Lei Geral de Proteção de Dados Pessoais

Lei Federal nº 13.709/2018

GUIA ORIENTATIVO PARA OS SERVIDORES PÚBLICOS DO MUNICÍPIO DE JOINVILLE

Prefeitura de Joinville

Comitê Municipal de Proteção de Dados Pessoais

Este Guia foi desenvolvido com o intuito de apresentar os pontos relevantes da Lei Geral de Proteção de Dados - LGPD, portanto seu conteúdo possui caráter meramente informativo e não substitui o aconselhamento jurídico, caso necessário.

O que é LGPD?

A Lei Geral de Proteção de Dados - LGPD - Lei Federal nº 13.709/2018, está vigente, na sua totalidade, desde agosto de 2021 e estabelece regras sobre o tratamento (utilização) de dados pessoais de pessoa natural (pessoa física), seja por meios físicos ou digitais, protegendo os direitos fundamentais de liberdade, privacidade e personalidade de qualquer indivíduo.

A Lei traz um conjunto de boas práticas/ações para a utilização responsável de dados pessoais em atividades econômicas.

Essas boas práticas dizem respeito à capacitação e mudança de cultura das equipes de trabalho, documentos jurídicos e segurança da informação.

Quem deve cumprir a Lei e qual é a sua importância?

Todos que utilizam **dados pessoais** em atividades econômicas - públicas, privadas e pessoa física quando MEI, profissional autônomo ou liberal - (independente do seu porte) com **finalidade econômica**.

No caso do **Poder Público**, não se obtém lucro, contudo a prestação do serviço ocorre. Há um intenso tratamento (utilização) de dados pessoais. Assim, aplica-se a LGPD.

Desta forma, os agentes e servidores públicos deverão conhecer e adotar as boas práticas de proteção e privacidade decorrentes de sua atividade funcional, preservando os direitos e garantias dos cidadãos em estrita conformidade com a Lei.

O que é Dado Pessoal?

É qualquer informação que possa identificar alguém de forma direta ou indireta. Nome, e-mail, endereço, RG, CPF, dados de saúde, opção sexual, origem racial, entre outras.

Quem é o titular dos dados pessoais?

É a própria pessoa natural (física), ou seja, o indivíduo a quem os dados pessoais se referem.

Exemplo: servidor público, munícipe, contribuinte, usuário do SUS, estudante da Rede Pública.

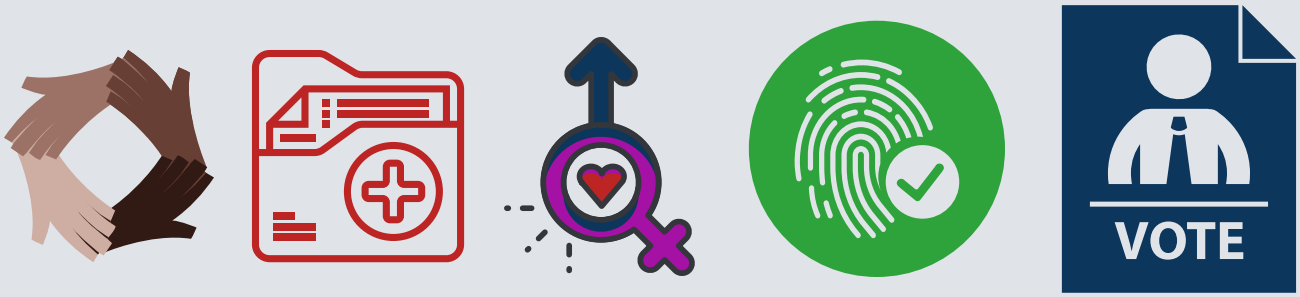
O que é o tratamento (utilização) de dados?

É tudo que é feito com o dado pessoal da pessoa natural (física) desde a sua coleta até a sua eliminação.

Exemplo: Quando um paciente/usuário do Sistema Único de Saúde vai a uma Unidade Básica de Saúde da Família, primeiramente preenche-se uma ficha de cadastro. Neste momento, são coletados dados cadastrais desse paciente, além de outras informações, como: motivo da consulta, se existe alergia a algum medicamento. Geralmente, tudo isso fica armazenado no banco de dados do Sistema de Saúde Municipal. A maneira de armazenar esses dados pessoais é regulamentado pela Lei Geral de Proteção de Dados. Não esquecendo que em um serviço de saúde, os dados pessoais de saúde são classificados como dados sensíveis.

A gestão dos dados pessoais, dentro da Administração, conforme a LGPD, deve ter um ciclo de vida definido:

O que são dados sensíveis?



São dados pessoais sobre 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 (física).

Dados de Crianças e Adolescentes também são considerados dados sensíveis.

O que a LGPD proíbe?

- O compartilhamento de dados pessoais para outras finalidades, além daquelas já especificadas para a pessoa natural (física)/titular dos dados pessoais.
- A Lei veda expressamente a comunicação ou o uso compartilhado de dados pessoais sensíveis referentes à saúde com o objetivo de obter vantagem econômica, exceto situações específicas.

As situações específicas são: o compartilhamento quando a finalidade é a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços de diagnóstico e terapia, em benefício dos interesses do titular, interesse público ou execução de políticas públicas.

Os dados pessoais utilizados precisam estar enquadrados em uma ou mais hipóteses autorizativas/bases legais trazidas pela LGPD:

CONSENTIMENTO

Autorização livre, informada e inequívoca da pessoa natural (física)/titular dos dados pessoais, concordando com o tratamento de dados para finalidade determinada.
Ex: aceite aos termos de privacidade após cadastro de plataforma de e-commerce.

CUMPRIMENTO DE OBRIGAÇÃO LEGAL OU REGULATÓRIA

Dados da pessoa natural (física) utilizados por determinação legal.
Ex: exposição da remuneração dos servidores no Portal da Transparência, por exemplo.

EXECUÇÃO DE POLÍTICAS PÚBLICAS

Justifica a utilização de dados pessoais para formulação de políticas públicas.
Ex: agendamento de vacinas mediante prévio cadastro.

ESTUDOS POR ÓRGÃOS DE PESQUISA

Sem fins lucrativos/ pesquisa de natureza científica, histórica, tecnológica ou estatística.
Ex: pesquisas sobre determinado diagnóstico/doença.

EXECUÇÃO DE CONTRATOS

Dados pessoais utilizados para cumprimento de termos contratuais
Ex: empresa que imprime os carnês de IPTU, envio de folha de pagamento dos servidores para o Banco.

EXERCÍCIO REGULAR DE DIREITO EM PROCESSO

Quando os dados pessoais precisam ser utilizados em processo judicial, administrativo, arbitral.
Ex: utilização de dados para ajuizamento de uma demanda.

PROTEÇÃO DA VIDA E SAÚDE DO TITULAR OU DE TERCEIROS

Ex: quando ocorre um acidente, o paciente/titular de dados se encontra inconsciente e os socorristas necessitam verificar seus documentos pessoais para informar a família.

PROTEÇÃO AO CRÉDITO

Ex: pesquisa de cadastro para concessão de crédito.

TUTELA DA SAÚDE

Essa hipótese autorizativa é destinada especificamente para procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Ex: equipe médica que compartilha informações sobre o paciente para chegar ao tratamento adequado.

GARANTIA DE PREVENÇÃO À FRAUDE E À SEGURANÇA DO TITULAR

É utilizada para autenticação de cadastro em sistemas eletrônicos. Ex: registro ponto por biometria.

LEGÍTIMO INTERESSE

Quando há comprovado legítimo interesse no tratamento (utilização) dos dados pessoais. Neste caso a Lei solicita a realização de um teste de Legítimo Interesse (LIA).
Ex: uma ação de marketing via e-mail, quando o titular de dados já é cliente.

A LGPD traz princípios específicos que devem ser observados quando do tratamento (utilização) de dados pessoais:

FINALIDADE

Deve existir uma finalidade específica e legítima para a utilização de cada dado pessoal.

Se não existir uma justificativa para a coleta de um dado pessoal, ele não deve ser utilizado.

ADEQUAÇÃO

Os dados pessoais devem ser relevantes e adequados para atingir a finalidade fixada.

Exemplo: é necessário ou adequado saber a convicção religiosa de um paciente para fins de um atendimento ambulatorial?

A resposta seria não.

Mas e se o atendimento for cirúrgico? Há religiões que proíbem a transfusão de sangue.

NECESSIDADE

Apenas os dados pessoais necessários para atingir a finalidade estabelecida devem ser coletados e utilizados.
Um dado pessoal não pode ser recolhido sob a hipótese de "quem sabe um dia será necessário".

TRANSPARÊNCIA

O titular dos dados pessoais deve ser informado de forma clara e ter o acesso garantido às informações sobre os seus dados pessoais, para que eles são utilizados, onde e por quanto tempo fica armazenado.

LIVRE ACESSO

Garantia aos titulares de dados pessoais, 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

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

SEGURANÇA

É necessário implementar medidas reais de segurança e planos de contingência em caso de incidentes, como vazamentos ou perda de dados.
Todo material com dados pessoais deve estar sob controle e só pode ser acessado, visualizado, copiado, modificado ou destruído por quem tenha autorização para tanto.
O titular dos dados pessoais deverá ser informado quanto ao necessário compartilhamento de seus dados aos operadores.

NÃO DISCRIMINAÇÃO

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

PREVENÇÃO

Adoção de medidas para prevenir a ocorrência do tratamento para fins discriminatórios ilícitos ou abusivos.

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.

Assim, não basta o enquadramento em uma das hipóteses autorizativas/bases legais para se iniciar o tratamento/utilização de dados pessoais. É fundamental garantir que todos os princípios listados sejam respeitados.

Quais são os direitos das pessoas naturais/titulares de dados em relação aos seus dados pessoais, trazidos pela LGPD? O que elas podem exigir?

1. Direito de obter a confirmação da utilização dos seus dados pessoais, bem como o acesso à eles.

2.Direito de requerer a correção de dados incompletos, inexatos ou desatualizados. A correção deverá ser providenciada imediatamente.

3.Direito de requerer a suspensão da utilização dos dados pessoais ou a sua exclusão quando forem desnecessários, excessivos ou utilizados em desconformidade com a LGPD.

4.Direito de obter informação das entidades públicas e privadas com as quais foram realizados o compartilhamento de dados pessoais.

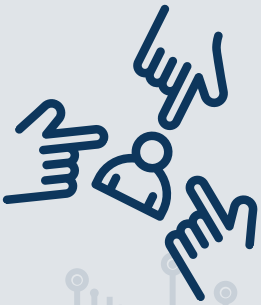
5.Direito de obter a informação sobre a possibilidade e as consequências de não fornecer o seu consentimento sobre a utilização de dados pessoais.

6.Direito de revogar a sua autorização (consentimento) anteriormente concedida para a utilização dos dados. Você não poderá mais utilizar os dados pessoais obtidos com base no consentimento, exceto para finalidades que se encaixem em outros fundamentos, como por exemplo, cumprimento de obrigação legal e exercício regular de direito.

7.Direito de solicitar a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa.

8.Direito da pessoa física em enviar à Autoridade Nacional de Proteção de Dados a sua avaliação pela forma que os seus dados pessoais são utilizados, informando, inclusive de imediato o descumprimento de alguma obrigação imposta pela lei.

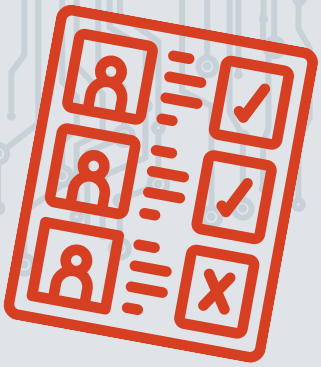
9.Direito de não ser tratado de forma discriminatória, ilícita ou abusiva com base nos dados pessoais informados.



10.Direito de se opor a utilização dos seus dados pessoais, quando realizados em desconformidade com os dispostos na LGPD.

ATENÇÃO: Informações simples devem ser apresentadas imediatamente à pessoa física e informações mais completas (direito de informação e direito de acesso) dentro do prazo de 15 (quinze) dias a partir da solicitação realizada.

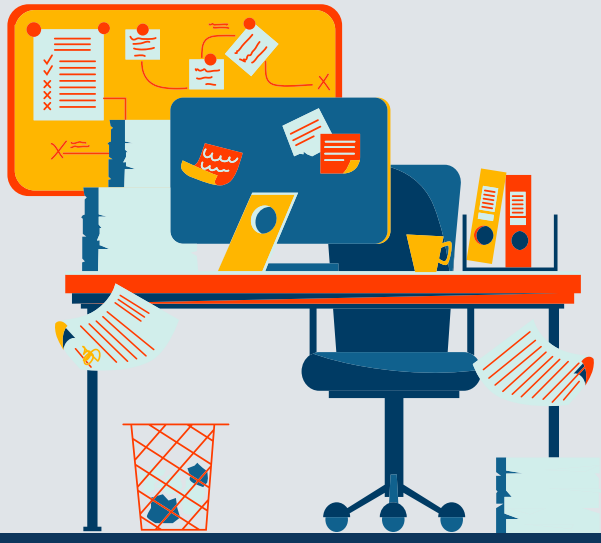
Na prática, em nosso ambiente de trabalho onde podemos encontrar os riscos? Quais são as situações diárias que devem ser observadas?



Lista de presença de reuniões publicadas, contendo nomes, telefones e e-mails.

Utilização de meios não oficiais para execução de trabalhos e o seu compartilhamento - como planilhas de Sistemas não utilizados e monitorados pelo Órgão Público, contendo dados pessoais de servidores, contribuintes, usuários do Sistema Único de Saúde, etc.

Papéis/planilhas/cópia de documentos, fotos, deixados sobre as mesas de trabalho.



Outras situações...

Senhas expostas, Anotadas em bloquinhos, agendas.

Senhas compartilhadas.

Utilização de mídias removíveis (pessoal) em equipamentos institucionais.

Arquivos físicos sem controle de acesso, sem proteção.

Outras situações...

Baixar documentos, fotos, sem a permissão da área competente.

Utilização de e-mail pessoal para compartilhamento de assuntos de trabalho.

Clicar em arquivos desconhecidos, recebidos via e-mail.

Sair da estação de trabalho e não bloquear o computador;

Utilização de WhatsApp particular para envio de documentos de trabalho, que muitas vezes contém dado pessoal.

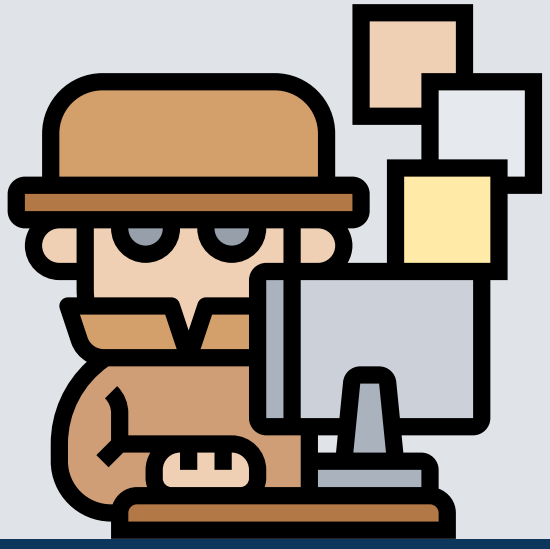
Profissionais de saúde que dividem o mesmo espaço, bem como recepcionistas e equipes administrativas, necessitam redobrar os cuidados e se atentarem às medidas para reduzir a ocorrência de incidentes de segurança relacionados, por exemplo o acesso de dados pessoais por quem não deve tê-los. Por isso é importante segmentar o acesso ao sistema utilizado.

Estudos apontam que o maior número de incidentes de vazamento de dados ocorre por falha humana.

Mesmo não se tratando de espaço compartilhado, os profissionais e funcionários devem ter restrições aos acessos de dados armazenados, acessando apenas dados estritamente necessários para o exercício de suas atividades.

ATENÇÃO

Compartilhar dados de saúde, como dados para DPVAT, por exemplo, bem como dados previdenciários, com empresas e outros profissionais que utilizarão esses dados pessoais e sensíveis para obter vantagem econômica em suas atividades, enseja responsabilização administrativa, civil e criminal.



Penalidades aplicadas pela Autoridade Nacional de Proteção de Dados

- Advertência, com indicação de prazo para adoção de medidas corretivas.
- Multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.
- Multa diária.
- 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.

Penalidades aplicadas pela Autoridade Nacional de Proteção de Dados

- 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.

Lembrando que ações indenizatórias também podem ser ajuizadas pelo titular de dados que se sentir prejudicado com condutas relacionadas a utilização de seus dados pessoais.

Processo de adequação à LGPD pela Prefeitura de Joinville

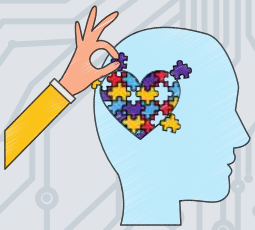
Ao longo dos próximos meses, a Prefeitura de Joinville, através do Comitê Municipal de Proteção de Dados Pessoais e a Área de Proteção de Dados promoverá uma série de ações visando a adequação das atividades do Poder Público Municipal à Lei Geral de Proteção de Dados Pessoais.

Para tanto, a colaboração de todos os servidores será imprescindível para o sucesso do processo.

Esta cartilha é o primeiro passo desse processo de adequação, e tem por objetivo a conscientização e sensibilização dos servidores sobre o texto legal, seu impacto e a necessidade de adequação de fluxos e procedimentos internos.

Fases do processo de adequação

1. Avaliação e Conscientização



2. Mapeamento

3. Análise de Riscos

4. Planejamento das ações de adequação e mitigação de riscos

5. Execução das ações de adequação e mitigação de riscos

Considerações Finais

Neste momento, não há aqui o propósito de se apresentar uma metodologia de implementação da LGPD ou abranger e esgotar todos os aspectos de tal lei, uma vez que algumas diretrizes de proteção de dados da LGPD necessitam de detalhamento, em regulamentos e procedimentos próprios, que futuramente serão elaborados e publicados no âmbito da administração pública municipal.

Capacitações e novas cartilhas com aprofundamento em cada um dos capítulos aqui existentes serão fornecidos periodicamente para que os servidores possam atuar no atendimento das diretrizes de adequação à LGPD de maneira mais consciente, sempre com o olhar na preservação da intimidade de cada cidadão que estiver sob os nossos cuidados, como servidores. Todavia, essa cartilha deverá nortear as práticas de segurança da informação quanto as práticas já mencionadas no nosso ambiente de trabalho.

Sobre a elaboração e revisão deste conteúdo

O presente guia foi elaborado por:

Sahmara Liz Botemberger

e revisado pelo Comitê Municipal de Proteção de Dados Pessoais do Município de Joinville, instituído pelos Decreto nº 44.844/2021 e Decreto nº 46.169/2022 e composto por:

Procuradoria Geral do Município
Christiane Schramm Guisso - Procuradora-Geral
Felipe Cidral Sestrem

Secretaria de Administração e Planejamento
Sahmara Liz Botemberger
Caio Amaral

Controladoria Geral do Município
Adriano Selhorst Barbosa
Marina Gonçalves Mendonça Benvenutti

Secretaria de Governo
Regiane Cristina Klug Patricio
Dixon Torres

Secretaria de Gestão de Pessoas
Fernanda Luiza Daniel Bonett Shcolze
Camila Arnoldo

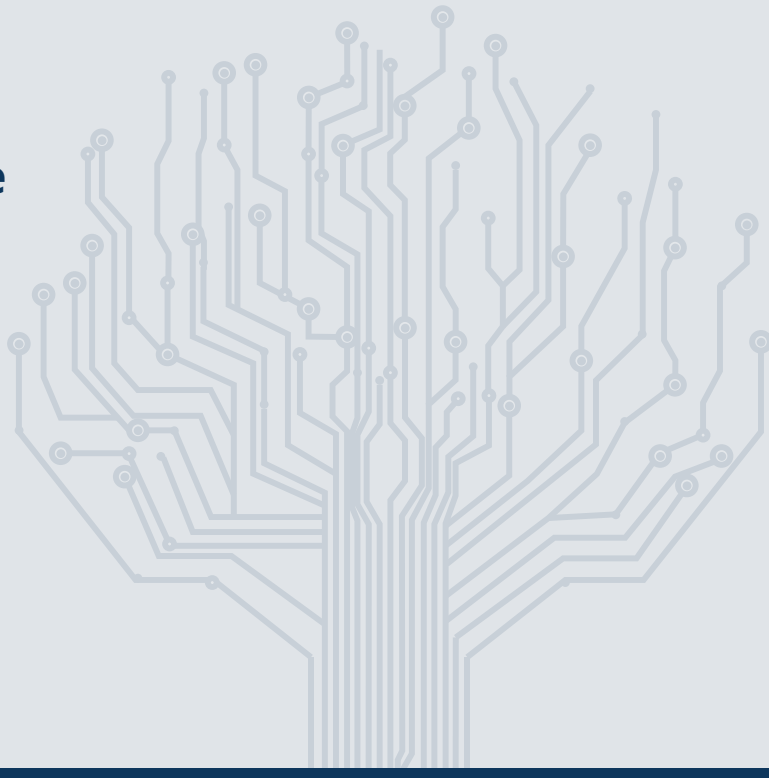
Secretaria da Fazenda
Milene Jonck Antunes
Heloísa de Moraes Menegazzo

Secretaria da Saúde
Felipe Canalli Massignan
Rodrigo Ponick

Secretaria de Educação
Felipe Hardt
Artur Nagel

Secretaria da Assistência Social
Rafael Fernando Rauber
Cleder Lourenço

Companhia Águas de Joinville
Giovani José Osmarini
Alexandre Damaceno



Versão 1.0

Prefeitura de Joinville

Comitê Municipal de Proteção de Dados Pessoais