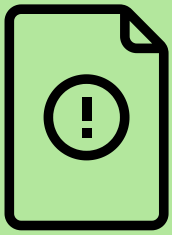

Privacidade e proteção de dados **pessoais para o público interno da DPE-PR**

1ª edição – agosto de 2025

DPE PR
DEFENSORIA PÚBLICA
DO ESTADO DO PARANÁ

DEFENSORIA PÚBLICA DO ESTADO DO PARANÁ

ADMINISTRAÇÃO SUPERIOR

Biênio 2024-2025

Defensor Público-Geral

Matheus Cavalcanti Munhoz

1ª Subdefensora Pública-Geral

Lívia Martins Salomão Brodbeck e Silva

2ª Subdefensora Pública-Geral

Thaisa Oliveira

Chefe de Gabinete

Pedro Henrique Piro Martins

Corregedor-Geral

Henrique de Almeida Freire Gonçalves

Subcorregedora-Geral

Josiane Fruet Bettini Lupion

CARTILHA PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS PARA O PÚBLICO INTERNO DA DPE-PR

1ª Edição – agosto de 2025

Elaborado pela equipe do Encarregado de Proteção de Dados da DPE-PR em parceria com a Diretoria de Comunicação (DICOM)

Encarregado de Proteção de Dados

Dezidério Machado Lima

Assessoria e Encarregada Substituta

Sarah Gomes Sakamoto

Projeto gráfico e diagramação

Sarah Jennifer da Silva de Lima

APRESENTAÇÃO

A Defensoria Pública é instituição essencial à função jurisdicional do Estado e constitucionalmente incumbida da promoção dos direitos humanos e da defesa dos interesses dos mais vulneráveis. No cumprimento de sua função institucional, a Defensoria realiza tratamento de um grande volume de informações, dentre elas, diversos dados pessoais, tanto no exercício de suas atividades finalísticas quanto em sua estrutura administrativa.

Com a promulgação da Lei Federal nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), iniciou-se um novo cenário no âmbito da era dos dados, trazendo um marco normativo que impõe deveres e responsabilidades a todos os agentes de tratamento. Mais do que uma exigência legal, a proteção de dados pessoais representa um compromisso com os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade.

Nesse cenário, é imperioso que todos os(as) integrantes da DPE-PR estejam não apenas cientes, mas também engajados na construção de uma cultura de privacidade e proteção de dados pessoais, com zelo no trato dos dados que lhes são confiados. Para tanto, a disseminação de conhecimento e o fortalecimento da capacitação interna são etapas indispensáveis.

É com esse propósito que a Cartilha Privacidade e Proteção de Dados Pessoais para o Público Interno da DPE-PR foi elaborada. A cartilha fornece uma introdução concisa e acessível aos principais conceitos, fundamentos e boas práticas relacionados à temática, visando apoiar a atuação dos(as) defensores(as), servidores(as), estagiários(as) e colaboradores(as) da instituição.

Que este material sirva como instrumento de conscientização, reflexão e aprimoramento, reafirmando o compromisso da Defensoria Pública do Estado do Paraná com a promoção da dignidade da pessoa humana em todas as suas dimensões.

Boa leitura!

A IMPORTÂNCIA DOS DADOS

Em uma era da informação marcada por uso massivo de recursos digitais e tecnologias ubíquas, dados pessoais são produzidos, coletados, compartilhados e analisados em alta escala, sendo um ativo valioso para as organizações.

A chamada “economia dos dados” já é uma realidade consolidada: cada clique, pesquisa e interação digital gera informações que alimentam algoritmos, moldam ofertas de produtos, definem decisões de empresas e influenciam até mesmo o comportamento social.

Neste cenário, os dados pessoais se tornaram ativos estratégicos e é por meio desses dados que plataformas financiam suas operações: hábitos, preferências, localização e contatos são fornecidos em troca de produtos e serviços digitais, movimentando uma economia global.

Assim, esses dados passaram a ter valor econômico, sendo negociados, armazenados e tratados de mais variadas formas e, se tratados de forma indevida, podem comprometer direitos individuais e coletivos, causando profundos impactos na vida das pessoas.

Um vazamento de dados pode ter efeitos severos para um(a) titular: exposição desde danos financeiros com uso de dados vazados para fraudes bancárias, até prejuízos reputacionais com roubos de identidade, tentativa de golpes a amigos e familiares, com constrangimentos e riscos de diversos tipos em casos mais extremos.

A depender do tipo de dado exposto, no caso de dados envolvendo saúde ou orientação sexual, os danos podem ser duradouros e irreversíveis. Portanto, a privacidade e a proteção dos dados pessoais surge como uma área de destaque e um compromisso com a dignidade da pessoa humana.

NA PRÁTICA

Alessandra, 28 anos, é servidora pública de órgão estadual. Ela participou voluntariamente de um programa interno de inclusão e diversidade promovido pela instituição, no qual, preencheu um formulário de identificação, em ambiente considerado seguro e, em um dos campos, preencheu sua orientação sexual. No entanto, por descuido de um servidor do setor de recursos humanos, a informação da lista de participantes foi exposta, o que originou fofocas e brincadeiras no ambiente de trabalho, além de mudança de comportamento de sua chefia imediata. O constrangimento foi tal que a servidora não se sentia mais confortável no ambiente trabalho, tendo crises de ansiedade e alguns impactos em seu rendimento nas atividades.

Ou seja, vazamento de dados teve impactos de violação de privacidade, exposição indevida de dados pessoais sensíveis, gerou constrangimento, assédio moral no ambiente de trabalho e sofrimento psicológico, além do rompimento da confiança institucional. Por isso é de imperiosa importância assegurar a privacidade e a proteção de dados pessoais, evitando danos aos titulares.

É SEU/NOSSO DIREITO

Cada dado pessoal está ligado a uma identidade, a uma história, a uma expectativa de privacidade e controle. É por isso que a proteção de dados pessoais não pode ser reduzida a uma questão técnica ou burocrática: trata-se de um direito fundamental. Garantir que cada pessoa tenha ciência, controle e segurança sobre o tratamento de suas informações é assegurar o respeito à sua liberdade, autonomia e integridade.

Com a promulgação da emenda constitucional 115/2022, em fevereiro de 2022, o direito à proteção de dados pessoais foi acrescentado ao rol de direitos e garantias fundamentais da Constituição Federal (CF), a partir do inciso LXXIX em seu Art 5º. Decorrente do direito à privacidade (Art 5º, X), o direito à proteção de dados pessoais está estritamente relacionado à autodeterminação informativa que garante a liberdade de decidir sobre o fluxo de seus dados pessoais.

Nesse contexto, a privacidade e a proteção de dados emergem como pilares essenciais para a construção de uma sociedade digital ética, transparente e justa. Mais do que cumprir normas, é preciso cultivar uma cultura de respeito às pessoas por meio do cuidado com as informações que as representam.

Para efetivar esse direito, não basta reconhecer os atos normativos, mas também realizar uma mudança de cultura nas organizações e aplicação de práticas de adequação e de governança. E a Lei Federal nº 13.709/2025, Lei Geral de Proteção de Dados Pessoais (LGPD), surge nesse contexto, estabelecendo regras para o tratamento de dados tanto por organizações públicas e privadas.

Mas a LGPD vai muito além da ADEQUAÇÃO institucional; ela transcende e interliga diversas questões sociais, desde os riscos associados, processos organizacionais e desafios de implementação, até novos paradigmas e oportunidades de atuação nessa área consolidada.

A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

Com a avanço das tecnologias e a intensa transformação digital ocorrida no Brasil nas últimas décadas, tornou-se imprescindível a discussão e necessidade de atos normativos que assegurem o uso de dados de forma ética, segura e transparente.

Diante deste cenário, surgiu a Lei Federal nº 13.709/2018, Lei Geral de Proteção de Dados Pessoais (LGPD) sancionada em agosto de 2018 e com vigência desde setembro de 2020.

A lei traz um marco normativo, estabelecendo princípios, direitos dos(as) titulares e deveres para os agentes de tratamento, com o objetivo de proteger a liberdade, intimidade e privacidade dos cidadãos. Seu âmbito de aplicação é amplo, alcançando tanto o setor público quanto o setor privado, desde que haja tratamento de dados pessoais de pessoas naturais.

Segundo seu Art 3º, tem-se que ela se aplica a qualquer operação de tratamento de dados pessoais realizada no território nacional, ou que tenha por objetivo a oferta ou fornecimento de bens ou serviços para pessoas localizadas no Brasil, independentemente da nacionalidade da organização ou do local onde os dados estejam armazenados, ou, ainda, os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

No setor público, a LGPD também se aplica integralmente. Órgãos da administração direta e indireta, autarquias, fundações, empresas públicas, sociedades de economia mista e todos os entes federativos devem cumprir a lei. Na Defensoria Pública não seria diferente e, ainda, devido à vulnerabilidade de seu fluxo alto, um desafio ainda maior.

As Defensorias Públicas possuem um papel dual: são agentes de tratamento de dados pessoais e, também, defensoras dos direitos dos titulares de dados pessoais. Nesse sentido, considerando seu papel de atuação, amplia-se a necessidade de adoção de medidas técnicas e administrativas de proteção e aplicação de projetos com a utilização de design como serviço. Mas, isso não ocorrerá repentinamente, o que envolve educar, compartilhar e divulgar os conceitos e as melhores práticas, para atingirmos um único objetivo.

A seguir, serão explicados alguns conceitos importantes da LGPD.

CONCEITOS

O QUE É DADO PESSOAL?

A Lei Geral de Proteção de Dados Pessoais (LGPD), em seu Art 5º, I, define dado pessoal como “toda informação relacionada a pessoa natural identificada ou identificável”. É qualquer informação relacionada a uma pessoa natural que permita identificá-la, direta ou indiretamente.

Alguns exemplos são dados evidentes, tais como nome, CPF, RG, endereço, telefone, e-mail, data de nascimento, e outros que, quando combinados, podem levar à identificação de alguém, tais como endereço IP, localização geográfica, hábitos de consumo. Outros tipos de DADOS também são dados pessoais, como: dados cadastrais (informações de cadastros de órgãos públicos), dados financeiros (cartão de crédito, dados bancários), dados digitais (histórico de navegação, cookies, localização).

Muitas pessoas se confundem e acreditam que todos os dados pessoais são sensíveis, mas há diferença!

- DADO PESSOAL SENSÍVEL

A LGPD determina em rol taxativo quais dados pessoais se enquadram na categoria de sensível, sendo estes: dados pessoais sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou 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. Esse tipo de dado requer maiores cuidados e recebe maior proteção da LGPD.

NA PRÁTICA

Eunice, 53 anos, procurou a Defensoria Pública para solicitar medidas protetivas após sofrer episódios de violência doméstica. Durante o atendimento, a equipe coletou diversas informações para oferecer assistência adequada. Dentre os dados pessoais coletados, constam dados sobre saúde física e mental, incluindo relatos de atendimentos anteriores por traumas decorrentes dos abusos, filiação a organização religiosa, pois a violência envolvia episódios de perseguição relacionados à sua prática de fé, além de dados referentes à vida sexual do casal, um dos motivos do conflito que gerou o último caso de violência relatado.

Todos esses dados são classificados como pessoais sensíveis, conforme Art. 5º, II, da LGPD, e exigem tratamento com medidas técnicas e administrativas reforçadas, especialmente por envolverem vulnerabilidade social, risco à integridade física e possíveis discriminações.

- TITULAR DO DADO

O titular de dados é o indivíduo (pessoa física/natural) cujos dados pessoais estão sendo coletados, armazenados, utilizados ou tratados de qualquer forma por uma organização pública ou privada. Exemplos de titulares: Um cliente de uma empresa; Um paciente em um hospital; Um estudante em uma escola; Um servidor público cujos dados são tratados por um órgão governamental.

- TRATAMENTO DE DADOS

Tratamento de dados é 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.

- O tratamento de dados pessoais é uma atividade essencial, tanto às rotinas administrativas quanto às finalísticas, e envolve qualquer operação realizada com esses dados. As operações precisam atender a uma finalidade legítima, embasadas em hipóteses legais específicas e durante o tempo mínimo necessário.

- Os dados pessoais tratados na instituição possuem um ciclo de vida dentro da instituição, que inicia com a coleta, ou seja, com a obtenção ou produção do dado; passa pela retenção, que refere-se ao armazenamento desses dados; em seguida, passa pela fase de processamento, no qual o dado é utilizado para uma determinada finalidade; pode passar pelo compartilhamento, que envolve toda operação de transmissão, transferência ou difusão desses dados; por fim, a eliminação, que envolve apagar esses dados. Em cada uma dessas fases, devem ser observados os princípios da LGPD, reduzindo riscos e assegurando seu uso de forma adequada.

- Ressalta-se, nesses fases, a aplicação dos princípios da finalidade, adequação e necessidade. Nesse contexto, destaca-se, ainda, a vedação da coleta excessiva de dados, restringindo-se o tratamento ao mínimo necessário, em relação aos dados em si coletados e, também, ao período de retenção, que deve obedecer prazos legais e normas de arquivos públicos.

- Atingindo-se o prazo de guarda e cessada a necessidade de tratamento, os dados devem ser eliminados. Portanto, faz-se necessário seguir os tempos de guarda definidos na tabela de temporalidade da instituição.

  Atingindo-se o prazo de guarda e cessada a necessidade de tratamento, os dados devem ser eliminados. Portanto, faz-se necessário seguir os tempos de guarda definidos na tabela de temporalidade da instituição.

Todas essas ações se aplicam aos dados pessoais em qualquer formato, seja físico ou digital. Embora os meios digitais possam dar a impressão de não ocuparem espaço, o armazenamento de arquivos eletrônicos também gera custos e exige cuidados. Por isso, os prazos de retenção definidos nas tabelas de temporalidade devem ser igualmente respeitados para os dados digitais. Quando atingido o período legal de guarda, os arquivos devem ser eliminados de forma segura, em conformidade com a LGPD.

- 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.

- DADO ANONIMIZADO

Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

- No setor público, a anonimização é um mecanismo de grande importância, tendo em vista que é uma ferramenta que viabiliza a compatibilização da publicidade dos atos administrativos e a proteção à privacidade e intimidade, ambos previstos em texto constitucional.
- A anonimização é uma técnica que permite o uso legítimo de dados para fins estatísticos, pesquisas, análise de políticas públicas e prestação de contas, ao passo que de previne exposições indevidas e riscos de vazamentos de dados, assegurando a proteção da privacidade dos(as) titulares.

- PSEUDOANONIMIZAÇÃO

Pseudoanonimização é o tratamento de dados pessoais de forma que não possam ser associados a um titular específico sem o uso de informações adicionais, desde que tais informações adicionais sejam mantidas separadamente e sujeitas a medidas técnicas e administrativas que assegurem a não associação.

Exemplo: Imagine uma base de dados onde:
1) O nome “João da Silva” é substituído por um código “ID00123”.
2) A tabela que relaciona “ID00123” a “João da Silva” é guardada separadamente e com acesso restrito.

Assim: Quem vê apenas o código não consegue identificar João diretamente. Mas quem tem acesso à tabela de correspondência consegue reidentificar o titular. Enquanto a anonimização é técnica irreversível, a pseudoanonimização pode ser revertida com informação adicional e por isso está dentro do escopo da LGPD.

NA PRÁTICA

No Portal da Transparência esses recursos são bastante utilizados e indicados para promover a compatibilidade entre a Lei de Acesso à Informação (LAI) e a LGPD. A ocultação parcial de dados de candidatos aprovados em concursos públicos e a descaracterização de CPF de servidores são exemplos de práticas adotadas.

- AGENTES DE TRATAMENTO

Os agentes de tratamento são as pessoas ou organizações responsáveis pelo tratamento de dados pessoais, cada uma com papéis e deveres específicos (controlador ou operador).

> OBS: A organização é entendida como agente de tratamento; seus funcionários apenas a representa.

- CONTROLADOR

Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

> Uma pessoa natural pode ser considerada agente de tratamento?
> Se age de forma independente e em nome próprio, sim – e não de forma subordinada a uma pessoa jurídica ou membro do órgão.
>
> No caso da Defensoria Pública, o CONTROLADOR é a instituição.

- OPERADOR

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais por conta e sob as instruções do controlador.

Exemplo: a empresa Google atua como operadora dos dados pessoais tratados pela Defensoria Pública (controladora), ao prestar serviços relacionados ao uso de e-mails institucionais e armazenamento de arquivos na plataforma Google Drive.

> O status de controlador ou operador é definido para cada operação de tratamento de dados pessoais. Portanto, a mesma organização poderá ser controladora e operadora, de acordo com sua atuação em diferentes operações de tratamento.
>
> **Exemplo:** a Defensoria Pública atua como operadora dos dados pessoais que recebe do sistema Projudi, tratando essas informações dentro do ambiente do sistema Solar, conforme as finalidades determinadas pelo Tribunal de Justiça do Paraná (TJPR), que, nesse contexto, exerce a função de controlador.
>
> Controlador x Operador: A principal diferença é o poder de decisão. O operador só pode agir no limite das finalidades determinadas pelo controlador.
>
> Em geral, possuem obrigações e responsabilidades distintas, porém, em caso de danos causados em razão do tratamento irregular realizado por operador, possuem responsabilidade solidária (equiparado ao controlador).

- OUTRAS FIGURAS

CO-CONTROLADOR: Quando dois ou mais responsáveis pelo tratamento determinam conjuntamente as finalidades e os meios desse tratamento (ambos são responsáveis conjuntos pelo tratamento).

SUBOPERADOR: Contratado pelo Operador para auxiliá-lo a realizar o tratamento de dados pessoais em nome do controlador.
Desempenha a função de operador em subordinação a outro operador.

> A compreensão dessas figuras é de fundamental importância para a correta execução das atividades, principalmente para os(as) agentes que estão em interface com outras instituições, que lidam diretamente com prestadores de serviço para a DPE-PR ou que estão envolvidos com contratações, termos de cooperação ou instrumentos congêneres.

- ANPD

Autoridade Nacional de Proteção de Dados, órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

> - A ANPD é uma autarquia de natureza especial (Lei nº 14.460, de 25 de outubro de 2022), vinculada ao Ministério da Justiça e Segurança Pública, com autonomia técnica e decisória.
> - Ela orienta, regulamenta e fiscaliza o cumprimento da LGPD, editando normas e resoluções para detalhar sua aplicação.

- ENCARREGADO

Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados - ANPD.

> - O controlador deverá indicá-lo e a indicação deve ser realizada por meio de ato formal.
> - A identidade e suas informações de contato deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador.
> - Deve ser indicado um substituto, obedecendo os mesmos procedimentos, requisitos e divulgação seguidos na indicação do encarregado titular.

- Deverá atuar com ética, integridade e autonomia técnica, evitando situações que possam configurar conflito de interesse.

- Qualificações profissionais devem ser definidas mediante um juízo de valor realizado pelo controlador que o indica, considerando conhecimentos multidisciplinares.

IMPORTANTE

Não possui competência decisória sobre o tratamento de dados pessoais, apenas auxilia na orientação da preservação da privacidade e proteção de dados pessoais.

NA PRÁTICA

As informações de contato podem ser obtidas na página da LGPD no site da DPE-PR. O e-mail de contato do encarregado é encarregadolgpd@defensoria.pr.def.br.
Também existe uma área no Sistema Eletrônico de Informações (SEI) correspondente identificada como “ENC” (Encarregado pelo Tratamento de Dados Pessoais), que trata expedientes administrativos relacionados à privacidade e proteção de dados.

OBRIGAÇÕES E RESPONSABILIDADES

CONTROLADOR

- O controlador necessita controlar as principais decisões;
- Deve definir elementos essenciais para o cumprimento da finalidade (finalidade, base legal, natureza dos dados pessoais tratados, duração do tratamento, prazo de eliminação dos dados);
- O tratamento não precisa ser realizado diretamente por ele, pode fornecer instruções para que um terceiro realize em seu nome (operador), no entanto, definindo sempre os elementos essenciais e verificando a observância das próprias instruções.

OPERADOR

- Realizar o tratamento segundo as instruções fornecidas pelo controlador;
- Firmar contratos que estabeleçam, dentre outros assuntos, o regime de atividades e responsabilidades com o controlador;
- Dar ciência ao controlador em caso de contrato com suboperador.

ATENÇÃO

Só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador

NA PRÁTICA

A DPE-PR assume, para as principais atividades de tratamento de dados pessoais, a figura do controlador. Em alguns tratamentos, ela também é o operador (quando a própria instituição realiza algumas atividades); em outros, possui operador(es), nos casos em que o tratamento ocorre por empresa(s) contratada(s).

Por exemplo, nos armazenamento de dados de folhas ponto no Sistema de Ponto Eletrônico, a DPE-PR assume o papel de controlador e operador, tendo em vista que o sistema é operado e mantido internamente pela equipe da DTI, dentro do ambiente da instituição. Já nos casos do armazenamento de um arquivo no Drive contratado, a DPE-PR atua como controlador e a empresa contratada para o fornecimento do serviço como operador. Nesses casos, a empresa deve seguir as instruções de tratamento de dados pessoais definidas pela DPE-PR.

ENCARREGADO

- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
- Receber comunicações da autoridade nacional e adotar providências;
- Orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.
- A autoridade nacional poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

NA PRÁTICA

Vale destacar que uma das atribuições do encarregado é passar orientações acerca de boas práticas que respeitem a proteção de dados pessoais. Portanto, apesar de não estar previsto expressamente na LGPD a atribuição para a adequação, no âmbito das Defensorias Públicas, o Encarregado ou a equipe de proteção de dados pessoais movimenta(m) o processo de adequação à LGPD, identificando problemas, respondendo dúvidas e repassando as melhores práticas para a comunidade interna. Na DPE-PR, o processo de adequação está em andamento e, em breve, seu setor será contatado para a identificação de atividades e processos para levantamento das que incluem tratamento de dados pessoais, a fim de realizar o mapeamento de dados da instituição. A sua colaboração é fundamental, pois a privacidade e a proteção de dados da instituição é feita por cada um dos integrantes da DPE-PR.

FIQUE DE OLHO

Para fins de cumprimento das responsabilidades previstas em normativas internas, bem como da LGPD, o encarregado pode encaminhar um processo administrativo para seu setor, solicitando informações. Trata-se do fluxo para atendimento do direito dos titulares e, neste caso, há prazo!

Segundo IN 90/2025, seu Art. 4º prevê o prazo de 03 (três) dias úteis para Coordenador(a) do Setor/Diretoria/Sede disponibilizar as informações solicitadas e encaminhá-las ao Encarregado. Conforme indicado no §1º do mesmo artigo, caso o setor identifique alguma dificuldade relevante que impossibilite a resposta nesse prazo, deverá justificar e apresentar novo prazo para resposta, remetendo ao Encarregado.

E EU, INTEGRANTE DA DPE-PR?

- A responsabilidade de assegurar a privacidade e a proteção de dados pessoais se aplica a todos os(as) agentes públicos(as) envolvidos(as) com as atividades de tratamento de dados pessoais que, como foi exemplificado anteriormente, trata-se de qualquer operação realizada com esses dados.

- É vedada a coleta excessiva e o uso indevido, para outra finalidade, por isso, faz-se necessário a compreensão dos conceitos e boas práticas para execução correta das atividades institucionais, respeitando os princípios expostos na legislação.

- A atuação em prol da privacidade e da proteção de dados pessoais é um dever institucional, mas também uma responsabilidade individual de cada integrante da instituição.

- O(A) **agente pública(a)** deve manter uma postura proativa de segurança, transparência e zelo ao realizar as atividades de tratamento, mostrando, assim, respeito ao cidadão.

- A observância dos princípios e o cumprimento da obrigações impostas pela LGPD é responsabilidade de todos(as) os(as) envolvidos(as), sob pena de responsabilização administrativa, civil e penal.

NA PRÁTICA

CONTRA-EXEMPLO: Edi, agente público, insere informações de um processo judicial na íntegra, com diversos dados pessoais de assistido em uma plataforma de IA não contratada para elaboração de uma peça jurídica, em caráter de teste e estudos. Ao fazer isso, Edi compartilhou dados com a empresa, sem quaisquer garantias, expondo dados pessoais do assistido, violando direitos, comprometendo a privacidade, a proteção dos dados pessoais e a reputação da instituição.

PRINCÍPIOS

A LGPD estabelece 10 princípios norteadores para o tratamento de dados pessoais que visam garantir a privacidade e a segurança das informações.

A premissa da lei é apenas coletar, processar e armazenar dados pessoais realmente necessários, além da adoção de medidas técnicas e administrativas para proteger os dados pessoais e prevenir danos aos titulares.

1. **FINALIDADE:** O tratamento precisa ter propósitos legítimos, específicos, explícitos e informados ao titular. Sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.

2. **TRANSPARÊNCIA:** Titulares devem receber informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento.

3. **QUALIDADE DE DADOS:** Dados devem ser exatos, claros, relevantes e atualizados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.

4. **SEGURANÇA:** Dados devem estar protegidos de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, com adoção de medidas técnicas e administrativas.
5. **NÃO DISCRIMINAÇÃO:** O tratamento não pode ser realizado para fins discriminatórios ilícitos ou abusivos.

6. **ADEQUAÇÃO:** O tratamento deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto definido.

7. **NECESSIDADE:** O tratamento limitado ao mínimo necessário para a realização de suas finalidades. Apenas dados pertinentes, proporcionais e não excessivos.
8. **LIVRE ACESSO:** Titulares podem consultar de maneira fácil e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

9. **PREVENÇÃO:** Devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

10. **RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS:** O agente de tratamento deve demonstrar a 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.

BASES LEGAIS

Todo tratamento de dados pessoais deve estar amparado por uma base legal específica, dentre as previstas em lei, justificando assim o tratamento. Isso assegura que os agentes de tratamento não tratem dados pessoais sem uma justificativa legal adequada. A LGPD define 10 bases legais para o tratamento de dados pessoais.

CONSENTIMENTO : mediante manifestação livre, informada e inequívoca pela qual titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

OBRIGAÇÃO LEGAL : para o cumprimento de obrigação legal ou regulatória pelo controlador.

POLÍTICA PÚBLICA : para execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

PESQUISA POR ÓRGÃO : para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais.

EXECUÇÃO DE CONTRATO : para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

PROTEÇÃO DA VIDA : para a proteção da vida ou da incolumidade física do titular ou de terceiro.

TUTELA DA SAÚDE : para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

LEGÍTIMO INTERESSE : para atender aos interesses legítimos do controlador ou de terceiro.

EXERCÍCIO REGULAR DE DIREITO : para o exercício regular de direitos em processo judicial, administrativo ou arbitral.

PROTEÇÃO AO CRÉDITO : para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

Dentre as bases legais mais utilizadas no setor público estão o cumprimento de obrigação legal ou regulatória, execução de política pública e execução de contrato.

DIREITOS DOS TITULARES

A LGPD garante diversos direitos aos titulares de dados pessoais. Os(As) titulares tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade. Para exercer esses direitos, deve entrar em contato através de um canal a ser fornecido pelo controlador, de forma gratuita e facilitada. Exemplos desses direitos:

CONFIRMAÇÃO DE EXISTÊNCIA : Confirmar se possui dados pessoais seus sendo tratados.

RETIFICAÇÃO : Corrigir seus dados (incompletos, inexatos ou desatualizados).

REVOGAÇÃO DO CONSENTIMENTO E ELIMINAÇÃO : Retirar seu consentimento acerca do tratamento e eliminar dados que utilizarem como base legal o consentimento.

ANONIMIZAÇÃO, BLOQUEIO OU ELIMINAÇÃO DE DADOS EXCESSIVOS : Anonimizar, bloquear ou eliminar dados desnecessários ou tratados irregularmente.

REVISÃO DAS DECISÕES (BASE TRATAMENTO AUTOMATIZADO) : Solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses.

ACESSO : Acessar seus dados pessoais.

PORTABILIDADE : Portabilidade de seus dados para outro agente de tratamento.

OPOSIÇÃO : Opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento.

EXPLICAÇÃO : Ser informado sobre: (a) compartilhamento de seus dados com terceiros e (b) a possibilidade de não fornecer consentimento e as consequências.

NA PRÁTICA

A DPE-PR assegura o atendimento aos direitos dos(as) titulares de dados pessoais por meio de um canal específico disponibilizado em seu site oficial. Na área do site disponibilizada para a LGPD, há informações básicas sobre a legislação e uma página para solicitações. Através de um formulário eletrônico, os(as) titulares podem realizar requisições relacionadas aos seus dados pessoais — como confirmação da existência de tratamento, acesso, entre outros previstos nos artigos 18 da LGPD. O formulário, disponível desde 2022, foi estruturado de forma a facilitar a solicitação, com praticidade, segurança e agilidade no processamento das demandas.

Para acessar acessar o formulário eletrônico, basta clicar aqui.

VAZAMENTO DE DADOS

O vazamento de dados pessoais ocorre quando dados pessoais são extraídos, acessados, expostos ou compartilhados de forma não autorizada, seja por falhas técnicas, humanas ou por ações maliciosas. Esse tipo violação é uma incidente de segurança, e seus impactos podem ser severos, afetando titulares de dados e os agentes de tratamento.

Para os(as) titulares, o **vazamentos de dados pessoais** podem causar impactos severos, com prejuízos financeiros, reputacionais, constrangimentos e emocionais. Para as instituições, um incidente desse tipo pode afetar sua reputação, credibilidade e ocasionar aplicação de sanções, além de, muitas vezes, terem que responder pelos danos causados.

A LGPD determina, nos seus artigos 46 a 49, que os agentes de tratamento, sejam públicos ou privados, devem adotar medidas de segurança técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados, destruição acidental ou ilícita, perda, alteração ou qualquer forma de tratamento inadequado ou ilícito.

Quando há um incidente de segurança que possa acarretar risco ou dano relevante aos titulares, a LGPD determina que o controlador comunique o ocorrido à ANPD (Autoridade Nacional de Proteção de Dados) e, sempre que necessário, também ao titular dos dados afetados, de forma clara e em prazo razoável.

O responsável por essas comunicações é o Encarregado. Portanto, a pessoa designada para essa função necessita tomar ciência, recebendo a comunicação da Alta Administração ou partir dos setores institucionais que estiverem ciente da ocorrência, de forma imediata, para iniciar o processo de comunicação à Autoridade Nacional.

NA PRÁTICA

Kiko é estudante e trabalha em um bar no período noturno para pagar a faculdade. Ele é atendido pelo sistema público de saúde e realiza acompanhamento psicológico e psiquiátrico para um quadro de depressão. Certa vez, ao procurar atendimento na UBS, encontrou um vizinho, que trabalha no local. Por curiosidade, o vizinho pesquisou a ficha do rapaz e, sabendo do diagnóstico, compartilhou os dados pessoais do quadro clínico em um grupo de amigos. Posteriormente, a informação acabou chegando ao conhecimento de seu empregador, que teme que o diagnóstico atrapalhe os negócios no estabelecimento, que envolve atendimento ao público, e o demite sob pretextos genéricos dias depois. A exposição do quadro de saúde mental também afeta a relação com o grupo do bairro onde praticava esportes e familiares, agravando sua situação de saúde mental. No caso relatado, houve violação da privacidade e dignidade, discriminação e estigma social, agravamento da vulnerabilidade econômica com a perda do emprego, além de prejuízo emocional. A partir da situação exposta, percebe-se que um vazamento de dados pode afetar severamente a vida de um(a) titular.

BOAS PRÁTICAS

Seguem algumas sugestões de boas práticas que podem ser adotadas no contexto organizacional:

POLÍTICA DE MESA LIMPA : Determinação de que o posto de trabalho permaneça organizado, sem informações sigilosas expostas.

CONTROLE DE ACESSO : Limitar o acesso aos dados apenas ao agentes necessários.

NÃO REAPROVEITAR SENHAS : Não utilize uma mesma senha para diferentes sistemas.

REVISE CUIDADOSAMENTE CONTEÚDO DE IA : Usar IA contratada como ferramenta de apoio, mas revisar sempre o conteúdo gerado.

NÃO ACEITAR POP-UPS SEM VERIFICAR : Verificar pop-ups, ler mensagens de aviso.

UTILIZAÇÃO DE DADOS PARA A FINALIDADE, SOMENTE PELO TEMPO NECESSÁRIO : Atentar para utilizar somente para a finalidade, pelo mínimo de tempo necessário.

DISPOSITIVOS PESSOAIS : Não armazenar dados pessoais de titulares de atendimentos e demais informações correlatas em dispositivos particulares.

USE AS PLATAFORMAS INSTITUCIONAIS : Utilize as plataformas institucionais para assuntos relacionados à DPE-PR.

PLATAFORMAS DE IA EXTERNAS : Se utilizar ferramentas externas, anonimizar dados pessoais. Não inserir dados pessoais de servidores e assistidos, tampouco dados sigilosos.

NA PRÁTICA

Luiza é servidora pública, entusiasta de tecnologia. Utiliza os diferentes recursos tecnológicos da instituição para aprimorar seu trabalho e participa de todos os treinamentos. Ao se cadastrar nos sistemas, atenta-se para cadastrar senhas diferentes, não reaproveitando anteriores, e não deixa as senhas salvas no navegador. Na execução das atividades institucionais, utiliza apenas o aplicativo de mensagens contratado e pede aos colegas que a contatem por meio oficial. Quando realiza atendimentos, utiliza os dispositivos institucionais e coleta apenas o estritamente necessário para atingir a finalidade. Ela é um exemplo!

NÃO COMPARTILHE LOGIN/SENHA : Não “empreste sua conta” para outra pessoa. Cada um deve ter seu acesso individual.

NÃO DEIXE SENHA ANOTADA EM PAPÉIS OU COLADA EM MONITORES : Zelar por suas credenciais, manter em sigilo.

NÃO CLICAR EM LINKS SUSPEITOS : Fique atento ao conteúdo das mensagens e nunca clique em links de fontes desconhecidas ou suspeitas.

ELIMINE RASCUNHOS : Triture, rasgue, delete. Não reaproveite rascunhos que tiverem dados pessoais ou pessoas sensíveis.

BLOQUEIO DE TELA OU ENCERRAMENTO DE SESSÃO : Ao se afastar do local de trabalho, bloquear a tela. Medidas de bloqueio de tela ou encerramento de sessão de forma automática (configuração de tempo-limite).

NÃO DEIXAR SENHAS SALVAS NO NAVEGADOR OU APPS : Fazer autenticação a cada acesso. De preferência, com duplo-fator.

HIGINIZAÇÃO DE DADOS NO DISPOSITIVO APÓS O USO : Exclusão de dados dos dispositivos após a utilização (arquivos, histórico, credenciais salvas, cache)

NA PRÁTICA

CONTRA-EXEMPLO: Theo é estagiário da Defensoria Pública e utilizou um smartphone para suporte aos atendimentos em um mutirão. Durante o período, coletou diversos dados pessoais dos(as) assistidos(as), alguns dados pessoais sensíveis, e mesmo repassando os dados coletados para o sistema SOLAR, deixou arquivos originais no dispositivo, pois ele não realizou a eliminação dos dados (processo de higienização de dados). Ao retornar, quando estava próximo à sede, teve o smartphone furtado por uma mulher. Após o ocorrido, a criminosa conseguiu desbloquear o dispositivo furtado e teve acesso aos dados pessoais de alguns atendimentos. Em seguida, tentou contatar alguns(mas) assistidos(as) passando-se por uma defensora pública, solicitando dinheiro para a prestação dos serviços. Na situação relatada, o vazamento de dados pessoais desses assistidos poderia ter sido evitada com a prática da higienização de dados, logo após o uso.

CONSIDERAÇÕES FINAIS

Neste material foram apresentados os principais conceitos relacionados à privacidade e à proteção de dados pessoais, além de boas práticas que devem orientar o tratamento de informações no contexto institucional, com destaque para o relevante papel do setor público. Além de conceitos básicos da temática, também foram repassados algumas responsabilidades e indicações específicas no âmbito da Defensoria Pública do Estado do Paraná (DPE-PR).

Alguns casos práticos demonstrados tornam o tema mais próximo do cotidiano, exemplificando riscos, situações de vulnerabilidade e de impactos para titulares. Por isso, é importante lembrar que a efetividade desses conceitos e práticas depende do engajamento coletivo.

A cultura de privacidade e proteção de dados pessoais, pautada pela ética, pela segurança da informação e pelo respeito aos titulares, exige a colaboração de todos e todas: servidores(as), defensores(as), estagiários(as), terceirizados(as), ou seja, qualquer pessoa que tenha acesso, direta ou indiretamente, a dados pessoais no exercício de suas funções.

Vale ressaltar que os princípios apresentados aqui vão além da LGPD. Eles podem e devem ser aplicados no cotidiano institucional, influenciando outras práticas, como o atendimento humanizado, o sigilo profissional, o uso responsável da tecnologia e o respeito à autonomia dos usuários dos serviços públicos.

A privacidade e a proteção de dados pessoais surgem como aspecto de justiça, cidadania e efetivação de diretos. Portanto, é imprescindível que a Defensoria Pública do Estado do Paraná atue de acordo com a legislação e auxilie na garantia desse direito fundamental.

Contamos com sua colaboração!

SAIBA MAIS

Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)
Acesse a lei completa aqui

"I Ciclo de Palestras de Privacidade e Proteção de Dados Pessoais da DPE-PR"
Palestras abertas organizadas pela DPE-PR, com certificados de participação emitidos pela EDEPAR - Escola da Defensoria Pública do Estado do Paraná

- **Palestra de abertura** (link) | João Victor Rozatti Longhi
- **Introdução à privacidade e proteção de dados pessoais** (link)
  Rafael Zanatta e Mariana Rielli
- **Privacidade, proteção de dados pessoais e as Defensorias Públicas** (link)
  Sarah Gomes Sakamoto
- **Privacidade e proteção de dados pessoais como direito fundamental** (link)
  José Luiz de Moura Faleiros Júnior
- **Agentes de tratamento, responsabilidades e novas tecnologias** (link)
  Filipe José Medon Affonso
- **Privacidade e proteção de dados pessoais de crianças e adolescentes** (link)
  Chiara Antonia Spadaccini de Teffé

Curso "Introdução à Lei Brasileira de Proteção de Dados Pessoais" (link)
Curso gratuito oferecido pela ENAP - Escola Nacional de Administração Pública (10h)

Curso "Proteção de Dados Pessoais no Setor Público" (link)
Curso gratuito oferecido pela ENAP - Escola Nacional de Administração Pública (15h)

Curso "Lei Geral de Proteção de Dados e a Administração Pública" (link)
Curso gratuito oferecido pela EGP - Escola de Gestão do Paraná (40h)

Guia Primeiros Passos para Adequação das Defensorias Públicas à LGPD (clique aqui)
Guia de contextualização da adequação à realidade das DPEs, produzido pela Data Privacy Brasil a partir do projeto em parceria com as Defensorias Públicas

Material de leitura "Oficina prática de adequação à LGPD" (link)
Relatório do evento de intercâmbio de experiências de Defensorias Públicas acerca dos desafios para proteção de dados

Curso "Como implementar a LGPD: bases, mecanismos e processos" (link)
Curso gratuito oferecido pela ENAP - Escola Nacional de Administração Pública (25h)