

Lei Geral de Proteção de Dados Pessoais

Guia para servidores e colaboradores

UFRN

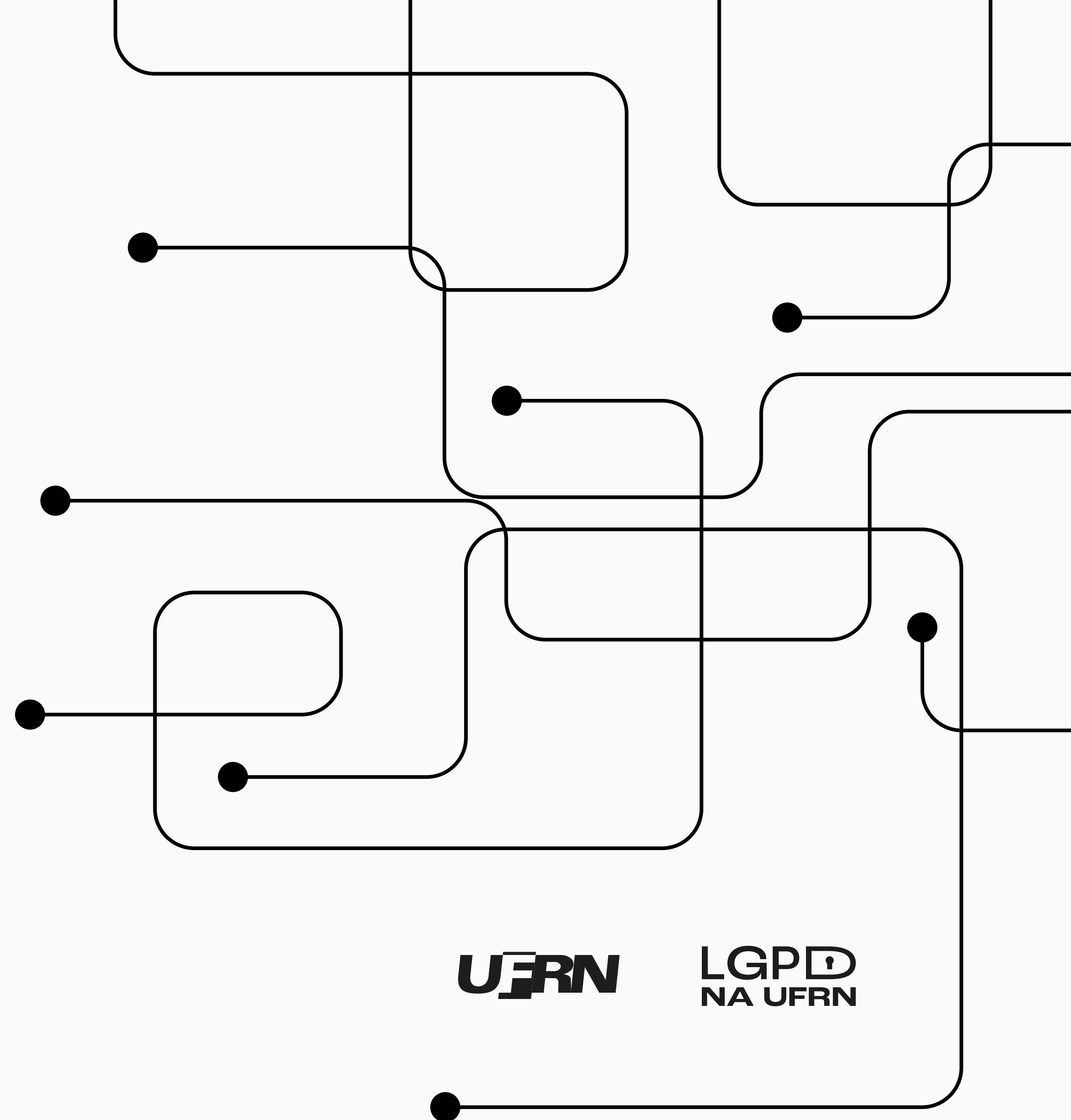
**LGPD
NA UFRN**

Lei Geral de Proteção de Dados Pessoais

Guia para servidores e colaboradores

UFRN

**LGPD
NA UFRN**



Ministério da Educação

Universidade Federal do Rio Grande do Norte

Reitor

José Daniel Diniz Melo

Vice-Reitor

Hênio Ferreira de Miranda

Elaboração

Comissão LGPD - Portaria Nº 973 / 2020 - R,
de 18 de agosto de 2020 publicada no Boletim
de Serviço UFRN nº 161 de 19/08/2020

Luan David Pereira do Nascimento

Administrador, matrícula nº 2249013
(presidente).

Adriane Paula Vieira de Andrade

Professora Adjunta, matrícula nº 1100806.

André Medeiros Dantas

Analista de Tecnologia da Informação,
matrícula nº 3083586.

Brunno Santiago e Silva

Analista de Tecnologia da Informação,
matrícula nº 3159204.

Clarissa Lorena Alves Coelho Lins

Analista de Tecnologia da Informação,
matrícula nº 2134722.

Elias Jacob de Menezes Neto

Professor Adjunto, matrícula nº 2353000.

Jose Alfredo Ferreira Costa

Professor Titular, matrícula nº 1142787.

Manoel Bezerra da Costa Neto

Analista de Redes e Comunicação de Dados
da FUNPEC, matrícula nº 4480.

Marcos Cesar Madruga Alves Pinheiro

Professor Associado, matrícula nº 1525670.

Revisão

André Medeiros Dantas

Elias Jacob de Menezes Neto

Luan David Pereira do Nascimento

Rafael da Cunha Pimenta

Projeto Gráfico e Diagramação

Gustavo Henrique Martins

Histórico de Versões

Versão	Principais Mudanças
Versão 1.0 04/2021	Criação do Documento

Este material será continuamente atualizado conforme novas disposições, normativos, jurisprudência e interpretações sobre o tema forem consolidados pela Administração Pública. Por isso, consulte sempre a última versão em ufrn.br, seção "Institucional", "Proteção de Dados Pessoais".

Este material se aplica a todas as unidades institucionais da UFRN, com exceção dos Hospitais Universitários, administrados pela Empresa Brasileira de Serviços Hospitalares (EBSERH).


Sumário

01	LGPD? Do que estamos falando?	6	04	Que princípios devo me atentar ao tratar dados pessoais?	21
	Dados Pessoais e Dados Sensíveis	8			
02	Fatos sobre a LGPD	9	05	Direitos dos Titulares	23
	Papéis e atores no tratamento de dados	12		Boas práticas de governança	28
03	LGPD no dia-a-dia O que preciso saber?	13		Descumprimento e sanções	29
	Consentimento na utilização dos dados pessoais	14			
	Dispensa de Consentimento	15			
	Medidas de Proteção	16			
	Dados de Crianças e Adolescentes	17			
	Dados Pessoais Anonimizados	18			
	Compartilhamento de Dados	19			
	Projetos de Pesquisa e Extensão	20			

LGPD?

Do que estamos falando?

A Lei Geral de Proteção de Dados Pessoais (LGPD) - oficialmente, Lei nº 13.709 de 14 de agosto de 2018 - é a lei que regulamenta a proteção dos dados pessoais de pessoas naturais que estão sob posse de qualquer pessoa física ou jurídica.



A LGPD surge no contexto de grande desenvolvimento das tecnologias da informação e comunicação (TIC), já que cada vez mais os dados se constituem como fator primordial para o desenvolvimento de pesquisas, organizações e nações.

A internet permite um compartilhamento de dados sem precedentes, de maneira relativamente fácil, causando uma revolução na maneira como trabalhamos, estudamos, consumimos conteúdo e aplicamos novas ideias para o desenvolvimento da sociedade.

Apesar dos grandes benefícios promovidos pelo compartilhamento de dados, esse cenário também provoca grandes desafios para pessoas e organizações na gestão e guarda desses dados. Existem tipos de dados que são secretos, classificados, restritos ou sensíveis, que merecem uma maior atenção por parte desses atores. Uma patente (método revolucionário de fazer alguma coisa nova, como um novo material, por exemplo) de uma indústria precisa ser protegida contra acesso indevido de terceiros.

O prontuário (conjunto de dados e documentos sobre a saúde, por exemplo) de um paciente, da mesma forma, merece proteção especial pelas pessoas e organizações que detêm esses dados, já que um eventual vazamento dessas informações pode constituir uma violação à privacidade do paciente.

Com os exemplos anteriores, já deu para perceber que os dados pessoais são dados críticos e que um eventual vazamento dessas informações pode causar sérios danos, por exemplo, à privacidade, à intimidade, à honra e à imagem da pessoa que teve seus dados compartilhados indevidamente.

Dessa forma, a LGPD surgiu para estabelecer diretrizes sobre o tratamento de dados pessoais de pessoas naturais realizadas por pessoas físicas ou jurídicas - públicas ou privadas.

Em síntese, a lei estabelece normas gerais e boas práticas para a manipulação dos dados pessoais, disciplina sanções em caso de descumprimento e cria uma nova estrutura responsável por fiscalizar o cumprimento dessas orientações, a ANPD - Autoridade Nacional de Proteção de Dados.



Dados Pessoais

São informações relacionadas a pessoa natural identificada ou identificável.

Pessoal natural é qualquer tipo de pessoa física, o que inclui alunos, servidores, colaboradores terceirizados, participantes de projetos de pesquisa e sociedade em geral.

Exemplos: CPF, RG, endereço, estado civil, endereço IP, dados de localização obtidos por GPS, cookies, etc.



Dados Pessoais Sensíveis

É um tipo de dado pessoal relacionado a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Exemplos: amostra de DNA, orientação sexual, dados de filiação a partido político, dados sobre enfermidade, prontuário médico, etc.

Fatos sobre a LGPD

Para entender como a LGPD protege seus dados, é preciso entender em quais situações ela se aplica.

01

A LGPD protege todas as operações de tratamento de dados pessoais

Toda e qualquer operação envolvendo 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 são protegidas pela LGPD.

Ou seja, todo o ciclo de vida do tratamento de dados pessoais, que inclui desde a coleta, até o armazenamento, arquivamento ou descarte, devem seguir boas práticas de proteção preconizadas pelo normativo.

02

O encarregado de dados pessoais é o responsável pelo atendimento dos usuários

O encarregado é a 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). A Lei ainda cria mais dois atores

03

A LGPD protege apenas os dados pessoais de pessoas físicas

O art. 1º é bem claro: “Esta lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, (...) com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da **pessoa natural**.” Dados de pessoa jurídica são protegidos por regramentos distintos da LGPD.

04

Documentos físicos e pendrives também são protegidos pela LGPD

Qualquer operação de tratamento de dados pessoais, incluindo aquelas que **não são realizadas em sistemas de informação e comunicação, são abrangidas pela LGPD.**

Dessa forma, a análise de um documento, em meio físico, que contenha dados pessoais, deve ser objeto de proteção da lei. Ainda nesse exemplo, os documentos ou qualquer outro tipo de material que contenha dados pessoais em meio físico, como **disquetes, CD's e pendrives**, armazenados em escaninhos, gavetas ou no sistema de arquivos setoriais ou geral também devem ter políticas de proteção.

05

A ANPD é o órgão responsável pela fiscalização

A LGPD prevê que a Autoridade Nacional de Proteção de Dados é a responsável pela fiscalização do cumprimento da lei por entidades públicas e privadas. Mais informações devem ser consultadas em anpd.gov.br.

06

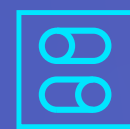
Algumas situações não são abrangidas pela LGPD

A LGPD não se aplica em alguns casos:

- operações de tratamento para fins particulares (por exemplo: reunião de dados de familiares para construção de árvore genealógica);
- operações para fins jornalísticos, artísticos e acadêmicos (neste último caso, seguindo algumas diretrizes da própria LGPD, detalhadas nas páginas seguintes, e do Comitê de Ética em Pesquisa);
- pelo Poder Público, no caso de processos relacionados à segurança pública, defesa nacional, defesa do Estado e atividades de investigação de delitos penais.

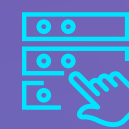
Papéis e atores no tratamento de dados

Os agentes públicos que possuem acesso ou manipulam dados pessoais são classificados como “controlador” e “operador”.



Controlador

O “controlador” é a própria instituição, representada pelo Reitor, a quem compete as decisões referentes ao tratamento de dados pessoais.



Operador

Quando não for a própria instituição, o “operador” será a pessoa que realizar o tratamento em nome dela, como, por exemplo, uma empresa contratada para gerenciar o acervo funcional de servidores.

Os “operadores” realizam o tratamento de dados pessoais em nome do “controlador”. O “controlador” e os “operadores” devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. Os “operadores” devem realizar o tratamento segundo as instruções fornecidas pelo “controlador”, que verificará a observância das próprias instruções e das normas sobre a matéria.

LGPD no dia-a-dia O que preciso saber?



Consentimento na utilização dos dados pessoais

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular (detentor dos dados) concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Por regra, a LGPD afirma que o tratamento de dados pessoais deve ser precedido de consentimento do titular desses dados (aluno, servidor, participante de pesquisa etc.).

Existem situações, no entanto, em que é permitido o tratamento dos dados com a dispensa do consentimento:

- para o cumprimento de obrigação legal ou regulatória;
- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;

- para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
- entre outras situações previstas na LGPD.

A maior parte das atividades da UFRN são amparadas em uma das hipóteses de dispensa de consentimento no tratamento de dados pessoais (pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis), não sendo necessário o termo de consentimento para a execução desses processos vinculados a essas políticas públicas.

Dispensa de Consentimento

Parte dos processos em execução na instituição não precisarão do Termo de Consentimento do titular dos dados pessoais para esse tipo de tratamento, já que se encaixam na hipótese de dispensa prevista no Art. 11, inc II, alínea "b", da LGPD.

Isso inclui, mas não se restringe a:

- matrícula de discentes com faixa etária superior a 18 anos (abaixo de 18 anos, ver seção "Dados de Crianças e Adolescentes");
- informações pessoais coletadas no âmbito de processo licitatório;
- utilização de dados pessoais na elaboração de contrato administrativo decorrente de processo licitatório;
- utilização de dados pessoais para cadastro e manejo de acervo funcional de servidores;
- anotação de dados de saúde, como laudos, prontuários médicos e outras informações

de atendimento em serviços de saúde (caso o atendimento seja no âmbito de projeto de pesquisa ou extensão, ver seção "Projetos de Pesquisa e Extensão");

- atendimento ao discente (serviço social, atendimento médico e psicológico e estudantes com necessidades educacionais especiais);
- Abertura de processo administrativo que contenha dados pessoais, para a petição ou defesa de direitos.

Apesar da dispensa do consentimento, a instituição é obrigada a seguir as demais medidas de proteção previstas na LGPD, especialmente aquelas relacionadas à observância dos princípios gerais e à garantia dos direitos do titular.

Medidas de Proteção

Independentemente da exigência ou não de Termo de Consentimento, o controlador e o operador deverão aplicar medidas técnicas e administrativas de proteção a esses dados pessoais. Isso inclui, mas não se restringe a:

No ato de disponibilização de documentos públicos (contratos, convênios, notas fiscais, etc) em transparência ativa ou passiva, realizar a ocultação parcial dos dados pessoais constantes nos documentos (exemplo: CPF 001***-**-48);

No âmbito de criação de processos administrativos na Mesa Virtual, marcar como "restrito" os documentos que contenham dados pessoais ou sensíveis;

Utilizar o e-mail institucional e as ferramentas oficiais de comunicação no caso de transferência ou compartilhamento **autorizado** de dados pessoais;

Não compartilhar dados pessoais ou arquivos que contenham dados pessoais por canais não oficiais, redes sociais, etc;

Evitar armazenar senhas de logins institucionais no navegador, em arquivos digitais ou em documentos físicos;

Esclarecer ao titular de dado pessoal como os seus dados são tratados e promover os direitos do titular, quando solicitado;

Tratar dados pessoais cujo acesso é público considerando a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização;

Seguir os princípios e diretrizes de tratamento preconizados pela LGPD.

Dados de Crianças e Adolescentes

O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, observados a LGPD, o ECA e legislações pertinentes.

No caso desse público, o tratamento de dados pessoais **deve ser precedido de consentimento específico por parte de um dos responsáveis legais**. O Estatuto da Criança e do Adolescente (ECA) considera "criança" a pessoa até doze anos de idade incompletos e "adolescentes" a faixa etária doze anos completo e dezoito anos de idade.

Isso inclui, mas não se restringe a:

- matrícula de discentes com faixa etária inferior a 18 anos;
- coleta e utilização de dados pessoais de discentes para fins de execução de políticas públicas (saúde, acompanhamento psicológico, acompanhamento a estudante com

necessidade educacional especial, etc);

- coleta e utilização de dados pessoais para participação em projeto de pesquisa ou extensão;
- repasse a terceiros dos dados pessoais.

As unidades que realizam o tratamento de dados de crianças e adolescentes devem utilizar o Termo de Consentimento padronizado pela instituição, e nele constar todas as possibilidades de tratamento de dados, evitando ter que solicitar o consentimento inúmeras vezes ao responsável pela criança ou adolescente. O consentimento deverá referir-se a finalidades determinadas e específicas (autorizações genéricas serão nulas). As informações deverão ser fornecidas de maneira simples, clara e acessível.

Poderão ser coletados dados pessoais de **crianças** sem o consentimento apenas quando

a coleta for necessária para contatar os pais ou o responsável legal, **utilizados uma única vez e sem armazenamento**, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento prévio por um dos responsáveis.

O controlador deve manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos quanto ao acesso aos dados, existência de tratamento desse público, etc. e deve realizar todos os esforços razoáveis para verificar que o consentimento específico para esse público dado pelo responsável pela criança, consideradas as tecnologias disponíveis.

Dados Pessoais Anonimizados

Os dados anonimizados são aqueles relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Atente-se que existe uma pseudoanonimização, que é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro.

Isso inclui, mas não se restringe a:

- Exclusão de dados pessoais (nome, CPF, e-mail, telefone, etc) coletados em formulário online de inscrição em eventos sobre o perfil dos participantes (vínculo institucional, sexo, escolaridade, etc);
- Transmissão de estatísticas sobre pacientes a terceiros, excluindo todos os dados pessoais

do arquivo bruto, como nome completo, matrícula, CPF, entre outros dados que possam identificar os titulares de direitos dos usuários.

- Mascaramento de dados pessoais em documentos institucionais (anonimização), mantendo-se a cópia original do arquivo (pseudoanonimização).

Dessa forma, a anonimização é a 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.

Os dados anonimizados não serão considerados dados pessoais e não são protegidos pela LGPD, EXCETO quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido (pseudoanonimização).



Compartilhamento de Dados

Os dados tratados pela Administração Pública deverão ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas,

A Administração Pública **não** pode transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto:

- em casos de execução descentralizada de atividade pública que exija a transferência (ex: gestão de acervo funcional de servidores)
- nos casos em que os dados forem acessíveis publicamente;

- quando houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres
- na hipótese de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

A transferência internacional de dados pessoais somente é permitida para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto na LGPD, ou quando o controlador (que estará recepcionando os dados) oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta legislação.



Projetos de Pesquisa e Extensão

Os projetos de pesquisa e extensão, devem, sempre que possível, realizar a anonimização dos dados tratados no âmbito da execução do projeto.

Apesar da LGPD prever a hipótese de dispensa de consentimento para a realização de estudos por órgão de pesquisa, ela não exime o pesquisador de seguir as orientações dos Comitês de Ética em Pesquisa quanto ao tratamento de dados pessoais, especialmente quanto a utilização do TCLE - Termo de Consentimento Livre e Esclarecido.

Na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de

segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudoanonimização dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

A divulgação dos resultados ou de qualquer excerto do estudo em nenhuma hipótese poderá revelar dados pessoais.

Caso o pesquisador utilize bases de dados que contenham dados pessoais públicos, este deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização.

Que princípios devo me atentar ao tratar dados pessoais?

O controladores e os operadores que realizam o tratamento dos dados deverão observar as seguintes diretrizes no momento da manipulação dos dados.

01

Finalidade

Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

02

Adequação

Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

03

Necessidade

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

04

Livre acesso

Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

05

Qualidade dos dados

Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

06

Transparência

Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

07

Segurança

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

08

Prevenção

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

09

Não discriminação

Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

10

Responsabilização e prestação de contas

Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Direitos dos Titulares

Os titulares dos dados pessoais **são as pessoas naturais (físicas) que têm os seus dados pessoais armazenados na instituição.**



O titular dos dados pessoais tem direito a obter da instituição, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:



Pedir confirmação da utilização de dados pessoais

Com ou sem dispensa de consentimento, o usuário terá direito a saber como os seus dados são tratados, desde o processo de coleta, até o processo de arquivamento ou descarte.



Solicitar cópia dos dados pessoais

Cópia dos dados pessoais armazenados na instituição.



Retificar os dados pessoais

Correção ou retificação de dados errados, incompletos ou desatualizados.



Solicitar a anonimização de dados

Anonimização de dados pessoais coletados excessivamente, que excedam o mínimo necessário para a execução dos processos organizacionais.

O titular dos dados pessoais tem direito a obter da instituição, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição:



Solicitar a exclusão dos dados pessoais

O titular pode solicitar a eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a LGPD, independentemente de consentimento ou não, EXCETO para aqueles dados imprescindíveis para a execução de políticas públicas ou cumprimento de obrigações legais ou contratuais, para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais ou quando necessário para atender aos interesses legítimos do controlador ou de terceiro.



Solicitar informações sobre o compartilhamento dos seus dados

Receber informações precisas, claras e compreensíveis acerca das entidades públicas e privadas com as quais o controlador realizou o uso compartilhado de seus dados.



Solicitar informações sobre a possibilidade de não fornecer consentimento e as suas implicações

Receber informações claras, simples e acessíveis sobre a possibilidade de não fornecer consentimento, com as consequências de sua negativa.



Ser comunicado sobre incidentes de segurança que envolvam os seus dados

O controlador deve comunicar aos titulares de dados e a ANPD, a ocorrência de incidentes ou vazamentos de dados pessoais.

O titular não poderá negar o tratamento de dados pessoais pela Administração Pública de maneira genérica, global ou desproporcional. A Administração Pública sempre poderá tratar os dados necessários para o atendimento de sua finalidade pública, na persecução do interesse público. O usuário somente poderá negar o tratamento ou solicitar a exclusão de dados, nos casos de dispensa de consentimento, ou diante de situações nas quais sejam constatadas desconformidade com os preceitos da LGPD.

Boas práticas de governança

O controlador deve implementar mecanismos de governança na instituição, que contemplem, no mínimo:

a) demonstração do processo de implementação e comprometimento da instituição em adotar práticas de proteção de dados pessoais;

b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independente dos métodos de coleta;

c) seja adaptado à estrutura, à escala e ao volume de tratamento, bem como à sensibilidade dos dados tratados;

d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) promova relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;

f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

g) conte com planos de resposta a incidentes e remediação; e

h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Descumprimento e sanções

O servidor público que concorrer ou colaborar, direta ou indiretamente, no descumprimento das diretrizes da LGPD, poderá sofrer sanções previstas na Lei 8.112/90 (Regime Jurídico Único), Lei 8.429/92 (Lei de Improbidade Administrativa) e na Lei 12.527/11 (Lei de Acesso à Informação).

- Ao órgão ou entidade pública, poderão ser adotadas as seguintes sanções:
 - advertência, com indicação de prazo para adoção de medidas corretivas;
 - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
 - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
 - eliminação dos dados pessoais a que se refere a infração;
 - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo

- período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;
 - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;
 - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Referências

Lei nº 13.709/2018, Lei Geral de Proteção dos Dados – LGPD.

Lei nº 13.853/2019, que altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências.

LEI GERAL DE PROTEÇÃO DE DADOS. Grupo de trabalho LGPD; Comitê de Governança Digital. Guia de Orientações sobre a Lei nº 13.709/2018. 1.0. [S. l.], 2020. Disponível em: http://governanca.ufs.br/uploads/page_attach/path/10073/CARTILHA_LGPD_.pdf. Acesso em: 30 janeiro 2021.

 LGPD
VEM AÍ