CNPJ Nº 05.466.164/0001-22
RUA MANOEL PIRES, Nº 471, JOSÉ GERALDO DA CRUZ
TELEFONE (88) 2141-9423

JUAZEIRO DO NORTE - CEARÁ

**PORTARIA 08/2026-DIREÇÃO-GERAL-CMJN**

INSTITUI A POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DA CÂMARA MUNICIPAL DE JUAZEIRO DO NORTE E DÁ OUTRAS PROVIDÊNCIAS.

A DIREÇÃO-GERAL DA CÂMARA MUNICIPAL DE JUAZEIRO DO NORTE, no uso de suas atribuições legais e administrativas,

**CONSIDERANDO** o art. 5º, inciso X, da Constituição Federal, que assegura a inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas;

**CONSIDERANDO** o art. 37 da Constituição Federal, que impõe à Administração Pública a observância dos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência;

**CONSIDERANDO** a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

**CONSIDERANDO** a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

**CONSIDERANDO** a Lei nº 8.159, de 08 de janeiro de 1991 (Política Nacional de Arquivos Públicos);

**CONSIDERANDO** o Decreto nº 10.046/2019, que dispõe sobre o compartilhamento de dados no âmbito da Administração Pública Federal;

**CONSIDERANDO** as Resoluções, Guias e Orientações expedidas pela Autoridade Nacional de Proteção de Dados – ANPD;

**CONSIDERANDO** a necessidade de estabelecer diretrizes estruturadas de governança, conformidade e segurança no tratamento de dados pessoais no âmbito da Câmara Municipal de Juazeiro do Norte,

**RESOLVE:**

**Art. 1º -** Fica instituída a Política Interna de Privacidade e Proteção de Dados Pessoais da Câmara Municipal de Juazeiro do Norte, na forma do Anexo I desta Portaria.

**Art. 2º -** A Política aplica-se a todas as operações de tratamento de dados pessoais realizadas pela Câmara, abrangendo servidores, colaboradores, prestadores de serviço, parceiros e terceiros que atuem em seu nome.

**Art. 3º -** Compete ao Encarregado de Dados (DPO):

I – Atuar como canal de comunicação entre a Câmara, os titulares e a Autoridade Nacional de Proteção de Dados;
II – Orientar as unidades administrativas quanto à aplicação da LGPD;
III – Monitorar a conformidade institucional;
IV – Coordenar a gestão de incidentes de segurança envolvendo dados pessoais;
V – Propor revisões periódicas desta Política.

**Art. 4º -** As unidades administrativas deverão adotar medidas técnicas e organizacionais adequadas à proteção de dados pessoais, observando os princípios do art. 6º da LGPD.

**Art. 5º -** O descumprimento das disposições desta Portaria poderá ensejar responsabilização administrativa, civil e penal, nos termos da legislação vigente.

**Art. 6º -** Esta Portaria entra em vigor na data de sua publicação interna.

Juazeiro do Norte/CE – 05 de janeiro de 2026

Francisco Wagner Santana Filgueiras

**FRANCISCO WAGNER SANTANA FILGUEIRAS**
Diretor-Geral / CMJN - Portaria 516/2025

**ANEXO I**
**POLÍTICA INTERNA DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS**
Câmara Municipal de Juazeiro do Norte

## 1. OBJETO, OBJETIVOS E ESCOPO DE APLICAÇÃO

A inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas naturais é um direito fundamental garantido pela Constituição Federal de 1988 (art. 5º, X). Nesse contexto, a Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) estabelece regras e princípios para o tratamento de dados pessoais, inclusive por meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

A proteção de dados pessoais no Brasil tem como fundamentos:

I. Respeito à privacidade e à autodeterminação informativa;
II. Liberdade de expressão, de informação, de comunicação e de opinião;
III. Inviolabilidade da intimidade, da honra e da imagem;
IV. Desenvolvimento econômico, tecnológico e inovação;
V. Livre iniciativa, livre concorrência e defesa do consumidor;
VI. Direitos humanos, dignidade da pessoa humana e exercício da cidadania.

A presente Política define as orientações gerais para a proteção de dados pessoais tratados no âmbito da Câmara de Juazeiro do Norte (“Câmara”).

A Câmara compromete-se a assegurar a implementação contínua e eficaz desta Política, esperando igual comprometimento de seus colaboradores e parceiros.

Qualquer violação será tratada com rigor e poderá resultar em medidas disciplinares ou legais cabíveis.

A presente Política de Atendimento aos Titulares de Dados é fundamentada na Lei nº 13.709/2018 (LGPD), que estabelece o marco legal para a proteção de dados pessoais, e requer a observância de um conjunto normativo que inclui o Decreto nº 10.046/2019 (sobre compartilhamento), a Lei nº 12.527/2011 (Lei de Acesso à Informação), a Lei nº 8.159/1991 (que dispõe sobre Arquivos Públicos), bem como as Resoluções e Guias emitidos pela ANPD, que, em conjunto, delimitam o escopo e os procedimentos de tratamento de dados pelo Poder Público.

## 2. ESCOPO DE APLICAÇÃO

Esta Política aplica-se a todas as operações de coleta, uso, armazenamento, eliminação, compartilhamento e demais formas de tratamento de dados pessoais realizadas pela Câmara, por seus colaboradores, prestadores de serviço e parceiros.

Conforme o art. 3º da LGPD, a aplicação se dá sempre que:

I. O tratamento for realizado no território nacional;
II. O tratamento tiver por objetivo a oferta de bens ou serviços para indivíduos localizados no Brasil;
III. Os dados pessoais tiverem sido coletados no território nacional.

Assim, esta Política vincula:

I. Todos os colaboradores da Câmara;
II. Parceiros e fornecedores que tratem dados pessoais em nome da Câmara.

## 3. BASE NORMATIVA

Esta Política fundamenta-se nos seguintes diplomas legais e normativos:

I. Constituição Federal de 1988 – art. 5º, X;
II. Lei nº 8.078/1990 – Código de Defesa do Consumidor (CDC);
III. Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
IV. Lei nº 12.965/2014 – Marco Civil da Internet e Decreto nº 8.771/2016;
V. Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD).

## 4. DEFINIÇÕES

Para fins desta Política, aplicam-se os seguintes conceitos:

I. Agentes de Tratamento – Controlador e Operador, bem como pessoas indicadas para atuar como canal de comunicação com titulares e a ANPD.
II. Anonimização – Processo que impossibilita associação direta ou indireta entre dados e um indivíduo.
III. ANPD – Autoridade Nacional de Proteção de Dados, órgão responsável por fiscalizar o cumprimento da LGPD.
IV. Aviso de Privacidade – Documento que informa ao titular como seus dados são coletados, utilizados e protegidos.
V. Banco de Dados – Conjunto estruturado de dados pessoais em suporte físico ou eletrônico.
VI. Bloqueio – Suspensão temporária de qualquer operação de tratamento, com guarda do dado.
VII. Consentimento – Manifestação livre, informada e inequívoca do titular que concorda com o tratamento para finalidade determinada.
VIII. Controlador – Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões sobre o tratamento de dados pessoais.
IX. Dado Pessoal – Informação relacionada a pessoa natural identificada ou identificável (ex.: nome, RG, CPF, endereço, telefone).
X. Dado Pessoal Sensível – Dado que pode gerar discriminação, como origem racial, convicção religiosa, opinião política, saúde, vida sexual, dado biométrico ou genético.
XI. Dado Público – Informação tornada manifestamente pública pelo titular ou disponível em meios de acesso público.
XII. DPO (Encarregado de Dados) – Pessoa indicada pelo Controlador como responsável por atuar como canal de comunicação entre controlador, titulares e ANPD.
XIII. Eliminação – Exclusão de dado armazenado em banco de dados, independentemente do procedimento utilizado.
XIV. Incidente de Segurança – Evento adverso confirmado ou sob suspeita que compromete a confidencialidade, integridade ou disponibilidade de dados pessoais.
XV. Legítimo Interesse – Hipótese legal que autoriza o tratamento de dados visando atender interesses legítimos do controlador ou de terceiros, desde que não prevaleçam os direitos do titular.
XVI. Medidas de Segurança – Ações técnicas e administrativas voltadas à proteção de dados contra acessos não autorizados, perdas, destruição ou uso inadequado.

XVII. Operador – Pessoa natural ou jurídica que realiza o tratamento de dados pessoais em nome do Controlador.
XVIII. Pseudonimização – Técnica que dificulta, mas não elimina, a associação de um dado a uma pessoa natural.
XIX. Relatório de Impacto à Proteção de Dados Pessoais (DPIA) – Documento do Controlador que descreve processos de tratamento e medidas para mitigar riscos.
XX. Terceiros – Fornecedores, parceiros e contratados que tenham acesso a dados pessoais no exercício de suas atividades.
XXI. Titular – Pessoa natural a quem se referem os dados pessoais.
XXII. Transferência Internacional de Dados – Envio de dados pessoais para país estrangeiro ou organismo internacional.
XXIII. Tratamento de Dados Pessoais – Toda operação com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração Uso Compartilhado de Dados – Comunicação ou interconexão de dados pessoais entre órgãos e entidades públicos ou privados, nos termos da legislação.
XXIV. Canal de atendimento ao titular: Mecanismo obrigatório a ser disponibilizado pelo agente de tratamento (público ou privado) para o recebimento de comunicações e requisições dos titulares de dados pessoais, assegurando o exercício facilitado de seus direitos. Nos termos da Resolução CD/ANPD nº 2/2022, agentes de tratamento de pequeno porte dispensados de indicar um Encarregado devem, obrigatoriamente, disponibilizar esse canal de comunicação.

## 5. FUNDAMENTOS GERAIS

Para que o tratamento de dados pessoais – comuns ou sensíveis – seja adequado, é essencial a estrita observância dos dez princípios do art. 6º da LGPD, que asseguram legalidade, proporcionalidade e respeito aos direitos dos titulares.

No âmbito da Câmara, esses princípios norteiam todas as atividades de coleta, uso, guarda, compartilhamento e eliminação de dados pessoais, de forma a atender às normas nacionais e às boas práticas de governança em proteção de dados (garantia de que as informações gerais sobre tratamento de dados estejam disponíveis no portal institucional).

## 6. HIPÓTESES LEGAIS E TRANSPARÊNCIA

O tratamento de dados pessoais somente será realizado quando houver fundamento jurídico válido. Entre as hipóteses autorizadas estão:

I. Cumprimento de obrigação legal ou regulatória;
II. Execução de contrato do qual o titular seja parte;
III. Exercício regular de direitos em processo judicial, administrativo ou arbitral;
IV. Atuação baseada em legítimo interesse do controlador ou de terceiros, desde que respeitados os direitos do titular;
V. Consentimento livre, específico e inequívoco do titular, quando nenhuma outra hipótese legal for aplicável.

O consentimento, quando necessário, será registrado de forma organizada e acessível, podendo ser retirado pelo titular a qualquer momento, com a mesma facilidade com que foi fornecido.

## 7. DADOS PESSOAIS SENSÍVEIS

O uso de dados sensíveis (como saúde, biometria, convicções religiosas ou políticas, orientação sexual, filiação sindical, origem racial/étnica, ou informações criminais) é, por regra, proibido, sendo permitido apenas em situações específicas, tais como:

I. Cumprimento de obrigação legal;
II. Defesa de direitos em processos judiciais ou administrativos;
III. Exercício de obrigações trabalhistas, previdenciárias ou de proteção social;
IV. Proteção da vida ou da integridade física do titular ou de terceiros;
V. Garantia da igualdade de oportunidades e combate à discriminação;
VI. Consentimento expresso e destacado do titular, quando aplicável;
VII. Cumprimento de determinação legal ou de autoridade competente.

Sempre que envolver dados sensíveis, a Câmara aplicará padrões reforçados de segurança e controle de acesso.

## 8. FINALIDADE, ADEQUAÇÃO E NECESSIDADE

O tratamento de dados deve respeitar o princípio da:

I. Finalidade: só pode ocorrer para propósitos legítimos, claros e informados previamente ao titular.
II. Adequação: o uso dos dados deve ser compatível com a finalidade declarada no momento da coleta.
III. Necessidade (Minimização): a coleta será limitada ao estritamente necessário para atingir os objetivos propostos. Dados excedentes ou não pertinentes não serão tratados.

## 9. QUALIDADE E ATUALIZAÇÃO DOS DADOS

A Câmara deve adotar medidas razoáveis para assegurar que os dados pessoais sejam exatos, completos e atualizados. O titular poderá solicitar, a qualquer tempo, a correção, complementação ou exclusão de dados incorretos ou desatualizados.

## 10. SEGURANÇA E CONFIDENCIALIDADE

Devem ser aplicadas medidas técnicas e administrativas adequadas para proteger dados pessoais contra:

I. Acesso não autorizado;
II. Perda acidental;
III. Destruição ou modificação indevida;
IV. Divulgação ou uso ilícito.

Entre essas medidas incluem-se:

I. Anonimização: tornar os dados irreversivelmente não vinculáveis a uma pessoa;
II. Pseudonimização: dificultar a associação a um titular, mantendo a possibilidade de reversão em condições controladas.

## 11. RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS

A Câmara deve comprovar a conformidade com a LGPD por meio de:

I. Registros de operações de tratamento;
II. Documentação de incidentes de segurança;
III. Avaliações de impacto à proteção de dados (DPIA), sempre que houver risco elevado;
IV. Verificação periódica de terceiros e parceiros que tratem dados em seu nome;
V. Disponibilização de canais para que os titulares exerçam seus direitos.

O princípio da accountability exige que os responsáveis demonstrem a efetiva aplicação de medidas técnicas e administrativas de proteção de dados, tanto em processos em andamento quanto no desenho de novos projetos, sistemas ou plataformas digitais.

## 12. PRIVACY BY DESIGN E PRIVACY BY DEFAULT

Aplicam-se, simultaneamente, os conceitos abaixo:

I. Desde a concepção (Privacy by design): desde a concepção de processos, serviços ou sistemas, devem ser incorporadas medidas de segurança e privacidade, levando em conta o contexto, o escopo do tratamento, os custos de implementação e o risco aos direitos do titular.
II. Por padrão (Privacy by Default): por padrão, serão tratados apenas os dados pessoais indispensáveis para cada finalidade, limitando extensão, tempo de retenção e acessibilidade.
III. Essas práticas serão periodicamente revisadas para alinhamento às melhores práticas de proteção de dados, podendo incluir certificações, códigos de conduta ou auditorias independentes como evidência de conformidade

## 13.GOVERNANÇA, ATRIBUIÇÕES E CONTROLES

### 13.1. Diretrizes de Conformidade e Escopo Operacional

A Câmara, com apoio do Encarregado (DPO), observará as orientações, normas e guias da ANPD referentes a tratamento e transparência, assegurando aderência contínua à LGPD.

Tratamento de dados pessoais compreende, entre outras, as seguintes operações: pesquisa; coleta por qualquer meio ou sensor; captação e gravação (imagem, áudio, vídeo); identificação; uso; gestão e organização; estruturação; armazenamento (físico e/ou em servidores/infraestrutura), manutenção; comparação; consolidação; perfilamento (profiling); conservação; adaptação e atualização; integração e correção; auditoria/inspeção; extração; consulta; comunicação e compartilhamento; transmissão; divulgação; segregação; eliminação, cancelamento e destruição; pseudonimização, anonimização e criptografia.

#### 13.1.1. Anonimização

Dados submetidos a processos efetivos de anonimização deixam de ser considerados dados pessoais, desde que o procedimento seja irreversível. Caso exista possibilidade técnica razoável de reversão, o dado é tratado como pessoal e sujeito à LGPD. Caberá a elaboração de parecer técnico ou jurídico prévio quando o pedido
envolver eliminação de dados arquivísticos.

13.2. Papéis e Responsabilidades

13.2.1. Encarregado de Dados (DPO)

I. Aprovar esta Política e suas alterações.
II. Orientar as áreas quanto ao uso adequado de dados pessoais e à observância das bases legais.
III. Atuar como canal com titulares e com a ANPD, inclusive em incidentes.
IV. Zelar por registros (ROPA), relatórios (DPIA) e evidências de conformidade.

13.2.2. Setor de Tecnologia (TI)

I. Aplicar medidas de segurança proporcionais ao risco (confidencialidade, integridade e disponibilidade).
II. Monitorar e responder a violações e vazamentos, coletando evidências técnicas.
III. Publicar e manter avisos de privacidade em sites/sistemas e documentação de segurança sob sua competência.
IV. Definir e operacionalizar procedimentos e templates para registro e resposta a incidentes.
V. Avaliar ferramentas e sistemas com foco em minimização de exposição e privacy by design/by default.
VI. Implantar mecanismos para exercício de direitos dos titulares (atendimento, prazos e trilhas de auditoria).
VII. Atender às solicitações encaminhadas para o e-mail [indicar email], cabendo a criação de protocolo interno padronizado (numeração de pedidos, armazenamento de registros e controle de prazos)

13.2.3. Procuradoria

I. Apoiar juridicamente a interpretação da LGPD e regulamentos conexos.
II. Revisar contratos que envolvam cessão/compartilhamento/tratamento de dados, com cláusulas de privacidade adequadas.
III. Atuar em incidentes, inclusive na comunicação a autoridades quando aplicável.
IV. Apoiar renegociações com fornecedores e parceiros que tratem dados.
V. Apoiar a interface com a ANPD e demais autoridades competentes.

13.2.4. Todos os Integrantes da Câmara

I. Usar dados pessoais apenas para finalidades autorizadas e compatíveis com suas atividades.
II. Cumprir esta Política, normas complementares e treinamentos periódicos.
III. Reportar prontamente ao DPO quaisquer incidentes, vulnerabilidades ou riscos de privacidade identificados.

13.3. Aviso de Privacidade (Momento, Conteúdo e Forma)

13.3.1. Momento de Fornecimento

I. O aviso deve ser disponibilizado: No ato da coleta dos dados pessoais; ou
II. Em prazo razoável, não superior a 30 dias úteis a partir da coleta, na primeira comunicação com o titular.

13.3.2. Conteúdo Mínimo

O Aviso de Privacidade conterá, no mínimo:

I. Identificação e contato do Controlador e do DPO;
II. Finalidades e base(s) legal(is) do tratamento;

III. Fonte dos dados (quando aplicável);
IV. Categorias de destinatários e hipóteses de compartilhamento;
V. Transferências internacionais (país/organização e fundamento de transferência);
VI. Responsabilidades de Controlador e Operador(es);
VII. Prazos de retenção;
VIII. Uso de decisões automatizadas e lógica envolvida, quando houver;
IX. Direitos dos titulares e meios de exercício (canais, prazos e requisitos).

13.3.3. Forma e Acessibilidade

O aviso será conciso, claro e acessível, em linguagem simples e adequada a públicos diversos (ex.: crianças, pessoas com deficiência), preferencialmente em formato eletrônico e com estrutura progressiva (camadas), conforme boas práticas.

13.4. Registros das Operações de Tratamento (ROPA)

13.4.1. Diretrizes Gerais

Controlador e Operador devem manter registros atualizados das operações de tratamento. Recomenda-se plataforma eletrônica integrada para refletir o mapeamento dinâmico do ciclo de vida (coleta → uso → compartilhamento → retenção → descarte), incluindo infraestruturas digitais, softwares e aplicativos envolvidos.

13.4.2. Conteúdo Mínimo — Controlador
I. Nome e contato do Controlador, Controladores Conjuntos (se houver), representante legal e DPO;
II. Finalidades do tratamento;
III. Categorias de titulares e de dados pessoais;
IV. Categorias de destinatários (incluindo terceiros países/organizações internacionais);
V. Transferências internacionais (identificação do país/organização e fundamento);
VI. Prazos de retenção por categoria de dado;
VII. Descrição geral das medidas de segurança (art. 46, LGPD), sempre que possível.

13.4.3. Conteúdo Mínimo — Operador
I. Nome e contato do(s) Operador(es) e de cada Controlador em cujo nome atua;
II. Categorias de operações realizadas para cada Controlador;
III. Transferências internacionais (quando houver) com identificação do destino;
IV. Descrição geral das medidas de segurança adotadas (art. 46, LGPD), quando aplicável.

13.5. Relatório de Impacto à Proteção de Dados (RIPD)

13.5.1. Finalidade e Estrutura

O RIPD descreve processos de tratamento que podem gerar riscos a direitos e liberdades, indicando medidas, salvaguardas e mecanismos de mitigação. Sempre que houver risco elevado, o RIPD será elaborado antes do início do tratamento ou quando houver mudanças relevantes no processo/sistema.

Elementos mínimos:

I. Descrição do projeto ou processo e suas finalidades;
II. Necessidade e proporcionalidade (minimização, retenção, acesso, compartilhamentos);
III. Avaliação de riscos aos direitos e liberdades;
IV. Medidas de mitigação (técnicas e organizacionais), responsáveis e prazos;
V. Consulta ao DPO e, quando cabível, consulta prévia à ANPD.

13.6. Avaliação de Risco — Critérios e Recomendações

13.6.1. Conceito

Risco é a probabilidade de ocorrência combinada com a gravidade do impacto negativo aos direitos e liberdades do titular (dano físico, material ou imaterial).

13.6.2. Exemplos de Situações de Alto Risco

I. Discriminação ou tratamento desigual;
II. Roubo/fraude de identidade;
III. Perdas financeiras e danos reputacionais;
IV. Quebra de sigilo profissional ou reversão indevida de pseudonimização;
V. Perda de controle pelo titular sobre seus dados;
VI. Tratamento de dados sensíveis (origem racial/étnica, convicções, filiação sindical, saúde, genética/biometria, vida sexual, orientação sexual);
VII. Dados relativos a condenações/infrações penais;
VIII. Avaliação de aspectos pessoais (perfilamento) para prever desempenho no trabalho, situação econômica, saúde, preferências, confiabilidade, comportamento, localização ou deslocamentos;
IX. Tratamento envolvendo pessoas em condição de vulnerabilidade (crianças e adolescentes);
X. Operações com grande volume de dados e/ou amplo número de titulares afetados.

13.6.3. Metodologia de Classificação

A probabilidade e a gravidade devem considerar natureza, escopo, contexto e finalidade do tratamento, culminando em classificação Baixo / Médio / Alto risco e plano de tratamento correspondente (evitar, reduzir, transferir, aceitar), com responsáveis, prazos e indicadores.

13.7. Privacy by Design e Privacy by Default (integração prática)

I. By Design: incorporar privacidade e segurança desde a concepção de processos, bases de dados, aplicações e fluxos (ex.: minimização, controle de acesso, logs, segregação de ambientes, testes de impacto).
II. By Default: por padrão, coletar e reter apenas o necessário, limitar acesso “need-to-know”, controlar prazos de retenção e desindexar/eliminar ao fim da finalidade.
III. Evidências de conformidade: registros, auditorias, códigos de conduta, certificações e testes periódicos.

13.8. Disposições Finais (Operacionalização)

I. Esta seção integra a matriz de governança de dados da Câmara e deve ser lida em conjunto com: Política de Segurança da Informação, Plano de Resposta a Incidentes, Padrões de Retenção e Eliminação, Gestão de Acessos e Treinamento.

II. Adoção de revisões periódicas (mínimo anual ou quando houver mudança relevante em tecnologia, processo, base legal ou risco).
III. Qualquer dúvida deverá ser encaminhada ao DPO, que poderá propor ajustes imediatos em caso de risco relevante.

## 14. DIRETRIZES PARA IMPLEMENTAÇÃO E DEMONSTRAÇÃO DE CONFORMIDADE

14.1 Princípios gerais

O Controlador e o Operador devem implementar medidas técnicas e organizacionais apropriadas e demonstrar conformidade com a LGPD, considerando a origem, natureza, probabilidade e gravidade dos riscos aos direitos dos titulares. Essa demonstração pode ser feita por meio de:

I. Códigos de conduta aprovados;
II. Mecanismos de certificação reconhecidos;
III. Diretrizes internas emitidas pelo DPO;
IV. Observância de boas práticas e recomendações da ANPD.

14.2 Direitos e liberdades afetados

Conforme orientação internacional (ex.: antigo WP29), os riscos devem ser avaliados à luz, sobretudo, dos direitos à:

I. Proteção de dados e vida privada;
II. Liberdade de expressão, pensamento e religião;
III. Liberdade de locomoção;
IV. Não discriminação.

14.3 Orientações do DPO

O DPO pode identificar operações de baixo risco e recomendar medidas mitigadoras proporcionais, bem como priorizar iniciativas de melhoria contínua.

## 15. AVALIAÇÃO DE IMPACTO (RIPD): NECESSIDADE, CONTEÚDO E GESTÃO DE RISCO

15.1 Quando realizar RIPD

Embora a LGPD não traga hipóteses taxativas, a ANPD pode determiná-lo. Para esta Política, adota-se referência a critérios internacionalmente aceitos (ex.: parecer WP29/2017). Realize RIPD sempre que o tratamento puder apresentar alto risco aos titulares, especialmente quando houver:

I. Avaliação/valoração/pontuação de pessoas;
II. Decisões automatizadas com efeitos jurídicos ou semelhantes (p. ex., seleção, concessão de crédito/benefício);
III. Perfilamento (profiling) e predição, notadamente sobre desempenho, situação econômica, saúde, preferências, confiabilidade, comportamento, localização/deslocamentos;
IV. Monitoramento sistemático em larga escala em áreas acessíveis ao público;
V. Tratamento de dados sensíveis (art. 11 da LGPD) e/ou dados criminais;
VI. Combinação/fusão de bases de múltiplas fontes para novas finalidades;
VII. Grande escala (volume elevado de dados e/ou de titulares);

VIII. Públicos vulneráveis (crianças e adolescentes) ou desequilíbrio de poder (ex.: relação de emprego);
IX. IoT, biometria, analítica preditiva, data lake/big data, ou uso intensivo de nuvem;
X. Restrição de direitos/serviços ao titular em razão do tratamento.

15.2 Quando o RIPD pode não ser exigido

Na ausência de risco elevado, e salvo determinação da ANPD ou do DPO, o RIPD pode não ser obrigatório. Em qualquer cenário, Controlador e Operador devem manter registros (ROPA) capazes de sustentar a decisão e permitir a elaboração posterior, se necessário.

15.3 Conteúdo mínimo do RIPD

O RIPD deve documentar:
I. Contexto e ciclo de vida do tratamento (coleta, classificação, uso, compartilhamentos, retenção e descarte);
II. Tipos de dados e categorias de titulares;
III. Finalidades e bases legais;
IV. Necessidade e proporcionalidade (minimização, retenção, acesso, transferência internacional);
V. Avaliação de riscos aos direitos e liberdades (probabilidade × gravidade);
VI. Medidas de mitigação (técnicas/organizacionais), responsáveis e prazos;
VII. Parecer do DPO (quando aplicável) e eventual consulta à ANPD.

15.4 Gestão de risco (metodologia)
I. Identificar ameaças e riscos;
II. Mensurar impacto e probabilidade (classificação: baixo/médio/alto);
III. Definir tratamento do risco (evitar, reduzir, transferir, aceitar) com planos de ação, indicadores e prazos;
IV. Evidenciar salvaguardas (ex.: controle de acesso, criptografia, anonimização/pseudonimização, trilhas de auditoria, testes).

## 16. ENCARREGADO (DPO): PAPEL E ATRIBUIÇÕES

16.1 Nomeação e perfil

O DPO será designado com base em experiência em privacidade, conhecimento normativo e capacidade de exercer as funções com independência.

16.2 Responsabilidades-chave
I. Canal com titulares e ANPD;
II. Orientar Controlador/Operador e áreas de negócio;
III. Projetar e monitorar programas de conformidade (governança, avisos-padrão, cláusulas contratuais, treinamentos);
IV. Apoiar contratos com operadores/terceiros (cláusulas LGPD, SCCs quando cabíveis);
V. Definir/validar metodologia de DPIA e acompanhar sua execução;
VI. Receber e tratar reclamações/comunicações de titulares;
VII. Cooperar com a ANPD, inclusive em incidentes.
VIII.

## 17. PAPÉIS DE CONTROLADOR(A) E OPERADOR(A)

17.1 Controlador

I. Define finalidades e meios do tratamento;
II. Implementa medidas técnicas e organizacionais e prova a conformidade;
III. Designa pessoas autorizadas ao tratamento e organiza governança interna;
IV. Planeja privacy by design/default e provê recursos anuais para proteção de dados;
V. Audita terceiros, promove treinamento contínuo e coopera com a ANPD;
VI. Apoia e é apoiado pelo DPO.

17.2 Operador (regido por contrato/ato jurídico com o Controlador). Deve, no mínimo:

I. Seguir instruções documentadas do Controlador (incluindo sobre transferências);
II. Assegurar confidencialidade das pessoas autorizadas;
III. Adotar medidas de segurança (art. 46, LGPD) e respeitar regras de subcontratação;
IV. Auxiliar o Controlador no atendimento aos direitos dos titulares e obrigações de segurança (notificação de incidentes, RIPD, etc.), conforme a natureza do tratamento;
V. Devolver/eliminar dados ao término do serviço, salvo obrigação legal de retenção;
VI. Disponibilizar evidências de conformidade e permitir auditorias;
VII. Responder por suboperadores, salvo prova inequívoca de ausência de culpa.

Observação: Autoridades públicas que recebam dados em investigações específicas não são Operadores; devem observar a legislação aplicável de proteção de dados e devido processo.

## 18. MEDIDAS DE SEGURANÇA (ART. 46, LGPD)

18.1 Princípios e critérios

Controlador e Operador devem aplicar medidas proporcionais ao estado da arte, custos, natureza/escopo/finalidade do tratamento e risco aos titulares, incluindo:

I. Privacy by design e by default;
II. Gestão de acessos (mínimo privilégio, MFA, segregação de funções);
III. Criptografia, anonimização e pseudonimização;
IV. Resiliência (backup, continuidade, recuperação de desastre);
V. Logs e trilhas de auditoria, testes e avaliações periódicas de eficácia;
VI. Qualidade de dados (exatidão, atualização) e limitação de retenção.

18.2 Evidências e conformidade

Aderir a códigos de conduta ou certificações aprovadas pode evidenciar conformidade. Qualquer pessoa sob autoridade do Controlador/Operador só deve tratar dados sob instrução do Controlador, salvo exigência legal diversa.

## 19. TRANSFERÊNCIA INTERNACIONAL DE DADO

19.1 Fundamentos

A LGPD admite transferências internacionais quando:

I. Decisão de adequação da ANPD; ou
II. Garantias contratuais adequadas (ex.: cláusulas contratuais padrão – SCCs),

regras corporativas globais, códigos de conduta ou certificações; ou

III. Exceções (ex.: obrigação legal, interesse público, defesa de direitos, consentimento específico, entre outras hipóteses legais).

19.2 Deveres adicionais

Antes da transferência, o Controlador/Operador deve:

I. Avaliar impacto técnico e organizacional do destinatário (RIPD de transferência quando aplicável);
II. Firmar contrato de proteção de dados com nível de garantia equivalente ao da LGPD;
III. Permitir auditoria independente do destinatário, quando pertinente.
IV. Transferências a autoridades estrangeiras devem observar acordos de cooperação (ex.: assistência judiciária mútua) ou instrumentos adequados.

## 20. GESTÃO DE INCIDENTES DE SEGURANÇA DE DADOS

20.1 Princípios

Medidas preventivas reduzem a probabilidade de incidentes. Ocorrido o evento, aplica-se o fluxo abaixo, detalhado em política específica:

I. Detecção – mecanismos para identificar incidentes e registrar alertas;
II. Avaliação – Comitê de Incidentes, coordenado pelo DPO, qualifica o evento, avalia riscos a direitos e define ações imediatas;
III. Comunicação – se configurada violação de dados, notificar ANPD e titulares em prazo razoável (nunca superior a 72 horas e sem atraso injustificado), sempre que houver risco ou dano relevante;
IV. Monitoramento e resposta – acompanhar mitigação até a solução;
V. Registro – documentar todo incidente (incluindo os não notificáveis), impactos e providências em repositório próprio do Controlador.

20.2 Treinamento e integração

A política de incidentes deve ser alinhada às demais normas internas (segurança da informação, continuidade, gestão de mudanças). Gestores são responsáveis por treinar e conscientizar colaboradores e terceiros.

## 21. DIREITOS DOS TITULARES

21.1 Princípios gerais

O Controlador deve assegurar que o exercício dos direitos previstos na LGPD esteja no centro das operações de tratamento. O direito à privacidade deve ser interpretado em harmonia com outros direitos fundamentais, à luz do princípio da proporcionalidade.

Todos os pedidos devem ser tratados de forma gratuita, clara e tempestiva, cabendo ao Controlador demonstrar se eventual solicitação for manifestamente excessiva ou infundada.

21.2 Procedimentos e prazos

I. Resposta simplificada: imediata, confirmando existência ou não de tratamento.
II. Resposta completa: até 15 dias corridos a partir da solicitação, contendo: origem dos dados, finalidade, critérios utilizados, inexistência de registro, observância de segredos comercial e industrial.
III. Formato: escrito ou eletrônico, a critério do titular, em linguagem acessível e gratuita.

21.3 Direitos garantidos

I. Confirmação e Acesso: O titular pode confirmar se há tratamento em curso e obter cópia integral dos dados pessoais, em meio eletrônico seguro ou em formato impresso.
II. Correção: O titular pode solicitar a retificação de dados incompletos, inexatos ou desatualizados.
III. Revogação do Consentimento: Pode ser exercida a qualquer momento, por meio simples, gratuito e acessível, produzindo efeitos prospectivos.
IV. Eliminação de Dados: O titular pode requerer a exclusão dos dados tratados com base em consentimento, observados:
    A. limites legais e regulatórios de retenção;
    B. custos e tecnologias disponíveis;
    C. obrigação de deletar cópias, links ou reproduções.
    D. tratamentos de dados já realizados;
V. Retenção e prazos: Quando previsto em lei, o período de armazenamento deve ser respeitado.
VI. Se houver retenção maior que a legal, o Controlador deve justificar no ROPA (Registro das Operações de Tratamento).
VII. Na ausência de previsão legal, o prazo deve observar os princípios de necessidade, adequação e responsabilização.
VIII. Notificação sobre incidentes, no caso de incidentes de segurança que possa gerar dano ou risco relevante.

## 22. AUTORIDADES, RESPONSABILIDADES E SANÇÕES

22.1 Canais de reclamação

O titular poderá recorrer:

I. À ANPD, se verificar violação à LGPD;
II. Ao Judiciário, para reparação de danos;
III. A órgãos de defesa do consumidor (ex.: MP, Senacon, Procons), se houver infração a normas consumeristas;
IV. Ao próprio Controlador/Operador, por meio dos canais internos disponibilizados.

22.2 Responsabilidade civil

I. Controlador e Operador respondem solidariamente por danos patrimoniais, morais, individuais ou coletivos decorrentes de tratamento ilícito.
II. O Operador responde solidariamente quando:
    A. descumprir a LGPD; ou
    B. agir fora das instruções lícitas do Controlador.
III. Excludentes de responsabilidade (art. 43, LGPD):
    A. quando provarem que não realizaram o tratamento;
    B. quando não houve violação da LGPD;

C. ou se o dano decorrer exclusivamente do titular ou de terceiro.

IV. Caberá ao Controlador garantir o Registro do Atendimento e o seu armazenamento em ambiente seguro, com controle de acesso e política de retenção definida.

V. O descumprimento ensejará a aplicação da Lei nº 8.112/1990 e do art. 52 da LGPD, que trata das sanções administrativas aplicáveis também ao setor público.

22.3 Sanções administrativas (art. 52, LGPD e Resolução CD/ANPD nº 4/2023)

As sanções são aplicadas após devido processo administrativo, com direito ao contraditório e ampla defesa, e podem ser:

I. Advertência, com prazo para correção;
II. Multa simples (até 2% do faturamento, limitada a R$ 50 milhões por infração);
III. Multa diária (observado o limite acima);
IV. Publicização da infração;
V. Bloqueio dos dados até regularização;
VI. Eliminação dos dados;
VII. Suspensão parcial do banco de dados por até 6 meses, prorrogável por igual período;
VIII. Suspensão da atividade de tratamento por até 6 meses, prorrogável por igual período;
IX. Proibição parcial ou total das atividades relacionadas ao tratamento.

22.4 Critérios para dosimetria da sanção

Na fixação da penalidade, a ANPD deve considerar:

I. Gravidade e natureza da infração;
II. Direitos pessoais afetados;
III. Boa-fé do infrator;
IV. Vantagem auferida;
V. Capacidade econômica;
VI. Reincidência;
VII. Extensão do dano;
VIII. Cooperação do infrator;
IX. Existência de políticas de boas práticas e governança;
X. Pronta adoção de medidas corretivas;
XI. Proporcionalidade entre a gravidade da falta e a intensidade da sanção.

## 23. ATUALIZAÇÃO DESTA POLÍTICA

A presente Política entra em vigor na data de sua publicação interna e será submetida a revisão anual ou sempre que houver alteração legislativa relevante.