privacidade
2. Inventário de Dados Pessoais
3. Termo de Uso
4. Avaliação de Riscos
5. Requisitos e obrigações quanto a segurança da Informação e Privacidade
6. Relatório de Impacto de Proteção de Dados – RIPD
7. Guia de Segurança em Aplicações Web
8. Guia de Framework de Segurança

PROGRAMA DE GOVERNANÇA E PRIVACIDADE

Apresenta os principais pontos da Lei Geral de Proteção de Dados, fornecendo os subsídios para a criação de um programa institucional de gerenciamento de privacidade.

É recomendável que uma Política de Privacidade contenha os seguintes tópicos:

1 – Controlador 2 – Operador 3 – Encarregado 4 - Quais dados são tratados 5 – Como os dados são coletados 6 – Qual o tratamento realizado e para qual finalidade 7 – Compartilhamento de dados 8 – Segurança dos dados 9 – Cookies 10 – Tratamento posterior dos dados para outras finalidades 11 – Transferência internacional de dados

A figura a seguir revela as características mínimas de um Programa de Governança em Privacidade – PGP:

1. Comprometimento do controlador em adotar processos e políticas internas que cumpram normas e boss práticas relativas à proteção de dados pessoas
2. Aplicável a todo conjunto de dados pessoais sob seu controle, indepedentemente da forma coletada
3. Adapatado à estrutura, à escala e ao volume de suas operações, bem como a sensibilidade dos dados tratados
4. Estabelecimento do políticas públicas e salva guardas adequadas, baseadas em processo de avaliação sistemático de impactos e riscos à pricacidade
5. Estabelecimento de relaçnão de confiança com o titular, por meio de atuação transparente com mecanismos de participação do titular
6. Integrado a sua estrutura geral de governança e estabeleça e aplica mecanismos de supervisão interno e externo
7. Com planos de resposta a incidentes e remediação
8. Constantemente atualizado com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas

"Fonte Guia Programa de Governança em Privacidade -PGP (LGPD), 2020, pag. 7"

INVENTÁRIO DE DADOS PESSOAIS - IDP

Inventário de todas as operações de tratamento de dados pessoais e suas avaliações sob a ótica dos princípios da LGPD.

A LGPD assim prescreve em seu art. 37:

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Recomenda-se que, no processo de elaboração do Inventário de Dados Pessoais - IDP, tome-se por parâmetro o modelo referido no Anexo I.

É mister que o Inventário de Dados Pessoais esclareça, conforme o caso, as seguintes informações:

Atores envolvidos (agentes de tratamento e o encarregado);

Finalidade (o que a instituição faz com o dado pessoal);

Hipótese (arts. 7º e 11 da LGPD) e previsão legal;

Dados pessoais tratados pela instituição;

Categoria dos titulares dos dados pessoais;

Tempo de retenção dos dados pessoais;

Instituições com as quais os dados pessoais são compartilhados;

Transferência internacional de dados (art. 33 LGPD); e

Medidas de segurança atualmente adotadas.

Inventário de todas as operações de tratamento de dados pessoais e suas avaliações sob a ótica dos princípios da LGPD.

A LGPD assim prescreve em seu art. 37:

Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse.

Recomenda-se que, no processo de elaboração do Inventário de Dados Pessoais - IDP, tome-se por parâmetro o modelo referido no Anexo I.

A figura a seguir destaca as fases de elaboração do IDP:

"Fonte: Apresentação Guia Inventário de dados Pessoais - IDP, (LGPD) 2020. pág 13"

TERMO DE USO

Termo de Uso ou **Contrato de Termo de Uso** é um documento que estabelece as regras e condições de uso de determinado serviço. Orienta a elaboração de Termos de Uso e Políticas de Privacidade vinculados à utilização de serviços públicos por meio de aplicações (sítios, sistemas ou aplicativos para dispositivos móveis) fornecidas por órgãos e entidades da administração pública.

Caso o Termo de Uso seja aceito pelo usuário, a utilização do serviço será vinculada às cláusulas dispostas nele. O Foco são as regras e condições. Portanto, o termo de uso constitui, um dever do controlador e um direito do titular.

O Termo de Uso deve evidenciar de forma clara quais são as responsabilidades de cada parte envolvida no serviço. Ao definir responsabilidades, a Administração Pública e o cidadão estabelecem direitos e deveres para ambas as partes e compreendem suas obrigações ao utilizar e prover o serviço, de forma a esclarecer quais situações configuram violações aos Termos e para quais situações cabe reparação de danos.

As seguintes informações devem estar presentes no Termo de Uso:

- O que é o serviço?
- Quais são as informações para contato.
- Qual a sua finalidade?
- Qual o foro?
- Em qual leis e normativos o tratamento está respaldado?
- Como serão comunicadas as mudanças no Termo de Uso?
- Quais são as responsabilidades do usuário e da Administração Pública?

O Titular tem direito a obter do Controlador, em relação aos dados por ele tratados, conferidos pela Lei de Proteção de Dados Pessoais:

- - Direito de confirmação e acesso (Art. 18, I e II)
- - Direito de retificação (Art. 18, III)
- - Direito à limitação do tratamento dos dados (Art. 18, IV)
- - Direito de oposição (Art. 18, § 2º)
- - Direito de portabilidade dos dados (Art. 18, V)
- - Direito de não ser submetido a decisões automatizadas (Art. 20, LGPD)
- - Direito do acesso à informação (Lei 12.527 - Lei de Acesso à Informação)
- - Direito do respeito à intimidade (Constituição Federal, Art. 5º, X

"Fonte: Guia Termo de Uso e Política de Privacidade-(LGPD) 2020. pág 7"

AVALIAÇÃO DE RISCOS

Orienta a identificação e mensuração de riscos de segurança e privacidade, mitigando-os com a utilização dos controles mais indicados.

Constitui um instrumento de identificação de controles que elevem a segurança da informação diante dos pilares de confidencialidade, integridade, disponibilidade e autenticidade no sistema a ser desenvolvido

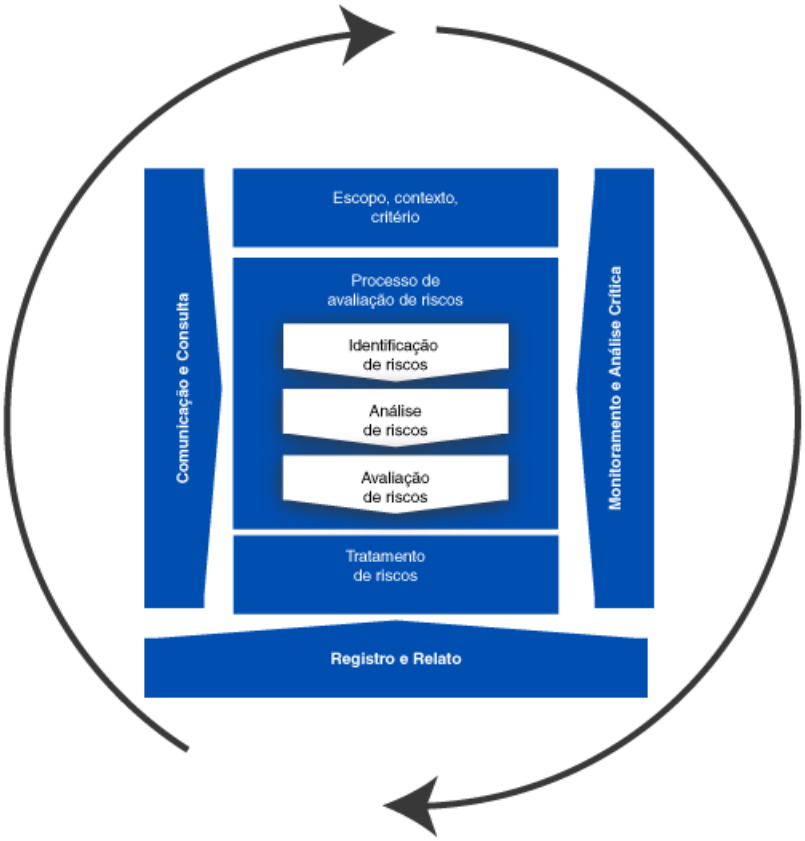
AVALIAÇÃO DE RISCOS

É importante destacar, nesse contexto, que os controles podem ser agrupados em dimensões abordando três distintos contextos: estrutura, sistema e privacidade.

Na dimensão estrutura são avaliados controles que tratam de aspectos estruturais do sistema (processos e infraestrutura que o sustentam), características de ambiente que expandem a análise, mas indispensável para identificar o estado atual da segurança e privacidade na organização responsável pelo tratamento de dados pessoais.

Na dimensão os controles de segurança propostos visam incorporar a segurança da informação durante todo o ciclo de vida do sistema, consequentemente auxiliam a redução da superfície de ataque para vulnerabilidades de sistema, incluindo temas como: desenvolvimento seguro, controles de acesso lógico, segurança web e outros.

Na dimensão privacidade, os controles estão relacionados ao alcance da conformidade legal com a privacidade de tratamento de dados pessoais, de forma a permitir que o controlador verifique se os requisitos de adequação à privacidade estão sendo atendidos.

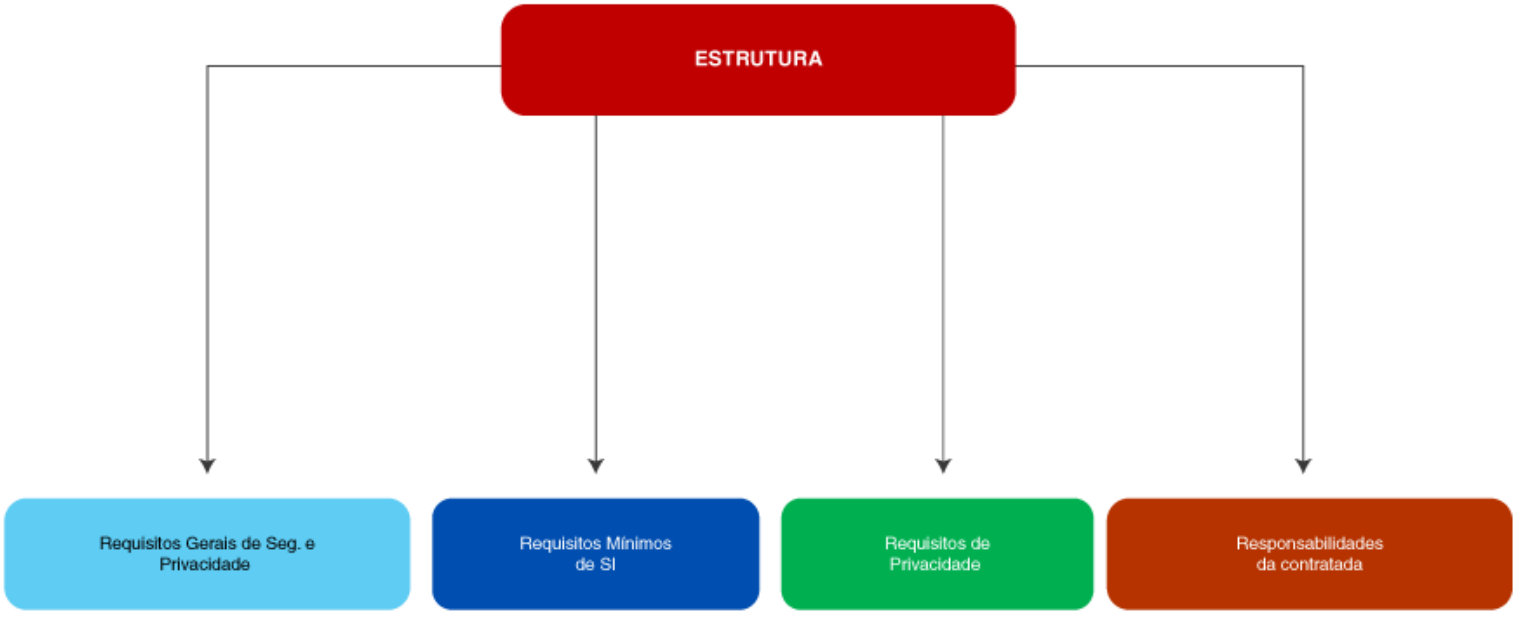


"Fonte: Guia de Avaliação de Riscos de Segurança e Privacidade-(LGPD) 2020. pág 6"

REQUISITOS E OBRIGAÇÕES QUANTO A SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

- Orienta a adequação do processo de contratação para contemplar os requisitos mais importantes de segurança e privacidade dos dados, conforme Instrução Normativa nº 31, de 23 de março de 2021.
- A Lei Geral de Proteção de Dados Pessoais aborda a implantação de mecanismos de gerenciamento de riscos e análise de impacto na privacidade dos dados pessoais, bem como diversos mecanismos de controle de privacidade.

A figura a seguir destaca a Estrutura da Especificação de Requisitos de Segurança da Informação e Privacidade em Contratações de Tecnologia da Informação:



"Fonte: Apresentação Guia de Requisitos e de Obrigações quanto a Segurança da Informação e Privacidade, (LGPD) 2020. pág 12"

REQUISITOS E OBRIGAÇÕES QUANTO A SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

Destacam-se a seguir Requisitos Gerais de Estruturação de Segurança e Privacidade:

- Política de Segurança da Informação (POSIN)
- Análise de Impacto na Privacidade de Dados Pessoais
- Análise e Avaliação de Riscos
- Arquitetura, Controles de Segurança e Matriz de Responsabilidades
- Continuidade Operacional e Contingência
- Gestão de Incidentes
- Coleta e preservação de evidências
- Gestão de Mudanças
- Gestão de Capacidade
- Desenvolvimento Seguro
- Segurança das Redes Corporativas
- Política de Backup

RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS - RIPD

O Relatório de Impacto de Proteção de Dados - RIPD é um documento de comunicação e transparência que orienta a descrição dos processos de tratamento de dados pessoais que podem gerar riscos, bem como medidas, salvaguardas e mecanismos de mitigação.

A LGPD (art. 5º, XVII) assim define relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Há situações específicas diante das quais se pode ou se deve elaborar o RIPD, conforme se extrai dos seguintes dispositivos da LGPD: art. 4º, III, § 3º; art. 10, § 3º; art. 31 c/c art. 32; art. 38.

Nesse contexto, e no que se refere ao conteúdo mínimo que o RIPD deve conter, cumpre destacar o art. 38 da LGPD:

Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

É indicada a elaboração ou atualização do Relatório de Impacto sempre que existir a possibilidade de ocorrer impacto na privacidade dos dados pessoais.

A elaboração do RIPD deve compreender as seguintes etapas:

- identificar os agentes de tratamento e o encarregado
- identificar a necessidade de elaborar o relatório
- descrever o tratamento
- identificar partes interessadas consultadas
- descrever necessidade e proporcionalidade
- identificar e avaliar os riscos
- identificar medidas para tratar os riscos
- aprovar o Relatório
- manter a revisão

No processo de elaboração do RIPD, sugere-se observar o modelo constante do Anexo II.

GUIA DE SEGURANÇA EM APLICAÇÕES WEB

Auxilia os profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação.

Objetiva auxiliar aos profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação, utilizando-se da abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas(Security by Design).

O Guia de Segurança em Aplicações Web estrutura-se basicamente em requisitos gerais e requisitos específicos.

Requisitos Gerais:

1. Gerenciamento de ambiente
2. Proteção do perímetro da aplicação

Requisitos específicos:

1. Validação dos dados de entrada
2. Codificação de dados de saída
3. Autenticação e gerenciamento de credenciais
4. Gerenciamento de sessões
5. Controle de acesso
6. Criptografia
7. Tratamento de erros e logs
8. Proteção de dados
9. Segurança nas comunicações
10. Configuração do sistema
11. Segurança em Banco de Dados
12. Gerenciamento de Arquivos
13. Gerenciamento de memória
14. Práticas Gerais de Codificação

GUIA DE SEGURANÇA EM APLICAÇÕES WEB

Auxilia os profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação.

Objetiva auxiliar aos profissionais de desenvolvimento e manutenção de sistemas a atenderem os requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação, utilizando-se da abordagem de desenvolvimento de software e hardware que visa minimizar as vulnerabilidades dos sistemas e reduzir a superfície de ataque em todas as fases do ciclo de vida de desenvolvimento de sistemas(Security by Design).

O Guia de Segurança em Aplicações Web estrutura-se basicamente em requisitos gerais e requisitos específicos.

Requisitos Gerais:

1. Gerenciamento de ambiente
2. Proteção do perímetro da aplicação

Requisitos específicos:

1. Validação dos dados de entrada
2. Codificação de dados de saída
3. Autenticação e gerenciamento de credenciais
4. Gerenciamento de sessões
5. Controle de acesso
6. Criptografia
7. Tratamento de erros e logs
8. Proteção de dados
9. Segurança nas comunicações
10. Configuração do sistema
11. Segurança em Banco de Dados
12. Gerenciamento de Arquivos
13. Gerenciamento de memória
14. Práticas Gerais de Codificação

No que se refere ao requisito Proteção de Dados, a aplicação deve proteger os dados tratados por ela, de forma que o acesso às suas informações se restrinja ao mínimo necessário (política de privilégio mínimo, restringindo aos usuários apenas às funcionalidades, dados e informações do sistema que são necessárias para executarem suas tarefas).

Deve-se ainda adotar controles de segurança ao armazenar as informações para garantir que os dados necessários sejam criptografados (criptografar informações altamente sensíveis quando armazenadas – como dados de verificação de autenticação – mesmo que estejam no lado servidor, usando sempre algoritmos conhecidos, padronizados e bem testados).

É também oportuno promover mecanismos que garantam a proteção de dados pessoais e de dados pessoais sensível, a exemplo do disposto do que a LGPD (art. 6º, XI) conceitua como anonimização: *utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.*

GUIA DE FRAMEWORK DE SEGURANÇA

Fornece aos profissionais de segurança da informação uma maneira de iniciar a identificação, o acompanhamento e o preenchimento das lacunas de segurança presentes na instituição com um conjunto de ações priorizadas que atuam coletivamente na defesa de sistemas e infraestrutura, por meio das melhores práticas para mitigar os tipos mais comuns de ataques.

O processo de proteção de dados pessoais deve estar alinhado com os procedimentos operacionais, segurança da informação, normas de governança, definindo as finalidades, limitações e controles.

A Figura abaixo representa o Framework de processos LGPD:

Ao tratar de dados pessoais a instituição deve promover a governança de forma a agir conforme os requisitos da LGPD.

Seus processos devem possibilitar que todos os envolvidos contem com um conjunto claramente definido de princípios, políticas e procedimento que estabeleçam a forma como os dados pessoais possam ser tratados e processados, passando por:

1. Estabelecer framework de proteção de dados pessoais;

2. Realizar a gestão do registro de processamento;

3. O estabelecimento de regras para consentimento;

4. A gestão de solicitações e de reclamações de dados pessoais; e

5. Garantia de Gestão imparcial.

A Figura abaixo representa o Framework de processos LGPD:

Neste momento deve-se proceder a coleta, gerenciamento e controle dos novos dados pessoais, identificando os já existentes para classificar de acordo com a LGPD e com o princípio da minimização de dados.

Os dados pessoais devem ser qualificados em níveis de classificação, analisando o nível de proteção em segurança da informação garantindo que os dados pessoais sejam corretamente reconhecidos e tratados

Todos os dados pessoais existentes (funcionários, ex. Funcionários e Terceiros) devem ser devidamente identificados e documentados, englobando ativos de informação existentes e os dados pessoais recém coletados.

Os dados pessoais sensíveis devem ser tratados com mais cautela de forma que seu processamento seja legítimo e justifica

A Figura abaixo representa o Framework de processos LGPD:

O processo de proteção de dados pessoais deve estar alinhado com os procedimentos operacionais de segurança da informação e normas de governança, definindo as finalidades, limitações e controles.

Os dados pessoais devem ser gerenciados usando um ciclo de vida relacionado com a classificação do dado, desde a coleta inicial até o arquivamento e eliminação.

Nesse sentido, seus subprocessos devem ser:

1. Realizar Avaliação de Riscos;

2. Conduzir Avaliação de Impacto da Proteção de Dados;

3. Gerenciar o Tratamento de Risco; e

4. Realizar a Validação de Risco.

Gerenciar Segurança de Dados Pessoais

Os dados pessoais devem ser qualificados em níveis de classificação, analisando o nível de proteção em segurança da informação, buscando garantir que os dados pessoais sejam corretamente reconhecidos e tratados de acordo com a LGPD.

Com isso deve-se buscar gerencia:

1. O anonimato;

2. A criptografia;

3. Os níveis de proteção;

4. Recuperação dos dados;

5. Os acessos; e

6. Testes e a maturidade da segurança.

Gerenciar Incidentes e Reclamações

Quaisquer incidentes ou violações relacionados a dados pessoais devem ser informados, de acordo com a LGPD, para a Autoridade Nacional de Proteção de Dados e aos titulares dos dados, sejam eles reais ou potencialmente afetados por sua violação.

Assim, deve-se gerenciar:

As Notificações;

A comunicação de dados pessoais;

Crises; e

As reinvindicações, reclamações e evidências.

Manter a Conscientização

A proteção de dados e a privacidade devem ser tratados como valores fundamentais da instituição e para tanto exigem conhecimento e informações contínuas sobre Proteção de Dados Pessoais. Seu processo da suporte a todos os outros processos, explicando, comunicando e reforçando os requisitos da LGPD.

O processo de conscientização inclui educação, treinamento, engajamento e elementos de qualificação para garantir que a instituição tenha os conjuntos de habilidades necessários, devendo para atingir seus objetivos:

1. Manter a conscientização em toda a instituição;
2. Gerenciar educação e habilidades; e
3. Gerenciar treinamentos

Manter Controles Internos

A LGPD exige um conjunto abrangente de controles que garanta a conformidade no tratamento de dados pessoais. fazendo com que seu processamento esteja alinhado com o sistema geral de controles internos da instituição.

Para atingir esse objetivo é necessário:

1. Manter controles de coleta de dados;
2. Manter Controles de Processamento;
3. Manter controles de armazenamento de dados;
4. Manter controles de exclusão;
5. Manter controles de monitoramento; e
6. Realizar revisão da qualidade

A LGPD determina a designação de um oficial de proteção de dados. Assim, é necessária a organização de um processo para garantir que este oficial realize tarefas regulares e interaja com outras partes da instituição. Ao fazer isso, deve garantir ainda a conformidade com leis e regulamentos, estruturado e bem organizado. Este processo deve englobar os seguintes sub-processos:

1. Manter a Função do DPO;
2. Gerenciar Orçamento e Recursos;
3. Gerenciar Interfaces Organizacionais;
4. Gerenciar Relatórios; e
5. Gerenciar Serviços Externos

IV - REFERENCIAL TEÓRICO E CRONOGRAMA DE EXECUÇÃO DOS MARCOS DE CONFORMIDADE COM A LGPD

Marco de Conformidade	Referencial Teórico
Programa de Governança em Privacidade	Vide Guia de elaboração de Programa de Governça em Privacidade (disponível em:https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)
Inventário de Dados Pessoais	Vide Guia de Elaboração de Inventário de Dados Pessoais (disponível em: https:// www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)
Termo de Uso	Vide Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos (disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)
Avaliação de Riscos	Vide Guia de Elaboração de Avaliação de Riscos (disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)

IV - REFERENCIAL TEÓRICO E CRONOGRAMA DE EXECUÇÃO DOS MARCOS DE CONFORMIDADE COM A LGPD

Marco de Conformidade	Referencial Teórico
Requisitos e Obrigações quanto a Segurança da Informação e Privacidade DTI	Vide Guia de elaboração de Requisitos e Obrigações quanto a Segurança da Informação e Privacidade (disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)
Relatório de Impacto de proteção de dados - RIPD	Vide Guia de Elaboração de Impacto de Proteção de Dados – RIPD (disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)
Guia de Segurança em Aplicações Web DTI	Vide Guia de Segurança em Aplicações Web (disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)
Guia de Framework de Segurança DTI	Vide Guia do Framework de Segurança (disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guias-operacionais-para-adequacao-a-lgpd)

CRONOGRAMA DE EXECUÇÃO

Plano de Ação para adequação da AGU à LGPD

Seq	Entregável	Detalhamento do entregável	Ações	Responsável	Julho (sem.)		Agosto (semanas)					Setembro (semanas)					Outubro (sem.)		
					4ª	5ª	1ª	2ª	3ª	4ª	5ª	1ª	2ª	3ª	4ª	5ª	1ª	2ª	3ª
1	Atendimento de relamações e comunicações dos titulares dos dados pessoais	Objetiva atender o direito do titular dos dados pessoais a obter da AGU: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção dos dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei; V - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei 13.709/2018; e VI - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.	Receber as reclamações e comunicações dos titulares dos dados pessoais e encaminhar para o órgão de direção superior da AGU responsável	Encarregado	Ação permanente														
			Encaminhar ao Encarregado os esclarecimentos e as providências relacionadas às reclamações e comunicações do titular dos dados pessoais	Responsáveis nos órgãos de direção superior															
			Responder ao titular dos dados pessoais com os esclarecimentos e providências adotadas	Encarregado															
2	Inventário de Dados Pessoais da AGU elaborado em planilha eletrônica	O Inventário de Dados Pessoais é o registro das operações de tratamento dos dados pessoais realizados pela AGU. O "Guia de Elaboração de Inventário de Dados Pessoais" do Ministério da Economia recomenda a organização do inventário em processos de trabalho por facilitar a sua elaboração. Por isso a necessidade da participação dos Gestores dos Processos de Trabalho.	a) Sugestão de concluir o curso "Proteção de Dados Pessoais no Setor Público" na Escola Virtual.Gov da Enap	Coordenação pelo Encarregado com auxílio e suporte técnico do DGE; representantes indicados pelos órgãos de direção superior															
			b) Sugestão de leitura do "Guia de Elaboração de Inventário de Dados Pessoais" e assistir o vídeo da Oficina*																
			c) Preencher o template de planilha eletrônica para os dados pessoais relativos ao processo de trabalho																
3	Termos de Uso e Políticas de Privacidade dos serviços prestados pela AGU publicados no Portal de Serviços ao Cidadão	A AGU possui 7 (sete) serviços no Portal de Serviços ao Cidadão**. É possível que existam mais serviços, o que vai exigir a revisão da lista. Cada serviço deve possui um Termo de Uso (documento que estabelece as regras e condições de uso do serviço) e uma Política de Privacidade (documento informativo pelo qual a AGU transparece ao usuário a forma como o serviço realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário).	a) Sugestão de leitura do "Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos" e assistir o vídeo da Oficina*	Coordenação pelo Encarregado com auxílio e suporte técnico do DGE; representantes indicados pelos órgãos de direção superior															
			b) Sugestão de revisão da lista de serviços do Portal de Serviços ao Cidadão.																
			c) Elaborar os Termos de Uso e Políticas de Privacidade dos serviços prestados pela AGU																
			d) Publicar os Termos de Uso e Políticas de Privacidade dos serviços prestados pela AGU no Portal de Serviços ao Cidadão																
4	Relatórios de Impacto à Proteção de Dados Pessoais – RIPD elaborados	O RIPD visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. Por meio da avaliação de riscos podemos dentificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição.	a) Sugestão de leitura do "Template do Relatório de Impacto à Proteção de Dados Pessoais" e assistir o vídeo da Oficina*	Coordenação pelo Encarregado com auxílio e suporte técnico do DGE; representantes indicados pelos órgãos de direção superior; monitoramento pela CISET/AGU															
			b) Sugestão de leitura do "Guia de Avaliação de Riscos de Segurança e Privacidade" e assistir o vídeo da Oficina*																
			c) Elaborar o RIPD																
			d) Aprovar o RIPD	Elaborador do Relatório, Encarregado, Autoridade representante do Controlador e Autoridade representante do Operador; monitoramento pela CISET/AGU															
			e) Publicar o RIPD	Encarregado															

5	Processos de trabalho de desenvolvimento e sustentação de software remodelados	Objetiva fortalecer o desenvolvimento e a sustentação de software por meio de requisitos de segurança da informação, antes e durante o desenvolvimento da aplicação (Security by Design).	a) Ler o "Guia de Segurança em Aplicações Web"*	DTI															
			b) A definir como será feita a formalização da remodelagem	DTI															
6	Framework de Segurança implementado	Objetiva identificar, acompanhar e o possibiltar o preenchimento das lacunas de segurança da informação presentes na instituição em relação aos 20 Controles de Segurança elaborados pelo Center for	a) Ler o "Guia do Framework de Segurança"*	DTI															
			b) A definir como será feita a formalização da remodelagem	DTI															
7	Portaria do AGU que institui o Programa de Governança em Privacidade da AGU (PGP-AGU) publicada	O PGP-AGU busca capturar e consolidar os requisitos de privacidade dentro da AGU de modo a viabilizar o efetivo gerenciamento da privacidade, incluindo estratégias, habilidades, pessoas, processos e ferramentas para conquistar a confiança dos servidores e dos cidadãos e, ao mesmo tempo, cumprir com exigências apresentadas nos normativos de privacidade.	a) Estabelecer os conceitos do ato normativo.	Coordenação pelo Encarregado com auxílio e suporte técnico do DGE; representantes indicados pelos órgãos de direção superior															
			b) Estabelecer as competências do Encarregado e dos demais colegiados.																
			c) Declarar a entrega, estabelecer forma, responsáveis e periodicidade de atualização do Inventário de Dados Pessoais da AGU.																
			d) Declarar a entrega, estabelecer forma, responsáveis e periodicidade na atualização dos Termos de Uso, Política de Privacidade, Política de Segurança da Informação e Relatórios de Impacto à Proteção de Dados Pessoais.																
			e) Declarar a entrega, estabelecer forma, responsáveis e periodicidade do: - Processo de trabalho de contratação em TIC remodelado e contratos readequados - Processos de trabalho de desenvolvimento e sustentação de software remodelados - Framework de Segurança implementado																
			f) Estabelecer forma e responsáveis pelo Processo de Trabalho de Gestão de Incidentes.																
			g) Estabelecer forma e responsáveis pelo Processo de Trabalho de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.																
			h) Estabelecer indicadores de desempenho e forma de seu monitoramento.																
			i) Analisar de forma prévia a minuta de Portaria antes de submeter ao AGU.	Comissão Técnica e Comitê de Governança da AGU															

V - Referências Bibliográficas

- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Constituição da República Federativa do Brasil. Brasília, DF, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm . Acesso em: 13 abr. 2021.

- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 13 abr. 2021.

- Controladoria Geral da União-CGU, Governo Aberto, 2014, disponível em: https://www.gov.br/cgu/pt-br/governo-aberto/a-ogp/o-que-e-a-iniciativa . Acesso em 15 abr. 2021.

- GUIA DE BOAS PRÁTICAS LEI GERAL DE PROTEÇÃO DE DADOS (LGPD). Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaLGPD.pdf. Último acesso em: 13 abr. 2021.

- GUIA DE ELABORAÇÃO DE PROGRAMA DE GOVERNANÇA EM PRIVACIDADE. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaProgramaGovernanaemPrivacidade.pdf. Último acesso em: 13 abr. 2021.

- GUIA DE ELABORAÇÃO DE INVENTÁRIO DE DADOS PESSOAIS. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaInventario.pdf. Último acesso em: 13 abr. 2021.

- GUIA DE ELABORAÇÃO DE TERMO DE USO E POLÍTICA DE PRIVACIDADE PARA SERVIÇOS PÚBLICOS. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaTermoUso.pdf Último acesso em: 13 abr. 2021.

- GUIA DE REQUISITOS E DE OBRIGAÇÕES QUANTO A SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE.Disponível em:https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf. Último acesso em: 15 abr. 2021.

- GUIA DE AVALIAÇÃO DE RISCOS DE SEGURANÇA E PRIVACIDADE. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-avaliacao-de-riscos-de-seguranca-e-privacidade.pdf. Último acesso em: 15 abr. 2021.

REFERÊNCIAS BIBLIOGRÁFICAS

- GUIA RELATÓRIO DE IMPACTO DE PROTEÇÃO DE DADOS - RIPD. Disponível em Template Versão 1.0 – Atualizado em 07/12/2020. Último acesso em: 15 abr. 2021.
- GUIA DE REQUISITOS E DE OBRIGAÇÕES QUANTO A SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE.Disponível em:https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaRequisitosdeSIparaContratacoesdeTI.pdf. Último acesso em: 15 abr. 2021.
- GUIA DE SEGURANÇA EM APLICAÇÕES WEB. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/GuiaSeguranaAplicaesWeb.pdf. Último acesso em: 15 abr. 2021.
- GUIA DE FRAMEWORK DE SEGURANÇA. Disponível em Microsoft Word - Guia do Framework de segurançav0_base_3.4_Tabulação (www.gov.br). Último acesso em: 15 abr. 2021.

Anexos

Anexo I - Inventário de Dados Pessoais - IDP (modelo)

2 - Agentes de Tratamento e Encarregado	Nome	Endereço	CEP	Telefone	E-mail
2.1 - Controlador					
2.1 - Controlador					
2.1 - Controlador					
2.1 - Controlador					

3 - Fases do Ciclo de Vida do Tratamento Dados Pessoais	Coleta	Retenção	Processa-mento	Comparti-lhamento	Eliminação
3.1 - Em qual fase do ciclo de vida o Operador atua					

4- De que forma (como) os dados pessoais são coletados, retidos/armazenados, processados/ usados, compartilhados e eliminados	
4.1 - Descrição do Fluxo do tratamento dos dados pessoais	

5 - Escopo e Natureza dos Dados Pessoais	
5.1 - Abrangência da área geográfica do tratamento	
5.2 - Fonte de dados utilizada para obtenção dos dados pessoais	

6 - Finalidade do Tratamento de Dados Pessoais	
6.1 - Hipótese de Tratamento	
6.2 - Finalidade	
6.3 - Previsão legal	
6.4 - Resultados pretendidos para o titular de dados	
6.5 - Benefícios esperados para o órgão, entidade ou para a sociedade como um todo	

7 - Categoria de Dados Pessoais				
7.1 -Dados de Identificação Pessoal	Descrição	Tempo Retenção dos dados	Fonte Retenção	Nome Base de Dados
7.1.1 - Informações de identificação pessoal				
7.1.2 - Informações de identificação atribuídas por instituições governamentais				
7.1.3 - Dados de identificação eletrônica				
7.1.4 - Dados de localização eletrônica				

8 - Categorias de Dados Pessoais Sensíveis	Descrição	Tempo Retenção dos dados	Fonte Retenção	Nome Base de Dados
8.1 - Dados que revelam origem racial ou ética				
8.2 - Dados que revelam convicção religiosa				
8.3 - Dados que revelam opinião política				
8.4 - Dados que revelam filiação a sindicato				
8.5 - Dados que revelam filiação a organização de caráter religioso				
8.6 - Dados que revelam filiação ou crença filosófica				
8.7 - Dados que revelam filiação ou preferências política				
8.8 - Dados referentes à saúde ou à vida sexual				
8.9 - Dados genéticos				
8.10 - Dados biométricos				

9 - Frequência e totalização das categorias de dados pessoais	
9.1 - Frequência de tratamento dos dados pessoais	
9.2 - Quantidade de dados pessoais e dados pessoais sensíveis tratados	

10 - Categorias dos titulares de dados pessoais	Tipo de Categoria	Descrição
10.1 - Categoria 1		
10.2 - Categoria 2		
10.3 - Trata dados de crianças e adolescentes		
10.4 - Além de crianças e adolescente trata dados de outro grupo vulnerável		

12 - Medidas de Segurança/ Privacidade	Tipo de medida de segurança e privacidadeDescrição do(s)	Controle(s)
12.1 - Medida de Segurança/ Privacidade 1		
12.2 - Medida de Segurança/ Privacidade 2		
12.3 - Medida de Segurança/ Privacidade 3		

13 - Transferência Internacional de Dados Pessoais	País	Dados pessoais transferidos	Tipo de garantia para transferência
13.1 - Organização 1			
13.2 - Organização 2			
13.3 - Organização 3			

14 - Contrato(s) de serviços e/ou soluções de TI que trata(m) dados pessoais do serviço/ processo de negócio	Nº Processo Contratação	Objeto	E-mail do Gestor do Contrato
14.1 - Contrato nº 1			
14.2 - Contrato nº 2			

Anexo II - Relatório de Impacto de Dados Pessoais - RIPD

OBJETIVO: O Relatório de Impacto de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de riscos. Referência: Art. 5º, XVII, da Lei 13.709/2018 (LGPD)

Anexo II - Relatório de Impacto de Dados Pessoais - RIPD

Controlador

Operador

Encarregado

Email Encarregado	Email Encarregado Telefone Encarregado

2. NECESSIDADE DE ELABORAR O RELATÓRIO

3. DESCRIÇÃO DO TRATAMENTO

3.1 Natureza do tratamento

3.2 Escopo do tratamento

3.3 Contexto do tratamento

3.4 Finalidade do tratamento

4. PARTES INTERESSADAS CONSULTADAS

5. NECESSIDADE E PROPORCIONALIDADE

6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

ID	RISCO REFERENTE AO TRATAMENTO DE DADOS PESSOAIS	P1	P2	NÍVEL DE RISCO (P X I)3

Legenda: P – Probabilidade; I – Impacto.

Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente; ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

mpacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

7. MEDIDAS PARA TRATAR OS RISCOS

RISCO	MEDIDA(S)	EFEITO SOBRE RISCO 1	RISCO RESIDUAL 2 P I (P X I)	MEDIDA(S) 3 APROVADA(S)

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6 do RIPD.

1. Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

2. Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratá-lo.

3. Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

Anexo III - LGPD x IN SGE/ME x ABNT NBR ISO/IEC 27.701/2019

Lei 13.709/2018 (LGPD) /IN SGD/ME 11/2020	ABNT NBR ISO/IEC 27.701/2019
art. 50 § 2º inciso I	item 5.4.
art. 50 § 2º inciso V	itens 6.5.2 e 7.2.8.
art. 50 § 2º inciso VI e VII	item 5.2.2.
art. 50 § 2º inciso VI; art 7º, § 5º	itens 5.2.2.
art. 37	item 7.2.8.
art. 5º, inciso I; art. 37	itens 6.5.2 e 7.2.8.
art. 5º, inciso I; art. 37	itens 6.5.1 e 7.2.8.
art. 50 § 1º e § 2º inciso I, alínea “d”	item 5.4.1.2.
art. 46; art 50, § 2º inciso I, alíneas “a” e “d”	itens 5.3.2 e 6.2
art. 46; art 50, § 2º inciso I, alíneas “a” e “d”	item 6.5.2.
art. 46; art 50, § 2º inciso I, alíneas “a” e “d”	item 6.2.1.
art. 5º, inciso VIII; art. 41. IN SGD/ME 11/2020	item 6.3.1.
art. 5º, inciso VIII; art. 41. IN SGD/ME 11/2020.art 2º	item 6.3.1.
art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 1º, § 1º, inciso II	item 6.3.1.

art. 5º, inciso I; art. 37	itens 6.5.2 e 7.2.8.
art. 5º, inciso I; art. 37	itens 6.5.1 e 7.2.8.
art. 50 § 1º e § 2º inciso I, alínea “d”	item 5.4.1.2.
art. 46; art 50, § 2º inciso I, alíneas “a” e “d”	itens 5.3.2 e 6.2
art. 46; art 50, § 2º inciso I, alíneas “a” e “d”	item 6.5.2.
art. 46; art 50, § 2º inciso I, alíneas “a” e “d”	item 6.2.1.
art. 5º, inciso VIII; art. 41. IN SGD/ME 11/2020	item 6.3.1.
art. 5º, inciso VIII; art. 41. IN SGD/ME 11/2020	item 6.3.1.
art. 5º, inciso VIII; art. 41. IN SGD/ME 11/2020.art 2º	item 6.3.1.
art. 5º, inciso VIII; art. 41. IN SGD/ME 117/2020, art 1º, § 1º, inciso II	item 6.3.1.
art. 5º, inciso VIII; art. 41,§ 1º. IN SGD/ME 117/2020, art 2º	item 6.3.1.
art. 6º, inciso I	item 7.2.1.
art. 7º	item 7.2.2.
art. 37	item 7.2.8.
art. 5º, inciso XVII; art. 38	tem 7.2.5.
art. art. 6º, inciso VI; art. 41. art 9º; art 23, inciso I; art. 50, inciso I, alíneas “a”, “d” e “e” 37	itens 7.3.2 e 7.3.3.

art. 17 - 22	item 7.3.
art. 50, § 2º, inciso I, alínea “g”	item 6.13.1.1.
art. 50, § 2º, inciso I, alínea “g”	item 6.13.1.5.
art. 50, § 2º, inciso I, alínea “g”	itens 6.13.1.4. e 6.13.1.5.
art. 48	tem 6.13.1.5.
art. 48	item 6.1.
art. 46	itens 6.6.2.1 e 6.6.2.2.
art. 46	item 6.9.4.1.
art. 46; art. 50, § 2º, inciso I, alínea “c”	item 6.7.
art. 46, § 2º	item 7.4.

FIM

PA-LGPD-AGU