GUIA LGPD

BOAS PRÁTICAS DA LEI GERAL DE PROTEÇÃO DE DADOS

PGE
RONDÔNIA

ELABORAÇÃO / CONTEÚDO

Thiago Denger Queiroz
Procurador-Geral do Estado

Fábio Henrique Pedrosa Teixeira
Secretário-Geral da Procuradoria Geral do Estado

Rod Daniel Gomes
Encarregado pelo Tratamento de Dados Pessoais

Diagramação:
Coordenação de Relações Públicas
da Procuradoria-Geral do Estado

Histórico de versões - Versão 2 – fevereiro/2024.

SUMÁRIO

SUMÁRIO

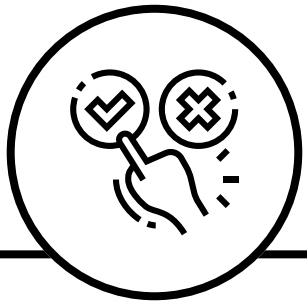
1

DIREITOS FUNDAMENTAIS DO TITULAR DOS DADOS

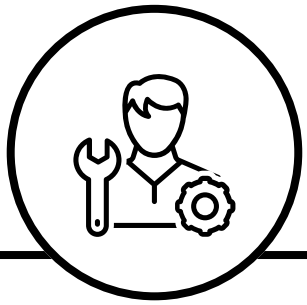
A LGPD (Lei nº 13.709, de 14 de agosto de 2018) é uma lei que visa resguardar os direitos básicos de liberdade e de privacidade e o livre desenvolvimento da personalidade de cada pessoa. Essa lei trata do uso de dados pessoais, que podem estar em formato físico ou digital, feito por pessoa física ou jurídica de direito público ou privado e abrange uma série de operações realizadas em meios manuais ou digitais.

Segundo a LGPD, o uso dos dados pessoais pode ser feito por dois tipos de “agentes de uso”, o Controlador e o Operador: O Controlador é a pessoa natural ou jurídica, de direito público ou privado, que tem a responsabilidade de tomar as decisões sobre o uso dos dados pessoais, como os objetivos e os meios do uso (art. 5º, VI).

Dentro da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública que está sujeita à lei, representada pela autoridade que tem o poder de decidir sobre o uso desses dados. O Operador é a pessoa natural ou jurídica, de direito público ou privado, que faz o uso dos dados pessoais em nome do controlador (art. 5º, VII), incluindo aí agentes públicos em sentido amplo que desempenhem essa função, bem como pessoas jurídicas diferentes daquela representada pelo Controlador, que façam atividade de uso no contexto de contrato ou instrumento similar. Além dos “agentes de uso”, outra figura importante para o cumprimento adequado da LGPD é o “Encarregado”, definido pelo art. 5º, VIII, como a pessoa escolhida pelo controlador e operador para atuar como meio de comunicação entre o controlador, os donos dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).



O **Controlador** toma as decisões sobre o uso dos dados pessoais.

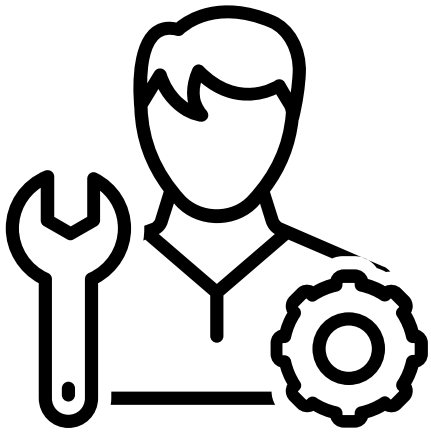


O **Operador** faz o uso dos dados pessoais em nome do controlador.

Segundo a LGPD, o uso dos dados pessoais pode ser feito por dois tipos de “agentes de uso”, o Controlador e o Operador: O Controlador é a pessoa natural ou jurídica, de direito público ou privado, que tem a responsabilidade de tomar as decisões sobre o uso dos dados pessoais, como os objetivos e os meios do uso (art. 5º, VI).

O **Controlador** toma as decisões sobre o uso dos dados pessoais.

Dentro da Administração Pública, o Controlador será a pessoa jurídica do órgão ou entidade pública que está sujeita à lei, representada pela autoridade que tem o poder de decidir sobre o uso desses dados. O Operador é a pessoa natural ou jurídica, de direito público ou privado, que faz o uso dos dados pessoais em nome do controlador (art. 5º, VII), incluindo aí agentes públicos em sentido amplo que desempenhem essa função, bem como pessoas jurídicas diferentes daquela representada pelo Controlador, que façam atividade de uso no contexto de contrato ou instrumento similar. Além dos "agentes de uso", outra figura importante para o cumprimento adequado da LGPD é o "Encarregado", definido pelo art. 5º, VIII, como a pessoa escolhida pelo controlador e operador para atuar como meio de comunicação entre o controlador, os donos dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).



O **Operador** faz o uso dos dados pessoais em nome do controlador.

Outro conceito essencial é o de “uso de dados”, que engloba qualquer ação que envolva um dado pessoal na realização da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Depois de ver os conceitos básicos de Controlador, Operador, Encarregado e “uso de dados”, é importante prestar atenção às especificidades de cada caso concreto, para evitar confusões que coloquem em risco a definição correta de responsabilidades entre os agentes que participam do uso de dados. Assim, é preciso destacar que a identificação dos Controladores depende sempre, em cada situação, da existência da capacidade de decidir sobre os meios e o objetivo do uso de dados.

Dessa forma, serão considerados Controladores, por exemplo, os órgãos públicos que contratarem empresa privada para administrar seu cadastro de visitantes, pois essa empresa atuará sob as ordens do órgão contratante. Nesse exemplo, o órgão contratante (Controlador) não só definirá o objetivo do uso, mas também exigirá da empresa contratada (Operador) a adoção dos meios técnicos necessários para assegurar o cumprimento dos princípios que orientam o uso dos dados pessoais, especificados no art. 6º da LGPD.

Para diferenciar entre Controlador e Operador, portanto, é essencial reconhecer qual entidade possui poder decisório sobre os fins e meios de uso (Controlador), e qual possui âmbito principalmente executivo (Operador), subordinado à vontade de outro.

Sobre o assunto do tratamento de dados, é importante esclarecer que a LGPD (Art. 4°) estabelece que as disposições da Lei não se aplicam ao tratamento de dados pessoais que ocorrem nas seguintes situações:

- feito por pessoa natural para fins somente particulares e sem fins econômicos;
- feito para fins somente jornalísticos, artístico e acadêmico (aplicando-se a esta última hipótese os arts. 7º e 11 da LGPD);
- feito para fins somente de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, ou;
- originados de fora do território nacional e que não sejam alvo de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de origem, desde que o país de origem ofereça grau de proteção de dados pessoais adequado ao previsto na LGPD.

Os casos de tratamento de dados que estão previstos e permitidos pela LGPD serão explicados a seguir. Mas é muito importante destacar que eles não são ilimitados e absolutos; ao contrário, existem limites para essa operação que estão dados pela boa-fé e demais princípios previstos no Art. 6º da mesma norma.

Antes de iniciar qualquer tipo de tratamento de dados pessoais, o agente deve se certificar previamente que a finalidade da operação esteja registrada de forma clara e explícita e os propósitos especificados e informados ao titular dos dados.

No caso do setor público, a principal finalidade do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Tais políticas públicas, vale destacar, devem estar inseridas nas atribuições legais do órgão ou da entidade da administração pública que efetuar o referido tratamento. Outra finalidade comum para o tratamento de dados no serviço público é o cumprimento de obrigação legal ou regulatória pelo controlador. Nessas duas situações, o consentimento do titular de dados é dispensado.

Além disso, no tratamento feito pelo poder público, as regras previstas nos artigos 23 (procedimentos de atuação) e 30 (regulamentos da ANPD) da LGPD sempre devem ser seguidas de forma complementar.

A LGPD previu expressamente em seu artigo 7°, dez hipóteses que autorizam o tratamento de dados, bem como estabeleceu os requisitos para execução de tal procedimento. São as chamadas bases legais de tratamento de dados pessoais.

Nos casos de tratamento de dados em que a base legal não é o consentimento, é possível o compartilhamento de dados com órgãos públicos ou transferência de dados a terceiro fora do setor público.

Quando isso acontecer, os agentes de tratamento devem comunicar as operações executadas, de forma clara, aos titulares dos dados, garantindo-lhes o exercício aos direitos previstos no art. 18 da LGPD, com destaque aos direitos de acesso, retificação, oposição, eliminação e informação das entidades públicas e privadas com as quais o controlador irá realizar o uso compartilhado de dados.

É importante registrar que tal comunicação deve ser renovada na alteração da finalidade ou em qualquer alteração nas operações de tratamento, inclusive de novo compartilhamento ou transferência.

Além disso, é necessário que a cada tratamento de dados seja feita uma análise de se os princípios da necessidade e adequação também estão sendo cumpridos pelo controlador. Já nos casos de tratamento de dados feitos com base no consentimento, cada nova operação realizada com os dados pessoais deve ser objeto de nova requisição de consentimento, inclusive para o compartilhamento dos dados com outras entidades, de dentro ou fora da administração pública.

1.1
DIREITOS DO TITULAR

A LGPD criou um marco legal que dá poder aos titulares de dados pessoais, concedendo-lhes direitos a serem exercidos junto aos controladores de dados. Esses direitos devem ser assegurados durante todo o tempo em que o órgão ou entidade realizar o tratamento dos dados pessoais do titular.

Os direitos que os titulares de dados devem ter estão divididos nas tabelas abaixo, as quais estão separadas em direitos baseados nos princípios definidos pelo art. 6º da LGPD e em direitos específicos dos titulares presentes nos outros artigos da mesma Lei.

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
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
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 exercíciode 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 Lei	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

1.2
COMO OS TITULARES PODEM EXERCER SEUS DIREITOS PERANTE O PODER PÚBLICO

A Lei estabelece uma série de instrumentos para que os titulares possam exercer seus direitos sobre seus dados pessoais, quando estes forem tratados pelo poder público. Esses instrumentos consistem em mecanismos que reforçam as obrigações de transparência ativa e passiva por parte da Administração Pública, assim como possibilitam meios processuais para questionar ou reclamar sobre o tratamento dos dados.

Neste documento, essas obrigações são descritas como:

- (I) obrigações de transparência ativa
- (II) meios de acesso à informação em transparência passiva; e
- (III) meios de petição e manifestação à administração pública.

Em qualquer situação, o titular do dado tem o direito de escolher receber a resposta por meio eletrônico, confiável e adequado para esse propósito ou em formato impresso.

1.3.1 Meios de acesso à informação em transparência passiva

Uma parcela importante dos direitos dos titulares sobre seus dados pessoais, quando estes forem tratados pelo poder público, depende do exercício do direito de acesso à informação. É sempre relevante lembrar que a Lei 12.527/2011, a LAI, já estabelecia, em seu art. 31, procedimentos e diretrizes básicas para o tratamento de dados pessoais no âmbito público.

Entre eles, estão o tratamento transparente, a garantia expressa aos direitos de personalidade e o consentimento do titular para a disponibilização de suas informações àqueles que não tivessem a necessidade de conhecê-la no exercício de sua função pública.

A LGPD, reconhecendo esse legado, informa que, no âmbito público, os prazos e procedimentos para o exercício dos direitos do titular perante o Poder Público seguirão o disposto em legislação específica, mencionando (mas não se limitando) a Lei de Acesso à Informação, a Lei do Processo Administrativo e a Lei do Habeas data (essa última no âmbito judicial).

Assim, estão sujeitos aos prazos e procedimentos já definidos pela Lei nº 12.527/2011 - inclusive com o recebimento dos requerimentos junto ao Serviço de Informação ao Cidadão - o exercício dos seguintes direitos expressamente previstos na Lei Geral de Proteção de Dados Pessoais: acesso à informação sobre a confirmação da existência de tratamento (art. 18, I); acesso aos dados pessoais de que é titular e que são objeto de tratamento pela Administração Pública Federal (art. 18, II);acesso à informação sobre entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados (art. 18, VII); nos casos em que o tratamento tiver origem no consentimento do titular ou em contrato, o acesso à cópia eletrônica integral de seus dados pessoais.

Devem ser observados os segredos comercial e industrial, nos termos de regulamentação da autoridade nacional, em formato que permita a sua utilização subsequente inclusive em outras operações de tratamento (art. 19, §3º); e acesso às informações sobre os critérios e os procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial (art. 20, §1º).

1.3.2 Meios de petição e manifestação à administração pública

Como já mencionado, no âmbito administrativo, a LGPD cita expressamente as Leis 12.527/2011 (LAI) e 9.784/1999 (processo administrativo) como referência não exclusiva para o exercício dos direitos dos titulares. É de se repisar que, ao mesmo tempo, ela aparta os procedimentos que ela prevê daqueles a serem utilizados em face do poder público, ao mencionar que o exercício de tais direitos seria realizado por meio de legislação específica.

Como a Lei não estabelece a observância exclusiva daquele conjunto da Lei de Acesso à Informação e da Lei Geral do Processo Administrativo, e considerando a existência de procedimentos mais benéficos ao titular para o exercício de seus direitos no que se refere a esse último conjunto apresentado, o mecanismo mais célere estabelecido pelo Código de Defesa dos Usuários de Serviços Públicos (Lei nº 13.460/2017) poderia ser adotado como padrão para o recebimento de solicitações de providências e reclamações relativas ao tratamento de dados.

Além da vantagem em termos de prazo e procedimentos padronizados, com unidades de recebimento de petições e reclamações padronizadas e coordenadas, a Lei 13.460/2017, diferentemente da Lei Geral do Processo Administrativo, tem abrangência nacional, permitindo melhor coordenação entre instituições públicas na defesa dos direitos dos titulares de dados.

O titular do dado tem o direito, mediante requerimento expresso seu ou de representante legalmente constituído, sem custos, nos prazos e nos termos previstos em regulamento, de requisitar manifestação conclusiva do controlador ou agente responsável pelo tratamento sobre os seguintes itens:

- correção de dados incompletos, inexatos ou desatualizados (art. 18, III);
- anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD (art. 18, IV);
- eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da LGPD (art. 18, VI); e
- revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20).

A resposta deve ser providenciada de imediato e em formato simplificado ou por declaração clara e completa, fornecida no prazo previsto em Lei e que indique: origem dos dados, a inexistência de registro, critérios utilizados, finalidade do tratamento (observados os segredos comercial e industrial).

O titular do dado tem a faculdade de optar por resposta por meio eletrônico, seguro e idôneo para esse fim ou sob forma impressa.

A petição deve ser respondida com agilidade, clareza e completude, sob pena de o titular dos dados ter a prerrogativa de representar contra o responsável na ANPD, organismos de defesa do consumidor ou ajuizar pretensão com tal causa de pedir.

Na impossibilidade de atendimento imediato do requerimento do titular do dado pessoal, o controlador poderá comunicar que não é agente de tratamento dos dados e indicar, sempre que possível, o agente ou indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

Por último, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Nas hipóteses acima, o controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial. Quando tais segredos impossibilitarem o oferecimento de informações, a ANPD poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento.

Os dados pessoais referentes ao exercício regular de direitos pelo titular, previstos no Art. 18 da LGPD (Capítulo III), não podem ser utilizados em seu prejuízo. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo, individual ou coletivamente, na forma do disposto na legislação pertinente, acerca dos instrumentos de tutela individual e coletiva.

1.3
TIPOS DE DADOS PESSOAIS

A Lei nº 12.527/2011, conhecida como LAI, introduziu na administração pública federal uma série de termos relacionados à proteção de dados pessoais, como “informação pessoal” e “informação pessoal sensível”. Para que possamos alinhar esses conceitos com os que foram estabelecidos pela LGPD e pelo Decreto nº 10.046/2019, vamos recordar como os aplicamos nos últimos anos. Segundo o artigo 4°, IV da Lei n° 12.527/11, informação pessoal é aquela que se refere a uma pessoa natural identificada ou identificável. Pessoa natural é o mesmo que pessoa física, isto é, o indivíduo.

O artigo 31 da LAI, regulamentado pelos artigos 55 a 62 do Decreto nº 7.724/12, detalha os aspectos mais importantes desse conceito. De acordo com o art. 31 da LAI, nem toda informação pessoal tem um regime específico de proteção. Somente aquela que pode afetar os direitos de personalidade, definidos no art. 5º, X da Constituição Federal, teria uma proteção especial. Dentro desse conjunto de dados, há o que se chamou, com base na doutrina existente, de informação pessoal sensível. Trata-se daquela informação que fere o direito de autodeterminação da imagem ou que pode gerar discriminação contra o titular daquele dado.

A existência de níveis diferentes de proteção foi muito relevante nos últimos anos, pois indicou limites à redução da expectativa de privacidade quando os titulares dos dados eram os próprios agentes públicos. A LGPD conservou o conceito de dado pessoal trazido pela Lei 12.527/2011 e aprimorou o conceito de informação 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” (Art. 5º, II).

Ao contrário da LAI, porém, os direitos e garantias sobre dados pessoais da LGPD abrangem todos os tipos de dados pessoais, respeitadas as legislações existentes, inclusive os regimes existentes de transparência e acesso à informação. Ou seja, a tutela da lei não se restringe mais apenas aos dados pessoais sensíveis ou diretamente ligados aos direitos de personalidade, mas, em maior ou menor grau, a todos os dados pessoais.

Com a edição do Decreto Estadual nº 26.451/2021, procurou-se adotar medidas destinadas à aplicação da Lei Geral de Proteção de Dados Pessoais - LGPD, no âmbito do Poder Executivo Estadual, instituindo competências, procedimentos e providências correlatas a serem observados pelos órgãos da Administração Direta, pelas autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais entidades controladas diretamente ou indiretamente pelo Estado visando garantir o cumprimento de suas determinações legais.

A relação entre os atributos que mencionamos e os conceitos que estudamos não é perfeitamente clara; contudo, é possível harmonizar esses conceitos de forma simples. Em primeiro lugar, é importante ressaltar que todos os atributos são informações pessoais, pois se referem a um indivíduo identificado ou identificável.

Atributos genéticos e biométricos, conforme a definição legal, são dados pessoais sensíveis. Atributos biográficos, juntamente com dados como números de registro como CPF, CNPJ, NIS, PIS, PASEP e Título de Eleitor, são o que chamamos de dados cadastrais, que são, sob a ótica da LGPD, dados pessoais. Isso ocorre porque, se algum dado, mesmo o cadastral, revelar informação relacionada a uma pessoa natural identificada ou identificável, será considerado um dado pessoal.

De acordo com a Lei, serão considerados sensíveis aqueles atributos biográficos que se relacionem à crença religiosa, posição política, associação a sindicato ou a entidade de natureza religiosa, filosófica ou política. Dessa forma, em geral, o tratamento de atributos biométricos e genéticos seguirá o regime de tratamento de dados pessoais sensíveis; já o tratamento de atributos biográficos dependerá do seu conteúdo, o qual determinará a tipologia do dado conforme a LGPD.

2

COMO REALIZAR O TRATAMENTO DOS DADOS PESSOAIS

2.1 HIPÓTESES DE TRATAMENTO

De acordo com o art. 23 da LGPD, os órgãos e entidades públicos podem tratar dados pessoais somente para cumprir a sua finalidade pública, no interesse público, com o intuito de exercer as competências legais ou as atribuições legais do serviço público, desde que informem ao titular as hipóteses de tratamento.

Conforme visto anteriormente, o tratamento de dados pessoais só pode ser feito se estiver de acordo com uma das hipóteses previstas na Lei. Essas hipóteses são os requisitos necessários para verificar se o tratamento de dados pelo controlador ou operador é autorizado. As hipóteses de tratamento de dados pessoais estão listadas no Art. 7º da LGPD. Nesta seção, também abordaremos as disposições do Art. 11, que trata das hipóteses autorizativas para o tratamento de dados pessoais sensíveis.

Segundo a LGPD, os dados pessoais sensíveis de pessoas naturais são aqueles relativos à origem racial ou étnica, crença religiosa, opinião política, filiação sindical ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico (Art. 5º, II). São dados que podem gerar discriminação contra o seu titular, e por isso, estão sujeitos a uma proteção mais rigorosa.

É importante ressaltar que a lei só permite o tratamento de dados sensíveis em situações imprescindíveis. Isso implica que o controlador deve comprovar a necessidade alegada. É preciso que os órgãos e entidades da Administração Pública conheçam as hipóteses para: Analisar os casos de tratamento de dados pessoais já efetuados, visando verificar se existe hipótese legal que os ampare; e Avaliar antecipadamente cada novo caso de tratamento que deseje realizar, identificando as hipóteses legais autorizativas aplicáveis.

A LGPD estabelece em seu art. 6º, que o tratamento de dados pessoais deve observar a boa-fé e dez princípios fundamentais específicos. São eles:

- finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de
- acordo com o contexto do tratamento;
- 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;
- 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;
- 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;
- 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;

- 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;
- prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do
- tratamento de dados pessoais;
- não discriminação: impossibilidade de realização do tratamento para fins discriminatórios
- ilícitos ou abusivos; e
- 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.

Para que o tratamento de dados pessoais seja legítimo, não é suficiente que se encaixe em uma das situações previstas em lei. É imprescindível que se observe os princípios estabelecidos na legislação.

2.1.1 Identificação das hipóteses de tratamento aplicáveis

Como escolher a base legal adequada para o tratamento de dados pessoais? Essa questão depende dos objetivos e cenários específicos de cada caso.

Para atender a uma obrigação legal ou regulamentar" e "Para realizar políticas públicas".Porém, não há uma regra geral que se aplique a todas as situações, mesmo que se trate de órgãos e entidades públicas.

Pode ocorrer também de haver mais de uma base legal possível, se existirem vários fins para o tratamento do dado. O relevante é analisar cada caso e registrar a(s) base(s) legal(is) pertinente(s), pois o titular tem o direito de saber qual é a base legal que autoriza o tratamento de seus dados pessoais.

Ademais, o princípio da accountability exige que o órgão ou entidade que realiza o tratamento de dados pessoais possa demonstrar que está em conformidade com a LGPD, evidenciando o respeito e o cumprimento das normas de proteção de dados pessoais estabelecidas, bem como a sua efetividade.

Por isso, é responsabilidade do órgão ou entidade pública avaliar bem a base de tratamento aplicável, pois alterações posteriores podem prejudicar a confiança do titular quanto aos interesses legítimos da instituição no uso de seus dados, além de afetar os requisitos de transparência, accountability e prestação de contas.

2.1.2 Verificação de conformidade do tratamento de dados quanto aos princípios da LGPD

Após verificar qual(is) a(s) modalidade(s) de tratamento de dados se adequa(m) aos casos específicos de processamento de informações por órgãos e entidades do Governo Federal, é preciso considerar outras questões relevantes para a conformidade com os princípios da LGPD. Nesse sentido, o órgão ou entidade pública deverá examinar outros aspectos, descritos a seguir. Estabeleça a finalidade para a qual o tratamento de dado é imprescindível. Os objetivos devem ser legítimos, específicos e explícitos (princípio da finalidade).

Determine como a finalidade do tratamento será comunicada ao titular, o que deve ser feito antes do início do tratamento do dado (princípio da finalidade). No caso de tratamento de dados que tenha sido iniciado antes da entrada em vigor da Lei, informe que medidas serão adotadas para notificar o titular sobre o tratamento efetuado e a finalidade a qual se destina (princípio da finalidade). Assegure que o tratamento do dado será somente para a finalidade comunicada ao titular (princípio da adequação).

Quaisquer alterações na finalidade de tratamento deverão ser também informadas ao titular do dado. Ao planejar a forma de tratamento de dados, atente para restringir a utilização ao mínimo de informações indispensáveis, garantindo abrangência pertinente e proporcional à realização das finalidades comunicadas ao titular (princípio da necessidade).

O objetivo é manter-se fiel à finalidade de tratamento comunicada (princípio da qualidade do dado). Atente para a necessidade de garantir ao titular a opção de obter facilmente informações claras e precisas, mediante requisição, sobre o tratamento que é dado a seus dados e sobre os respectivos agentes de tratamento (princípio da transparência).

Observação: Os órgãos e entidades deverão garantir o acesso às informações sobre o tratamento do dado do titular, resguardadas as informações de acesso restrito, conforme legislação vigente. Defina e documente as medidas técnicas e administrativas que serão adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão (princípio da segurança).

Identifique e registre as medidas que serão adotadas para prevenir a ocorrência de danos ao titular ou a terceiros em virtude do tratamento de dados pessoais (princípio da prevenção). Comprometa-se a não realizar o tratamento do dado para fins discriminatórios ilícitos ou abusivos (princípio da não discriminação). Comprometa-se a adotar 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).

Para iniciar novos tratamentos de dados, é fundamental que os órgãos e entidades da Administração Pública analisem todas as questões citadas acima e documentem a forma de aplicação de cada um dos princípios da LGPD. O Relatório de Impacto à Proteção de Dados Pessoais – RIPD representa um instrumento importante de verificação e demonstração da conformidade do tratamento de dados pessoais realizado pela instituição. Serve tanto para a análise quanto para a documentação.

A análise das questões acima deve também ser realizada para os casos de tratamento de dados anteriores à vigência da Lei. Nesses casos, é importante identificar os pontos de não conformidade com a LGPD, para os quais deverão ser elaborados planos para adaptação à Lei.

2.2
COLETA

Segundo o art. 5º, inciso X da LGPD, a coleta é uma das operações de tratamento que consiste em obter os dados pessoais do cidadão (titular dos dados). Essa operação é a primeira etapa de um ciclo de vida do tratamento de dados.

Para que a instituição possa realizar a coleta dos dados pessoais, ela deve respeitar as condições de tratamento, as medidas de segurança, os princípios, os direitos do titular e as demais normas estabelecidas pela LGPD.

Todo o conteúdo deste documento visa justamente orientar as instituições para os cuidados que elas devem ter ao coletar e tratar os dados pessoais dos cidadãos de forma a assegurar a privacidade dos titulares de dados.

2.3
ANONIMIZAÇÃO E PSEUDONIMIZAÇÃO

De acordo com a LGPD, dado anonimizado é aquele que não pode ser relacionado, direta ou indiretamente, a um indivíduo, levando-se em conta os meios técnicos razoáveis disponíveis no momento do tratamento. Essa impossibilidade de associação entre o dado e o seu proprietário se dá por meio da técnica de anonimização, que impede que se estabeleça qualquer vínculo entre eles, seja de forma direta ou indireta.

Quando o dado é anonimizado, e não há mais como identificar o seu titular, ele deixa de ser abrangido pela legislação, pois não se trata mais de um dado pessoal, conforme estabelecido no art. 12 da LGPD. É preciso destacar que, se o dado for considerado anonimizado pelo controlador, mas houver a possibilidade de reverter o processo que gerou a anonimização, permitindo a reidentificação do titular de dados, então o dado não é realmente anonimizado, mas sim potencialmente pseudonimizado.

Pseudonimização é a técnica de tratar dados pessoais de uma forma em que os dados só podem ser atribuídos a um titular de dados se houver o uso de informações adicionais, que não são acessíveis a todos, e que são mantidas em ambiente separado, controlado e seguro.

Por exemplo, criptografia é um método de pseudonimização, quando os dados só podem ser atribuídos a um titular se houver o conhecimento da chave criptográfica. Sem a chave, os dados são incompreensíveis. Conforme a legislação vigente, esses processos devem ser empregados, sempre que possível, por meio da utilização de meios técnicos razoáveis e disponíveis, no momento do tratamento dos dados.

A seguir, algumas recomendações para auxiliar na escolha da técnica a ser empregada:

- Listar os principais processos de trabalho que realizam tratamento de dados pessoais para a realização de estudos, especialmente em órgão de pesquisa, conforme Art. 7º, IV.
- Identificar os dados pessoais que são objeto dos processos de trabalho listados, que não podem ter os titulares identificados.
- Analisar o ciclo de vida de tratamento do dado para reduzir riscos de violação de dados que não são mais de uso frequente.
- E, ainda, sugerir arquivamento ou eliminação dos dados, visto que a gestão de dados desnecessários no ambiente de produção acarreta aumento não apenas do volume de dados a serem gerenciados, como também do custo operacional relacionado a este processo (em atividades como armazenamento e gestão da segurança). Avaliar o risco de identificação do titular dos dados identificados. Deve-se considerar que, quanto maior o uso de tecnologias de análise de dados, quanto maior o volume de dados processados e quanto mais relevantes forem estes dados, maior será o risco de violação.

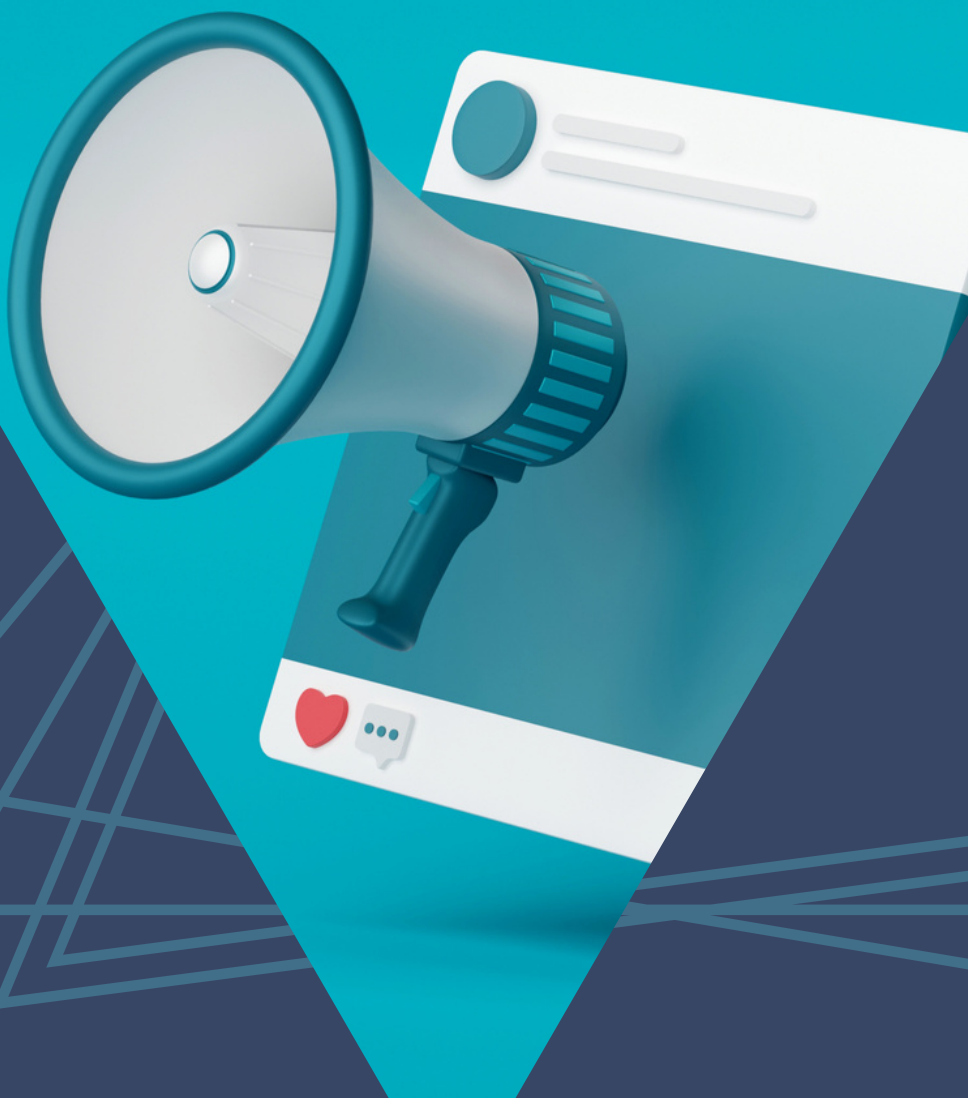
Quando houver a exigência de proteção de dados pessoais, sem a necessidade de guarda dos dados que associam estes aos titulares, pode-se optar pelo processo de anonimização, sem prejuízo de atividades do órgão ou entidade. Caso contrário, pode-se optar pela técnica de pseudonimização.

Definir um plano de comunicação para incidentes de violação de dados. O objetivo é proporcionar maior agilidade na solução de incidentes e padronização de atividades a serem realizadas, assim como prever responsáveis pelo cumprimento das atividades. Documentar violações comprovadas e incidentes ocorridos, a fim de analisar riscos de violação periodicamente. Promover a conscientização contínua sobre a importância da proteção de dados no órgão ou entidade.

Uma das técnicas empregadas para resguardar os dados pessoais é a pseudonimização, que consiste em substituir os elementos que identificam uma pessoa por outros que não permitem a sua identificação direta, por exemplo:

1. Substituição de nomes por códigos: Em uma base de dados de pacientes de um hospital, os nomes dos pacientes podem ser substituídos por códigos únicos. Por exemplo, “João Silva” pode se tornar “Paciente 12345”.
2. Tokenização de números de cartão de crédito: Em um sistema de pagamento, os números de cartão de crédito podem ser substituídos por tokens únicos. Por exemplo, “1234 5678 9012 3456” pode se tornar “abcd efgh ijkl mnop”.
3. Substituição de endereços de e-mail por hashes: Em uma base de dados de usuários de um site, os endereços de e-mail podem ser substituídos por hashes. Por exemplo, “joao.silva@example.com” pode se tornar “b2d1234a567e”.

2.4
PUBLICIDADE



O inciso I do art. 23 da LGPD impõe às pessoas jurídicas de direito público obrigações de transparência ativa. Isto é, de publicar informações sobre os tratamentos de dados pessoais por elas realizados em seus sítios eletrônicos de forma clara e atualizada, detalhando a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução desses tratamentos.

Também deve ser dada publicidade aos tratamentos de dados pessoais sensíveis em que seja dispensado o consentimento do titular, seja para cumprimento de obrigação legal ou regulatória, seja para tratamento compartilhado de dados necessários para a execução de políticas públicas previstas em leis ou regulamentos, conforme prevê o §2º do art. 11 da LGPD.

Outra informação a ser publicizada é a identidade e informações de contato do encarregado, por força do art. 41, §1º da LGPD.

Quando o tratamento de dados pessoais envolver a obrigação legal de difusão destes em transparência ativa, estes devem ser publicados em formato interoperável e estruturado para o uso compartilhado, em cumprimento ao disposto no art. 25 da LGPD e como já previa o art. 8º, §3 da Lei nº 12.527/2011, a Lei de Acesso à Informação.

2.5
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

O RIPD (Relatório de Impacto à Proteção dos Dados Pessoais) é um documento essencial para comprovar que o controlador fez uma análise dos riscos envolvidos nas operações de tratamento dos dados pessoais que são obtidos, manipulados, utilizados, compartilhados e quais ações são tomadas para reduzir os riscos que possam prejudicar as liberdades civis e os direitos fundamentais dos donos desses dados.

De acordo com o art. 5º inciso XVII da LGPD, o RIPD é uma documentação que deve ser preservada pelo Controlador dos dados pessoais. Art. 5º Para os fins desta Lei, considera-se: XVII - 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; Enquanto o art. 5º inciso XVII define o que é um RIPD, o seu conteúdo mínimo é indicado pelo parágrafo único do art. 38, destacado abaixo:

> 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.

2.6 TÉRMINO DO TRATAMENTO

A Lei Geral de Proteção de Dados (LGPD) estabelece quatro situações em que o tratamento de dados pessoais deve ser encerrado:

- quando a finalidade que motivou a coleta dos dados for atingida ou quando os dados não forem mais necessários ou relevantes para essa finalidade;
- quando o período de tratamento previsto em contrato ou em lei terminar;
- quando o consentimento do titular for revogado ou quando ele solicitar o fim do tratamento, salvo se houver interesse público envolvido;
- quando a autoridade nacional determinar o fim do tratamento por violação da Lei.

Em qualquer dessas situações, a Lei prevê que os dados sejam eliminados, exceto se: houver uma obrigação legal ou regulatória que exija a manutenção dos dados pelo controlador; os dados forem necessários para pesquisa científica, garantindo-se, sempre que possível, a sua anonimização; os dados forem transferidos para terceiros, desde que observados os requisitos legais para o tratamento de dados; e os dados forem usados exclusivamente pelo controlador, sem acesso por terceiros, e desde que anonimizados.

No caso da Administração Pública, é importante que essa norma seja compatibilizada com a legislação de arquivos, especialmente com a Lei nº 8.159/1991, e seus regulamentos. Isso porque, sob essa perspectiva, os dados pessoais coletados pelo poder público passam a integrar o que se chama de arquivo público (art. 7°) e a sua eliminação deve seguir os procedimentos de gestão documental. A eliminação de documentos arquivísticos deve ser realizada pelas respectivas Comissões Permanentes de Avaliação de Documentos (CPAD) dos órgãos e entidades da Administração Pública.

3

BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

4.1
PRIVACIDADE DESDE A CONCEPÇÃO E POR PADRÃO (PRIVACY BY DESIGN E BY DEFAULT)

4.1.1 Privacidade desde a concepção

O tratamento de dados pessoais deve seguir medidas adequadas que assegurem que, por padrão, somente sejam processados os dados pessoais imprescindíveis para atender à(s) finalidade(s) específica(s) estabelecida(s) pela instituição que exerce o papel de controladora dos dados pessoais. Essa exigência de implementação implica que a instituição deve restringir a quantidade de dados pessoais coletados, abrangência do tratamento, duração do armazenamento e acessibilidade ao estritamente necessário para a efetivação da finalidade do tratamento dos dados pessoais. Essa medida deve assegurar, por exemplo, que não haja acesso ilimitado e indefinido aos dados pessoais tratados pela instituição por parte de todos os usuários dos agentes de tratamento.

Na LGPD, a Privacidade por Padrão (do inglês Privacy by Default) tem relação direta com o princípio da necessidade, expresso pelo art. 6º, inciso III.

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

A privacidade por padrão é alcançada por meio da adoção das seguintes práticas: Especificação da finalidade - os propósitos para os quais os dados pessoais são coletados, utilizados, retidos e divulgados devem ser informados ao titular dos dados antes ou no momento em que as informações são coletadas. **As finalidades especificadas devem ser claras, limitadas e relevantes em relação ao que se busca ao tratar os dados pessoais.**

Limitação da coleta - a coleta de dados pessoais deve ser legal e limitada ao necessário para os fins especificados.

Minimização dos dados - a coleta dos dados pessoais que possa identificar individualmente o titular de dados deve obter o mínimo necessário de informações pessoais. A concepção de programas, tecnologias e sistemas de informação e comunicação deve iniciar com interações e transações não identificáveis, como padrão. Qualquer vinculação de dados pessoais deve ser minimizada.

A possibilidade de informações serem usadas para identificar o titular de dados deve ser minimizada. Limitação de uso, retenção e divulgação - o uso, retenção e divulgação de dados pessoais devem limitar-se às finalidades relevantes identificadas para o titular de dados, para as quais ele consentiu ou é exigido ou permitido por lei. Os dados pessoais serão retidos apenas pelo tempo necessário para cumprir as finalidades declaradas e depois eliminados com segurança.

Quando a necessidade ou uso de dados pessoais não forem claros, deve haver uma presunção de privacidade e o princípio da precaução deve ser aplicado. Dessa forma, as configurações padrão devem ser as de maior proteção à privacidade.

4

USO SEGURO DE CREDENCIAIS DE ACESSO

- Sempre que disponível, ative a autenticação em duas etapas.
- A senha é pessoal e intransferível, não a divulgue e nem compartilhe. A senha é sua e de mais ninguém!
- Não escreva sua senha em local público ou de fácil acesso como em papéis, em arquivos sem proteção no computador ou em outro tipo de mídia.
- Feche sua sessão (logout) ao acessar sites que requeiram o uso de senhas, principalmente ao usar equipamentos compartilhados.
- Nunca use dados pessoais ou sequências de teclado como senha.
- Tente criar senhas fortes contendo letras (maiúsculas e minúsculas), números aleatórios e caracteres especiais, de pelo menos 10 (dez) dígitos.
- Evite usar a mesma senha para cadastro e acesso aos sistemas.
- Tente mudar suas senhas regularmente, principalmente se acessar sistemas em dispositivos que são utilizados por várias pessoas.
- Caso desconfie que sua senha tenha sido descoberta, vazada ou usada em um equipamento invadido ou infectado, altere-a imediatamente.
- Use conexões seguras (https) quando o acesso a um site, envolver o fornecimento de credenciais de acesso.

5

CUIDADOS COM O USO DO CORREIO ELETRÔNICO

Sempre verifique a procedência de e-mails em nome de bancos, provedores de serviços, lojas, órgãos públicos, etc. observando o cabeçalho e o conteúdo completo da mensagem. Nunca saia clicando de imediato em links e anexo da mensagem. Verifique se o remetente é mesmo quem diz ser.

Caso desconfie de alguma mensagem, consulte o Catálogo de Fraudes da Rede Nacional de Pesquisa (https://catalogodefraudes.rnp.br/) que tem como objetivo conscientizar a comunidade sobre os principais golpes que estão em circulação na internet, identificando e divulgando fraudes reportadas pela comunidade ou coletadas por seus sensores. Mesmo que tenha utilizado o antivírus, evite abrir arquivos enviados por fontes não confiáveis. Desconfie sempre de arquivos executáveis recebidos, mesmo vindos de fontes confiáveis. Eles podem vir mascarados com extensão compactada (.zip, .rar, .gz, ...). Verifique a veracidade das informações e use sempre seu bom senso antes de repassar a mensagem.

Desconfie de links e arquivos anexados à mensagem mesmo que tenham sido enviados por pessoas ou instituições conhecidas (pode ser uma conta de email invadida que está sendo utilizada para aplicar golpes).

Antes de abrir um arquivo anexado à mensagem tenha certeza de que ele não apresenta riscos, verificando-o com ferramentas antivírus. Seja cuidadoso ao acessar a página do seu webmail para não ser vítima de golpe (phishing).

6

NÍVEIS DE ACESSO NO SEI

A fim de fazer cumprir a principal diretriz da Lei de Acesso à Informação - LAI 12.527, que é a publicidade e a transparência das informações, orientamos que, em regra, o nível de acesso seja sempre público para o Memorando, Memorando-Circular, Ofícil e Ofício-Circular.

Documentos com caráter informativo devem ter o nível de acesso público. Com o propósito de elucidar quais assuntos possuem restrição de acesso, vejamos:

Documentos sigilosos: Informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para segurança da sociedade e do Estado, e aquelas abrangidas pelas demais hipóteses legais do sigilo.

Documentos restritos: São aqueles que contêm informações pessoais e funcionais com respeito à intimidade, vida privada, honra e imagem, prevenção e diagnóstico médico, apuração de responsabilidade e representação contra servidor. O acesso ao processo que contém o nível "Restrito" será apenas reservado ao setor que o criou e para o local onde foi tramitado.

Lembrando que conforme a LAI a restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com intuito de prejudicar processo de apuração de irregularidades em que o titular das informações tiver envolvido.

7

A PGE E A LGPD

Instituição do Comitê Gestor de Proteção de Dados-CGPD no âmbito da PGE-RO

A publicação da Portaria nº 345 de 29 de março de 2022, institui o comitê responsável pela avaliação dos mecanismos de tratamento e proteção dos dados existentes e pela proposição de ações voltadas a seu aperfeiçoamento, com vistas ao cumprimento das disposições da Lei nº 13.709, de 14 de agosto de 2018.

Instituição do Programa de Governança de Proteção de Dados no âmbito da PGE-RO

Por intermédio da Portaria nº 457 de 26 de maio de 2022, a PGE-RO busca estabelecer, de forma sucinta, um roteiro de atividades que devem ser realizadas para a implementação de um Programa de Governança em Privacidade, em conformidade com o disposto na Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709, de 14 de agosto de 2018) e o Decreto Estadual nº 26.451, de 4 de outubro de 2021.

Instituição da Política de Privacidade de Proteção de Dados no âmbito da PGE-RO

A Procuradoria-Geral do Estado de Rondônia, reafirmando o compromisso legal de cumprir as normas previstas na Lei Geral de Proteção de Dados Pessoais (LGPD), publicou a Portaria nº 681 de 13 de setembro de 2022, para proteger os direitos fundamentais de liberdade e de privacidade.

Aviso de privacidade e Cookies

Aviso de Privacidade, por sua vez, é uma comunicação direcionada aos indivíduos externos à organização na condição de titulares de dados pessoais, informando e descrevendo as operações de tratamento de dados realizadas pela organização. O sítio eletrônico da Procuradoria-Geral do Estado possui este documento, estando disponível no seguinte link: https://pge.ro.gov.br/aviso-de-privacidade/ . Ademais, possui a configuração de cookies em respeito as normas da Autoridade Nacional de Proteção de Dados – ANPD.

Comitê Gestor Estadual de Proteção de Dados

A Procuradoria-Geral do Estado faz parte do Comitê Gestor de Privacidade e Proteção de Dados Pessoais – CGPD, que é um colegiado criado pelo art. 14 do Decreto Estadual nº 26.451/2021, cuja composição se dá por meio de seus membros titulares e suplentes, representantes de 12 (doze) órgãos e entidades estaduais (Casa Civil, PGE, SETIC, OGE, SEFIN, CGE, SESAU, SEPOG, SESDEC, SEDUC, DETRAN e SEGEP). O Comitê Gestor tem por objetivo estabelecer o conjunto de regras de boas práticas e de governança, diretrizes, políticas, projetos, ações e metas estratégicas, a serem observados pelos órgãos do Poder Executivo.

ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS (DPO)

Na Procuradoria-Geral do Estado de Rondônia, o Encarregado pelo Tratamento de Dados Pessoais é o servidor Rod Daniel Gomes Sussuarana do Nascimento para apoiar e atuar na implementação da LGPD.

DÚVIDAS

Para esclarecer quaisquer dúvidas sobre esta Política de Privacidade ou sobre os dados pessoais coletados e tratados, entre em contato com nosso Encarregado através dos canais mencionados abaixo:

lgpd@pge.ro.gov.br
(69) 3212-9153
Edifício Rio Pacaás Novos, Complexo Rio Madeira – Av. Farquar, 2986, Pedrinhas, Porto Velho/RO, CEP 76801-470

8

REFERÊNCIAS BIBLIOGRÁFICAS

- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 12.527, de 18 de novembro de 2011. 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 dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2011/Lei/L12527.htm#art1>. Acesso em: 20 fev. 2024.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº
- 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o
- uso da Internet no Brasil. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 20 fev. 2024.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm>. Acesso em: 20 fev. 2024.
- 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: 20 fev. 2024.
- BRASIL. Ministério do Planejamento Desenvolvimento e Gestão. Guia de Gestão de Processos do Governo, 2011. Disponível em: <http://www.gespublica.gov.br/content/guia-de-gest%C3%A3o-de-processos>. Acesso em: 20 fev. 2024.

- Cavoukian, Ann. Privacy by Design: The 7 Foundational Principles. August, 2009. Disponível em: <https://iapp.org/media/pdf/resource_center/Privacy%20by%20Design%20-%20 7%20Foundational%20Principles.pdf>. Acesso em: 20 fev. 2024.
- Conselho Nacional de Arquivos. Resolução nº 25, de 27 de abril de 2007. Dispõe sobre a adoção do Modelo de Requisitos para Sistemas Informatizados de Gestão Arquivística de Documentos - e-ARQ Brasil pelos órgãos e entidades integrantes do Sistema Nacional de Arquivos - SINAR. Disponível em: < http://conarq.gov.br/resolucoes-do-conarq/267- resolucao-n-25,-de-27-de-abril-de-2007.html >. Acesso em: 20 fev. 2024.
- Information Commissioner's Office. Sample DPIA template. Disponível em: < https://ico. org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf >. Acesso em: 20 fev. 2024.
- PROJECT MANAGEMENT INSTITUTE. Um Guia de Conhecimento em Gerenciamento de Projetos. Guia PMBOK 5ª edição. Project Management Institute, 2013.
- Guia Orientativo Sobre Segurança Da Informação Para Agentes De Tratamento De Pequeno Porte Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_seguranca_da_informacao_para_atpps___defeso_eleitoral.pdf >. Acesso em: 19 fev. 2024.
- Tratamento de dados pessoais pelo Poder Público Disponível em: < https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf >. Acesso em: 19 fev. 2024.
- Guia Orientativo Para Definições Dos Agentes De Tratamento De Dados Pessoais E Do Encarregado Disponível em: < guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf (www.gov.br) . Acesso em: 19 fev. 2024.

PGE

RONDÔNIA