



CARTILHA DE BOAS PRÁTICAS EM PROTEÇÃO DE DADOS PESSOAIS



Ministério Público
do Distrito Federal
e Territórios

ADMINISTRAÇÃO SUPERIOR DO MPDFT

Procuradora-Geral de Justiça do Distrito Federal e Territórios
Promotora de Justiça Fabiana Costa Barreto

Vice-Procuradoria-Geral Jurídico-Administrativa
Procuradora de Justiça Selma Leite do Nascimento Sauerbronn de Souza

Vice-Procuradoria-Geral de Justiça Institucional
Procurador de Justiça André Vinícius Espírito Santo de Almeida

Chefe de Gabinete
Promotor de Justiça Georges Carlos Fredderico Moreira Seigneur

Secretaria-Geral
Promotor de Justiça Wagner de Castro Araújo

Assessoria de Políticas Institucionais
Promotor de Justiça André Luiz Cappi Pereira
Promotora de Justiça Thaienne Nascimento Fernandes

Assessoria Especial do Planejamento Estratégico
Promotora de Justiça Hiza Maria Silva Carpina Lima

Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec)
Promotor de Justiça Frederico Meinberg Ceroy

Esta é uma publicação do Comitê Executivo de Privacidade (Cepri) do Ministério Público do Distrito Federal e Territórios

Endereço: Eixo Monumental, Praça do Buriti, Lote 2, Sede do MPDFT, Brasília-DF

Telefone: (61) 3343-6484 e 3343-6483
E-mail: cepri@mpdft.mp.br

Texto: Cepri

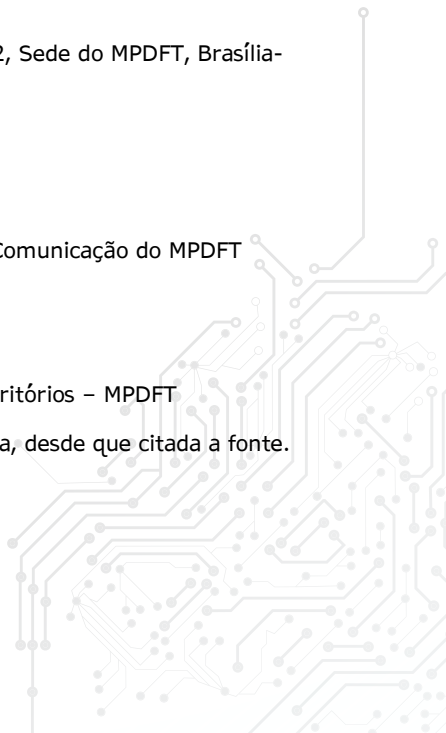
Programação visual e diagramação: Secretaria de Comunicação do MPDFT

Revisão de texto: Samara Almeida

© 2022 Ministério Público do Distrito Federal e Territórios – MPDFT

É permitida a reprodução parcial ou total desta obra, desde que citada a fonte.

1ª impressão – 2022



Apresentação

A proteção de dados pessoais é uma preocupação do Ministério Público do Distrito Federal e Territórios que afeta diretamente a segurança de cada indivíduo. Desde 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) define condições e limites para o tratamento de dados pessoais por empresas e entidades públicas ou privadas.

Essa legislação padronizou normas e práticas que promovem a proteção dos dados pessoais de qualquer pessoa que esteja no Brasil. Dessa forma, foram estabelecidos padrões mínimos a serem seguidos no uso de algum dado pessoal, de tal maneira que seja garantido ao cidadão o protagonismo nas decisões fundamentais a este respeito.

Em 2018, este Ministério Público instituiu a Unidade Especial de Proteção de Dados e Inteligência Artificial (Espec), primeira iniciativa nacional dedicada exclusivamente à proteção dos dados pessoais e da privacidade dos brasileiros.

Desde agosto de 2019, o MPDFT possui o Programa de Governança de Dados Pessoais (PGDP) para implementar diretrizes, obrigações e protocolos que visam preservar direitos previstos na LGPD e no Marco Civil da Internet. O MPDFT foi o primeiro Ministério Público no Brasil a desenvolver tal iniciativa.

Já em setembro de 2020, foi criado o Comitê Executivo da Privacidade para a finalização do PGDP. O documento também traz diretrizes complementares de adequação do órgão à Lei Geral de Proteção de Dados Pessoais.

Esta cartilha é fruto do trabalho do Comitê Executivo de Privacidade (Cepri) do MPDFT e tem o objetivo de sensibilizar os integrantes da Instituição sobre a importância da LGPD, além de trazer dicas de boas práticas relacionadas à proteção de dados. Aqui, o leitor entenderá porque, e em quê, essa legislação pode impactar nas suas rotinas de trabalho e as motivações para agir com ainda mais ética e responsabilidade.

A edição desta Cartilha decorre do nosso compromisso com a cidadania e a defesa dos direitos dos cidadãos do Distrito Federal numa área relativamente nova, que demanda acompanhamento contínuo das inovações tecnológicas e, por consequência, do aprimoramento da legislação.

Boa leitura!

Fabiana Costa
Procuradora-Geral de Justiça
do Ministério Público e Territórios

Conteúdo

Introdução

- O que é a LGPD?—7
- O que é um dado?—7
- O que são dados pessoais? —7

Resumo

- O que são dados pessoais sensíveis? —8
- Quem é titular de dados? —9
- Quem são os agentes de tratamento? —9
- Quem é o encarregado de dados? —11
- Quais as hipóteses de tratamento de dados pessoais na LGPD?—11
- Direitos dos titulares—13
- Como as organizações públicas devem atuar no tratamento de dados pessoais?—16

Boas práticas e medidas de segurança

- Rotina de segurança da informação—19
- Conscientização e treinamento—20
- Segurança dos dados pessoais armazenados—21
- Segurança em dispositivos móveis—22
- Segurança das comunicações—23

Introdução

Boa parte do trabalho nas unidades do MPDFT envolve tratamento de dados pessoais.

A Lei Geral de Proteção de Dados (Lei n. 13.709/2018), conhecida também como LGPD, é uma realidade e sua aplicação se estende a todas as atividades realizadas pelo MPDFT, em todos os setores e níveis.

Seja no contato com o público, seja com outros departamentos, seja na apreciação dos procedimentos de sua responsabilidade, a LGPD tem aplicação direta no dia a dia funcional de membros e servidores, pois a grande maioria opera com dados pessoais e precisará compreender e realizar adequações em suas rotinas de trabalho.



Para tanto, o Comitê Executivo de Privacidade, instituído pela a Portaria Normativa PGJ n. 697/2020, para a finalização do Programa de Governança de Dados Pessoais (PGDP) do MPDFT, elaborou Código de Boas Práticas para que membros e servidores pudessem se familiarizar com o que determina a lei e verificar as adaptações necessárias em suas atividades e fluxos de trabalho.

Resumo

O que é a LGPD?

LGPD é a sigla para Lei Geral de Proteção de Dados Pessoais – Lei n. 13.709, de 14 de agosto de 2018.

Esta lei estabelece os direitos, as condições e os limites do tratamento de dados pessoais. Possui como principal objetivo a proteção aos direitos fundamentais da liberdade, privacidade e do livre desenvolvimento da personalidade das pessoas naturais.

O que é um dado?

Dado é qualquer registro solto, aleatório e sem qualquer análise ou estruturação. Dados são as matérias-primas da informação, que poderá se tornar um conhecimento para finalidades diversas.

O que são dados pessoais?

A LGPD estabelece um conceito amplo, definindo que dados pessoais são as informações que podem identificar, direta ou indiretamente, um indivíduo.

Por exemplo: nome, sobrenome, número de telefone, endereço residencial, usuário de redes sociais; geolocalização, endereço de e-mail, profissão, renda, número do cartão bancário, número do RG, CPG, CTPS, PIS, PASEP; marcas características, grau de escolaridade etc.



O que são dados pessoais sensíveis?

A lei qualifica alguns dados pessoais como sensíveis por haver maior risco de danos às pessoas naturais, são eles:

- origem racial ou étnica;
- convicção religiosa;
- opinião política;
- filiação a sindicato e a organização religiosa, filosófica ou política;
- dados sobre saúde;
- informação sobre vida sexual;
- dado genético; e
- dado biométrico.

Quem é titular de dados?

De acordo com a LGPD, é titular de dados pessoais é toda pessoa natural a quem se referem os dados tratados. Portanto, qualquer pessoa é titular de dados pessoais em algum contexto.

Quem são os agentes de tratamento?

Os agentes de tratamento são aqueles que realizam a coleta, o uso, o compartilhamento ou outra atividade com os dados pessoais.

São considerados agentes de tratamento pessoas naturais ou jurídicas, públicas ou privadas que tratam dados pessoais para quaisquer finalidades previstas na LGPD.

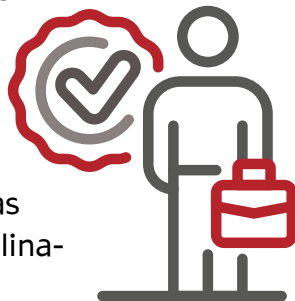
A Lei elenca expressamente como agentes de tratamento o controlador e o operador de dados, os quais possuem funções e responsabilidades distintas.

Controlador é o agente de tratamento de dados que toma as decisões sobre o tratamento dos dados, bem como define a finalidade e os elementos essenciais que o tratamento terá. É o responsável pela aplicabilidade dos direitos criados pela LGPD aos titulares dos dados.

No MPDFT, é a pessoa jurídica de direito público que exerce a função de controlador e, portanto, detém o poder sobre o tratamento dos dados pessoais, ou seja, na nossa instituição, o controlador é o próprio MPDFT, representado pela Procuradoria-Geral de Justiça.

Membros e servidores do MPDFT atuam em nome do controlador e, portanto, são responsáveis pelos tratamentos dos dados pessoais realizados no exercício de suas atividades.

Assim, os membros, servidores, estagiários, voluntários ou prestadores de serviço terceirizado são responsáveis por garantir a segurança da informação em relação aos dados pessoais a que tenham acesso, atendendo às orientações do controlador e aos preceitos legais, estando sujeitos às penalidades e às sanções legais e disciplinares cabíveis.



Atenção! Nos termos do art. 28 do Decreto-Lei n. 4.657/1992, conhecido como Lei de Introdução às Normas de Direito Brasileiro, “o agente público responderá pessoalmente por suas decisões ou opiniões técnicas em caso de dolo ou erro grosseiro”. Portanto, o tratamento indevido ou inadequado dos dados pode levar à responsabilização administrativa, cível e penal do agente/servidor público que praticou o ato ilegal.

O operador é o agente de tratamento que realiza o tratamento de dados em nome do controlador. O operador não pertence ao MPDFT. Em geral, é uma empresa contratada para tal finalidade.

Quem é o encarregado de dados?

É a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a autoridade nacional de proteção de dados (ANPD).

Assim, o titular dos dados poderá requerer os direitos sobre os seus dados pessoais diretamente ao encarregado.

Quais as hipóteses de tratamento de dados pessoais na LGPD?

Toda atividade realizada pela instituição deve estar vinculada a uma base legal certa e determinada prevista em lei. O art. 7º da LGPD prevê as situações em que é possível o tratamento de dados pessoais, quais sejam:

- mediante o fornecimento de consentimento pelo titular;
- para o cumprimento de obrigação legal ou regulatória pelo controlador;
- pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de po-

líticas 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;

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

- para o exercício regular de direitos em processo judicial, administrativo ou arbitral, este último nos termos da Lei n. 9.307/1996 (Lei de Arbitragem);

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

- para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

- para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

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



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

Direitos dos titulares

A LGPD garante aos titulares de dados os seguintes direitos:

- confirmação da existência de tratamento;
- acesso aos dados;
- correção de dados incompletos, inexatos ou desatualizados;
- anonimização;
- bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
- portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
- eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;



- informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; e
- informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa revogação do consentimento.

Como as organizações públicas devem atuar no tratamento de dados pessoais?

Entre outras ações espera-se que a Administração Pública, nas suas atividades rotineiras e na sua prestação de contas:

garanta que todo tratamento de dados pessoais tenha uma base legal;

mantenha registro das operações de tratamento de dados;

elabore relatório de impacto na proteção de dados pessoais quando o tratamento puder gerar riscos às liberdades civis e aos direitos fundamentais dos titulares;

conceba sistemas seguros que protejam os dados desde a sua concepção;

informe ao titular dos dados e à ANPD as violações de segurança dos dados pessoais que possam causar risco ou dano relevantes, com as devidas medidas de contenção ou mitigação;

informe ao titular dos dados, caso haja alguma alteração na finalidade para a coleta de dados;

repare os danos causados em razão do tratamento de dados pessoais que viole a legislação;

confirme a existência e providencie o acesso a dados pessoais, mediante requisição do titular;

- divulgue os tipos de dados coletados;
- avale de forma permanente as salvaguardas e mecanismos de mitigação de riscos adotados;
- indique o encarregado de dados pessoais e divulgue publicamente as suas informações de contato;
- aceite reclamações, comunicações e preste esclarecimentos aos titulares de dados quando instada a respeito.



Boas práticas e medidas de segurança

O tratamento de dados é tarefa intrínseca às diversas atividades realizadas no MPDFT:

atendimento ao público; elaboração de pareceres, perícias laudos; acessos às unidades do MPDFT; divulgação de eventos; registros de atendimentos médicos, odontológicos e psicológicos; utilização de e-mail, teams e mensagens via celular.

MPDFT



Nesse contexto, é fundamental que a instituição consiga garantir a proteção dos dados armazenados em banco de dados contra acessos indevidos, ações de hackers e incidentes técnicos, motivo pelo qual é premente a adoção de medidas de segurança por todos os membros e servidores.

É oportuno que essas medidas possam ser implementadas paulatinamente em rotinas e fluxos de trabalho de cada unidade.



Rotina de segurança da informação

Estabelecer uma rotina de segurança simplificada, que estabeleça controles relacionados ao tratamento de dados pessoais, como:



- cópias de segurança dos dados armazenados, principalmente em nuvem;
- uso de senhas com alto grau de segurança;
- verificação de senhas em duas etapas, sempre que disponível, principalmente em sistemas de armazenamento em nuvem e aplicativos de mensagens;
- controle de acesso à informação;
- controle de compartilhamento de dados;
- ativação de criptografia nos discos e mídias externas, como pendrives;
- instalação de aplicativos somente de fontes confiáveis;
- atualização do sistema operacional e dos aplicativos;
- limpeza dos dados armazenados antes de se desfazer dos equipamentos e das mídias; e
- utilização prioritária de ferramentas disponibilizadas pela instituição, tal como o teams;

Conscientização e treinamento

Membros e servidores devem ser instruídos sobre:

- a necessidade de saber as respectivas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais conforme disposto na LGPD;
- a existência de treinamento específico sobre a LGPD por meio do curso autoinstrucional “Noções Gerais sobre a Lei 13.709 - Lei Geral de Proteção de Dados”, disponibilizado pela Secretaria de Educação e Desenvolvimento Corporativo (Secor).
- como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;
- como evitar de se tornarem vítimas de incidentes de segurança corriqueiros;
- a orientação de documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;
- a proibição de compartilhar logins e senhas de acesso das estações de trabalho;
- a conduta de bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;
- a recomendação de seguir as orientações da política de segurança da informação;
- a necessidade de notificar a chefia acerca de incidentes e vulnerabilidades detectadas.

Segurança dos dados pessoais armazenados

- Coletar e processar apenas os dados pessoais que são realmente necessários para atingir os objetivos do tratamento para a finalidade pretendida, minimizando a coleta de dados.
- Orientar os usuários a não desativar ou ignorar as configurações de segurança de estações de trabalho.
- Evitar a transferência de dados pessoais de estações de trabalho para dispositivos de armazenamento externo, como pendrives e discos rígidos externos, priorizando o compartilhamento por meio das ferramentas aprovadas e disponibilizadas pelo MPDFT.
- Formatar e sobrescrever mídias físicas que contenham dados pessoais antes de descartá-las, ou, quando não for possível a sobrescrita, destruir as mídias físicas.

Segurança em dispositivos móveis

- Utilizar técnicas de autenticação multifator para controle de acesso de dispositivos móveis – como smartphones e laptops.
- Separar os dispositivos móveis de uso privado daqueles de uso institucional, quando possível.
- Implementar funcionalidades que permitam apagar remotamente os dados pessoais armazenados em dispositivos móveis.

Segurança das comunicações

- Utilizar conexões cifradas (TLS/HTTPS) ou aplicativos com criptografia fim a fim para serviços de comunicação.
- Instalar e manter um sistema de firewall e/ou utilizar um Web Application Firewall (WAF – Filtro de Aplicação).
- Proteger e-mails via adoção de ferramentas AntiSpam, filtros de e-mail e integrar o antivírus ao sistema de e-mail.
- Remover quaisquer dados sensíveis e outros dados pessoais que estejam desnecessariamente disponibilizados em redes públicas.





Ministério Público
do Distrito Federal
e Territórios

Missão do MPDFT

Promover a justiça, a democracia,
a cidadania e a dignidade humana,
atuando para transformar em
realidade os direitos da
sociedade.



Ouvidoria
MPDFT

127

www.mpdft.mp.br/ouvidoria

Eixo Monumental, Praça do Buriti, Lote 2,
Sede do MPDFT, Brasília-DF, CEP 70.091-900
Telefone: (61) 3343-9500 | www.mpdft.mp.br



mpdftoficial



mpdftoficial



mpdft



mpdftoficial

