

LGPD LGPD

LEI

GERAL DE

PROTEÇÃO

DE DADOS

PESSOAIS



PREFEITURA DE
HOLAMBRA
O TRABALHO CONTINUA
2025 - 2028

1. APRESENTAÇÃO

VOCÊ SABE O QUE É A LEI GERAL DE PROTEÇÃO DE DADOS - LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) – **Lei Federal nº 13.709/2018** – representa um importante avanço na garantia da privacidade e da segurança das informações pessoais no Brasil, a LGPD estabelece diretrizes claras sobre como empresas, órgãos públicos e demais entidades devem tratar os dados pessoais que coletam e utilizam, assegurando aos titulares maior controle sobre suas próprias informações. No município de Holambra, a aplicação da LGPD no âmbito da administração pública foi regulamentada pelo **Decreto Municipal nº 1.732/2022**.

Diante da relevância do tema e da necessidade de orientar servidores, gestores e demais interessados sobre os cuidados exigidos pela legislação, elaboramos este guia com informações essenciais. Aqui, você encontrará explicações objetivas sobre os principais conceitos da LGPD, suas implicações no dia a dia da administração pública e as ações práticas que devem ser adotadas para garantir conformidade com a norma.

Boa Leitura!

ESTE GUIA TEM CARÁTER INFORMATIVO E NÃO SUBSTITUI A LEI!

2. CONCEITOS IMPORTANTES

DADO PESSOAL: Informação ligada a uma pessoa que pode ser identificada ou identificável, como **nome, CPF e endereço**.

DADO PESSOAL SENSÍVEL: são dados que podem colocar o titular sob situação de vulnerabilidade ou discriminação e, portanto, devem observar um cuidado maior do que os dados pessoais. Exemplos: **dados de saúde, filiação política, dados biométricos, etnia ou origem racial, convicção religiosa e etc.**

TITULAR: pessoa natural a quem os dados pessoais e dados pessoais sensíveis se referem.

TRATAMENTO: qualquer ação feita com dados pessoais, como coletar, compartilhar, armazenar, entre outros.

CONTROLADOR: agente ao qual competem as decisões referentes ao tratamento de dados pessoais. Por exemplo, o Município de Holambra é o controlador dos dados tratados na realização de suas atividades.

OPERADOR: agente que realiza tratamento de dados pessoais em nome e por ordem do Controlador.

ENCARREGADO: é a pessoa encarregada de interagir com os titulares (manter comunicação, fornecer esclarecimentos e tomar providências), lidar com a ANPD (receber comunicações e tomar providências) e dentro da Administração (orientar, auxiliar e implementar as melhores práticas para proteção de dados pessoais).

COMPARTILHAMENTO: divulgação de dados pessoais no exercício de suas responsabilidades

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.



3. COMO IDENTIFICAR SE ESTOU TRATANDO DADOS PESSOAIS?

A Lei Geral de Proteção de Dados (LGPD) define de maneira abrangente o que constitui o tratamento de dados pessoais no âmbito do Poder Público. Todas as etapas relacionadas a esses dados, desde a coleta até a eliminação, são compreendidas, abarcando ações cotidianas como produção, classificação, utilização, acesso, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação, controle, modificação, comunicação, transferência, difusão ou extração.

Mesmo atividades aparentemente simples, como uma pesquisa em um sistema ou o envio de informações para outro setor, são consideradas operações de tratamento de dados pessoais pela LGPD. Independentemente da complexidade da ação, é imperativo que as organizações do setor público observem as bases legais e princípios estabelecidos na LGPD, além de atender às normativas específicas do município. Esse cuidado é essencial para garantir a continuidade das atividades públicas de forma alinhada às novas regras de proteção aos dados pessoais.



4. OS 10 PRINCÍPIOS DA LGPD

1 FINALIDADE

Direito ao tratamento de dados para propósitos específicos, legítimos e relevantes, informados ao titular. Impossibilidade de finalidade genérica e indeterminada, não sendo possível aos agentes modificar a finalidade do tratamento.

2 ADEQUAÇÃO

Direito ao tratamento compatível com a finalidade informada pelo agente.

3 NECESSIDADE

Direito à limitação do tratamento ao mínimo necessário para a sua finalidade, com abrangência dos dados pertinentes, dispensando a coleta excessiva. Os agentes devem utilizar apenas os dados estritamente necessários para alcançar a sua finalidade.

4 LIVRE ACESSO

Direito à consultoria facilitada e gratuita sobre a forma e a duração do tratamento de dados.

5 QUALIDADE

Direito à clareza, exatidão, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade.

6 TRANSPARÊNCIA

Direito a informações claras, precisas e facilmente acessíveis sobre o tratamento dos dados e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

7 SEGURANÇA

Direito à segurança dos dados, devendo os agentes de tratamento, utilizar medidas aptas a proteger os dados pessoais.

8 PREVENÇÃO

Direito à prevenção de danos, obrigando o agente de tratamento a adotar medidas para prevenir a sua ocorrência.

9 NÃO-DISCRIMINAÇÃO

Direito de anti-discriminação. Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

10 RESPONSABILIZAÇÃO

Direito de exigir a responsabilização e prestação de contas aos agentes de tratamento. Os agentes devem comprovar a adoção de medidas eficazes ao cumprimento das normas de proteção de dados.

5. BASES LEGAIS

O TRATAMENTO DE DADOS PODERÁ SER REALIZADO NAS SEGUINTE HIPÓTESES:

- Mediante o fornecimento de consentimento pelo titular ou responsável legal;
- Para o cumprimento de obrigação legal ou regulatória pelo controlador;
- Para execução de políticas públicas, pela administração pública;
- Para a realização de estudos por órgãos de pesquisa;
- 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;
- Para a proteção da vida ou da incolumidade física do titular ou de terceiro;
- Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- 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;
- Para a proteção do crédito.

E NA PREFEITURA?



Sempre que a administração pública efetuar o tratamento de dados pessoais no exercício de suas competências legais vinculadas à políticas públicas e entrega de serviços públicos, não precisará colher o consentimento; mas, necessariamente, **será obrigada a informar a finalidade e a forma como o dado será tratado.**

6. DIREITO DOS TITULARES

OS TITULARES POSSUEM OS SEGUINTE DIREITOS:



Confirmação de que existe um ou mais tratamento de dados sendo realizado



Acesso aos dados pessoais conservados que lhe digam respeito



Correção de dados pessoais incompletos, inexatos ou desatualizados



Eliminação de dados pessoais desnecessários, excessivos ou caso o seu tratamento seja ilícito



Portabilidade de dados a outro fornecedor de serviço ou produto, observados os segredos comercial e industrial



Eliminação de dados (exceto quando o tratamento é legal, mesmo que sem o consentimento do titular)



Informação sobre compartilhamento de seus dados com entes públicos e privados, caso isso exista



Informação sobre o não consentimento, ou seja, sobre a opção de não autorizar o tratamento e as consequências da negativa



Revogação do consentimento, nos termos da lei



Reclamação contra o controlador dos dados junto à autoridade nacional



Oposição, caso discorde de um tratamento feito sem seu consentimento e o considere irregular

COMO EXERCER OS DIREITOS?

O município de Holambra oferece aos titulares dos dados um canal de comunicação com o Encarregado, para o exercício dos direitos relacionados à proteção de dados pessoais, tais direitos podem ser exercidos através do link ou Qr Code:

<https://holambra.sp.gov.br/lgpd.html>



Dúvidas, sugestões ou relatos de incidentes de segurança devem ser realizadas por meio dos contatos abaixo:

E-mail: lgpd@holambra.sp.gov.br

Telefone: (19) 3802-8007



7. CONSEQUÊNCIAS E PENALIDADES

QUAIS SÃO AS CONSEQUÊNCIAS POR NÃO AGIR DE ACORDO COM A LEI?

No caso específico de **entidades e órgãos públicos**, são **excluídas as possibilidades de multa simples e multa diária**, entretanto, outras sanções poderão ser aplicadas, como:

ADVERTÊNCIA: com indicação de prazo para adoção de medidas corretivas.

PUBLICIZAÇÃO DA INFRAÇÃO: apenas após confirmada a ocorrência.

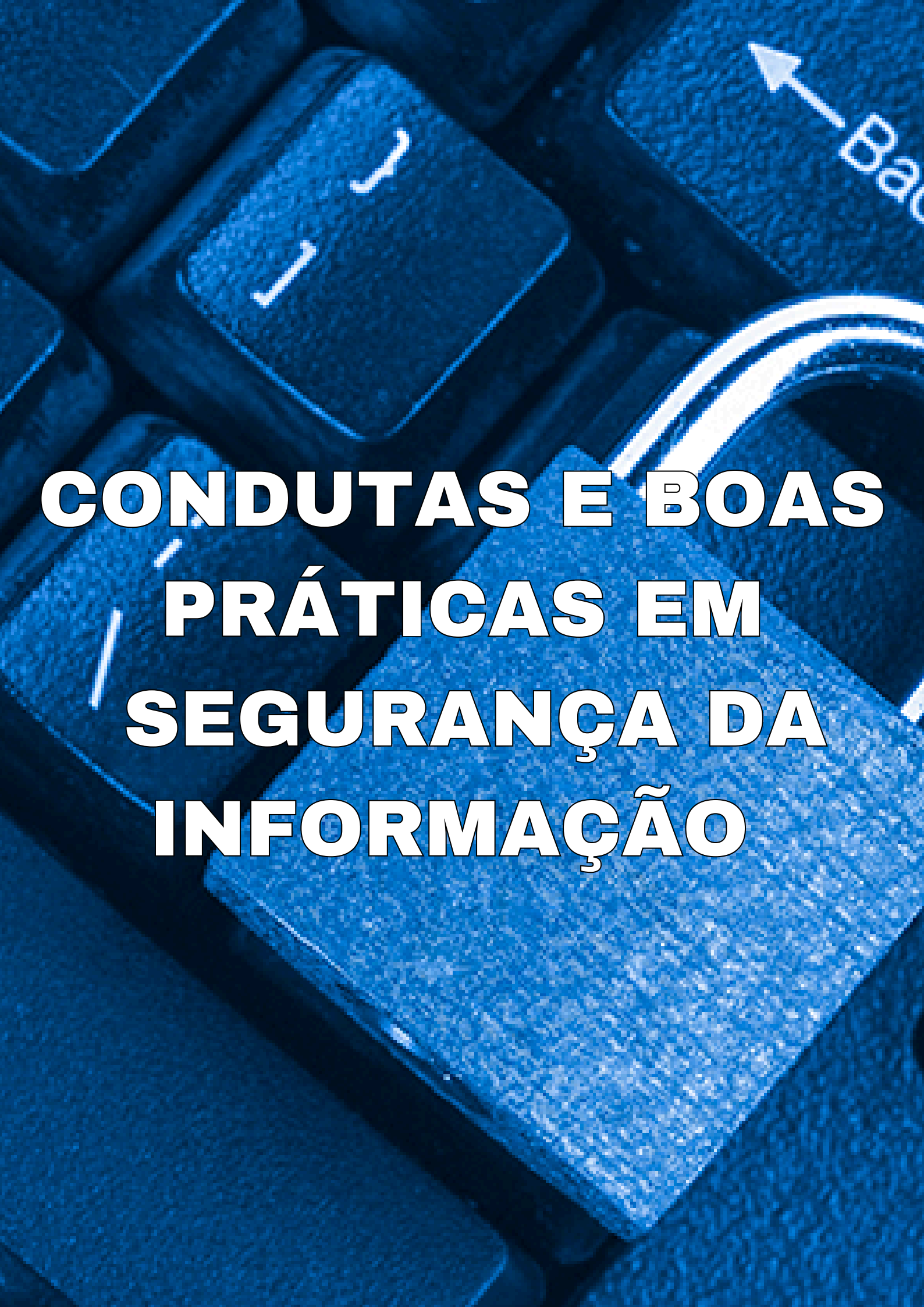
BLOQUEIO: até a regularização da situação, os dados ficarão bloqueados.

REPUTAÇÃO: Os impactos não se restringem a sanções administrativas. Também podem afastar outras entidades que busquem parcerias, pelo risco de serem impactados.

ELIMINAÇÃO: confirmada a infração, os dados pessoais a ela relacionados serão eliminados.



Os órgãos públicos não estão sujeitos às sanções de multas financeiras, mas isso **não significa** que **servidores públicos envolvidos nos casos não sejam punidos ou penalizados nas esferas da improbidade administrativa e criminal.**

A close-up, high-angle shot of a computer keyboard, heavily tinted with a vibrant blue color. The focus is on the central and right-hand keys, including the spacebar and the 'Backspace' key with its arrow. The keys have a textured, slightly worn appearance. Overlaid on this background is the title text in a bold, white, sans-serif font.

CONDUTAS E BOAS PRÁTICAS EM SEGURANÇA DA INFORMAÇÃO

- **Seguir as Políticas e diretrizes:** Ao tratar informações pessoais, atente-se às regulamentações aplicáveis, assim como às políticas, diretrizes e boas práticas adotadas pelo Município;



As políticas de Segurança da Informação do Município podem ser acessadas na íntegra através do qr code ao lado

- **Reduzir a utilização de dados:** procure empregar apenas as informações indispensáveis para o desenvolvimento das atividades, evitando a aquisição de dados desnecessários, especialmente os sensíveis e/ou pertencentes a titulares que sejam crianças/adolescentes.
- **Tela limpa e mesa limpa:** esteja atento aos documentos dispostos sobre as mesas, armários, ou demais móveis que possam ser visíveis a servidores ou outras pessoas não relacionadas com aquela atividade. Evite manter arquivos na área de trabalho do computador e efetue logout ao se ausentar.
- **Utilização da infraestrutura computacional local, telefones e e-mails institucionais:** evite empregar dispositivos destinados ao uso profissional para armazenar informações de caráter pessoal ou que não estejam relacionadas ao interesse público.
- **Documentos físico:** ao imprimir qualquer documento que contenha dados pessoais, retire-o imediatamente da impressora compartilhada para evitar que outros servidores tenham acesso indevido a informações.

- **Descarte de documentos:** ao realizar a eliminação de dados em formato físico (papel), assegure-se de que o papel foi inutilizado de maneira a impossibilitar a identificação das informações anteriormente presentes.
- **Atendimento:** não forneça informações pessoais ou certidões de qualquer natureza a terceiros durante os atendimentos, a menos que haja autorização legal ou consentimento expresso da pessoa a quem essas informações se referem.
- **Compartilhamento:** não compartilhe dados pessoais com outros servidores não autorizados ou usuários não relacionados à atividade.
- **Utilização dos dados para fins públicos:** o tratamento de dados pessoais deve ter propósitos legítimos e visar ao interesse público no cumprimento de competências legais e atribuições do serviço público.
- **Repasse de informações por e-mail e ligações:** não envie informações e documentos para desconhecidos e pessoas não autorizadas. Questionar sempre a finalidade e, em caso de dúvida, consulte o Encarregado de Dados Pessoais.
- **Links ou arquivos desconhecidos:** evite clicar em links e abrir documentos cuja origem não seja conhecida.

- **Comentários:** evite discutir assuntos relacionados a dados pessoais em locais públicos ou de uso coletivo, como banheiros, saguões e corredores.
- **Utilização de rascunhos:** evite o uso de documentos em papel contendo informações importantes para rascunhos.
- **O Acesso:** Restrinja o acesso aos dados pessoais somente aos agentes que necessitem deles para as atividades da administração pública.
- **Correção de dados:** realize a correção de dados pessoais que estejam imprecisos, incorretos ou incompletos.
- **Violação:** informe ao encarregado de dados pessoais sobre a ocorrência de violações à LGPD.
- **Senhas:** nunca compartilhe suas senhas. Utilize senhas robustas, conforme estipulado na Política de Segurança da Informação do Município. Não anote suas senhas em *post-it* ou adesivos similares.
- **Revisão periódica de acessos e permissões:** verifique regularmente se você (ou sua equipe) possui apenas os acessos necessários aos sistemas e pastas. Solicite a revogação de acessos que não sejam mais pertinentes à função exercida.
- **Evite armazenar arquivos localmente:** sempre que possível, salve os documentos em pastas da rede institucional, que contam com políticas de backup e controle de acesso. Evitar o uso do armazenamento local (como “Área de Trabalho” ou “Meus Documentos”) reduz o risco de perda de dados e facilita a recuperação em caso de falhas ou incidentes.

ORGANIZAÇÃO:

Edson Jose Tonon Junior

Yuri Gabriel Pinheiro

FONTES PARA ELABORAÇÃO DESTA CARTILHA:

Lei Geral de Proteção de Dados - Lei 13.709/2018

Município de Limeira/SP

Município de Travesseiro/RS

ANPD - Bibliotecas

SERPRO

