

LGPD | Lei nº 13.709/18

Proteção de Dados Pessoais

Como a Lei Geral de Proteção de Dados
impacta na sua vida e na atividade do MPRJ



Cepdap | MPRJ

COMECE A NAVEGAR





Luciano Oliveira Mattos de Souza
Procurador-Geral de Justiça

Guilherme Magalhães Martins
Procurador de Justiça
Encarregado pelo Tratamento de Dados Pessoais

Comitê Estratégico de Proteção
de Dados Pessoais (CEPDAP/MPRJ)
Revisão e validação

Gerência de Portal e Comunicação Visual
(GPPV/MPRJ)
Projeto gráfico

SUMÁRIO

S E L E C I O N E O T E M A

1. APRESENTAÇÃO

1.1. O que é a proteção de dados pessoais?

2. FUNDAMENTOS E ALCANCE DA LGPD

2.1. A quem se aplica a LGPD?

2.2. Quando não se aplica a LGPD?

3. CONCEITOS IMPORTANTES PARA ENTENDER A PROTEÇÃO DE DADOS PESSOAIS

3.1. Dicionário LGPD.

3.2. Direitos dos titulares de dados pessoais.

4. PRINCIPAIS ATORES DA PROTEÇÃO DE DADOS PESSOAIS



5. TRATAMENTOS DE DADOS PESSOAIS

5.1. O tratamento de dados pessoais é igual para todo mundo?

5.2. Quais são os princípios da proteção de dados?

5.3. Ciclos de vida do tratamento de dados pessoais.

6. BOAS PRÁTICAS - MANTENDO OS DADOS PROTEGIDOS

7. DÚVIDAS? CEPDAP RESPONDE!

8. CONCLUSÃO

9. REFERÊNCIAS



1. Apresentação

Esta cartilha tem por objetivo informar o cidadão e os membros e servidores do Ministério Público do Estado do Rio de Janeiro (MPRJ) sobre os conceitos, os fundamentos, os princípios da Lei Geral de Proteção de Dados, os direitos dos titulares de dados pessoais e os deveres do controlador.

Com a finalidade de contribuir e promover a proteção de dados pessoais e incentivar a cultura de proteção de dados tanto dentro quanto fora da Instituição, o MPRJ, por intermédio do Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP), disponibiliza esta Cartilha sobre Proteção de Dados Pessoais.

1.1. O que é a proteção de dados pessoais?

A proteção dos dados pessoais é um direito e uma garantia fundamental, prevista no artigo 5º, inciso LXXIX, da Constituição Federal, e está regulamentada, no Brasil, sobretudo pela Lei Geral de Proteção de Dados - LGPD (Lei nº 13.709/2018).

Com o avanço das tecnologias, o desenvolvimento da economia digital e o advento da globalização, houve considerável aumento no fluxo de informações e dados, dentre os quais os de caráter pessoal. Esses dados, se relativos a uma pessoa natural, servem para identificar o respectivo titular e, quando combinados, podem ser utilizados para a formulação de perfis de personalidade e de comportamento, cuja aplicação é usual no mercado de consumo e de trabalho, além de serem utilizados para fins de estatística política, econômica e social, tanto nos órgãos de governo (Poder Público) quanto na iniciativa privada.

Dados pessoais são condição essencial para o funcionamento e para a organização da sociedade da informação, seja em âmbito privado ou público. Por representarem a pessoa humana em suas diversas manifestações, notadamente existenciais, são caracterizados como ativos valiosos para o mercado. Por isso, além de serem considerados pela doutrina há longo tempo como o “novo petróleo”, podem ser comparados ao ar que se respira e à água que se bebe, justamente por sua essencialidade, dada a imposição da condição de titular de dados pessoais ao cidadão para a plena vivência no século XXI.

MPRJ
MINISTÉRIO PÚBLICO
DO ESTADO DO RIO DE JANEIRO



Cepdap

Acompanhando as mudanças tecnológicas e visando sobretudo à concretização desse direito fundamental, em 14 de agosto de 2018 foi sancionada a LGPD, que tem por objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural (o cidadão). A redação da LGPD foi inspirada no Regulamento Geral sobre a Proteção de Dados (GDPR), de 2016, da União Europeia.

Para isso, a Lei não pretende proibir ou restringir o uso dos dados pessoais, mas disciplinar o seu tratamento, tanto nos meios físicos quanto nos digitais, seja realizado por instituições públicas ou privadas, com regras claras e transparentes, a fim de que a circulação de dados não resulte em abusos pelos responsáveis pelo tratamento e em prejuízos ou injustiças ao titular.

É importante saber o que são os dados pessoais, como eles podem ser tratados, por quem, quais os limites desse tratamento, quais são os direitos do titular e os deveres dos agentes de tratamento. A busca pelo equilíbrio de interesses e a segurança jurídica, aqui, são vias de mão dupla: servem tanto para os agentes de tratamento quanto para o titular dos dados pessoais.



2. Fundamentos e alcance da Proteção de Dados Pessoais

A LGPD elenca alguns fundamentos que devem ser necessariamente observados no tratamento de dados pessoais (artigo 2º e incisos):

- O respeito à privacidade;
- 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.





2.1. A quem se aplica a LGPD?

Os destinatários dessa norma são, no que tange ao objeto de proteção, exclusivamente, as pessoas naturais titulares de dados pessoais.

Porém a Lei se aplica e deve ser observada por todo aquele agente que realize o tratamento de dados pessoais, nos meios físicos ou digitais, por pessoa física ou jurídica, com finalidade econômica, institucional ou governamental, seja pela esfera pública ou privada.





2.2. Quando não se aplica a LGPD?

Quando o tratamento de dados pessoais for realizado:

- Por pessoa natural para fins exclusivamente particulares e não econômicos;
- Para fins exclusivamente artísticos, jornalísticos ou acadêmicos;
- Para fins exclusivos de segurança nacional, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;
- De fora do território nacional, sem comunicação ou compartilhamento com agentes de tratamento brasileiros, e desde que o país onde se encontra a sede do agente de tratamento estrangeiro possua uma legislação de proteção de dados adequada.

3. Conceitos importantes para entender a proteção de dados pessoais

3.1. Dicionário LGPD

Dado pessoal

É a informação relacionada à pessoa natural identificada ou identificável, como o nome, sobrenome, números de identidade, CPF, CNH, carteira de trabalho, passaporte, título de eleitor, matrícula do servidor, data de nascimento, e-mail, telefone, fotos, vídeos, sons, impressão digital etc.

Dado pessoal sensível

É aquele dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, dado genético ou biométrico, sempre quando vinculado a uma pessoa natural. São considerados sensíveis pelo alto potencial de gerar discriminação ou tratamento diferenciado injusto, levando o titular à vulnerabilidade ou ao seu agravamento. É por esse motivo que a Lei prevê um maior cuidado, maior cautela para o tratamento desses dados.



Dado anonimizado

É o dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (processo de anonimização). No MPRJ, eventual anonimização é responsabilidade da Secretaria de Tecnologia de Informação e Comunicação (STIC).

Banco de dados

É o conjunto estruturado de dados, dentre os quais os de caráter pessoal, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Tratamento

É o nome dado à toda operação realizada com dados pessoais, como a que se refere à coleta, à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, à transmissão, à distribuição, ao processamento, ao arquivamento, ao armazenamento, à eliminação, à avaliação ou ao controle da informação, à modificação, à comunicação, à transferência, à difusão ou à extração.

3.2. Quais são os direitos dos titulares de dados, de acordo com a LGPD?

- 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 a LGPD;
- 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 artigo 16 da LGPD;
- Obter informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Obter informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa;
- Revogar o consentimento, nos termos do § 5º do artigo 8º da LGPD;
- Peticionar em relação aos seus dados contra o controlador perante a Autoridade Nacional de Proteção de Dados.

3.2. Quais são os direitos dos titulares de dados, de acordo com a LGPD?

- Solicitar a cópia eletrônica integral de seus dados pessoais, observados os segredos comercial e industrial e na forma da regulamentação da Autoridade Nacional;
- Solicitar a revisão de decisões automatizadas que afetem os interesses dos titulares de dados pessoais, incluídas aquelas destinadas à formação de perfis digitais;
- Receber informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para as decisões automatizadas, observados os segredos comercial e industrial;
- Opor-se ao tratamento dos seus dados quando houver descumprimento da LGPD, ainda que o tratamento dos dados tenha sido feito baseado nas hipóteses em que o consentimento do titular é dispensado.

O Ministério Público do Rio de Janeiro está legalmente dispensado de obter consentimento pelos respectivos titulares nos tratamentos de dados pessoais para uso em sua atividade funcional ou para a execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres. Todavia, está obrigado a proteger todos os dados objeto de tratamento na condição de controlador.

4. Principais atores da proteção de dados pessoais

Quem é quem na proteção de dados:

Titular de dados pessoais

Trata-se da pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

Controlador

É a pessoa natural ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais. Ele possui autonomia para decidir quais os fins e os meios de tratamento. O MPRJ atua como controlador dos dados pessoais tratados na realização das suas competências constitucionais e legais. Assim, membros, servidores, estagiários, alunos residentes e terceirizados compõem o corpo do controlador (MPRJ), razão pela qual são todos responsáveis por observar fielmente a LGPD;



Operador

Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (o executor das ordens do controlador). Não se confunde com os membros, servidores ou estagiários do MPRJ. Ao contrário, o operador é externo à Instituição, porém contratado para executar uma finalidade específica, agindo sob o comando e diretrizes previamente definidas pelo controlador;

Agentes de tratamento

São o controlador e o operador;

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). Cabe a ele responder às solicitações sobre a LGPD;

Autoridade Nacional de Proteção de Dados

É o órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

5. Tratamento de dados pessoais

5.1. O tratamento de dados pessoais é igual para todo mundo?

A LGPD diferencia o tratamento de dado e o tratamento de dado pessoal de criança e adolescente.

Tratamento

É o nome dado a toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Tratamento de dado pessoal de criança e adolescente

Crianças e adolescentes têm proteção especial conferida pela Constituição da República, e tudo o que as envolver deve ser guiado pelo princípio da absoluta prioridade e considerando o seu melhor interesse. A LGPD determina que o tratamento de dados referentes às crianças e adolescentes deverá ser realizado com o consentimento específico e em destaque, dado por, pelo menos, um dos pais ou pelo responsável legal, quando a base legal for o consentimento (§1º do artigo 14 da LGPD). O MPRJ pode realizar esse tratamento sem o consentimento quando os dados forem imprescindíveis para a defesa dos direitos da criança e do adolescente, isto é, para a sua proteção.

5.2. Quais são os princípios da proteção de dados?

Todo tratamento de dados pessoais deve observar a boa-fé, bem como diversos princípios previstos na LGPD.

Finalidade

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

Adequação

É a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

Necessidade

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

Livre acesso

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



Qualidade dos dados

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

Transparência

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

Segurança

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

Prevenção

Constitui na adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

Não discriminação

É a impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;

Responsabilização e prestação de contas

É a 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.

5.3. Ciclos de vida do tratamento de dados pessoais:

O tratamento dos dados pessoais, por vezes, segue uma linha do tempo. Nela, podem ocorrer operações de: 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 diversas as etapas possíveis, a depender do dado pessoal e do tratamento que será dispensado a ele.

Vamos abordar, aqui, o ciclo de vida do tratamento de dados pessoais:

Coleta

É a obtenção, recepção ou produção de dados pessoais independente do meio utilizado (pode ser documento em papel, documento eletrônico, sistema de informação etc.);

Processamento

Diz respeito a qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais;

Retenção

É o arquivamento ou armazenamento de dados pessoais independentemente do meio utilizado (armazenamento de documento em papel, documento eletrônico, por meio de banco de dados, arquivo de aço etc.);

Compartilhamento

Consiste em qualquer operação que envolva a transmissão, distribuição, comunicação, transferência, difusão e/ou compartilhamento de dados pessoais;

Eliminação

Constitui qualquer operação que visa apagar ou eliminar dados pessoais. Essa fase também contempla descarte dos ativos organizacionais nos casos necessários às funções da Instituição.

6. Boas práticas - mantendo os dados protegidos

A proteção dos dados pessoais depende de cada um de nós. Não acontece do dia para a noite, sendo uma questão de adoção de boas práticas que, com o tempo, se transforma em uma verdadeira cultura de proteção de dados.

Existem medidas simples que devemos adotar e comportamentos que devemos evitar para a adequação à LGPD. Assim, servidores e membros do MPRJ devem estar atentos às boas-práticas quanto ao tratamento de dados pessoais. Nesse sentido:



O QUE FAZER

Use senha forte e exclusiva para os sistemas do MPRJ e realize a troca sempre que solicitado. Ative a verificação em duas etapas: assim, mesmo que descubram sua senha, dificilmente conseguirão invadir sua conta.

Utilize uma chave de segurança física, um aplicativo de celular que gere códigos de verificação, ou mesmo receber códigos por mensagens de texto ou voz.



O QUE NÃO FAZER

Usar a mesma senha para acessar tanto sistemas do MPRJ quanto sites, aplicativos e cadastros de uso pessoal. No caso da sua senha ser descoberta, o invasor terá acesso tanto às suas redes pessoais (e-mails, redes sociais, logins em sites e aplicativos), quanto ao seu ambiente de trabalho, colocando em risco os dados e sistemas do MPRJ.



O QUE FAZER

Troque periodicamente as suas senhas, preferencialmente a cada seis meses: isto aumenta a sua segurança e dificulta o trabalho de um hacker/cracker/invasor. Escolha senhas com no mínimo 16 caracteres, e que contenha letras maiúsculas e minúsculas, números e caracteres especiais.

Ex.: S3nHacom+1secur@ **Este exemplo não deve ser utilizado**



O QUE NÃO FAZER

Compartilhar senha: a senha é pessoal e intransferível, pois ela protege os seus dados, os dados de terceiro a que você tenha acesso, e mantém as informações em segurança. A rastreabilidade dos acessos indicará o responsável em caso de tratamento inadequado ou desconformidade com a LGPD.

Instale um antivírus (*antimalware*) e mantenha-o atualizado: configure o antivírus para verificar automaticamente toda e qualquer extensão de arquivo, arquivos anexados aos e-mails, obtidos pela internet e os discos rígidos e as unidades removíveis. Não se esqueça de verificar os arquivos recebidos antes de abri-los ou executá-los.

Baixar arquivos ou abrir arquivos de pen drives sem prévia varredura de antivírus. Esquecer de atualizar ou deixar de renovar a assinatura do seu antivírus: os computadores do MPRJ possuem proteção antivírus, não a desative.



O QUE FAZER

Utilize os programas homologados ou adquiridos pelo MPRJ. Além disso, mantenha os programas atualizados, instalando as atualizações disponíveis (se possível, opte pela atualização automática), e remova as versões antigas e os programas que você não utiliza mais.

Descarte papéis e documentos que contenham dados pessoais de forma correta: use um fragmentador de papel ou, se não o tiver, corte/ pique/rasgue o papel a fim de evitar a leitura do seu conteúdo.

Bloqueie a tela do seu computador ou aparelho celular com senha, e ative este bloqueio sempre que se ausentar da estação de trabalho ou não estiver usando o celular.



O QUE NÃO FAZER

Usar programas não originais, os chamados “piratas”; esses programas de procedência duvidosa colocam a sua segurança e a segurança do MPRJ em risco: se você trabalha usando o aplicativo Word, por exemplo, mas o seu pacote Office é pirata, seu computador fica vulnerável a vírus e malwares ocultos.

Deixar papéis ou documentos que contenham dados pessoais à vista de qualquer um (na mesa, impressora, copiadora, fax).

Deixar a tela do computador ou do celular aberta/ exposta ou desbloqueada quando se ausentar da estação de trabalho: corre o risco de um terceiro acessar informações pessoais e/ou confidenciais.



O QUE FAZER

Utilizar a opção sair ou desconectar para fechar os sistemas em uso mantendo a conexão VPN apenas pelo tempo necessário para realização do trabalho.

Armazene dados pessoais preferencialmente nos sistemas de informação do MPRJ: as ferramentas de armazenamento da instituição possuem varreduras de segurança e/ou são protegidas por senha (*One Drive, One Note, Teams etc.*).

Tomando ciência de alguma falha de segurança ou violação de dados pessoais, reporte imediatamente ao Encarregado pela Proteção de Dados do MPRJ, com o máximo de informações possíveis sobre o ocorrido.



O QUE NÃO FAZER

Deixar VPN conectado depois de finalizadas as atividades laborais: aumentam as chances de terceiros ou invasores acessarem os sistemas internos.

Coletar informações desnecessárias: menos é mais. Lembre-se do princípio da finalidade, limite o tratamento ao mínimo necessário, de forma proporcional e não excessiva.

Abrir e-mails suspeitos, quando não conhecer o remetente ou tiver dúvidas quanto à origem: abrir, acessar ou clicar em links de e-mails desconhecidos, falsos ou maliciosos é uma das maiores causas de incidentes de segurança.



O QUE FAZER

Use o e-mail funcional apenas para atividades afetas ao exercício da função no MPRJ: o e-mail funcional serve para a comunicação entre membros e servidores sobre a realização e desempenho das funções. A [Resolução GPGJ nº 1.767/12](#) determina que as caixas postais de correio eletrônico são de propriedade do MPRJ, devendo limitar-se às atividades precípuas da instituição, vedando-se a utilização desse e-mail para cadastro em formulários de empresas ou sites.



O QUE NÃO FAZER

Use seu e-mail funcional para realizar cadastro em sites ou compras em lojas, para se comunicar com pessoas de fora do MPRJ, ou sobre assuntos que não digam respeito às atividades desenvolvidas na instituição: caso ocorra um vazamento das informações das bases de dados dessas empresas, seu e-mail, senha e dados pessoais estarão visíveis para todos e, caso utilize uma mesma senha para acessar tanto o cadastro desses sites quanto os sistemas do MPRJ, o risco de incidente de segurança é potencialmente maior.

Limite o uso de notebooks/desktops e celulares funcionais apenas para atividades relacionadas ao trabalho: Caso haja algum incidente de segurança envolvendo o aparelho funcional, os seus dados pessoais não serão atingidos.

Utilizar os notebooks, desktops e celulares funcionais para assuntos pessoais, ou permitir que terceiros façam uso desses equipamentos.





O QUE FAZER

Ao tratar dados pessoais, observe as normas aplicáveis, políticas e boas práticas adotadas pelo MPRJ. Na dúvida, pergunte ao Encarregado, ele é responsável pela adequação da instituição à LGPD.

Reduzir os riscos relacionados à segurança da informação.

Evite o acesso não autorizado aos dados controlados pelo MPRJ. É sua responsabilidade tomar as cautelas necessárias para que terceiros não acessem dados pessoais tratados pela instituição e utilizados por você na realização das suas atividades institucionais.



O QUE NÃO FAZER

Utilizar dados pessoais desatualizados ou inexatos. Os dados pessoais pertencem a uma pessoa natural, devem assim condizer com a verdade. A desinformação pode ser extremamente prejudicial tanto para o titular quanto para o trabalho desenvolvido pelo MPRJ.

Enviar e-mails para pessoas ou grupo maior do que o necessário: quanto menor o grupo, mais fácil de resguardar a segurança ou sigilo da informação compartilhada.

Postar nas redes sociais dados pessoais, inclusive dados sensíveis de terceiros. A proteção de dados pessoais é um direito e um dever. Seja consciente.



O QUE FAZER

Limitar o acesso aos dados pessoais apenas aos agentes que necessitem destes para as atividades da Administração Pública, e compartilhar informações apenas pelos meios adequados.

Retirar documentos impressos com dados pessoais da impressora rapidamente.

Conectar-se com redes *wifi* seguras e conhecidas.

Utilizar como rascunho materiais que não contenham dados pessoais. É também sua responsabilidade prezar pelo atendimento à LGPD e, portanto, deve-se estar atento a qualquer possibilidade de manejo de dados pessoais.



O QUE NÃO FAZER

Fornecer dados pessoais por e-mail, telefone ou qualquer outro canal inadequado.

Mandar imprimir um documento com dados pessoais e deixar para pegar depois.

Conectar-se em redes *wifi* desconhecidas ou de livre acesso, facilitando eventual invasão ao dispositivo e compartilhamento indevido de dados.

Utilizar como rascunho papéis com dados pessoais e não os descartar apropriadamente.

7. Dúvidas? O CEPDAP responde!

O MPRJ vem se adequando à Lei Geral de Proteção de Dados Pessoais e está engajado na criação de uma verdadeira cultura institucional de proteção de dados pessoais. Com este objetivo, foi criado o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) por meio da Resolução GPGJ nº 2.434/2021, que definiu as atribuições do órgão colegiado, bem como do Encarregado pelo Tratamento de Dados Pessoais. Dentre estas atribuições, está a de receber e analisar os pedidos encaminhados pelos titulares dos dados pessoais e pelos servidores e membros, como reclamações e comunicações, prestar esclarecimentos e adotar providências relacionadas ao tratamento de dados pessoais.

Qualquer requisição com relação aos dados pessoais tratados pelo MPRJ pode ser feita pelo titular ao Encarregado de Dados através de Procedimento SEI (Sistema Eletrônico de Informações). Se for titular de dados sem vínculo institucional com o MPRJ, poderá ser realizada solicitação mediante o ícone “Acesso Externo” do SEI. O titular deverá realizar um cadastro prévio, para assim criar um login e senha de acesso. Feito isto, é só seguir o passo-a-passo previsto na página <https://portalsei.mprj.mp.br/>.

MPRJ
MINISTÉRIO PÚBLICO
DO ESTADO DO RIO DE JANEIRO



Cepdap



8. Conclusão

A Lei Geral de Proteção de Dados é aplicável tanto ao setor privado como ao setor público, onde se insere o Ministério Público do Rio de Janeiro.

ALGPD dedicou um capítulo inteiro ao tratamento de dados pelo Poder Público (artigos 23 ao 32). Quanto ao Ministério Público, na maioria das vezes o tratamento de dados pessoais pode ser realizado sem o consentimento prévio do titular, justamente porque o MPRJ realiza 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. Além disso, o MPRJ compromete-se a atender à finalidade pública e a perseguir o interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Ainda, cabe ao MPRJ, na condição de controlador, informar as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seu [sítio eletrônico](#).

A LGPD impôs à Administração Pública o dever de revisar e adequar as atividades que envolvem o tratamento de dados pessoais. A lei resguarda os direitos fundamentais de liberdade, privacidade e proteção de dados pessoais, além do livre desenvolvimento da personalidade da pessoa natural.

No Ministério Público do Estado do Rio de Janeiro, o Comitê Estratégico de Proteção de Dados Pessoais (CEPDAP) é o responsável pelo cumprimento e a implementação da LGPD na Instituição.



MPRJ
MINISTÉRIO PÚBLICO
DO ESTADO DO RIO DE JANEIRO

Cepdap

Entre as últimas realizações do CEPDAP, destaca-se a publicação, em 28 de outubro de 2022, da Política de Privacidade e Proteção de Dados Pessoais, que fixou parâmetros para o tratamento de dados pessoais de usuários do portal do MPRJ, seus sistemas e serviços. O órgão também atua em cláusulas gerais de proteção de dados para os contratos firmados pelo MPRJ e estabeleceu o Programa de Governança em Privacidade, assim como o Plano de Resposta e Remediação de Incidentes de Segurança de Dados.

Como órgão colegiado de natureza permanente, cabe ao CEPDAP, entre outras funções, propor e monitorar o Programa de Governança em Privacidade do MPRJ e a Política de Privacidade e Proteção de Dados Pessoais, bem como elaborar um Manual de Processos Organizacionais sobre as medidas de execução relacionadas a eles, além de aprovar Relatórios de Impacto à Proteção de Dados Pessoais (RIPD).

O CEPDAP é presidido pelo encarregado de dados da Instituição, que atua como um elo entre a Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e o MPRJ. Cabe-lhe coordenar as políticas e programas relacionados à temática, receber e analisar pedidos de titulares de dados pessoais, prestar esclarecimentos e adotar eventuais medidas necessárias, receber as comunicações da ANPD, comunicar ao Procurador-Geral de Justiça e ao titular de dados pessoais a ocorrência de incidente de segurança que acarrete risco ou dano relevante ao titular, elaborar o Relatório de Impacto de Dados Pessoais, opinar sobre as cautelas de privacidade em sistemas de informação, produtos ou serviços que envolvam tratamentos de dados pessoais, dentre outras atribuições.

Para conhecer mais o CEPDAP e suas iniciativas, basta [acessar a página na internet](#).

Em conclusão, para garantir a observância da LGPD, toda a Instituição deve conhecer o seu conteúdo. O conhecimento, somado às boas práticas, permite que cada membro, servidor, estagiário, aluno residente e terceirizado se certifique de que o tratamento dos dados pessoais se coaduna com os fins legítimos e restritos à finalidade pública e interesse públicos.

9. Referências

ANPD - Autoridade Nacional de Proteção de Dados, Guia orientativo: Tratamento de Dados Pessoais pelo Poder Público. Brasília: jan./2022. Disponível em [guia-poder-publico-anpd-versao-final.pdf \(www.gov.br\)](http://www.gov.br/guia-poder-publico-anpd-versao-final.pdf). Acesso em 08/03/2023.

CCGD - Comitê Central de Governança de Dados, Guia de Boas Práticas - Lei Geral de Proteção de Dados (LGPD). Brasília: abr./2020. Disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 01/02/2023.

Centro de Estudos, Respostas e Tratamento de Incidentes de Segurança no Brasil, Cartilhas de Segurança para Internet. Disponível em: [Fascículos - Cartilha de Segurança para Internet \(cert.br\)](http://cert.br/fasciculos-cartilha-de-seguranca-para-internet) Acesso em 01/02/2023.

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. Acesso em: 01/02/2023.

MPRS - Ministério Público do Rio Grande do Sul, Cartilha LGPD. Rio Grande do Sul. Disponível em https://www.mprs.mp.br/media/areas/igpd/arquivos/cartilha_lgpd.pdf. Acesso em 01/02/2023.

Proteção de Dados Pessoais



Cepdap | MPRJ

Projeto Gráfico

 **gppv** Gerência de Portal
e Programação Visual