PARANACIDADE

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DAS CIDADES

LGPD no PARANACIDADE:

tudo o que você sempre quis saber,

explicado de forma simples e acessível.

Serviço Social Autônomo PARANACIDADE.
Rua Eurípides Garcez do Nascimento, 1195 | 3 andar | Ahú | Curitiba/PR | CEP 80540-280 | 41 3350.3300

www.paranacidade.org.br

PARANACIDADE

PARANÁ
GOVERNO DO ESTADO
SECRETARIA DAS CIDADES

Serviço Social Autônomo PARANACIDADE

Guto Silva
Superintendente

Camila Mileke Scucato
Superintendente Executiva

Hélio Sabino Deitos
Diretor de Operações Estaduais

Jaime Antônio de Camargo Ferreira
Diretor de Operações Municipais

Francisco Luís dos Santos
Diretor de Administração e Finanças

SUMÁRIO

APRESENTAÇÃO

A **Lei Geral de Proteção de Dados Pessoais**, ou simplesmente **LGPD**, como é mais conhecida, entrou em vigor no Brasil com o propósito de estabelecer regras claras e responsáveis sobre o uso de informações que dizem respeito a cada um de nós.

A LGPD trata de algo muito valioso: os **dados pessoais**. E eles estão presentes em quase tudo o que fazemos.

Mas, se mesmo após a entrada em vigor da LGPD, você é uma daquelas pessoas que achou o seu conteúdo complicado demais ou nunca entendeu direito como isso se conecta com seu dia a dia ou com o trabalho que você realiza... não se preocupe! Você não está sozinho, e essa leitura é especialmente recomendada para você.

Este material foi pensado e criado para explicar, com clareza e sem juridiquês, o que você precisa saber para entender a LGPD. Ao longo das próximas páginas, você encontrará respostas para perguntas sobre essa temática tão importante. A ideia é essa: **responder aquilo que você sempre quis saber sobre a LGPD no PARANACIDADE, explicado de maneira simples e acessível.**

De forma prática, acessível e conectada à realidade do PARANACIDADE, serão abordados temas essenciais da LGPD: o que são dados

pessoais, quando a lei se aplica ou não, quem são os agentes de tratamento, quais são os direitos dos titulares, além dos fundamentos, princípios, bases legais e responsabilidades previstas.

A proteção de dados é parte essencial da confiança que as pessoas depositam em nós enquanto organização. Todos temos um papel importante na construção de um ambiente organizacional mais seguro, transparente e responsável no uso de informações que tratamos diariamente. Por essa razão, este material tem como principal objetivo **fortalecer a cultura organizacional de proteção de dados no PARANACIDADE.**

Sempre que uma informação se conecta diretamente a uma pessoa natural, ela deixa de ser apenas um dado e passa a expressar traços da sua identidade, da sua trajetória e da sua dignidade. Proteger os dados pessoais é, portanto, proteger aquilo que torna cada pessoa única.

Porque, no final das contas, cuidar dos dados é cuidar das pessoas e esse compromisso começa com cada um de nós.

Espero que este documento seja útil, acessível e inspirador.

Boa leitura!

Ademir Lopes dos Santos Paz
Analista de Desenvolvimento Municipal
Encarregado pelo tratamento dos dados pessoais
Portaria nº 010/2021

O QUE É A LGPD?

A **LGPD**, sigla para **Lei Geral de Proteção de Dados Pessoais**, é a Lei nº 13.709, de 14 de agosto de 2018. Embora tenha sido sancionada em 2018, a LGPD entrou em vigor efetivamente em 18 de setembro de 2020, com exceção das sanções administrativas, que só passaram a valer em 1º de agosto de 2021.

Desde então, a LGPD é a legislação brasileira que define regras sobre como os dados pessoais devem ser tratados. Isso inclui desde a coleta e o armazenamento até o uso, o compartilhamento e a proteção dessas informações, seja no meio físico ou digital, por pessoas físicas ou jurídicas, públicas ou privadas.

A LGPD foi inspirada no Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation – GDPR), em vigor desde 2018. Muitos países, incluindo o Brasil, seguiram esse mesmo caminho, criando leis semelhantes para garantir mais segurança no uso de dados pessoais.

E o que significa “tratar” dados pessoais?

De acordo com a LGPD, o termo tratamento tem um sentido amplo e abrange todas as operações realizadas com dados pessoais, como: **coletar, produzir, receber, classificar, utilizar, acessar, transmitir, reproduzir, armazenar, eliminar, avaliar, compartilhar, arquivar**, entre outras.

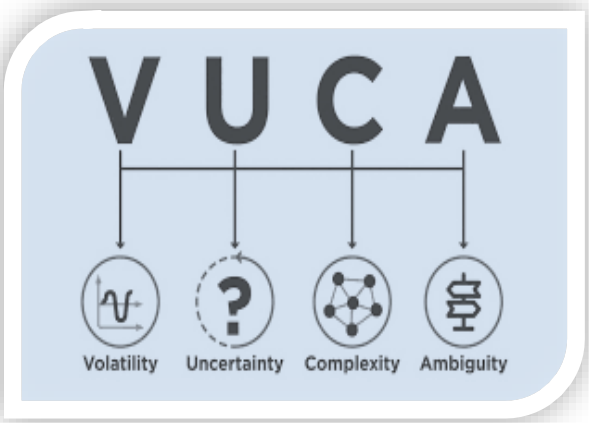
Ou seja, **qualquer ação que envolva dados pessoais, do momento em que são recebidos até o seu descarte, é considerada tratamento.** Isso vale tanto para documentos **digitais** quanto **físicos**. Com isso, fica claro que praticamente todas as áreas e colaboradores de uma organização tratam dados pessoais no seu cotidiano, e por isso estão sujeitos às regras da LGPD.

Importante destacar que a **LGPD não proíbe o uso de dados pessoais**. O que ela faz é organizar esse uso, estabelecendo critérios, limites e responsabilidades. Ela determina que tratar dados pessoais exige cuidado, fundamento legal e respeito aos direitos das pessoas envolvidas.

Mas afinal, por que uma lei para isso?

A LGPD não surgiu por acaso. Ela foi criada em resposta a um cenário de profundas transformações sociais, tecnológicas e organizacionais.

Vivemos no que especialistas chamam de mundo VUCA, um ambiente volátil, incerto, complexo e ambíguo, em que nossas informações pessoais circulam com rapidez em redes sociais, cadastros, formulários, plataformas, aplicativos e sistemas diversos.



Esse crescimento no uso de dados trouxe muitas oportunidades, mas também novos riscos, exigindo mais proteção, responsabilidade e transparência. A LGPD busca responder a esse contexto, preservando direitos fundamentais como **a liberdade, a privacidade, a dignidade e o livre desenvolvimento da personalidade**. Ela reconhece que dados pessoais são valiosos e que o seu uso exige respeito, cautela e compromisso ético.

Muito mais que uma lei: uma mudança de comportamento

Entender a LGPD, portanto, vai além de conhecer uma norma jurídica. Trata-se de compreender um novo jeito de pensar e agir: com mais consciência, empatia e responsabilidade em relação às informações de outras pessoas. **Esses valores se tornaram centrais nas relações humanas e institucionais**.

O termo **VUCA** surgiu no final dos anos 1980 e início dos anos 1990, após a Guerra Fria, no U.S. Army War College, para descrever o novo cenário global que ser formava. Um cenário de transformações rápidas, desafiadoras e, muitas vezes, difíceis de prever. A sigla, em inglês, reúne quatro características que ajudam a entender esse contexto: ***V**olatility* (volatilidade), ***U**ncertainty* (incerteza), ***C**omplexity* (complexidade) e ***A**mbiguity* (ambiguidade). Em ambientes **voláteis**, as mudanças acontecem de forma acelerada e nem sempre seguem padrões previsíveis. Já a **incerteza** diz respeito à dificuldade de antecipar o que pode acontecer, mesmo com informações disponíveis. A **complexidade** aparece quando há muitos fatores interligados, exigindo atenção a diferentes variáveis ao mesmo tempo. E a **ambiguidade** surge quando a interpretação dos fatos não é clara e um mesmo evento pode ter diferentes significados, dependendo do ponto de vista. Esse conceito ajuda a compreender os desafios do presente e reforça a importância de desenvolver estratégias mais ágeis, conscientes e preparadas para lidar com contextos imprevisíveis.

Para que a proteção de dados faça sentido, é preciso entender os **fundamentos** que sustentam essa responsabilidade. Afinal, eles representam a razão da existência da LGPD. No próximo capítulo, você conhecerá esses fundamentos e entenderá por que eles estão diretamente ligados à dignidade, ao respeito e à confiança nas relações institucionais.

OS FUNDAMENTOS DA PROTEÇÃO DE DADOS

Quando uma organização trata dados pessoais, ela está lidando com a confiança de pessoas reais. São informações que dizem respeito à vida, às escolhas e à identidade de cada pessoa. O cuidado com esses dados não é apenas uma exigência legal, é um compromisso com a ética e a responsabilidade.

É por isso que a proteção de dados se apoia em **fundamentos**. São esses fundamentos que dão sentido à LGPD, sustentam sua lógica e explicam por que proteger dados é tão importante. **Eles ajudam a construir relações de confiança entre pessoas e organizações**. Mostram que é possível utilizar dados para melhorar serviços, atender demandas e tomar decisões, sempre com responsabilidade, ética e respeito.

Quais são esses fundamentos?

Os fundamentos da proteção de dados representam a razão de existir da LGPD. São valores que orientam o uso responsável das informações pessoais no contexto de qualquer organização. Esses fundamentos reforçam que, ao lidar com dados pessoais, é preciso garantir: **o respeito à privacidade das pessoas; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; os**

direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Esses fundamentos mostram, portanto, que proteger dados pessoais é mais do que cumprir uma regra: **é garantir que as pessoas sejam respeitadas em sua individualidade e tratadas com responsabilidade**.

E como isso se conecta com o PARANACIDADE?

No PARANACIDADE, os fundamentos da proteção de dados estão diretamente ligados ao compromisso organizacional com a ética, a

integridade e a qualidade das nossas ações. Eles orientam como os dados devem ser tratados, sempre com responsabilidade, clareza e respeito às pessoas.

Essa postura fortalece a confiança nas relações institucionais e contribui para a prevenção de riscos jurídicos, operacionais e reputacionais. Mais do que cumprir a lei, trata-se de **incorporar valores na cultura organizacional do PARANACIDADE**.

Fundamentos, princípios e bases legais são a mesma coisa?

É comum confundir esses conceitos, mas eles têm papéis **diferentes** no contexto da LGPD:

Os fundamentos explicam **por que** a proteção de dados existe;

As bases legais indicam em **quais** situações o tratamento é permitido;

Os princípios orientam **como** os dados devem ser tratados.

Entender essa diferença é essencial para aplicar corretamente a LGPD no dia a dia do PARANACIDADE.

A Política de Governança Organizacional do PARANACIDADE, em seu artigo 10, inciso XXXIX contempla a diretriz que trata do compromisso da organização com a privacidade e a proteção dos dados pessoais. Esse compromisso envolve a adoção de boas práticas de governança de dados com o objetivo de promover um ambiente físico e digital mais seguro e sustentável, o que **demonstra forte conexão com os fundamentos da LGPD**.

No próximo capítulo, a conversa é sobre um tema que está no centro da LGPD: os **dados pessoais**. Você já parou para pensar o que, de fato, são esses dados e por que eles são tão importantes no contexto de uma organização?

O QUE SÃO DADOS PESSOAIS?

A LGPD gira em torno de um conceito-chave: **dados pessoais**. Entender o que esse termo significa é o ponto de partida para aplicar a lei de forma adequada no dia a dia de qualquer organização.

Dados pessoais são **informações relacionadas a uma pessoa natural identificada ou identificável**. Isso inclui tanto dados que identificam alguém diretamente, como nome ou CPF, quanto aqueles que, quando combinados com outros, tornam possível reconhecer uma pessoa específica.

Estes são alguns exemplos de dados pessoais: **nome e sobrenome; RG, CPF, CNH, título de eleitor; data de nascimento; endereço (residencial, comercial ou eletrônico); número de telefone; imagem (fotografia, vídeo), voz gravada; localização em tempo real (GPS); matrícula funcional, prontuário ou número de registro interno; endereço IP, cookies, identificadores de dispositivos.**

Essas informações podem estar registradas em arquivos **digitais**, como sistemas, planilhas e formulários eletrônicos, ou mesmo em documentos **físicos**. O meio de armazenamento não importa: se for possível identificar uma pessoa, o dado é considerado pessoal.

Dados pessoais sensíveis: atenção redobrada

A LGPD traz uma categoria especial de dados: os **dados pessoais sensíveis**. São informações que, se tratadas de forma inadequada, podem causar discriminação, constrangimento ou prejuízos à dignidade da pessoa. Ou seja, são dados que implicam riscos e vulnerabilidades potencialmente mais graves aos direitos e liberdades fundamentais dos titulares.

São considerados dados sensíveis: **origem racial ou étnica; crença religiosa; opinião política; filiação a sindicato, organização religiosa, filosófica ou política; saúde, vida sexual; dados genéticos ou biométricos, quando vinculados a uma pessoa natural**.

O tratamento desses dados exige regras mais rigorosas para coleta, uso e compartilhamento. Em geral, só podem ser tratados com **consentimento específico e destacado do titular, para finalidades claramente determinadas**.

Dados de crianças e adolescentes: proteção reforçada

Crianças e adolescentes recebem proteção reforçada da LGPD, por serem mais vulneráveis e estarem em fase de desenvolvimento.

Importante destacar que, de acordo com a Lei nº 8.069/1990, conhecida pelo Estatuto da Criança e do Adolescente ou, simplesmente, ECA, **criança** é a pessoa com até 12 (doze) anos incompletos, e **adolescente** é aquela entre 12 e 18 anos incompletos. Assim, ao tratar dados desse grupo, deve-se sempre observar o melhor interesse da criança e do adolescente.

Atenção para as regras:

Para **crianças**, é obrigatório o **consentimento específico e destacado** de pelo menos um dos pais ou responsáveis;

Para **adolescentes**, é suficiente a obtenção do seu **próprio consentimento**, desde que respeitados os princípios da proteção integral previstos no ECA.

As informações fornecidas devem ser sempre apresentadas de forma simples, clara e acessível, **adequada à faixa etária da criança ou do adolescente**.

Mas o que é “consentimento específico e destacado”?

É a autorização expressa que a pessoa natural fornece para o uso de seus dados, com três características fundamentais:

Clareza: sem ambiguidades ou linguagem técnica excessiva;

Especificidade: para uma finalidade determinada e transparente;

Destaque: visualmente separado do restante do texto, de forma que o titular consiga perceber com facilidade.

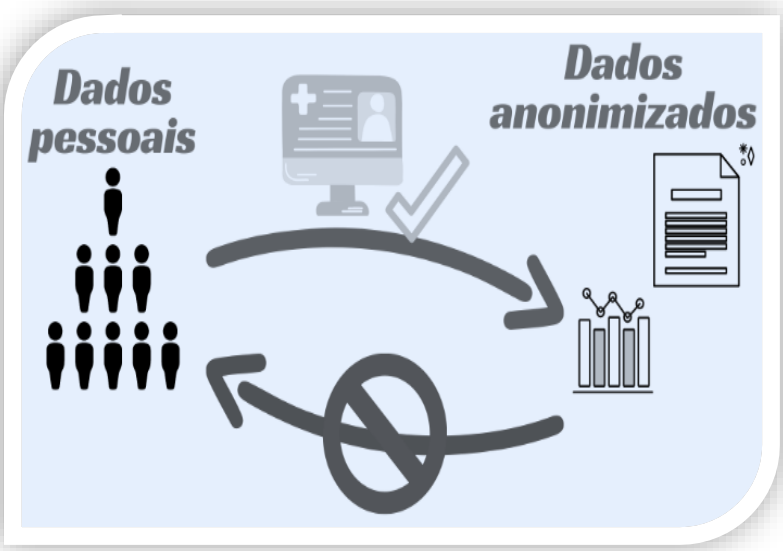
Esse tipo de consentimento garante que a pessoa compreenda de fato para que está autorizando o uso dos seus dados, especialmente importante em contextos de dados sensíveis ou envolvendo menores de idade.

Dados anonimizados: estão fora da LGPD?

A LGPD considera **dados anonimizados** aqueles que passaram por um processo técnico que os torna **não identificáveis**, mesmo com uso de tecnologias ou informações adicionais. Por meio da anonimização, ocorre a quebra do vínculo entre o dado e a pessoa natural a que ele se referia.

Exemplo prático

Um relatório estatístico com dados agregados sobre hábitos de consumo, sem qualquer possibilidade de identificar as pessoas envolvidas.



Esses dados **não estão sujeitos à LGPD**, desde que a anonimização seja verdadeira e **irreversível**. Se houver qualquer possibilidade de reidentificação, mesmo que remota, a proteção prevista na LGPD continua sendo exigida.

Pseudonimização: o dado ainda está lá, mas oculto

A pseudonimização é uma técnica que substitui informações identificadoras por códigos ou outros elementos que dificultam a identificação direta da pessoa, mas **sem eliminar completamente essa possibilidade**. Ou seja, os dados continuam sendo pessoais e, por isso, **seguem protegidos pela LGPD**.

Exemplo prático

Um sistema que substitui os nomes de alunos por números ou siglas internas, mas mantém uma chave de referência que pode reidentificar a pessoa, se necessário.

Aluno	Nota	Horas de estudo
Pedro Silva	10,0	55
Maria Eduarda	7,0	40
Lucas Lima	9,0	42
Carlos Melo	8,5	50
Beatriz Gomes	6,0	30

Aluno	Nota	Horas de estudo
12576	10,0	55
34861	7,0	40
21067	9,0	42
48007	8,5	50
36902	6,0	30

VOCÊ SABIA?

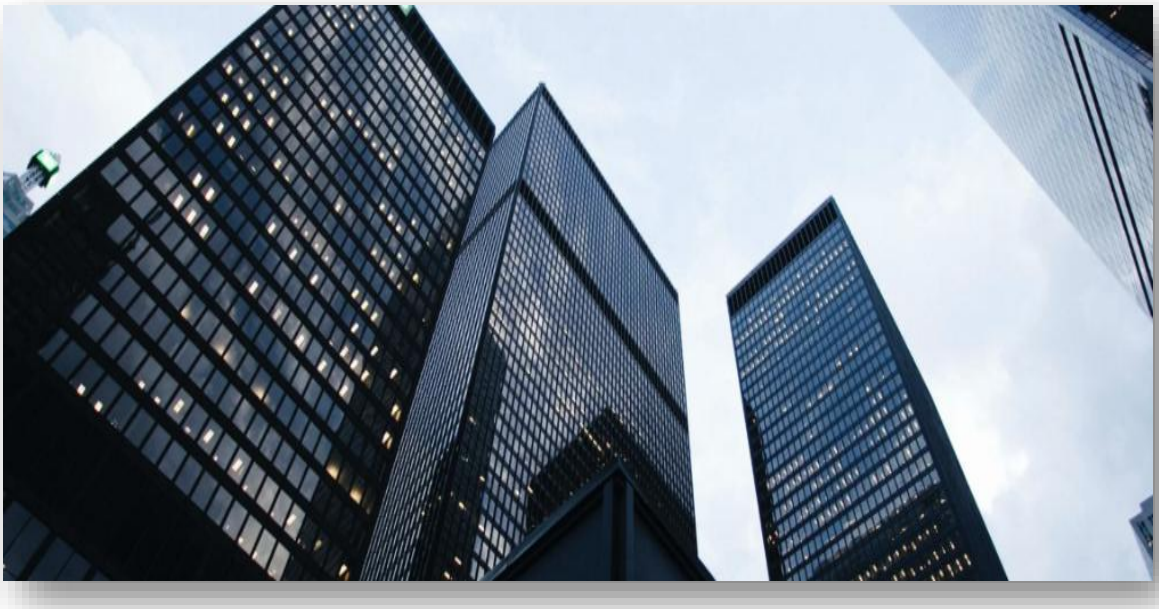
A expressão **"dados pessoais"** aparece **150 vezes** no texto da LGPD. Isso mostra o quanto esse conceito é fundamental para a aplicação da lei e está presente em praticamente todos os seus artigos.

Agora que você já sabe o que são dados pessoais, o próximo passo é entender se **a LGPD se aplica à realidade do PARANACIDADE**. A resposta envolve mais do que uma simples afirmação: trata-se de compreender as responsabilidades legais que acompanham o tratamento de dados na nossa organização.

A LGPD SE APLICA AO PARANACIDADE?

É comum pensar que a LGPD foi criada apenas para regular grandes empresas de tecnologia, redes sociais ou o comércio eletrônico. Mas a verdade é que a LGPD se aplica a **qualquer organização** que trate dados de pessoas naturais, independentemente de ser pública ou privada, de grande ou pequeno porte, com ou sem fins lucrativos.

Sempre que uma organização coleta, utiliza, compartilha, arquiva ou simplesmente acessa informações que permitam identificar uma pessoa física, ela está realizando um tratamento de dados pessoais. E isso significa que precisa seguir os cuidados e deveres estabelecidos pela LGPD. Não importa a tecnologia utilizada para a realização do tratamento, seja por meio **digital** ou **físico**, com o uso de inteligência artificial, de forma automatizada ou manualmente.



Aplicação nacional e internacional

A LGPD se aplica, principalmente, a operações de tratamento realizadas no Brasil ou que envolvam dados de pessoas localizadas no território nacional. Mas sua aplicação vai além das fronteiras: mesmo que o tratamento ocorra em outro país, as regras da LGPD continuam valendo quando houver conexão com o contexto brasileiro.

Em resumo, a LGPD se aplica sempre que uma ou mais destas situações ocorrerem:

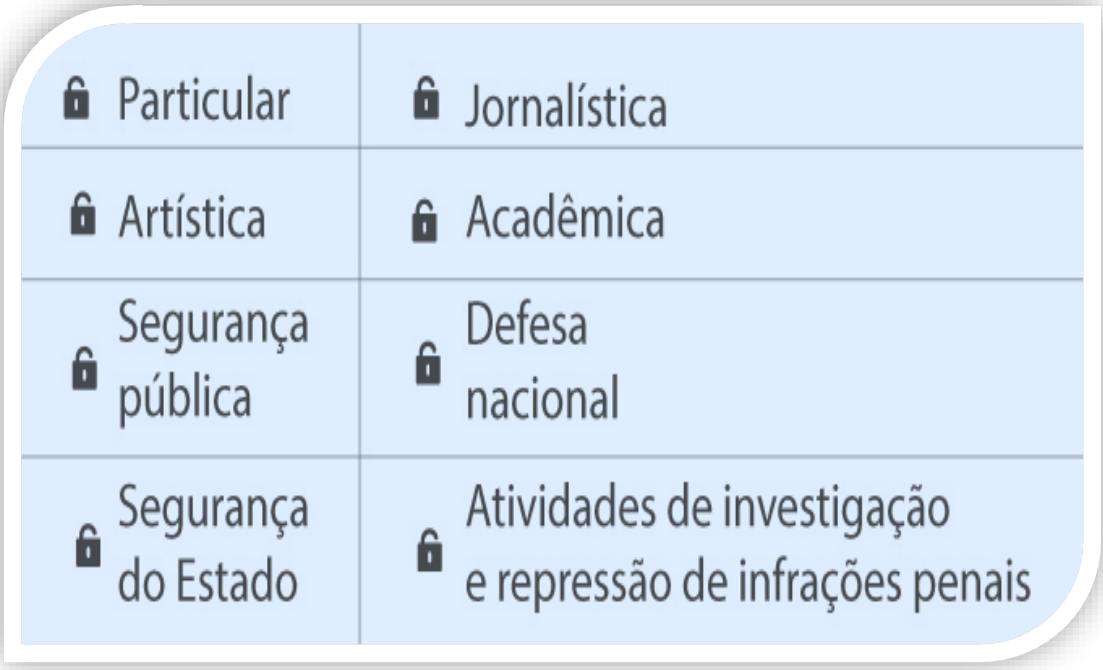
O tratamento acontece em território nacional;

Os dados se referem a pessoas localizadas no Brasil;

As informações foram coletadas no país, ainda que armazenadas fora dele.

E quando a LGPD não se aplica?

Também é importante saber em que situações a LGPD não é aplicável. A LGPD não alcança: **dados utilizados por pessoa física para fins exclusivamente particulares e não econômicos; informações tratadas com propósitos exclusivamente jornalísticos, acadêmicos ou artísticos; situações relacionadas à segurança pública, defesa nacional ou segurança do Estado; dados que identificam exclusivamente pessoas jurídicas, como CNPJ, razão social ou nome fantasia; informações técnicas, algoritmos, planos estratégicos e segredos industriais, desde que não vinculados a pessoas naturais**.



Esses casos não significam ausência total de proteção, mas indicam que, nessas situações específicas, **a LGPD não é o instrumento regulador aplicável.**

E no caso do PARANACIDADE?

O PARANACIDADE é uma organização de direito privado, sem fins lucrativos, com atuação de interesse público. Sua missão inclui o apoio técnico e operacional ao desenvolvimento urbano e regional dos municípios paranaenses, por meio da gestão de recursos, projetos e ações estratégicas que contribuem para o desenvolvimento sustentável.

Durante a execução de suas atividades, o PARANACIDADE lida frequentemente com dados pessoais. Isso ocorre, por exemplo, quando há: **cadastro e gerenciamento de colaboradores, estagiários, residentes, fornecedores, consultores; trocas de e-mails e mensagens com representantes municipais e parceiros institucionais; preenchimento de formulários, planilhas, relatórios e sistemas internos; celebração e acompanhamento de convênios e contratos administrativos**.

Essas situações fazem parte da rotina do PARANACIDADE e, por envolverem dados pessoais, precisam seguir os critérios e cuidados exigidos pela LGPD.

Portanto, a resposta à pergunta que dá nome a este capítulo é simples e direta: **sim, a LGPD se aplica ao PARANACIDADE**.

E o que isso significa, na prática?

Significa que o PARANACIDADE tem o dever legal e ético de proteger essas informações. A LGPD impõe responsabilidades, mas também oferece diretrizes para realizar esse cuidado da maneira certa, com segurança e transparência. No contexto do PARANACIDADE, envolve:

Garantir que os dados coletados tenham uma finalidade clara e legítima;

Adotar medidas de segurança para proteger essas informações;

Respeitar os direitos das pessoas a quem os dados pertencem;

Evitar acessos indevidos, vazamentos ou usos desnecessários;

Agir com responsabilidade, transparência e atenção em todas as etapas do tratamento.

Proteger os dados pessoais é uma medida essencial para fortalecer a confiança, reduzir riscos e assegurar que as atividades do PARANACIDADE estejam alinhadas às melhores práticas de transparência e governança.

Um compromisso que envolve toda a organização

A proteção de dados não é responsabilidade exclusiva de uma área técnica, jurídica ou da figura do Encarregado. No PARANACIDADE, a atuação conjunta de todas as equipes e colaboradores é essencial para o cumprimento da LGPD.

Quem preenche uma planilha com nomes e contatos, organiza pastas com documentos, responde mensagens que contenham informações pessoais ou elabora relatórios com dados identificáveis está lidando com dados pessoais.

A proteção dessas informações começa com consciência e atenção. E se fortalece quando isso se transforma em **cultura organizacional**. Por isso, a proteção de dados deve estar presente em cada ação realizada pelos colaboradores do PARANACIDADE, desde os pequenos gestos até as grandes decisões.

O PARANACIDADE utiliza diariamente ferramentas cujos servidores podem estar localizados fora do Brasil. Ainda assim, os dados tratados nessas plataformas, como documentos, planilhas, e-mails e registros institucionais, continuam **protegidos pela LGPD**, justamente porque se referem a pessoas situadas no território nacional. Ou seja: não importa onde os dados estão armazenados fisicamente. Quando há conexão com o contexto brasileiro, as regras da LGPD permanecem aplicáveis.

No próximo capítulo, o conteúdo avança para mostrar quem são os **agentes envolvidos no tratamento de dados pessoais**. Conhecer esses papéis, inclusive o seu, ajuda a entender melhor as responsabilidades, as funções e a participação de cada um nessa estrutura.

AGENTES DE TRATAMENTOS E SEUS PAPÉIS

Quando uma organização trata dados pessoais, diferentes áreas e profissionais podem estar envolvidos. Para garantir que tudo ocorra com responsabilidade, ética e clareza, a LGPD define papéis centrais, conhecidos como **agentes de tratamento**.

A definição de quem faz o quê na posição de agente de tratamento é importante para estabelecer obrigações e responsabilidades de quem participa do processo de tratamento de dados. Assim, cada agente precisa adotar processos internos, medidas técnicas, controles administrativos e políticas que garantam o tratamento adequado das informações sob sua responsabilidade.

Quem são os agentes de tratamento?

A LGPD reconhece dois agentes principais no processo de tratamento de dados: o **controlador** e o **operador**.

Controlador

É quem tem competência **para tomar as decisões referentes ao tratamento dos dados pessoais**. Decide, por exemplo, o motivo pelo qual os

dados serão coletados, como serão usados e por quanto tempo serão armazenados.

No PARANACIDADE, a organização atua, na maioria dos casos, como controladora dos dados que trata, como ocorre no gerenciamento de dados dos colaboradores, fornecedores e gestores municipais.

Operador

É quem **realiza o tratamento de dados em nome do controlador**, seguindo suas orientações. Pode ser uma empresa contratada ou um prestador de serviço. No contexto do PARANACIDADE, o operador pode ser, por exemplo, empresas responsáveis pela hospedagem de sistemas ou um prestador de serviços de tecnologia da informação que armazena dados para a nossa organização.

VOCÊ SABIA?

A LGPD também traz a figura do **Encarregado pelo tratamento de dados pessoais**. É a pessoa responsável por atuar como canal de comunicação entre o PARANACIDADE, os titulares dos dados e a Agência Nacional de Proteção de Dados (ANPD). Essa função também é conhecida internacionalmente como **DPO**, sigla em inglês para **Data Protection Officer**, expressão utilizada no Regulamento Geral de Proteção de Dados da União Europeia (General Data Protection Regulation – GDPR) e amplamente adotada como referência em boas práticas globais de governança de dados. Além de cumprir com essa função institucional, também exerce um papel educativo e de orientação interna nas organizações, promovendo a adoção de boas práticas e o uso correto e responsável de dados pessoais. No PARANACIDADE, você pode falar diretamente com o Encarregado pelo email institucional falecomodpo@paranacidade.org.br.

Sempre que surgirem dúvidas, sugestões ou questionamentos relacionados sobre a temática da proteção de dados no PARANACIDADE, esse canal está disponível.

No próximo capítulo, você vai entender o que permite o tratamento de dados ser feito de forma legítima. São as chamadas **bases legais** e elas definem se uma ação com dados é ou não permitida no contexto da LGPD.

BASES LEGAIS PARA O TRATAMENTO DE DADOS

Para que uma organização possa tratar dados pessoais de forma legítima, é necessário haver uma **base legal**, ou seja, uma justificativa que autorize a coleta, o uso, o armazenamento ou qualquer outra operação com esses dados.

As bases legais são **hipóteses autorizadoras** descritas na LGPD que legitimam o uso de informações pessoais, garantindo que o tratamento ocorra dentro de critérios bem definidos.

No contexto do PARANACIDADE, compreender corretamente essas bases é fundamental para assegurar segurança jurídica, transparência e responsabilidade institucional nas atividades que envolvem dados pessoais.

Mapear a base legal é uma etapa essencial do tratamento

Sempre que for realizado o tratamento de dados pessoais, deve-se identificar, com clareza, qual é a base legal que justifica essa ação. Essa identificação deve estar registrada e acessível, especialmente para fins de auditoria, revisão ou eventuais questionamentos.

No PARANACIDADE, foi conduzido o mapeamento de **111 processos organizacionais**, todos com suas respectivas bases legais registradas.

Essa prática resultou no documento denominado RoPA (Record of Processing Activities), que registra as operações de tratamento, integra a governança de dados e fortalece a cultura de proteção de dados pessoais na nossa organização.

As hipóteses legais que autorizam o tratamento de dados pessoais

A LGPD estabelece **10 (dez) hipóteses** que legitimam o tratamento de dados pessoais. Toda organização, inclusive o PARANACIDADE, deve respeitar essas bases para assegurar que o uso de dados seja ético, seguro e dentro dos limites legais.

A seguir, conheça cada uma dessas hipóteses em que o tratamento de dados pessoais é permitido:

1. Consentimento do titular

Quando a pessoa titular autoriza, de forma livre, informada e inequívoca, o uso de seus dados para uma finalidade específica previamente informada.

2. Cumprimento de obrigação legal ou regulatória

Quando o tratamento é necessário para atender exigências previstas em normas legais, como envio de informações a órgãos de controle ou manutenção de registros obrigatórios.

3. Execução de políticas públicas

Aplica-se quando os dados são utilizados em programas, ações ou iniciativas ligadas às funções institucionais da organização, com foco em atender demandas da sociedade.

4. Realização de estudos por órgãos de pesquisa

Autoriza o uso de dados para fins científicos, estatísticos ou históricos, sempre que possível com técnicas de anonimização que impeçam a identificação do titular.

5. Execução de contratos ou procedimentos preliminares

Refere-se ao tratamento necessário para formalizar ou executar contratos firmados com o titular dos dados ou com pessoas interessadas em sua celebração.

6. Exercício regular de direitos

Permite o uso de dados em processos administrativos, judiciais ou arbitrais, incluindo situações em que a organização precise comprovar direitos ou obrigações.

7. Proteção da vida ou da integridade física

Base aplicável a situações emergenciais em que o tratamento de dados é essencial para proteger a vida ou a integridade física de alguém.

8. Tutela da saúde

Autorização voltada a tratamentos realizados por profissionais da saúde, serviços médicos ou autoridades sanitárias, visando à proteção e cuidado com a saúde.

9. Legítimo interesse do controlador ou de terceiros

Admite o tratamento de dados quando houver uma justificativa legítima e proporcional, desde que não se sobreponha aos direitos e liberdades do titular.

10. Proteção do crédito

Base que autoriza o uso de dados com a finalidade de viabilizar a análise ou proteção do crédito do titular, conforme as regras aplicáveis ao setor.

Importante destacar que essas **hipóteses não são meras sugestões**. Elas são **taxativas**. Isso significa que **nenhum tratamento de dados pode ser realizado fora dessas situações previstas**. Sempre que houver tratamento de dados pessoais, é obrigatório identificar claramente em qual dessas hipóteses ele se enquadra. Caso contrário, o tratamento será considerado irregular, mesmo que não haja intenção de causar danos.

Consentimento nem sempre é a base legal mais adequada

É comum imaginar que o tratamento de dados sempre depende do **consentimento do titular**. Na verdade, essa é apenas uma das hipóteses legais, e pode não ser a mais segura ou viável em determinados contextos institucionais.

No caso do PARANACIDADE, por exemplo, não há necessidade de solicitar consentimento quando o tratamento se baseia em obrigações legais,

políticas públicas ou contratos. Nessas situações, outras bases legais são mais apropriadas.

O consentimento deve ser utilizado apenas quando nenhuma das demais hipóteses se aplica. Além disso, ele precisa ser livre, informado, específico e revogável a qualquer momento.

Um mesmo dado pode ser tratado com base em diferentes hipóteses legais, dependendo do contexto e da finalidade. Por exemplo, o endereço de um colaborador pode ser utilizado tanto para cumprir uma obrigação trabalhista quanto para executar um contrato. O essencial é que a base escolhida esteja bem justificada e documentada.

Entender as hipóteses legais é um passo importante, mas não é tudo. Além de ter uma base válida, o tratamento de dados deve seguir **princípios** que orientam como esse processo deve ocorrer. É isso que será abordado no próximo capítulo: os princípios da LGPD e como eles estruturam o uso responsável das informações pessoais.

PRINCÍPIOS DA LGPD

A proteção de dados pessoais vai além do cumprimento de regras. Ela envolve um compromisso com valores éticos e condutas responsáveis no dia a dia da organização. É justamente esse compromisso que a LGPD traduz por meio dos **princípios**.

Esses princípios funcionam como uma **bússola que indica como os dados devem ser tratados** em todas as etapas, da coleta ao descarte. Eles não apenas orientam a tomada de decisão, como também moldam o comportamento organizacional diante do uso de informações pessoais.

Em outras palavras, mesmo quando há uma a base legal e uma finalidade legítima, **o tratamento de dados só será considerado adequado se também estiver alinhado aos princípios da LGPD**.

Por que os princípios são indispensáveis?

Em ambientes organizacionais, as decisões sobre dados nem sempre são simples. Muitas vezes, há diferentes caminhos possíveis. Os princípios existem justamente para oferecer um ponto de referência seguro e confiável quando surgem dúvidas sobre e como fazer.

Respeitar esses princípios significa:

Atuar com integridade e respeito à privacidade das pessoas;

Evitar o uso indevido, exagerado ou desnecessário de dados;

Fortalecer a confiança entre a organização e seus públicos de relacionamento;

Prevenir riscos legais, reputacionais e operacionais;

Construir uma cultura organizacional alinhada à ética e à transparência.

Organizações que seguem os princípios da LGPD demonstram maturidade institucional, comprometimento com boas práticas e zelo com informações que não lhes pertencem, mas que estão sob sua responsabilidade.

Os 10 princípios da LGPD

A seguir, apresenta-se os **10 (dez) princípios** da LGPD que devem ser observados sempre que houver qualquer tipo de tratamento de dados pessoais.

1. Finalidade

O tratamento de dados deve ser realizado para propósitos legítimos, específicos, explícitos e previamente informados ao titular.

Não é permitido utilizar os dados posteriormente para finalidades distintas, incompatíveis ou genéricas. Esse princípio exige clareza e objetividade na definição do motivo pelo qual os dados estão sendo tratados.

2. Adequação

Impõe que o tratamento esteja em conformidade com as finalidades informadas ao titular, respeitando o contexto da coleta e do uso dos dados.

Ou seja, os dados só podem ser utilizados de forma que seja coerente com o motivo original de sua coleta.

3. Necessidade

Determina que o tratamento seja limitado ao mínimo necessário para alcançar sua finalidade.

Os dados tratados devem ser pertinentes, proporcionais e não excessivos, restringindo-se aos elementos indispensáveis à realização do objetivo legítimo declarado.

4. Livre Acesso

Garante ao titular o direito de consultar, de forma facilitada e gratuita, informações completas sobre o tratamento de seus dados pessoais.

Essa consulta inclui a forma como os dados são tratados, sua duração e o conteúdo integral das informações armazenadas.

5. Qualidade dos Dados

Exige que os dados pessoais sejam exatos, claros, relevantes e atualizados, sempre de acordo com a necessidade e com a finalidade do tratamento.

É responsabilidade do agente de tratamento garantir a integridade e a correção das informações durante todo o ciclo de uso dos dados.

6. Transparência

Assegura que os titulares recebam informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados e sobre os agentes responsáveis por esse tratamento.

A transparência deve ser garantida sem prejudicar segredos comerciais ou industriais, preservando o equilíbrio entre o direito à informação e a proteção de interesses legítimos da organização.

7. Segurança

Impõe a adoção de medidas técnicas e administrativas apropriadas para proteger os dados pessoais contra acessos não autorizados, bem como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

O princípio da segurança exige que a organização atue de forma preventiva, contínua e estruturada.

8. Prevenção

Reforça o dever de adotar medidas proativas com o objetivo de evitar a ocorrência de danos aos titulares em decorrência do tratamento de dados pessoais.

Trata-se de uma postura preventiva e antecipatória, que exige avaliação de riscos e implementação de práticas de mitigação.

9. Não Discriminação

Estabelece a proibição do tratamento de dados pessoais para fins discriminatórios, ilícitos ou abusivos.

É vedado utilizar os dados como base para qualquer tipo de tratamento que possa promover desigualdades, injustiças ou exclusões indevidas.

10. Responsabilização e Prestação de Contas

Exige que os agentes de tratamento comprovem a adoção de medidas eficazes e aptas a demonstrar o cumprimento da LGPD.

Isso inclui não apenas a implementação das medidas, mas também a capacidade de demonstrar sua eficácia, garantindo controle, monitoramento e documentação das ações adotadas.

Princípios na prática cotidiana

No ambiente organizacional, os princípios da LGPD não devem ser vistos como conceitos abstratos ou restritos a documentos normativos. Eles se **aplicam diretamente às atividades rotineiras** de diferentes áreas, guiando decisões e comportamentos que envolvem, mesmo que de forma indireta, o uso de dados pessoais.

Tratar dados com base nesses princípios significa agir com responsabilidade, mesmo em tarefas simples, como:

Elaboração de planilhas internas contendo nomes, contatos ou registros pessoais: é necessário verificar se os dados inseridos são adequados à finalidade e se o acesso à planilha está devidamente controlado.

Criação de formulários físicos ou digitais: a definição dos campos a serem preenchidos deve respeitar o princípio da necessidade, coletando apenas informações essenciais, com linguagem clara e propósito bem definido.

Escolha e uso de sistemas e ferramentas digitais: é fundamental adotar soluções tecnológicas que garantam a segurança, a rastreabilidade e a transparência no tratamento dos dados, evitando vulnerabilidades e garantindo o cumprimento da finalidade declarada.

Gestão de contratos, relatórios e documentos com informações pessoais: a forma como esses documentos são armazenados, compartilhados ou descartados deve estar em conformidade com os princípios da segurança, da prevenção e da responsabilização.

Comunicações internas e externas que envolvam dados: ao enviar ou divulgar qualquer informação que contenha dados pessoais, é preciso garantir que a comunicação esteja alinhada aos princípios da transparência e da qualidade dos dados.

Quando os princípios da LGPD são incorporados às rotinas operacionais da organização, passam a fazer parte da sua **cultura organizacional**. Isso fortalece a confiança dos titulares, reduz riscos legais e demonstra, na prática, que a organização leva a sério seu papel na proteção das informações que estão sob sua guarda.

VOCÊ SABIA?

Mesmo quando uma organização adota todas as medidas necessárias para proteger os dados, **a violação dos princípios da LGPD pode, por si só, configurar um tratamento irregular**. Ou seja, o simples fato de tratar dados sem respeitar princípios como finalidade, necessidade ou transparência já é suficiente para gerar responsabilização, independentemente de ter ocorrido um incidente ou vazamento. Por isso, os princípios devem ser aplicados desde o planejamento até a execução de qualquer atividade que envolva dados pessoais, com registro, monitoramento e revisão contínua.

Conhecer os princípios da LGPD é essencial para orientar o uso correto dos dados. Mas tão importante quanto saber como tratar informações é entender quais são os **direitos de quem fornece esses dados**. O próximo capítulo apresenta de forma clara e objetiva os **direitos dos titulares de dados pessoais** e o que a organização deve fazer para garanti-los.

DIREITOS DOS TITULARES

A LGPD estabelece que **toda pessoa tem o direito de saber, controlar e questionar o uso de seus dados pessoais**. Esses direitos reforçam o fundamento da **autodeterminação informativa**, ou seja, o poder do titular de decidir sobre as informações que dizem respeito à sua identidade, trajetória e privacidade.

No contexto organizacional, isso significa que qualquer pessoa que tenha seus dados tratados pelo PARANACIDADE, como por exemplo, colaboradores, fornecedores, parceiros, usuários ou representantes de municípios, tem o direito de solicitar informações, correções, exclusões e explicações sobre esse tratamento.

Para que esses direitos sejam respeitados, é necessário que a organização esteja preparada para reconhecê-los, respondê-los com agilidade e adotá-los como parte da sua rotina institucional.

Por que os direitos dos titulares são fundamentais?

Os direitos garantem equilíbrio na relação entre o titular e a organização. Eles asseguram:

Transparência no uso das informações;

Segurança na relação com os dados pessoais;

Poder de escolha sobre como os dados serão utilizados;

Mecanismos de correção, revogação e contestação;

Redução de assimetrias entre quem fornece e quem trata os dados.

Ao atender corretamente esses direitos, a organização fortalece sua cultura de proteção de dados, demonstra respeito às pessoas e evita riscos legais e reputacionais.

Quais são os principais direitos previstos pela LGPD?

A seguir, estão os principais direitos que devem ser assegurados ao titular dos dados. Esses direitos devem ser garantidos de forma gratuita, acessível, clara e tempestiva:

1. Confirmação da existência de tratamento

O titular tem o direito de saber se a organização realiza ou não o tratamento de seus dados pessoais, independentemente de quais dados estejam envolvidos.

2. Acesso aos dados

O titular pode solicitar o acesso integral aos dados que a organização mantém sobre ele, bem como às informações sobre a forma, a finalidade e a duração desse tratamento.

3. Correção de dados incompletos, inexatos ou desatualizados

Se os dados estiverem incorretos ou desatualizados, o titular pode solicitar a retificação das informações com base em dados corretos ou atualizados.

4. Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD

Sempre que os dados forem tratados de maneira inadequada ou além do necessário, o titular pode exigir a remoção, bloqueio ou anonimização desses dados.

5. Portabilidade dos dados a outro fornecedor de serviço ou produto

O titular pode solicitar a transferência de seus dados pessoais a outra organização, quando tecnicamente viável, respeitados os segredos comercial e industrial.

6. Eliminação dos dados tratados com base no consentimento

Nos casos em que o tratamento foi feito com base em consentimento, o titular tem o direito de revogar esse consentimento e solicitar a exclusão dos dados, salvo se houver outra base legal que justifique sua manutenção.

7. Informação sobre compartilhamento de dados

A organização deve informar com quem os dados são compartilhados, inclusive os terceiros, parceiros ou órgãos públicos envolvidos, quando houver.

8. Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências dessa negativa

O titular deve ser informado sobre quais dados são facultativos, e o que pode acontecer caso decida não os fornecer.

9. Revogação do consentimento

Quando o tratamento se baseia no consentimento, o titular pode revogar sua autorização a qualquer momento, e a organização deverá interromper o uso desses dados, salvo se houver outra base legal aplicável.

10. Oposição ao tratamento

Se o titular identificar que seus dados estão sendo tratados de forma irregular, ou discordar do uso que está sendo feito, ele pode se opor e solicitar a interrupção do tratamento, desde que devidamente fundamentado.

Vale o destaque que os direitos do titular de dados pessoais trazidos na LGPD **não são taxativos**. Eles são exemplificativos pois os titulares possuem a proteção de dados como um direito fundamental da pessoa humana.

Como esses direitos se aplicam na prática?

Na prática, esses direitos se manifestam por meio de requerimento formal feito pelo titular à organização, o qual deve ser atendido com agilidade, clareza e registro.

A organização precisa manter canal de atendimento, preferencialmente digital, além de fluxos internos bem definidos para processar as solicitações, com envolvimento do Encarregado pelo tratamento de dados pessoais, das áreas responsáveis e, quando necessário, da alta gestão.

Implementar esses direitos é também uma forma de:

Promover a confiança de colaboradores, parceiros e usuários;

Prevenir conflitos e responsabilizações;

Demonstrar transparência e preparo institucional;

Atuar de forma compatível com a legislação e com padrões éticos.

O PARANACIDADE tem um **canal de atendimento ao titular dos dados**, que pode ser acessado na aba LGPD do nosso site ou diretamente nesse link http://www.cge.pr.gov.br/Pagina/Registre-sua-Reivindicacao. No Estado do Paraná, por força do Decreto nº 6.474/2020, o atendimento ao titular dos dados é realizado pelo Sistema Integrado para Gestão de Ouvidorias – SIGO.

Quando uma organização trata de forma inadequada os dados pessoais dos titulares, não apenas compromete a relação de confiança com as pessoas envolvidas, como também se expõe a consequências legais e administrativas. É justamente sobre essas **sanções** que trata o próximo capítulo.

SANÇÕES ADMINISTRATIVAS

Tratar dados pessoais exige responsabilidade e quando a organização falha nesse compromisso, seja por descuido, desorganização ou desconhecimento, **as consequências podem ser sérias**.

A LGPD prevê **sanções administrativas** que buscam corrigir essas falhas e incentivar o respeito aos direitos dos titulares. Isso inclui desde advertências até sanções mais graves, como bloqueio de dados ou multas administrativas.

Mas as consequências não param por aí. O descumprimento das normas também pode trazer impactos à imagem da organização, prejudicar a confiança de colaboradores, parceiros e até comprometer o funcionamento de atividades importantes.

E o risco vai além...

Em muitos casos, **o maior prejuízo está no desgaste institucional**. Vazamentos de dados, por exemplo, podem gerar desconfiança generalizada, dificultar parcerias e comprometer projetos. Além disso, a organização pode precisar interromper serviços, revisar contratos e reorganizar processos, o que gera custos, retrabalho e instabilidade.

O que pode levar às sanções administrativas?

Alguns exemplos de situações que podem resultar em sanções administrativas:

Não responder às solicitações dos titulares de dados;

Tratar dados sem informar de forma clara o motivo;

Compartilhar dados com terceiros sem justificativa;

Não adotar medidas mínimas de segurança da informação;

Utilizar dados de forma desnecessária, inadequada ou excessiva.

Evitar essas situações depende de preparo

Ter regras claras, registrar os processos de tratamento, orientar os colaboradores e responder com agilidade às demandas de titulares são atitudes que fazem a diferença no dia a dia. Quando a organização adota a LGPD como parte de sua rotina, ela reduz riscos e fortalece sua **cultura de proteção de dados**.

Em 2023, a então Autoridade Nacional de Proteção de Dados (ANPD) aplicou a sua primeira sanção administrativa: **uma multa a uma empresa de pequeno porte por descumprimento de obrigações básicas da LGPD**. O motivo? A organização ignorou, dentre outros aspectos, solicitações de titulares e não demonstrou medidas mínimas de segurança da informação. A sanção aplicada reforçou que o porte da organização não exclui a responsabilidade pelo tratamento adequado de dados pessoais.

O próximo capítulo apresenta **recomendações simples** e aplicáveis para estruturar ações concretas de adequação à LGPD, com foco na realidade do PARANACIDADE e no papel de cada área.

MEDIDAS PRÁTICAS

Adotar **boas práticas no tratamento de dados pessoais** não exige fórmulas complexas. Na maioria das vezes, proteger os dados começa com atitudes simples, que fazem parte da rotina de trabalho. A seguir, são apresentadas orientações que podem ser aplicadas por qualquer colaborador, independentemente da área em que atua.

Essas ações não substituem os processos formais, mas complementam a estrutura de proteção de dados da organização e ajudam a prevenir riscos, reforçar a segurança e demonstrar compromisso do PARANACIDADE com a LGPD.

Cuidados essenciais no dia a dia

No PARANACIDADE, proteger os dados pessoais deve fazer parte da nossa rotina. Pequenas atitudes conscientes fazem uma grande diferença! Veja alguns cuidados que ajudam a manter a segurança e o respeito com as informações que tratamos todos os dias:

Peça só o que for realmente necessário

Evite solicitar informações que não tenham relação direta com o serviço que está sendo prestado. Coletar dados "por precaução" ou sem uma justificativa clara pode representar um risco desnecessário.

Esclareça sempre que alguém quiser saber

Se alguém quiser entender por que seus dados estão sendo usados, esteja pronto para explicar com clareza:

Quais dados estão sendo coletados;

Por qual motivo;

Como serão utilizados;

Por quanto tempo ficarão armazenados;

Se serão compartilhados e com quem.

Prefira sempre os canais oficiais

Evite usar redes sociais, e-mails pessoais ou aplicativos de mensagens para compartilhar informações pessoais. Sempre que possível, utilize os sistemas e ferramentas institucionais da organização.

Cuide bem de documentos e arquivos

Guarde pastas, formulários e processos com dados pessoais em locais de acesso restrito;

Ao se afastar do computador, lembre-se de bloqueá-lo;

Crie senhas seguras e nunca compartilhe com ninguém.

Respeite os níveis de acesso

Os acessos a sistemas e documentos com dados pessoais devem seguir as regras definidas por área ou função. Não permita que pessoas não autorizadas tenham acesso às informações.

Evite deixar dados visíveis

Listas, planilhas ou relatórios com dados pessoais não devem ficar expostos em mesas, murais ou áreas de circulação. Toda informação deve ser protegida, mesmo em papel.

Descarte com cuidado

Documentos em papel com dados pessoais devem ser descartados de forma segura, com fragmentação ou por empresa especializada.

Já os arquivos digitais devem ser apagados de forma definitiva, conforme as orientações da equipe de tecnologia da informação.

Mantenha o controle das atividades

Anote e mantenha o controle das atividades que envolvam dados pessoais, especialmente em situações que envolvam dados sensíveis ou compartilhamento com terceiros. Isso ajuda a reforçar a responsabilidade e a rastreabilidade.

Avise se notar algo fora do normal

Percebeu alguma falha, acesso indevido ou risco para os dados? Avise imediatamente o coordenador da sua área, a equipe de TI ou o Encarregado pelo tratamento dos dados.

Siga as orientações de segurança

As regras internas sobre uso de sistemas, proteção de arquivos e segurança da informação são essenciais para evitar incidentes. Mantenha-se sempre atualizado.

Use a tecnologia com responsabilidade

Se for utilizar ferramentas como inteligência artificial, evite inserir dados pessoais ou sensíveis sem a devida autorização. Use esses recursos com atenção e de acordo com as políticas da organização.

Deixe os sistemas sempre protegidos

Verifique se o computador está com antivírus ativo e atualizado. Esses cuidados são importantes para prevenir vazamentos, falhas e invasões.

Garanta o backup das informações

Certifique-se de que arquivos importantes estão sendo incluídos nas rotinas de backup da equipe responsável. Isso ajuda a evitar perdas e garante continuidade do trabalho.

Conte com DPO sempre que precisar

Em caso de dúvidas ou situações que envolvam o uso de dados pessoais, o Encarregado pelo tratamento de dados está à disposição para orientar e ajudar nos encaminhamentos necessários.

VOCÊ SABIA?

Quando há falhas no tratamento de dados pessoais, o PARANACIDADE pode ser responsabilizado e obrigado a reparar os danos causados. Mas essa responsabilidade pode ser afastada **se ficar comprovado que o tratamento não foi realizado pela organização, que não houve descumprimento das regras ou que o problema foi causado exclusivamente por terceiros ou pelo próprio titular**. As atitudes simples apresentadas neste capítulo ajudam a evitar esses riscos e contribuem para que o PARANACIDADE esteja protegido contra sanções e exposições desnecessárias.

No próximo capítulo, você encontrará informações sobre o papel da **Agência Nacional de Proteção de Dados (ANPD)** e um **glossário** com os principais termos utilizados neste material, uma ferramenta de apoio para reforçar o entendimento e a aplicação da LGPD no dia a dia.

A ANPD E O GLOSSÁRIO OFICIAL

A LGPD criou, junto com seus princípios, direitos e obrigações, uma autoridade específica para zelar pela aplicação correta da norma: a **Autoridade Nacional de Proteção de Dados (ANPD)**.

Mais recentemente, por conta da Medida Provisória 1.317/2025, a ANPD tornou-se **Agência Nacional de Proteção de Dados**, uma autarquia federal de natureza especial, vinculada ao Ministérios da Justiça e Segurança Pública, dotada de autonomia funcional, técnica, decisória, administrativa e financeira, com patrimônio próprio e com sede e foro no Distrito Federal. Seu papel é **zelar pela proteção dos dados pessoais, por orientar, regulamentar e fiscalizar o cumprimento da LGPD em todo o território nacional, além de aplicar sanções quando houver descumprimento das regras estabelecidas**.

O que faz a ANPD?

A ANPD atua em diversas frentes para consolidar a cultura de proteção de dados no país:

Elaborar as diretrizes para a Política Nacional de Proteção de Dados e da Privacidade;

Promover a disseminação de conhecimentos sobre as normas e as políticas públicas relacionadas à proteção de dados pessoais e às medidas de segurança;

Promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e da privacidade;

Estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;

Fiscalizar e aplicar sanções em caso de tratamento de dados realizados em descumprimento à legislação.

Glossário de Proteção de Dados Pessoais e Privacidade

Com o objetivo de facilitar a compreensão dos principais termos utilizados na legislação e nos documentos técnicos sobre proteção de dados, a ANPD elaborou o **Glossário de Proteção de Dados Pessoais e Privacidade**.

Esse glossário reúne, de forma sistematizada, os conceitos mais utilizados na aplicação da LGPD, servindo como uma ferramenta de referência para titulares de dados, colaboradores e agentes de tratamento. Ele foi construído com base em diversos documentos oficiais da própria ANPD e está em constante evolução.

Além de padronizar a linguagem usada nas comunicações e orientações técnicas, o glossário contribui para ampliar o entendimento comum de expressões e conceitos muitas vezes dispersos em diferentes fontes.

É importante lembrar que esse glossário é voltado exclusivamente ao universo normativo da proteção de dados pessoais. Outros significados atribuídos a termos semelhantes em outras áreas do Direito não se confundem com as definições consolidadas pela ANPD.

Onde encontrar o glossário da ANPD?

O conteúdo completo pode ser acessado em formato PDF pelo site oficial neste link https://www.gov.br/anpd/pt-br/centrais-de-conteudo/documentos-tecnicos-orientativos/glossario-anpd-protecao-de-dados-pessoais-e-privacidade.pdf.

O material também está disponível na aba LGPD do site do PARANACIDADE, como apoio à consulta rápida e padronizada de termos usados no dia a dia.

O Glossário da ANPD é um **documento aberto a sugestões e contribuições**. Sempre que surgirem dúvidas, comentários ou propostas de novos termos, qualquer pessoa pode enviar sugestões pela Plataforma Fala.BR, acessando esse link https://falabr.cgu.gov.br/. Essa abertura contínua ajuda a manter os conceitos atualizados e alinhados com a realidade prática de quem lida com dados pessoais.

O fortalecimento da cultura de proteção de dados no PARANACIDADE passa pelo conhecimento, mas também pelo comprometimento de cada colaborador. Ferramentas como o glossário oficial da ANPD ajudam a esclarecer dúvidas, padronizar conceitos e oferecer mais segurança às ações do dia a dia.

Mais do que compreender os termos da LGPD, é essencial aplicar os valores que eles representam: respeito à privacidade, responsabilidade no uso das informações e transparência nas relações institucionais.

Esse compromisso está presente em todas as áreas da organização e é reforçado, com clareza e convicção, por quem lidera essa transformação.

A seguir, uma mensagem da **Superintendente Executiva do PARANACIDADE** sobre o papel coletivo e estratégico da proteção de dados pessoais no contexto do PARANACIDADE.

O COMPROMISSO QUE NOS UNE

Cuidar das pessoas sempre foi e sempre será parte essencial do que fazemos no PARANACIDADE. Seja por meio do apoio técnico aos municípios ou da execução de obras e projetos, **nosso trabalho impacta diretamente a vida de milhares de pessoas nos municípios paranaenses**. Nesse contexto, proteger os dados pessoais de todos que se relacionam com o PARANACIDADE deixou de ser apenas uma boa prática: tornou-se um dever **estratégico e permanente**.

A Lei Geral de Proteção de Dados Pessoais convida cada um de nós a repensar a forma como lidamos com informações que identificam pessoas. Mais do que uma exigência legal, a LGPD representa um compromisso ético com a transparência e a confiança nas relações institucionais.

No PARANACIDADE, esse compromisso está sendo construído com base em conhecimento, responsabilidade compartilhada e ações concretas que se integram ao cotidiano de todas as áreas. Cada colaborador tem um papel fundamental nesse processo, independentemente da função que exerce.

Este conteúdo foi elaborado justamente com esse propósito: aproximar o tema com a realidade de cada setor, esclarecer dúvidas com linguagem acessível e fortalecer a cultura da proteção de dados no PARANACIDADE.

Estamos, juntos, construindo uma organização ainda mais ética, transparente e respeitada. Cada atitude consciente, cada cuidado com a informação, fortalece não apenas a nossa estrutura organizacional, mas também a confiança da sociedade em nosso trabalho.

A proteção de dados começa com pequenas atitudes e ganha força quando se transforma em **cultura**. São essas atitudes que garantem segurança, integridade e respeito nas relações que o PARANACIDADE estabelece com a sociedade.

Vamos seguir em frente com o compromisso de quem compreende que **proteger dados é, acima de tudo, proteger pessoas**.

E essa é uma missão que nos une!

Camila Mileke Scucato
Superintendente Executiva do PARANACIDADE

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

_____. Medida Provisória nº 1.317, de 17 de setembro de 2025. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para tratar da Agência Nacional de Proteção de Dados, a Lei nº 10.871, de 20 de maio de 2004, para criar a Carreira de Regulação e Fiscalização de Proteção de Dados, transforma cargos no âmbito do Poder Executivo federal, e dá outras providências**. Disponível em https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Mpv/mpv1317.htm.

_____. Decreto Estadual nº 6.474, de 14 de dezembro de 2020. **Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD), no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo do Estado do Paraná**. Disponível em https://www.legislacao.pr.gov.br/legislacao/pesquisarAto.do?action=exibir&codAto=244066&indice=1&totalRegistros=8&dt=1.9.2025.14.27.3.847.

JOHANSEN, Bob. **Leaders Make the Future: Ten New Leadership Skills for an Uncertain World**. 2. ed., rev. e expandida. Reino Unido: ReadHowYouWant, 2015.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. **LGPD: Lei Geral de Proteção de Dados Pessoais comentada**. 3. ed., rev. atual. e ampl. São Paulo: Thomson Reuters Brasil, 2021.

Documento assinado eletronicamente por:

Ademir Lopes dos Santos Paz (14/10/2025 10:15:54), Camila Mileke Scucato (14/10/2025 10:22:03), Helio Sabino Deitos (14/10/2025 10:32:32), Jaime Antonio de Camargo Ferreira (14/10/2025 10:33:26), Francisco Luis dos Santos (14/10/2025 15:05:41) e Guto Silva (15/10/2025 15:52:23)

Nome/controle do arquivo:

2025101410155445.pdf

Aponte a sua câmera e verifique a autenticidade:

https://dss.paranacidade.org.br/validaAssinatura.htm?controle=2025101410155445