

Guia para Elaboração de Avisos de Privacidade

Programa de Privacidade e
Segurança da Informação

PPSI 2.0



MINISTÉRIO DA
GESTÃO E DA
INOVAÇÃO EM
SERVIÇOS PÚBLICOS

Versão 1.0
Brasília, 17 de junho de 2026



GUIA PARA ELABORAÇÃO DE AVISOS DE PRIVACIDADE

MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS

Esther Dweck

Ministra

SECRETARIA DE GOVERNO DIGITAL

Rogério Souza Mascarenhas

Secretário de Governo Digital

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Leonardo Rodrigo Ferreira

Diretor de Privacidade e Segurança da Informação

COORDENAÇÃO-GERAL DE PRIVACIDADE

Marta Juvina de Medeiros

Coordenadora-Geral de Privacidade

COORDENAÇÃO-GERAL DE SEGURANÇA DA INFORMAÇÃO

Loriza Andrade Vaz de Melo

Coordenadora-Geral de Segurança da Informação

EQUIPE TÉCNICA DE ELABORAÇÃO

Anderson Souza de Araújo

Ricardo Borges Almeida

EQUIPE TÉCNICA DE EDITORAÇÃO

Flávia Patrícia Donata Vieira

Rejane Monique Brelaz Castro

EQUIPE DE REVISÃO

Marta Juvina de Medeiros



Histórico de versões

Data	Versão	Descrição	Autor
15/05/2026	1.0	Construção do Guia para Elaboração de Avisos de Privacidade (PPSI 2.0)	Equipe Técnica de Elaboração



Sumário

Medidas do <i>framework</i> do PPSI 2.0 apoiadas por esse documento	6
1 Termos e definições	7
2 Introdução	8
3 Considerações iniciais	10
3.1 Em quais situações os avisos devem ser elaborados?	10
3.2 Quem é responsável pela elaboração dos avisos de privacidade?	10
3.3 Linguagem simples	10
3.4 Aviso de privacidade multilíngue	11
3.5 Uso de recursos visuais	11
3.6 Serviços em formato presencial (não digital) ou misto.....	12
3.7 Serviços disponibilizados em diferentes plataformas	12
3.8 Inclusão do aviso de privacidade na Carta de Serviços ao Usuário.....	13
4 Conteúdo dos avisos de privacidade.....	14
4.1 Finalidades específicas dos tratamentos realizados	14
4.2 Tipos de dados pessoais tratados.....	14
4.3 Descrição do tratamento de dados pessoais	14
4.4 Hipóteses legais dos tratamentos	16
4.5 Duração dos tratamentos.....	16
4.6 Compartilhamento de dados pessoais	17
4.7 Transferência internacional de dados pessoais	18
4.8 Medidas de segurança aplicadas.....	18
4.9 Agentes de tratamento e respectivas responsabilidades legais	19
4.10 Identificação e informações de contato do encarregado	19
4.11 Informações sobre consentimento do titular dos dados pessoais	20
4.12 Informações sobre cada tratamento posterior.....	21
4.13 Utilização de Cookies.....	22
4.14 Direitos do titular dos dados pessoais	23
4.15 Decisão automatizada	24
4.16 Comunicação de mudanças nos avisos de privacidade.....	24
4.17 Versão e data do documento	25
5 Formatos	27
5.1 Versão sintética	27
5.2 Versão completa.....	28
5.3 Versão em imagem ou vídeo.....	28
6 Considerações finais.....	29
7 Referências bibliográficas	30



Licença *Creative Commons*

Esta obra está licenciada sob a Licença *Creative Commons* Atribuição-NãoComercial-SemDerivações 4.0 Internacional¹.

Você está autorizado a copiar e redistribuir o conteúdo deste Guia e respectivo *framework* para uso interno e externo à sua organização, somente para fins não comerciais, desde que (i) o devido crédito seja dado à Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), e (ii) um *link* para a licença seja fornecido. Além disso, não é permitida a distribuição de obras derivadas, remixadas, transformadas ou desenvolvidas a partir deste Guia ou respectivo *framework*.

¹ Disponível em: <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>.



Medidas do *framework* do PPSI 2.0 apoiadas por esse documento

Controle	Id	Medida	Segmento
21	21.4	O órgão divulga publicamente e mantém atualizadas a identidade e as informações de contato do encarregado e de seu substituto?	Privacidade
25	25.1	O órgão realiza tratamento de dados pessoais para propósitos legítimos, específicos, explícitos e informados ao titular?	Privacidade
25	25.6	O órgão assegura aos titulares informações claras, precisas e facilmente acessíveis sobre os tratamentos de dados pessoais?	Privacidade



1 Termos e definições

Algumas definições relevantes ao entendimento do conteúdo exposto neste guia são dispostas a seguir. Demais termos utilizados neste guia podem ser encontrados na **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025** [1], na **Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD)** [2], ou no Glossário de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), aprovado pela **Portaria GSI/PR nº 93, de 18 de outubro de 2021** [3].

Aviso de privacidade: documento voltado aos titulares que objetiva informar como os dados pessoais são tratados e para quais finalidades, quais os direitos dos titulares e como podem exercê-los, além de outras características que garantam ao titular a transparência em relação ao tratamento de seus dados pessoais, facilmente acessível e escrito em linguagem clara e simples.

Infográfico: representação visual de informações e dados, combinando elementos de imagem, texto, gráfico, diagrama e vídeo. Um infográfico é uma ferramenta eficaz para apresentar dados e explicar questões complexas de uma forma que pode proporcionar, rapidamente, uma visão mais clara e melhor compreensão.

Política de Proteção de Dados Pessoais (PPDP): instrumento normativo que estabelece diretrizes institucionais para o tratamento de dados pessoais no âmbito do órgão ou entidade, com o objetivo de assegurar os direitos fundamentais de liberdade, de intimidade e de privacidade dos titulares de dados pessoais.

Serviço digital: serviço público cuja prestação ocorra por meio eletrônico, sem a necessidade de atendimento presencial no todo ou em parte das suas etapas [4].

Serviço público: ação dos órgãos e das entidades do Poder Executivo federal para atender, direta ou indiretamente, às demandas da sociedade relativas a exercício de direito ou a cumprimento de dever [4].

Unidade responsável ou unidade: unidade do órgão ou entidade gestora do serviço público ofertado ao cidadão.

Usuário: pessoa física ou jurídica que pode fazer uso individual do serviço [4].



2 Introdução

Em um contexto digital cada vez mais dinâmico e orientado por dados, a transparência no tratamento de dados pessoais tornou-se um valor essencial para a construção de relações de confiança entre organizações e titulares de dados pessoais. O disposto no *caput* do art. 25 da **Lei nº 14.129, de 29 de março de 2021** [5], que dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública, reforça a necessidade de transparência ao estabelecer que as **Plataformas de Governo Digital** devem dispor de ferramentas de transparência e de controle do tratamento de dados pessoais que sejam claras e facilmente acessíveis, permitindo ao cidadão o exercício dos direitos previstos na Lei nº LGPD [2].

Os avisos de privacidade cumprem, fundamentalmente, o dever de transparência quanto ao tratamento de dados pessoais, conforme disposto no art. 6º, inciso VI, da LGPD [2]. Este princípio visa garantir, aos titulares, informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial [2].

Em síntese, os avisos de privacidade consistem em documentos, digitais ou físicos, voltados aos titulares de dados pessoais cujo objetivo é traduzir, de forma clara e acessível, como, por que e com que finalidade os dados pessoais são tratados (coletados, usados, armazenados, compartilhados, descartados, entre outros).

Para tanto, os órgãos e entidades devem criar e manter atualizados os avisos de privacidade relacionados aos seus produtos e serviços que realizam tratamento de dados pessoais. A elaboração de avisos de privacidade que sejam compreensíveis, precisos e realmente úteis para os titulares de dados pessoais é um desafio que exige não apenas conhecimento sobre a temática de proteção de dados pessoais, mas também compreensão dos tratamentos de dados pessoais relacionados ao escopo do aviso de privacidade – além de competência para tornar a linguagem acessível e contextualizada ao público-alvo.

O objetivo central deste **Guia para Elaboração de Avisos de Privacidade** é fornecer orientações práticas e aplicáveis aos órgãos e entidades da administração pública federal direta, autárquica e fundacional, que possuem unidades que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP), para a elaboração de avisos de privacidade eficazes, coerentes com os princípios e as diretrizes estabelecidas na LGPD [2].

O presente Guia integra o conjunto de instrumentos de apoio à implementação das medidas estabelecidas no *framework* do **Programa de Privacidade e Segurança da Informação (PPSI 2.0)** [6], instituído pela **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025** [1]. De forma complementar, visa atender diretamente ao inciso VI do art. 6º, ao art. 9º e ao § 1º do art. 41 da LGPD [2], e aos arts. 8º e 9º da **Resolução CD/ANPD nº 18, de 16 de julho de 2024** [7], e ao § 2º do art. 17 da **Resolução CD/ANPD nº 19, de 23 de agosto de 2024** [8].

Este Guia está organizado em cinco seções. A seção 1 apresenta os termos e definições relevantes. A seção 2 (esta) traz a introdução e contextualiza o Guia no âmbito do PPSI 2.0. A seção 3 apresenta considerações iniciais sobre elaboração, linguagem, formatos e distribuição



dos avisos. A seção 4 detalha os elementos de conteúdo obrigatório e recomendado. A seção 5, por fim, orienta sobre os diferentes formatos de apresentação dos avisos de privacidade.



3 Considerações iniciais

Destaca-se, inicialmente, que um mesmo serviço pode atender a públicos-alvo de interesses distintos, que fazem uso das diferentes plataformas em que o serviço público pode estar disponível – sejam digitais, presenciais ou mistas. Em cada público, há pessoas com diferentes capacidades de absorção do conteúdo, ou que são melhor alcançadas por um tipo específico de comunicação. Assim, para que seja efetivo e cumpra os propósitos para os quais é destinado, o aviso de privacidade deve:

- i. ser editado em linguagem acessível, clara e simples;
- ii. ter o foco no público-alvo do serviço;
- iii. considerar que o usuário não deve precisar ter conhecimento técnico ou jurídico para compreender as informações nele contidas;
- iv. conter informações atualizadas.

Sendo assim, esta seção tem como objetivo apresentar considerações que devem ser avaliadas pela unidade responsável previamente à elaboração dos avisos de privacidade, incluindo quando se deve produzi-los e orientações sobre a linguagem e recursos visuais a serem utilizados.

3.1 Em quais situações os avisos devem ser elaborados?

Os avisos de privacidade devem ser elaborados e disponibilizados pelo órgão ou entidade para todos os produtos e serviços ofertados que envolvam o tratamento de dados pessoais, quer sejam informatizados ou não.

3.2 Quem é responsável pela elaboração dos avisos de privacidade?

A elaboração dos avisos de privacidade deve ser realizada pela unidade responsável pelo serviço público que está sendo ofertado. Caso o serviço seja informatizado, a unidade pode, eventualmente e para questões técnicas, contar com o apoio e as informações da área desenvolvedora do serviço, seja ela do próprio órgão ou entidade ou da empresa contratada.

3.3 Linguagem simples

Ao elaborar os avisos de privacidade, é necessário comunicar-se de forma clara, direta, evitando-se o uso de expressões técnicas que venham a inviabilizar ou dificultar o entendimento pelo público-alvo do serviço. Para isso, é fundamental o uso de uma linguagem de fácil compreensão com textos, imagens ou vídeos curtos, disponibilizando avisos de privacidade que sejam realmente eficientes no alcance de seus objetivos.

Além da simplicidade vocabular, também é importante observar a precisão dos termos empregados e a maneira como são apresentados; um texto simples não é necessariamente um texto descuidado ou mal formatado. Uma exposição clara, bem apresentada e organizada dos avisos de privacidade motiva o usuário do serviço a lê-los e, principalmente, a compreendê-los.



No aspecto normativo, a Lei nº 14.129/2021 [5] estabelece o uso de linguagem clara e compreensível a qualquer cidadão (art. 3º, VII) e a acessibilidade da pessoa com deficiência ou com mobilidade reduzida (art. 3º, XIX) entre os princípios e diretrizes do Governo Digital e da eficiência pública. Além disso, o **Decreto nº 9.094, de 17 de julho de 2017** [9] dispõe sobre a necessidade de órgãos e entidades do Poder Executivo Federal utilizarem linguagem clara, que evite o uso de siglas, jargões e estrangeirismos (art. 1º, VIII).

Se o serviço público é também voltado a idosos, pessoas com deficiência ou outros grupos que necessitem de atendimento diferenciado, os avisos de privacidade devem ser elaborados para também atender às suas necessidades. A título de exemplo, traz-se algumas referências do **Estatuto da Pessoa com Deficiência, Lei nº 13.146, de 6 de julho de 2015** [10], que se destina a assegurar e a promover, em condições de igualdade, o exercício dos direitos e das liberdades fundamentais por pessoa com deficiência. O atendimento a tal público deve ser priorizado, incluindo-se a disponibilização de recursos que garantam atendimento em igualdade de condições com as demais pessoas, além do acesso a informações e comunicação acessíveis. Também dispõe sobre a necessária acessibilidade² nos sítios da internet para uso da pessoa com deficiência, assim como a existência de informações corretas e claras sobre os serviços ofertados. A referida Lei também define que os arquivos digitais em formatos acessíveis são aqueles reconhecidos e acessados por *software* leitor de telas ou outras tecnologias assistidas que vierem a substituí-los, permitindo leitura com voz sintetizada, ampliação de caracteres, diferentes contrastes e impressão em Braille. Logo, todos esses dispositivos impactam os avisos de privacidade, e devem ser considerados pela unidade responsável quando de sua elaboração.

3.4 Aviso de privacidade multilíngue

Caso o produto ou serviço em que dados pessoais são tratados seja ofertado também para estrangeiros, sugere-se que o aviso seja apresentado nos mesmos idiomas do seu público-alvo. Sobre o tema, a ABNT NBR ISO/IEC 29184:2021 [11] recomenda que a organização forneça as informações constantes nos avisos considerando os idiomas de acordo com as expectativas do público-alvo, com a possibilidade de o usuário do serviço escolher o idioma no qual quer ser informado.

3.5 Uso de recursos visuais

A exibição dos avisos de privacidade pode ser realizada em diferentes meios, físicos ou digitais, e em formatos variados, incluindo versões resumidas e completas. Para quaisquer dos formatos utilizados, recomenda-se a apresentação do conteúdo de forma estruturada.

Com vistas a facilitar o entendimento do conteúdo dos avisos de privacidade, sugere-se, quando aplicável, o uso dos conceitos do *Visual Law*, uma subárea do *Legal Design* voltada ao *design* de informação que se utiliza de recursos visuais tais como vídeos, fluxogramas, infográficos, figuras e gamificação. O uso de vídeos curtos tem grande receptividade pelos usuários e facilitam sobremaneira a comunicação.

² Sobre acessibilidade, recomenda-se a leitura do Modelo de Acessibilidade em Governo Eletrônico (eMAG), disponível em <https://emag.governoeletronico.gov.br/>



Segundo Vainzoff *et al.* [12], o *design* deve ser centrado no usuário para que ele possa ter a melhor experiência com o documento. Entre os recursos que melhor traduzem o *Visual Law* na prática estão os ícones, os fluxogramas, as imagens, os gráficos, os infográficos e as tabelas – elementos que facilitam a compreensão e aumentam o engajamento do titular com o conteúdo dos avisos de privacidade.

Quando as informações forem destinadas a crianças, deve-se considerar quais as adaptações podem ser realizadas para tornar o conteúdo particularmente acessível a tal público-alvo, como histórias em quadrinhos, pictogramas³ e animações.

Caso a unidade responsável pelo produto ou serviço opte por apresentar o conteúdo do aviso de privacidade por meio de vídeo, deve-se considerar a **Lei nº 10.436, de 24 de abril de 2002** [13], que dispõe sobre a **Língua Brasileira de Sinais (Libras)**, reconhecida como meio legal de comunicação e expressão, e o apoio a seu uso deve ser garantido pelo Poder Público como meio de comunicação objetiva e de utilização corrente das comunidades surdas do Brasil. As instituições públicas devem assegurar atendimento e tratamento adequado aos portadores de deficiência auditiva, conforme estabelecido no art. 3º da referida Lei.

3.6 Serviços em formato presencial (não digital) ou misto

Outro fator relevante diz respeito ao espaço em que o aviso de privacidade será disponibilizado, seja na página eletrônica do produto ou serviço ou no local presencial onde é prestado, desde que seja exposto em local de fácil acesso e visualização.

Sobre o tema, a ABNT NBR ISO/IEC 29184:2021 [11] recomenda que a organização forneça avisos de maneira apropriada para o produto ou serviço em questão, de forma que os titulares de dados pessoais possam encontrá-los e acessá-los facilmente, sem a necessidade de solicitação do usuário e próximo ao ponto em que o serviço é prestado ao público-alvo, inclusive em locais on-line.

O aviso de privacidade deve observar o que foi abordado até aqui, obedecendo a uma apresentação em um meio físico que possa ser acessível a qualquer titular, de forma independente e segura, atentando também para a necessária acessibilidade de pessoas com deficiência e idosos ao seu conteúdo.

3.7 Serviços disponibilizados em diferentes plataformas

Caso o mesmo serviço público seja disponibilizado em diversas plataformas (aplicativo, *web*, físico ou presencial, entre outras), o aviso de privacidade deve ser replicado igualmente em todas elas, mantendo-se a coerência do serviço proposto com versões idênticas e atualizadas simultaneamente nas plataformas utilizadas – evitando-se, assim, dúvidas ou desentendimentos por parte do titular que acessar uma ou outra plataforma.

Uma sugestão neste sentido é que o serviço das diferentes plataformas seja programado para buscar o conteúdo do aviso de uma mesma fonte, facilitando assim o seu gerenciamento. Esta

³ Um pictograma ou pictógrafo é um símbolo que representa um objeto ou conceito por meio de desenhos figurativos.



fonte pode estar, por exemplo, em um banco de dados, em um arquivo em formato *Portable Document Format* (PDF), ou, ainda, disponível através de uma página *web* – para a qual o aplicativo e a interface *web* do serviço façam referência.

Um caso especial que merece atenção é a disponibilização do serviço em meio físico ou presencial; nesta situação, é importante ter um processo claro para gestão do conteúdo do aviso de privacidade e disseminação das suas últimas versões. O caso concreto estabelecerá os requisitos para definição da melhor abordagem de apresentação do aviso, o que pode incluir desde a exibição de um *Quick Response Code* (QR Code) no balcão de atendimento até a entrega em papel anexado a um formulário de coleta de dados pessoais.

Admite-se exceção quanto às versões do aviso de privacidade disponibilizadas em plataformas diferentes exclusivamente nas situações em que há distinção dos serviços ofertados entre elas – em razão de facilidades e especificidades disponíveis em cada plataforma –, motivo pelo qual as diferenças entre os avisos disponibilizados devem ser informadas ao usuário.

3.8 Inclusão do aviso de privacidade na Carta de Serviços ao Usuário

A **Carta de Serviços ao Usuário** tem por objetivo informar o usuário sobre os serviços prestados pelo órgão ou entidade, as formas de acesso a esses serviços e seus compromissos e padrões de qualidade de atendimento ao público, nos termos do art. 7º, § 1º, da **Lei nº 13.460, de 26 de junho de 2017** [21]. O § 2º do mesmo artigo determina que a Carta deverá trazer informações claras e precisas em relação a cada um dos serviços prestados – exigência que se conecta diretamente ao dever de transparência no tratamento de dados pessoais disposto no art. 6º, inciso VI, da LGPD [2].

Nesse sentido, recomenda-se incluir, na página da Carta de Serviços ao Usuário em que estão descritas as características de cada serviço, uma seção denominada "Lei Geral de Proteção de Dados Pessoais (LGPD)" contendo o *link* para o aviso de privacidade elaborado pela unidade responsável, conforme exemplo ilustrado na **Figura 1**.

Essa prática assegura que o cidadão, ao consultar a Carta de Serviços ao Usuário, tenha acesso facilitado às informações sobre o tratamento de seus dados pessoais no âmbito daquele serviço específico, em conformidade tanto com o princípio da transparência da LGPD quanto com o dever de clareza e precisão das informações na Carta de Serviços ao Usuário.



Figura 1: exemplo de inclusão de *link* para o aviso de privacidade na Carta de Serviços ao Usuário



4 Conteúdo dos avisos de privacidade

Esta seção tem como objetivo apresentar o conteúdo que deve constar nos avisos de privacidade. Inicialmente, é importante destacar que uma das principais fontes de conteúdo para elaboração dos avisos de privacidade deve ser o registro das operações de tratamento de dados pessoais do órgão ou entidade, realizado em conformidade com o art. 37 da LGPD e com o Controle 19 do *framework* do PPSI. Portanto, pressupõe-se sua elaboração prévia pela unidade responsável.

4.1 Finalidades específicas dos tratamentos realizados

O princípio da finalidade, disposto no inciso I do art. 6º da LGPD, diz respeito à realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades [2]. Para o Poder Público, ainda, o tratamento deve atender a uma finalidade pública (LGPD, art. 23).

Dessa forma, as finalidades do tratamento devem estar registradas nos avisos de privacidade, de modo a demonstrar também a legitimidade e especificidade da operação ao titular de dados pessoais. Ainda, na hipótese de haver mais de uma finalidade de tratamento de dados pessoais para o produto ou serviço, todas devem ser registradas no aviso.

4.2 Tipos de dados pessoais tratados

Para cada uma das finalidades, devem ser registrados nos avisos de privacidade todos os tipos de dados pessoais tratados no âmbito do serviço ofertado, assim como a natureza dos dados e a necessidade (LGPD, art. 6º, III) de cada dado pessoal tratado para cumprir o objetivo do produto ou serviço.

Para fins de registro nos avisos, pode ser útil agrupar os dados pessoais por categoria, de modo a facilitar a compreensão pelo titular. Exemplos de categorias comumente utilizadas:

- dados cadastrais: nome completo, data de nascimento, número de documento de identificação (CPF, CNH), estado civil;
- dados de contato: endereço residencial, endereço de e-mail, número de telefone;
- dados funcionais ou de vínculo: cargo, matrícula, órgão de lotação, regime de trabalho;
- dados financeiros: dados bancários, informações sobre benefícios, rendimentos;
- dados de localização: endereço geográfico, coordenadas *Global Positioning System* (GPS), registros de acesso físico.

A indicação da natureza de cada dado pessoal – comum ou sensível – é especialmente relevante, pois permite evidenciar a adequação da base legal aplicada e os requisitos adicionais de proteção exigidos pela LGPD que foram aplicados no caso concreto.

4.3 Descrição do tratamento de dados pessoais

A LGPD define tratamento como toda operação realizada com dados pessoais, abrangendo desde a coleta até a eliminação, passando por armazenamento, utilização, compartilhamento e outras operações (LGPD, art. 5º, X) [2]. Embora a Lei enumere diversas operações



específicas, o aviso de privacidade não deve reproduzir essa lista nem descrever cada operação individualmente – pois fazê-lo tornaria o documento excessivamente técnico e de difícil compreensão para o titular.

O objetivo desta descrição do tratamento no aviso é responder, de forma simples, objetiva e clara, à seguinte pergunta, sob a perspectiva do titular: o que acontece com os meus dados a partir do momento em que os forneço? A resposta deve ser construída em linguagem acessível, sem se prender à nomenclatura jurídica da LGPD nem aos aspectos técnicos da operação. O titular não precisa saber que seus dados são "classificados", "recepcionados" ou "avaliados" – precisa entender, em termos práticos, o que o órgão ou entidade fará com eles.

Para tanto, recomenda-se que a descrição do tratamento:

- seja orientada pela perspectiva do titular, descrevendo o que ocorre com seus dados ao longo do serviço, e não pela perspectiva técnica ou jurídica do controlador;
- use linguagem próxima do cotidiano, como "seus dados pessoais são registrados no sistema ao realizar o cadastro", "suas informações são utilizadas para análise do benefício solicitado" ou "seus dados são guardados pelo prazo legal e depois excluídos";
- descreva o ciclo relevante para o titular, contemplando, quando pertinente, como os dados são obtidos, para que são utilizados, com quem são compartilhados e quando são eliminados – sem necessidade de detalhar cada etapa técnica intermediária e evitando repetições caso algumas dessas informações já estejam descritas em seções diferentes no aviso;
- evite reproduzir a lista de operações da LGPD como estrutura da descrição; o uso de verbos como "classificar", "recepcionar", "difundir" ou "extrair" tende a dificultar a compreensão e não acrescenta informação útil ao titular.

A seguir, são apresentados exemplos comparativos para ilustrar a distinção entre uma descrição orientada ao titular e uma orientada às operações jurídicas.

Exemplo de descrição inadequada – centrada nas operações da LGPD:

- "Os dados pessoais serão coletados, recepcionados, classificados, utilizados, armazenados, arquivados e eliminados em conformidade com as finalidades previstas neste aviso."

Exemplo de descrição adequada – centrada na experiência do titular:

- "Ao solicitar o serviço, seus dados são registrados em nosso sistema e utilizados exclusivamente para análise e concessão do benefício requerido. Eles ficam armazenados pelo prazo legal aplicável e são excluídos após o cumprimento da finalidade, salvo obrigação de guarda prevista em Lei."

Quando o produto ou serviço envolver operações com impacto mais significativo para o titular, como o compartilhamento dos dados pessoais com outros órgãos, a utilização para decisões automatizadas ou a transferência internacional, essas operações específicas devem ser destacadas na descrição, pois representam aspectos que o titular tem interesse legítimo



em conhecer. Os detalhes sobre cada uma dessas operações podem ser aprofundados nas subseções correspondentes do aviso (vide subseções 4.6, 4.7 e 4.15 deste Guia).

4.4 Hipóteses legais dos tratamentos

As hipóteses para tratamento de dados pessoais, denominadas comumente de bases legais, estão dispostas nos arts. 7º e 11 da LGPD; especificamente para o Poder Público, o tratamento também deve considerar as disposições contidas no art. 23 da Lei [2].

A escolha da base legal não é uma formalidade: ela define a legitimidade jurídica do tratamento e condiciona os demais elementos dos avisos de privacidade, especialmente as finalidades, os direitos do titular aplicáveis e as condições de compartilhamento. Tratar dados pessoais sem amparo em hipótese legal é, segundo o Regulamento de Dosimetria e Aplicação de Sanções Administrativas da ANPD, circunstância que caracteriza infração grave [2].

A experiência internacional reforça essa perspectiva. Desde a entrada em vigor do [Regulamento Geral de Proteção de Dados \(GDPR\)](#) da União Europeia, em maio de 2018, o tratamento com base legal insuficiente ou inadequada consolidou-se como a principal categoria de violação em número de autuações e como a de maior impacto financeiro acumulado, conforme registrado pelo [GDPR Enforcement Tracker Report](#) em suas sucessivas edições [23], [24]. No contexto brasileiro, a primeira sanção pecuniária aplicada pela ANPD, em julho de 2023, teve como um de seus fundamentos exatamente a ausência de comprovação de hipótese legal para o tratamento de dados pessoais [25].

Neste sentido, um conteúdo relevante para disposição nos avisos de privacidade são as bases legais que autorizam o órgão ou entidade a realizar as operações de tratamento que ocorrem no âmbito do produto ou serviço. Caso ocorra tratamento de dados pessoais com base em mais de uma hipótese legal, todas elas devem ser registradas. Para isso, recomenda-se que a definição das bases legais seja estabelecida para cada finalidade de tratamento de dados pessoais, de forma que haja correspondência clara e verificável entre a finalidade declarada e o fundamento jurídico que a autoriza.

Para aprofundamento sobre as bases legais aplicáveis ao Poder Público, recomenda-se a leitura do [Guia para Tratamento de Dados Pessoais pelo Poder Público da ANPD](#) [15], especialmente as páginas 6 a 12, que detalham: (i) consentimento, (ii) legítimo interesse, (iii) cumprimento de obrigação legal e regulatória e (iv) execução de políticas públicas.

4.5 Duração dos tratamentos

Diversos aspectos sobre o tratamento devem ser registrados pela unidade responsável nos avisos de privacidade, inclusive o que diz respeito ao prazo de retenção dos dados pessoais – que, conforme ABNT NBR ISO/IEC 29184:2021 [11], podem ser especificados:

- i. períodos específicos, como 5 anos a partir da data da coleta ou da ocorrência de um evento específico;
- ii. data específica, como 1º de janeiro de 2030;
- iii. critérios para determinar este período ou cronograma.

O tema é tão relevante que possui abordagem específica na LGPD [2] (vide arts. 15 e 16).



A duração do tratamento deve considerar todo o prazo para integral alcance das finalidades do tratamento, inclusive eventual obrigação legal de arquivamento – que também é um tipo de tratamento. Há de se lembrar que o tempo de retenção dos dados deve ser limitado ao mínimo necessário ao alcance de cada finalidade.

Frazão e Cueva [16] identificam quatro hipóteses de término do tratamento no âmbito do art. 15 da LGPD: esgotamento funcional da utilização dos dados, cumprimento do prazo, autodeterminação do titular e ilegalidade do tratamento. Os autores ressaltam que a conservação posterior apenas se admite excepcionalmente, sob interpretação restritiva, e que a Lei não previu prazo para a conservação nas hipóteses do mesmo artigo [16].

A Lei nº 14.129/2021 [5], quanto à prestação digital de serviços públicos, estabelece que “o formato e o armazenamento de documentos digitais deverão garantir o acesso e a preservação das informações, nos termos da legislação arquivística nacional” [2, art. 12] e “a guarda dos documentos digitais e dos processos administrativos eletrônicos considerados de valor permanente deverá estar de acordo com as normas previstas pela instituição arquivística pública responsável por sua custódia” [2, art. 13].

4.6 Compartilhamento de dados pessoais

O compartilhamento de dados pessoais consiste na operação de tratamento pela qual o órgão ou entidade confere acesso aos dados pessoais sob sua responsabilidade a outro controlador, seja ente público ou entidade privada. No âmbito da LGPD, essa operação é denominada “uso compartilhado de dados”, nos termos do inciso XVI do art. 5º [2].

Para o Poder Público, o fundamento mais frequente do compartilhamento é o inciso III do art. 7º da LGPD, que autoriza o tratamento e o uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres [2]. O **Decreto nº 10.046, de 9 de outubro de 2019** [18], estabelece normas e diretrizes específicas para o compartilhamento de dados entre os órgãos e as entidades da administração pública federal, com a finalidade de simplificar a oferta de serviços públicos e promover a melhoria da qualidade e da fidedignidade dos dados custodiados. Para aprofundamento sobre o tema, recomenda-se a leitura do Guia para Tratamento de Dados Pessoais pelo Poder Público [15].

Caso o serviço não envolva compartilhamento de dados pessoais com terceiros, essa informação também deve constar do aviso de forma expressa, de modo a assegurar a transparência integral perante o titular.

Quando houver compartilhamento, todos os destinatários e as condições correspondentes devem ser registrados no aviso de privacidade, contemplando, para cada destinatário:

- identificação precisa do destinatário: razão social e CNPJ do ente com quem os dados pessoais são compartilhados, de forma que o titular possa identificá-lo inequivocamente;
- finalidade do compartilhamento: descrição clara do propósito que justifica o compartilhamento dos dados pessoais ao destinatário;



- tipos de dados pessoais compartilhados: indicação dos tipos de dados pessoais compartilhados, com precisão suficiente para que o titular compreenda o escopo do compartilhamento;
- enquadramento do destinatário como agente de tratamento: indicação se o destinatário atua como controlador singular ou controlador conjunto, distinção relevante para que o titular saiba a quem dirigir eventual requisição ou reclamação. Tal informação pode estar disposta em seção específica sobre a lista de agentes de tratamento.

4.7 Transferência internacional de dados pessoais

A transferência internacional de dados pessoais ocorre quando um agente de tratamento transmite, compartilha ou disponibiliza acesso a dados pessoais a outro agente de tratamento localizado em país estrangeiro ou organismo internacional do qual o país seja membro (LGPD, art. 5º, XV) [2]. Para ser lícita, a transferência internacional deve, cumulativamente: estar amparada em base legal prevista na LGPD; ter finalidade legítima, específica, explícita e informada ao titular; e ser realizada por meio de um dos mecanismos previstos na Resolução CD/ANPD nº 19, de 23 de agosto de 2024 [8].

Caso o serviço realize transferência internacional de dados pessoais, essa informação deve ser registrada no aviso de privacidade de forma clara e acessível ao titular. Para cada destinatário no exterior, o aviso deve conter:

- identificação precisa do destinatário: razão social e CNPJ ou equivalente do ente para quem os dados pessoais são transferidos, com informação que permita ao titular identificá-lo inequivocamente;
- tipos de dados pessoais transferidos: especificação dos tipos de dados pessoais transmitidos ao destinatário;
- enquadramento do destinatário como agente de tratamento: indicação se o destinatário atua como controlador singular, controlador conjunto ou operador. Assim como sugerido no conteúdo proposto sobre compartilhamento, tal informação pode estar disposta em seção específica sobre a lista de agentes de tratamento;
- localização geográfica de destino: país ou organismo internacional para onde os dados pessoais são transferidos.

4.8 Medidas de segurança aplicadas

Quanto às medidas de segurança implementadas no tratamento dos dados pessoais, vale destacar que estão diretamente relacionadas à abrangência, ao escopo e às operações de tratamento de dados pessoais do produto ou serviço, e obviamente precisarão considerar o tipo e o volume de dados pessoais tratados.

Sendo assim, recomenda-se que sejam apresentadas nos avisos de privacidade as medidas aplicadas para mitigar os riscos de privacidade, proteção de dados e segurança da informação decorrentes das atividades de tratamento de dados pessoais do produto ou serviço escopo do aviso.

Nesse quesito, o desafio é observar a profundidade do detalhamento das medidas de segurança: recomenda-se não descrever apenas as suas categorias, tampouco detalhá-las de



modo a expor o órgão ou entidade – evidenciando possíveis ausências ou detalhando sobremaneira, e de forma excessivamente técnica, uma medida implementada.

Como o nível de detalhamento das medidas de segurança no aviso de privacidade pode dificultar a compreensão por parte do titular, prejudicando inclusive a transparência do documento, recomenda-se que as medidas que de fato foram implementadas sejam descritas em uma linguagem o menos técnica possível – observando que o aviso é voltado aos titulares, o que inclui também os perfis não técnicos.

Por exemplo:

- i. se há criptografia dos dados pessoais em trânsito e armazenados, informe: “Seus dados pessoais são transmitidos e armazenados de forma protegida, o que reduz significativamente o risco de acesso não autorizado durante a transmissão ou o armazenamento.”;
- ii. se há controle de acesso, consigne “O acesso aos seus dados pessoais é restrito aos agentes públicos que necessitam deles para a execução de suas atribuições, mediante controles formais de autorização.”.

Deve-se atentar, ainda, para explicitar apenas as principais medidas aplicadas, ou seja, aquelas que fazem mais sentido demonstrar ao titular; por exemplo, sugere-se evitar explicitar os controles especialmente técnicos, como utilização de *firewall*, *Web Application Firewall* (WAF), entre outros. Além de serem controles de difícil compreensão ao titular, a exposição de determinadas configurações técnicas pode facilitar ataques direcionados. Por essa razão, o aviso deve descrever as medidas em linguagem acessível ao titular, sem revelar parâmetros técnicos específicos que possam comprometer a segurança do órgão ou entidade.

4.9 Agentes de tratamento e respectivas responsabilidades legais

O aviso de privacidade deve trazer informações do controlador dos dados pessoais. Portanto, identificação, endereço e informações de contato do órgão ou entidade, além das respectivas responsabilidades no tratamento dos dados pessoais, devem ser explicitadas neste tópico.

Ainda, na hipótese de haver outros controladores diretamente envolvidos no tratamento, suas informações também devem ser consignadas no aviso. Para esclarecimentos acerca do conceito de controladoria singular e conjunta, sugerimos a leitura do [Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado](#), da ANPD, item 3 (pgs. 12 a 15) [26].

Outro agente de tratamento que pode estar presente no serviço ofertado é o operador. Por essa razão, caso o serviço conte com operadores para o tratamento dos dados pessoais, sua identificação deve ser consignada no aviso.

4.10 Identificação e informações de contato do encarregado

O encarregado pelo tratamento de dados pessoais desempenha papel central na interlocução entre o órgão ou entidade, os titulares de dados pessoais e a Agência Nacional de Proteção de Dados (ANPD), sendo responsável, entre outras atribuições, por receber comunicações dos



titulares, prestar esclarecimentos e adotar as providências cabíveis, bem como atuar como canal de recebimento de comunicações da ANPD (LGPD, art. 41, § 2º) [2].

O exercício dessas atribuições pressupõe o apoio coordenado das unidades do órgão ou entidade envolvidas no tratamento de dados pessoais. Cabe às unidades responsáveis pelos serviços fornecer ao encarregado as informações necessárias para o atendimento tempestivo das demandas dos titulares, em consonância com os fluxos e prazos definidos na Política de Proteção de Dados Pessoais e nas normas internas do órgão ou entidade.

Para que os titulares possam exercer seus direitos e a ANPD possa manter contato institucional com o órgão ou entidade, é imprescindível que as informações de identificação e contato do Encarregado sejam divulgadas publicamente, de forma clara, em local de destaque e de fácil acesso no sítio eletrônico institucional – conforme determinado pela medida 21.4 do *framework* do PPSI 2.0 [1] e pelo § 1º do art. 41 da LGPD [2]. Além disso, a Resolução CD/ANPD nº 18, de 16 de julho de 2024, que aprova o Regulamento sobre a atuação do Encarregado, estabelece requisitos específicos quanto à sua identificação, publicidade das informações de contato e relacionamento com os titulares e a ANPD [6].

O aviso de privacidade deve conter as informações de identificação e contato do encarregado e seu respectivo substituto, contemplando, minimamente: nome completo, endereço físico para correspondência e os canais de contato disponibilizados ao titular – incluindo, no âmbito do Poder Executivo Federal, a remissão à Plataforma Integrada de Ouvidoria e Acesso à Informação (Fala.BR), quando adotada como canal oficial. Caso o serviço envolva outros controladores atuando em conjunto, as informações de contato do encarregado e substituto de cada controlador devem igualmente ser identificadas.

Para facilitar a manutenção e a atualização dessas informações, em especial diante de eventual substituição do encarregado ou seu substituto, hipótese que exigiria a revisão de todos os avisos de privacidade do órgão ou entidade, uma sugestão possível é a apresentação nos avisos de um *link* para a página institucional onde essas informações estejam centralizadas, atualizadas e de fácil acesso ao titular. Essa página deve observar os requisitos de publicidade previstos no § 1º do art. 41 da LGPD [2] e na Resolução CD/ANPD nº 18/2024 [6], e deve ser mantida permanentemente acessível, em local de destaque no sítio eletrônico do órgão ou entidade. A adoção desse modelo é compatível com o princípio da transparência ativa e com a lógica de centralização de informações institucionais já adotada neste Guia para outros elementos do aviso, como a inclusão do *link* do aviso na Carta de Serviços ao Usuário (subseção 3.8).

4.11 Informações sobre consentimento do titular dos dados pessoais

Inicialmente, cumpre destacar que, para os órgãos e entidades do Poder Público, o consentimento não é a base legal predominante para o tratamento de dados pessoais. O Guia para Tratamento de Dados Pessoais pelo Poder Público, publicado pela ANPD, esclarece que "em muitas ocasiões, o consentimento não será a base legal mais apropriada para o tratamento de dados pessoais pelo Poder Público, notadamente quando o tratamento for necessário para o cumprimento de obrigações e atribuições legais", em razão do desequilíbrio de forças que caracteriza a relação entre o Estado e o cidadão [15]. Não obstante, o mesmo Guia reconhece que o consentimento poderá eventualmente ser admitido como base legal,



desde que a utilização dos dados não seja compulsória e a atuação estatal não se baseie no exercício de prerrogativas estatais típicas, assegurando ao titular a efetiva possibilidade de autorizar ou não o tratamento sem que de sua recusa resultem restrições significativas a direitos [15]. Para aprofundamento sobre as bases legais aplicáveis ao Poder Público, recomenda-se a leitura integral do referido Guia [15].

Esta seção aborda especificamente as situações em que o consentimento é a base legal aplicável ao produto ou serviço. Nesses casos, além da identificação da base legal na tabela de finalidades descrita na subseção 4.4, o aviso de privacidade deve conter as informações adicionais detalhadas a seguir, que permitem ao titular compreender e exercer suas escolhas relativas ao tratamento.

- **Canal e procedimento para revogação do consentimento:** o aviso deve informar de forma clara como e por qual canal o titular pode revogar seu consentimento a qualquer momento, por procedimento gratuito e facilitado (LGPD, art. 8º, § 5º) [2]. Deve também esclarecer que a revogação não compromete a licitude dos tratamentos realizados durante o período em que o consentimento esteve vigente.
- **Consequências da negativa ou da revogação:** o aviso deve indicar, quando aplicável, as consequências práticas de não fornecer o consentimento ou de revogá-lo – por exemplo, a impossibilidade de acesso a determinada funcionalidade do serviço que dependa especificamente desse tratamento. Essa informação é condição de validade do próprio consentimento, que deve ser livre e informado (LGPD, art. 8º, caput) [2].
- **Mudança de finalidade:** quando houver alteração da finalidade do tratamento incompatível com o consentimento original, o aviso de privacidade deverá ser atualizado e o titular informado previamente sobre as mudanças, assegurada a possibilidade de revogação (LGPD, art. 9º, § 2º) [2]. Essa atualização corresponde a uma revisão de primeiro nível do aviso, nos termos da subseção 4.17 deste Guia.
- **Dados pessoais sensíveis:** quando o consentimento for a base legal para tratamento de dados pessoais sensíveis, o aviso deve indicar essa condição de forma específica, em consonância com a exigência de consentimento específico e destacado prevista no inciso I do art. 11 da LGPD [2]. A dispensa do consentimento para dados pessoais sensíveis tratados por órgãos e entidades públicas, quando aplicável, igualmente deve ser publicizada no aviso (LGPD, art. 11, § 2º) [2].
- **Dados de crianças e adolescentes:** quando o serviço tratar dados pessoais de crianças ou adolescentes com base no consentimento, o aviso deve identificar que a anuência específica de pelo menos um dos pais ou do responsável legal é exigida, nos termos do art. 14 da LGPD [2].
- **Compartilhamento dependente de consentimento específico:** quando dados pessoais tratados com base no consentimento forem compartilhados com outros controladores, o aviso deve informar essa condição e indicar que o consentimento do titular para esse compartilhamento é necessário, salvo as hipóteses de dispensa previstas na Lei (LGPD, art. 7º, § 5º) [2].

4.12 Informações sobre cada tratamento posterior

É possível o tratamento posterior de dados pessoais apenas se compatível com a finalidade original do tratamento (LGPD, art. 6º, inciso I). Ademais, nas hipóteses em que os dados cujo acesso é público ou que houve a dispensa do consentimento dos dados tornados



manifestamente públicos pelo titular, o tratamento posterior poderá ser realizado para novas finalidades – desde que observados os propósitos legítimos e específicos e a preservação dos direitos do titular, assim como os fundamentos e os princípios previstos na LGPD (LGPD, art. 7º, § 7º).

Portanto, caso haja tratamento posterior dos dados coletados no âmbito do serviço, devem ser registrados no aviso de privacidade – indicando também a fundamentação legal do tratamento posterior e sua finalidade.

4.13 Utilização de Cookies

Cookies são conjuntos de dados gerados durante o acesso de um usuário a uma aplicação e armazenados em seu dispositivo, visando ao atendimento de diferentes finalidades, como gerenciamento de sessões, personalização e rastreamento [19], [20].

De forma geral, compreende-se que a utilização de *cookies* implica tratamento de dados pessoais; assim, tal como toda operação de tratamento de dados pessoais, as informações sobre o tratamento dos dados armazenados em *cookies* devem ser apresentadas aos titulares, conforme abordado nos tópicos anteriores do aviso de privacidade.

Ademais, sugere-se a indicação se os *cookies* utilizados são de sessão ou persistentes, além das categorias:

1. *cookies* primários: são aqueles gerenciados pelo próprio controlador ou operador, sendo registrados apenas para seu uso. Por exemplo: se dentro de uma determinada página do serviço tiver *cookies*, quando o usuário acessar o endereço, suas informações ficarão registradas para análise do órgão ou entidade. Sua utilização é comum, por exemplo, para armazenar preferências de idioma e facilitar a funcionalidade básica do sítio eletrônico;
2. *cookies* de terceiros: são aqueles disponibilizados por terceiros que não sejam o controlador ou operador de dados original. Estes *cookies* estão geralmente associados à publicidade.

É igualmente relevante classificar os *cookies* quanto às finalidades. Nesse caso, algumas classificações comumente encontradas são: estritamente necessários (como os de sessão de navegação, principalmente aqueles empregados em sistemas que requerem autenticação, além de *cookies* para operações de segurança), de personalização, analíticos, de multimídia ou de publicidade.

Também é importante consignar no aviso como o titular pode gerenciar os *cookies* – lembrando que ao utilizar a base legal de consentimento é recomendado que o sistema possibilite que, a qualquer momento e em qualquer lugar, o titular possa acessar suas escolhas feitas anteriormente e alterá-las.

Além disso, o detalhamento sobre os *cookies* utilizados deve estar disposto em uma área separada do aviso, primando pela clareza dos avisos de privacidade, e consequentemente propiciando transparência ao titular. Assim sendo, sugere-se que no aviso tenha apenas a referência aos *cookies*, remetendo-a a uma área que pode ser denominada de “Declaração de *cookies*”.



4.14 Direitos do titular dos dados pessoais

O aviso de privacidade deve informar ao titular quais são seus direitos em relação aos dados pessoais tratados pelo órgão ou entidade no âmbito do produto ou serviço, os canais disponíveis para exercê-los e as condições de atendimento aplicáveis.

Os direitos dos titulares estão previstos nos arts. 18 e 20 da LGPD [2] e podem ser agrupados em dois conjuntos segundo sua aplicabilidade:

Direitos aplicáveis a qualquer tratamento não realizado com base no consentimento:

- confirmação da existência do tratamento dos seus dados pessoais;
- acesso aos seus dados pessoais, de forma simplificada e gratuita;
- 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 e observados os segredos comercial e industrial;
- informação sobre as entidades públicas e privadas com as quais o órgão ou entidade realizou uso compartilhado de dados;
- revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem os interesses do titular, incluídas as decisões destinadas a definir perfis pessoal, profissional, de consumo e de crédito (LGPD, art. 20) [2].

Direitos condicionados ao uso do consentimento como base legal:

- eliminação dos dados pessoais tratados com o consentimento do titular, ressalvadas as hipóteses de conservação previstas no art. 16 da LGPD – aplicável quando o consentimento for a base legal (LGPD, art. 18, VI) [2];
- informação sobre a possibilidade de não fornecer o consentimento e sobre as consequências da negativa – aplicável quando o consentimento for a base legal (LGPD, art. 18, VIII) [2];
- revogação do consentimento, por procedimento gratuito e facilitado – aplicável quando o consentimento for a base legal (LGPD, art. 18, IX) [2].

O aviso de privacidade também deve informar que o titular tem o direito de apresentar petição em relação a seus dados pessoais perante a ANPD, nos termos do § 1º do art. 18 da LGPD [2] e do inciso VI do § 2º do art. 17 da Resolução CD/ANPD nº 19/2024 [8].

O aviso também deve informar ao titular o canal oficial pelo qual pode exercer seus direitos e, quando aplicável, a existência de procedimento simplificado de acesso imediato, na forma do art. 19, § 1º [2].

Ao elaborar essa seção do aviso, recomenda-se apresentar apenas os direitos efetivamente aplicáveis ao serviço, evitando listar direitos que não têm pertinência com o tratamento descrito. A apresentação de direitos inaplicáveis ao caso concreto pode confundir o titular e comprometer a clareza do aviso. Em especial, os direitos condicionados à base legal só devem ser listados quando o tratamento do serviço efetivamente estiver amparado na base correspondente.



4.15 Decisão automatizada

Caso o serviço utilize tratamento automatizado de dados pessoais para produzir decisões que afetem os interesses dos titulares – incluindo, por exemplo, a definição de perfis pessoal, profissional, de consumo ou de crédito – essa condição deve ser explicitada no aviso de privacidade, em conformidade com o direito à revisão de decisões automatizadas (LGPD, art. 20) [2].

O aviso deve conter, em linguagem simples e acessível ao titular, sem necessidade de descrição matemática ou técnica dos algoritmos envolvidos:

- identificação da existência do tratamento automatizado, informando que o serviço utiliza processos automatizados para tomada de decisão ou definição de perfis;
- tipos de dados pessoais que alimentam o processo de decisão automatizada, bem como os demais dados pessoais produzidos como resultado;
- finalidade e impacto para o titular, descrevendo, em termos práticos, o tipo de decisão produzida e seus efeitos sobre o titular – por exemplo, aprovação ou reprovação de benefício, classificação de risco, personalização de serviço;
- canal para exercício do direito de revisão, em alinhamento com o estabelecido na subseção 4.14, indicando como o titular pode solicitar a revisão da decisão e obter informações sobre os critérios e procedimentos utilizados, observados os segredos comercial e industrial (LGPD, art. 20, § 2º) [2].

Quando o detalhamento da lógica da decisão automatizada puder comprometer informações classificadas ou sigilosas nos termos da Lei nº 12.527, de 18 de novembro de 2011 [11], ou envolver segredos comercial e industrial protegidos pelo § 2º do art. 20 da LGPD [2], o aviso deve informar a existência do tratamento automatizado e seus efeitos para o titular, sem necessidade de detalhar os parâmetros específicos do processo. Nessas situações, recomenda-se que o aviso informe expressamente que determinados aspectos metodológicos não podem ser divulgados em razão de restrição legal, assegurando ao titular clareza sobre o que pode e o que não pode ser informado.

4.16 Comunicação de mudanças nos avisos de privacidade

O aviso de privacidade deve informar ao titular como será comunicado sobre futuras atualizações que impactem o tratamento de seus dados pessoais, em consonância com o dever de prévia comunicação nas hipóteses de mudança de finalidade incompatível com o tratamento original (LGPD, art. 9º, § 2º) [2].

O aviso deve conter, minimamente:

- canal de disponibilização das atualizações, indicando o endereço eletrônico ou página institucional onde a versão atualizada do aviso estará sempre acessível ao titular;
- forma de comunicação ativa, indicando por qual meio – e-mail, notificação no sistema, publicação em sítio institucional, entre outros – o titular será diretamente comunicado nas hipóteses de atualização de primeiro nível, assim definidas na subseção 4.17 deste Guia;



- escopo das atualizações que geram comunicação ativa, informando ao titular que nem toda alteração no aviso implicará comunicação direta – apenas aquelas que alterem o sentido do documento, como mudança de finalidade, de base legal, de destinatários do compartilhamento ou de prazo de retenção. A ABNT NBR ISO/IEC 29184:2021 exemplifica entre essas situações a alteração dos dados de contato do controlador e do período de retenção dos dados pessoais [11].

Para as atualizações de segundo nível, que são correções formais que não alteram o sentido do documento, é suficiente a disponibilização da versão atualizada no canal indicado no aviso, sem necessidade de comunicação direta ao titular. Os critérios sugeridos para classificação das atualizações estão descritos na subseção 4.17 deste Guia.

4.17 Versão e data do documento

O aviso de privacidade deve indicar a sua versão atual e a data de entrada em vigor, de modo que o titular possa identificar se está consultando a versão vigente e verificar quando ocorreram eventuais atualizações anteriores.

Essas informações devem estar posicionadas de forma destacada no aviso, preferencialmente no início ou no final do documento, acompanhadas de canal de acesso ao histórico de versões anteriores, nos termos do princípio da transparência (LGPD, art. 6º, VI) [2] e do dever de publicidade dos atos da administração pública (CF, art. 37, *caput*; LAI, art. 8º) [11].

Gatilhos para revisão: a revisão dos avisos de privacidade deve ser realizada, no mínimo, nas seguintes situações:

- alteração na legislação ou regulamentação aplicável ao tratamento de dados pessoais do produto ou serviço;
- inclusão de nova finalidade ou mudança nas características das operações de tratamento de dados pessoais, como novo tipo de dado pessoal, novo agente de tratamento ou alteração no prazo de retenção;
- alteração no canal de contato com o encarregado;
- mudança na forma de obtenção ou de compartilhamento dos dados pessoais;
- encerramento do serviço ou de parte das operações de tratamento.

Recomenda-se, ainda, a revisão ordinária periódica em intervalos definidos pela unidade responsável, independentemente da ocorrência de quaisquer dos gatilhos acima. Quando o serviço disponibilizar o aviso também em formato físico – como em atendimentos presenciais ou materiais impressos –, as versões físicas devem ser mantidas atualizadas em consonância com a versão digital vigente.

Crítérios de versionamento: para fins de controle e comunicação ao titular, recomenda-se adotar os seguintes critérios:

- **versões de primeiro nível (1.0, 2.0, 3.0):** reservadas para atualizações que alterem o sentido do documento – como mudança de finalidade, de base legal, de destinatários do compartilhamento ou de prazo de retenção. Recomenda-se, conforme disposto na subseção 4.16 deste Guia, que essas atualizações sejam comunicadas ativamente aos titulares;



- **versões de segundo nível (1.1, 1.2, 1.3):** utilizadas para ajustes que não alterem o sentido do documento, como correções gramaticais, atualizações de dados de contato do encarregado sem mudança de canal, ou melhorias de legibilidade. Nessas hipóteses, é suficiente a disponibilização da versão atualizada no canal indicado no aviso, sem necessidade de comunicação ativa ao titular.

Histórico de versões: o órgão ou entidade deve manter registro das atualizações do aviso, contemplando versão, data de entrada em vigor, unidade responsável pela atualização e descrição resumida das alterações realizadas. A tabela a seguir ilustra um formato recomendado:

Tabela 1: Histórico de mudanças do aviso de privacidade

Versão	Data	Autor	Comentário da versão
1.0	[dd/mm/aaaa]	[unidade responsável]	Publicação da primeira versão deste aviso
1.1	[dd/mm/aaaa]	[unidade responsável]	[exemplo: correção gramatical na seção X]
2.0	[dd/mm/aaaa]	[unidade responsável]	[exemplo: inclusão de nova finalidade de tratamento]

O histórico pode ser disponibilizado em página específica no sítio eletrônico do órgão ou entidade, com *link* de acesso indicado no próprio aviso, dispensando sua reprodução integral em cada versão do documento. Para promover ainda mais transparência, junto à tabela de histórico pode ser disponibilizado *link* para acesso às versões anteriores do aviso.



5 Formatos

Os avisos de privacidade podem ser apresentados em diferentes formatos – físicos ou digitais, completos ou sintetizados –, conforme a natureza do produto ou serviço, o perfil do público-alvo e os recursos disponíveis para a sua elaboração, em consonância com as orientações sobre recursos visuais descritas na subseção 4.5 deste Guia.

De modo independente do formato adotado, o conjunto integral das informações previstas na seção 5 deve estar disponível ao titular em um único local de fácil acesso, seja o próprio documento, seja página específica no sítio eletrônico do órgão ou entidade para a qual o aviso remeta expressamente. Formatos sintetizados ou parciais são complementares à versão completa, nunca substitutivos.

A ABNT NBR ISO/IEC 29184:2021 [11], assim como a *Information Commissioner's Office* (ICO) – autoridade de proteção de dados pessoais do Reino Unido –, identificam técnicas que podem ser utilizadas para apresentar as informações ao titular com maior clareza e facilidade de leitura, entre as quais⁴:

- avisos em camadas: apresentam inicialmente um resumo com as informações mais relevantes, como a identidade do órgão ou entidade e as finalidades principais do tratamento, com *links* que expandem cada elemento para um nível de detalhe maior. Úteis para serviços digitais com grande volume de informações, pois permitem ao titular acessar progressivamente o nível de detalhe que deseja sem ser confrontado com todo o conteúdo de uma vez;
- painéis de preferências: ferramentas que permitem ao titular visualizar e gerenciar suas escolhas em relação ao tratamento, especialmente relevantes quando o consentimento é a base legal para uma ou mais finalidades. Devem estar vinculados ao aviso de privacidade e não o substituem;
- avisos *just-in-time*: exibidos no momento exato em que determinado dado pessoal é solicitado, fornecendo ao titular informação contextualizada sobre a finalidade daquela coleta específica, especialmente úteis em formulários com múltiplos campos;
- ícones: elementos visuais padronizados que sinalizam a ocorrência de determinado tipo de tratamento, como o uso de dados de localização ou a existência de compartilhamento. Complementam o texto do aviso sem substituí-lo, e sua efetividade depende de padronização reconhecível pelo titular. Essa abordagem é frequentemente usada em processamentos intermitentes, como em smartphones para indicar se um aplicativo específico está ou não processando dados de localização, inserindo um ícone reconhecível na barra de *status*.

5.1 Versão sintética

A versão sintética do aviso de privacidade apresenta, de forma condensada, os elementos de conteúdo mais relevantes para a compreensão imediata do titular, com linguagem direta e estrutura visual que facilite a leitura. Deve sempre conter acesso explícito à versão completa

⁴ Descrição das técnicas adaptada de ICO [21] e ABNT NBR ISO/IEC 29184:2021 [10]. Data de acesso: 12 mai. 2026.



– por *link*, botão ou remissão expressa –, que permanece o documento de referência para o conjunto integral das informações previstas na seção 5 deste Guia.

A estrutura da versão sintética pode ser organizada por tópicos, com o uso de recursos visuais como *dropdowns*, acordeões ou ícones que permitam ao titular expandir cada item conforme seu interesse. A seguir, apresenta-se um exemplo de estrutura:

Aviso de Privacidade

Este aviso informa como o [órgão ou entidade] trata seus dados pessoais no âmbito do [nome do produto ou serviço].

Tópicos:

1. Quais tipos de dados pessoais são tratados?
2. Como e para quais finalidades são tratados?
3. Com quem são compartilhados?
4. Por quanto tempo são retidos?
5. Quais medidas de segurança dos dados são implementadas?
6. Quais são os seus direitos e como exercê-los?
7. Quais os dados de contato com o encarregado?
8. Versão e data deste aviso

Cada tópico deve remeter ao conteúdo correspondente da versão completa ou apresentá-lo de forma condensada ao ser expandido pelo titular.

5.2 Versão completa

A versão completa do aviso de privacidade deve contemplar integralmente os elementos de conteúdo descritos na seção 5 deste Guia, observada a aplicabilidade de cada elemento ao serviço específico e ao tratamento de dados pessoais a ele relacionado. É o documento de referência do aviso e deve estar sempre acessível ao titular, independentemente dos demais formatos adotados pelo órgão ou entidade.

5.3 Versão em imagem ou vídeo

Quando houver possibilidade de apresentar o aviso de privacidade em formato de imagem, como infográfico, ou de vídeo, esses formatos funcionam como versões sintéticas de apoio à compreensão do titular e devem observar as mesmas orientações da seção 4. Em qualquer hipótese, devem conter remissão expressa à versão completa do aviso, garantindo ao titular acesso ao conjunto integral das informações.

Nesses formatos, deve-se assegurar a acessibilidade do conteúdo, com legendas ou transcrição textual para vídeos e texto alternativo para imagens, em consonância com os requisitos de acessibilidade digital aplicáveis aos sítios eletrônicos do Poder Executivo Federal.



6 Considerações finais

O aviso de privacidade é, antes de tudo, um instrumento de diálogo. Ao informar o titular de dados pessoais sobre como, para quê e com quem seus dados são tratados, o órgão ou entidade não apenas cumpre uma obrigação legal decorrente da LGPD e do marco normativo do Governo Digital – cumpre também um compromisso ético com a transparência e com o respeito à autonomia do cidadão sobre seus próprios dados.

As orientações reunidas neste Guia visam apoiar os órgãos e entidades do SISP na elaboração de avisos de privacidade que sejam, simultaneamente, juridicamente fundamentados, operacionalmente viáveis e genuinamente compreensíveis pelo titular. Esses três atributos não são excludentes: um aviso claro é também mais eficaz como instrumento de conformidade, porque reduz ambiguidades na interpretação das obrigações do controlador e facilita o exercício dos direitos pelo titular.

A elaboração do aviso de privacidade, contudo, não é um ato isolado. Ela pressupõe que o órgão ou entidade tenha previamente mapeado as operações de tratamento de dados pessoais realizadas no âmbito do serviço – identificando finalidades, bases legais, tipos de dados pessoais, agentes de tratamento envolvidos e prazos de retenção. Sem esse mapeamento prévio, o aviso corre o risco de ser um documento genérico, desconectado da realidade do tratamento, e, portanto, incapaz de cumprir sua função de informar o titular com precisão. Nesse sentido, o aviso de privacidade é também um produto do amadurecimento institucional em proteção de dados pessoais, e a sua qualidade reflete o grau de governança do órgão ou entidade sobre as próprias operações de tratamento.

Dois aspectos práticos merecem destaque ao final deste Guia. O primeiro é a manutenção: um aviso de privacidade elaborado com rigor perde progressivamente sua utilidade se não for revisado quando o tratamento muda. Os gatilhos e critérios de versionamento descritos na subseção 4.17 devem ser tratados não como recomendações opcionais, mas como parte do ciclo de vida dos produtos e serviços – tão necessários quanto a atualização dos sistemas que o suportam. O segundo é a linguagem: a tentação de reproduzir dispositivos legais ou adotar a nomenclatura técnica da LGPD no aviso deve ser permanentemente resistida; isso porque o titular não é operador jurídico nem especialista em proteção de dados, é uma pessoa que usa o produto ou serviço e que tem o direito de entender, sem esforço adicional, o que acontece com seus dados.

Por fim, cabe situar o aviso de privacidade no contexto mais amplo da relação entre o Estado e o cidadão. A LGPD não impôs ao Poder Público apenas obrigações de conformidade – impôs um novo padrão de relacionamento informacional com a sociedade. O cidadão que acessa um serviço público digital passa a ter o direito de saber, com clareza e antecedência, quais dados serão coletados, com quem serão compartilhados e por quanto tempo serão retidos. Esse direito, quando respeitado genuinamente, fortalece a confiança institucional e contribui para a legitimidade da atuação pública. O aviso de privacidade bem elaborado é, assim, uma expressão concreta do compromisso do Estado com a transparência, com a dignidade da pessoa humana e com os direitos fundamentais que a Constituição Federal [27] e a LGPD [2] consagram.



7 Referências bibliográficas

1. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Portaria SGD/MGI nº 9.511, de 28 de outubro de 2025**. Institui o Programa de Privacidade e Segurança da Informação (PPSI 2.0) no âmbito dos órgãos e entidades integrantes do SISP. Brasília, DF, 2025.
2. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 12 mai. 2026.
3. BRASIL. Gabinete de Segurança Institucional da Presidência da República. **Portaria GSI/PR nº 93, de 18 de outubro de 2021**. Aprova o Glossário de Segurança da Informação. Brasília, DF: GSI/PR, 2021.
4. BRASIL. Secretaria de Governo Digital do Ministério da Economia. **Portaria SGD/ME nº 548, de 29 de setembro de 2022**. Aprova normas complementares ao Decreto nº 9.756, de 11 de abril de 2019. Brasília, DF: SGD/ME, 2022.
5. BRASIL. **Lei nº 14.129, de 29 de março de 2021**. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública. Disponível em: <https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132>. Acesso em: 12 mai. 2026.
6. BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Secretaria de Governo Digital. **Guia do Framework de Privacidade e Segurança da Informação: Programa de Privacidade e Segurança da Informação (PPSI 2.0)**. Versão 1.2. Brasília, DF: MGI, 2026. Disponível em: <https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi-2.0/arquivos/guiafwppsi2-0-v1-2-11062026.pdf>. Acesso em: 12 jun. 2026.
7. BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 18, de 16 de julho de 2024**. Aprova o Regulamento sobre a atuação do Encarregado pelo Tratamento de Dados Pessoais. Brasília, DF: ANPD, 2024.
8. BRASIL. Agência Nacional de Proteção de Dados. **Resolução CD/ANPD nº 19, de 23 de agosto de 2024**. Aprova o Regulamento de Transferência Internacional de Dados Pessoais e as Cláusulas-Padrão Contratuais. Brasília, DF: ANPD, 2024.
9. BRASIL. **Decreto nº 9.094, de 17 de julho de 2017**. Dispõe sobre a simplificação do atendimento prestado aos usuários dos serviços públicos. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/decreto/d9094.htm. Acesso em: 12 mai. 2026.
10. BRASIL. **Lei nº 13.146, de 6 de julho de 2015**. Institui a Lei Brasileira de Inclusão da Pessoa com Deficiência (Estatuto da Pessoa com Deficiência). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm. Acesso em: 12 mai. 2026.
11. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 29184:2021**: tecnologia da informação — avisos de privacidade on-line e consentimento. Rio de Janeiro: ABNT, 2021.
12. VAINZOFF, Rony; SERAFINO, Danielle; STEINWASCHER, Aline. **Legal innovation: o futuro do Direito e o Direito do futuro**. São Paulo: Thomson Reuters Brasil, 2022.
13. BRASIL. **Lei nº 10.436, de 24 de abril de 2002**. Dispõe sobre a Língua Brasileira de Sinais – Libras. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/2002/L10436.htm. Acesso em: 12 mai. 2026.



14. BRASIL. Secretaria de Governo Digital. **Cartilha sobre Finalidade e Hipóteses Legais**. Brasília, DF: SGD/MGI, [s.d.]. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/cartilha_finalidade_hipoteses_legais.pdf. Acesso em: 12 mai. 2026.
15. BRASIL. Agência Nacional de Proteção de Dados. **Guia para Tratamento de Dados Pessoais pelo Poder Público**. Brasília, DF: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Acesso em: 12 mai. 2026.
16. FRAZÃO, Ana; CUEVA, Ricardo Villas Bôas (coord.). **Compliance e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. (Cap. 10, por GUEDES, Gisela; MEIRELES, Rose).
17. BRASIL. Conselho Nacional de Arquivos. **Resolução CONARQ nº 54, de 8 de dezembro de 2023**. Estabelece diretrizes e regras para a aplicação da Lei nº 13.709/2018 para os arquivos permanentes. Disponível em: <https://www.gov.br/conarq/pt-br/legislacao-arquivistica/resolucoes-do-conarq/resolucao-no-54-de-8-de-dezembro-de-2023>. Acesso em: 12 mai. 2026.
18. BRASIL. **Decreto nº 10.046, de 9 de outubro de 2019**. Dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/D10046.htm. Acesso em: 12 mai. 2026.
19. BRASIL. Agência Nacional de Proteção de Dados. **Guia orientativo: cookies e proteção de dados pessoais**. Brasília, DF: ANPD, 2022. Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-cookies-e-protecao-de-dados-pessoais.pdf>. Acesso em: 7 mai. 2026.
20. BARTH, Adam. RFC 6265: **HTTP State Management Mechanism**. Internet Engineering Task Force (IETF), abr. 2011. Disponível em: <https://datatracker.ietf.org/doc/html/rfc6265>. Acesso em: 12 mai. 2026.
21. BRASIL. **Lei nº 13.460, de 26 de junho de 2017**. Dispõe sobre participação, proteção e defesa dos direitos do usuário dos serviços públicos da administração pública. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm. Acesso em: 12 mai. 2026.
22. INFORMATION COMMISSIONER'S OFFICE (ICO). **What methods can we use to provide privacy information?** Wilmslow: ICO, [20--]. Disponível em: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/the-right-to-be-informed/what-methods-can-we-use-to-provide-privacy-information/>. Acesso em: 12 mai. 2026.
23. CMS LAW. **GDPR Enforcement Tracker Report 2024/2025**. 6. ed. [S.l.]: CMS, mar. 2025. Disponível em: <https://cms.law/en/int/publication/gdpr-enforcement-tracker-report>. Acesso em: 12 mai. 2026.
24. SURFSHARK. **GDPR fines in 2025: most frequent and most costly violations**. [S.l.]: Surfshark, jan. 2026. Disponível em: <https://surfshark.com/research/study/gdpr-fines-2025>. Acesso em: 12 mai. 2026.
25. BRASIL. Agência Nacional de Proteção de Dados. **Processo Administrativo Sancionador nº 00261.000489/2022-21**. Decisão de aplicação de sanções administrativas à Telekall Infoservice. Brasília, DF: ANPD, jul. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-aplica-primeira-sancao-administrativa>. Acesso em: 12 mai. 2026.



26. BRASIL. Agência Nacional de Proteção de Dados. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Versão 2.0. Brasília, DF: ANPD, 2022.

Disponível em: <https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-orientativo-para-definicoes-dos-agentes-de-tratamento-de-dados-pessoais-e-do-encarregado>. Acesso em: 12 jun. 2026.

27. BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, 1988. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm Acesso em: 12 jun. 2026.



gov.br

Dúvida?

Entre em contato
conosco

Sítio do PPSI:

[PPSI 2.0 — Governo Digital](#)