GUIA DE BOAS PRÁTICAS EM

LEI GERAL DE PROTEÇÃO DE DADOS

Ouvidoria Geral do Sistema de Segurança Pública

Secretaria de Segurança Pública

AMAZONAS
GOVERNO DO ESTADO
TRABALHO QUE TRANSFORMA

Sumário

Governador do Estado
Wilson Miranda Lima

Secretário de Estado de Segurança Pública
Cel. Marcus Vinícius Oliveira de Almeida

Secretário Executivo de Segurança Pública
Cel. QOPM Anézio Brito de Paiva

Secretário Executivo Adjunto de Operação – SEAOP
Cel. QOPM Algenor Maria da Costa Teixeira Filho

Secretário Executivo Adjunto de Planejamento e Gestão Integrada de Segurança – SEAGI
Cel. QOPM José Almir Cavalcante Rodrigues

Secretário Executivo Adjunto de Inteligência – SEAI
José Divanilson Cavalcanti Júnior

Corregedor-Geral do Sistema de Segurança Pública
Cel. QOPM Franciney Machado Bó

Diretora do Departamento de Polícia Técnico Científica-DPTC
Sanmya Beatriz Tiradentes Leite

Ouvidor-Geral do Sistema de Segurança Pública
Sérgio Augusto Costa da Silva

Apresentação

A adequação da Secretaria de Segurança Pública do Estado do Amazonas, à Lei Geral de Proteção de Dados está diretamente relacionada a uma transformação cultural da instituição, de modo que sejam atingidos todos os níveis, desde o estratégico até o operacional.

Essa mudança cultural envolve: (i) refletir sobre a privacidade dos dados pessoais do cidadão em todas as fases que envolvem o tratamento; e (ii) desenvolver ações de conscientização dos servidores, no sentido de incorporar o respeito à privacidade e proteção dos dados pessoais nas atividades institucionais cotidianas.

Neste contexto, este material tem por escopo prestar orientações sobre boas práticas para o adequado tratamento de dados pessoais em situações rotineiras do ambiente de trabalho, em especial ao que se refere a segurança da informação.

1. DIREITOS DO TITULAR

A Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) dispõe sobre o tratamento de dados pessoais e tem como objetivo proteger os diretos de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

O direito à proteção dos dados pessoais passou a ser um Direito Fundamental (art. 5º, LXXIX), por meio da Emenda Constitucional nº 115/2022.

O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de finalidade específica do tratamento; forma e duração do tratamento, observados os segredos comercial e industrial; identificação do controlador; informações de contato do controlador; informações acerca do uso compartilhado de dados pelo controlador e a finalidade; e responsabilidades dos agentes que realizarão o tratamento.

Além daqueles elencados no art. 18 da LGPD, quais são:

• Confirmação da existência de tratamento;
Acesso aos dados;
• Correção de dados incompletos, inexatos ou desatualizados; anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;
• Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial;
• Eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;
• Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
• Informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; e
• Revogação do consentimento.

2. PRINCÍPIOS

Além da boa-fé, a LGPD estabelece a observância de 10 (dez) princípios para o tratamento de dados pessoais, dentre os quais importa destacar:

Além da boa-fé, a LGPD estabelece a observância de 10 (dez) princípios para o tratamento de dados pessoais, dentre os quais importa destacar:

- **Finalidade:** realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
- **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
- **Necessidade:** limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
- **Livre Acesso:** garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
- **Transparência:** garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.

3. DADOS PESSOAIS

Dado Pessoal: é toda e qualquer informação que torna possível a identificação, ainda que indireta de um indivíduo, tais como RG, CPF ou qualquer documento de identificação, inclusive fotografias, cartão bancário, endereço de IP e cookies.

Dado Pessoal Sensível: é aquele que tem vínculo com características pessoais do indivíduo e podem acarretar alguma prática discriminatória, como a origem racial, étnica, escolha religiosa, opinião política e orientação sexual.

A Autoridade Nacional de Proteção de Dados (ANPD), bem como o Ministério Público poderá determinar ao controlador que elabore relatório de impacto à proteção de dados, contendo a descrição detalhada dos tipos de dados coletados, a metodologia que é utilizada para garantir a segurança dos dados e informações e também sobre os mecanismos utilizados para a mitigação dos riscos adotados.

4. BOAS PRÁTICAS PARA TRATAR DADOS PESSOAIS

O tratamento de dados pessoais deve ser realizado de forma cautelosa, obedecidas as diretrizes estabelecidas na Lei Geral de Proteção de Dados.

Assim, o servidor público deverá estar sempre vigilante às boas práticas relativas ao tratamento, sejam eles dos usuários dos serviços públicos, bem como dos próprios servidores. O inadequado tratamento de dados pode acarretar responsabilização de agentes públicos, além de sanções administrativas, civis e penais.

Portanto, é importante estar atento aos princípios da necessidade, finalidade e adequação, coletando e tratando os dados estritamente necessários para alcançar o escopo pretendido de forma apropriada.

4.1. SENHAS

Regra geral, as senhas de acesso a sistemas e e-mails institucionais são sigilosas, pessoais e intransferíveis e só poderão ser utilizadas pelo usuário cadastrado.

Portanto, em caso de compartilhamento da mesma, não poderá ser feita a alegação de uso indevido.

Independente da senha ter sido criada pelo seu titular ou pelo órgão ou entidade, que detém a propriedade ou o controle total sobre os sistemas nos quais será utilizada, continua sendo de domínio exclusivo de seu titular, ou seja, a pessoa natural que ela visa proteger.

4.2. USO DE COMPUTADORES

Para evitar incidentes de segurança, tais como acesso indevido e/ou vazamento de dados, é imprescindível que o servidor público, quando se ausentar da sua estação de trabalho, utilize o recurso de bloqueio de tela.

Ademais, a realização de prints, fotos ou vídeos de telas do computador que contenham dados pessoais expostos e o encaminhamento por meio de canais de comunicação não oficiais é temerário, devendo observar as regras contidas nas Políticas de Segurança da Informação de cada órgão ou entidade.

4.3. USO DE IMPRESSORAS

A impressão de documentos contendo dados pessoais também requer cuidados, tais como:

- Retirá-los da impressora com brevidade;
- Armazená-los em locais seguros; e
- No caso de descarte, os dados pessoais deverão ser descaracterizados e o documento triturado.

4.4. SUGESTÕES PARA PROTEÇÃO DE DADOS

Abaixo diretrizes e práticas que os servidores devem seguir para proteger a privacidade dos dados sob guarda da SSP/AM:

• Manter senhas seguras e não as compartilhar: Os servidores devem criar senhas fortes, contendo uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Além disso, eles devem evitar compartilhar suas senhas com outras pessoas ou anotá-las em locais facilmente acessíveis.

• Utilizar apenas sistemas autorizados para acessar informações confidenciais: Os servidores devem utilizar apenas os sistemas e aplicativos autorizados para acessar informações confidenciais. O acesso não deve ser feito através de dispositivos pessoais ou não autorizados.

• Garantir a devida proteção física e digital dos dados de Segurança Pública: Os servidores devem proteger adequadamente os dados tanto em formato físico quanto digital. Isso envolve manter os arquivos físicos trancados em armários seguros quando não estiverem em uso, evitar deixar dispositivos eletrônicos desbloqueados e proteger os computadores com senhas e softwares de segurança atualizados.

• Comunicar imediatamente qualquer incidente de segurança ou violação de privacidade: Caso um servidores identifique ou suspeite de uma violação de privacidade dos pacientes, deve comunicar à equipe responsável pela segurança da informação ou à pessoa designada. A notificação precoce é essencial para adotar as medidas necessárias e mitigar os danos.

• Participar de treinamentos regulares sobre segurança e privacidade: Os servidores devem participar de treinamentos regulares sobre segurança da informação e privacidade. Isso ajuda a manter-se atualizado sobre as melhores práticas, ameaças atuais e mudanças nas políticas e regulamentações relacionadas à proteção de dados.

• Limitar o acesso às informações confidenciais: Os servidores devem ter acesso somente às informações necessárias para realizar suas funções. O acesso deve ser estritamente limitado às informações que são relevantes para o desempenho de suas tarefas e devem evitar acessar ou divulgar informações desnecessárias.

• Criptografar informações confidenciais durante a transmissão: Sempre que informações confidenciais precisarem ser transmitidas eletronicamente, os servidores devem garantir que elas sejam criptografadas para proteger a privacidade dos pacientes durante o trânsito.

• Compartilhamento seguro de informações: Ao compartilhar informações sensíveis por e-mail ou por meio de outros meios eletrônicos, verifique se você está usando métodos seguros, como criptografia ou sistemas seguros de compartilhamento de arquivos.

Dicas para o descarte adequado:

• Ao descartar informações em papel ou dispositivos eletrônicos, certifique-se de fazer isso de forma segura.
• Utilize trituradoras de papel para documentos físicos e utilize softwares especializados para garantir a exclusão segura de dados em dispositivos eletrônicos.
• Folhas com informações de usuários ou de servidores não podem ser jogadas em lixo comum, devem ser trituradas ou incineradas!
• Sempre que possível disponibilizar um lixo lacrado no setor para colocação deste tipo de conteúdo.
• Esteja atento aos sinais de engenharia social: Esteja ciente de tentativas de manipulação, como e-mails ou ligações suspeitas solicitando informações pessoais ou confidenciais de titulares. Além disso, fique alerta para mensagens de phishing que possam tentar enganá-lo para divulgar informações sensíveis ou clicar em links maliciosos, tanto por e-mail, aplicativo de mensagens ou SMS.
• Essas diretrizes e boas práticas visam promover uma cultura de segurança e privacidade dos dados, protegendo a confidencialidade e a privacidade dos pacientes.
• Não deixe notas com login e senha ou com informações que possam facilitar o acesso de terceiros em seu equipamento. Mantenha guardado documentos físicos com informações sigilosas e confidenciais.

Atenção aos comportamentos incomuns

• Verifique se há sinais de manipulação ou invasão em dispositivos, como computadores ou dispositivos móveis.
• Atente-se às atividades e comportamentos incomuns em seu ambiente de trabalho, como tentativas repetidas de acesso não autorizado, solicitações de informações confidenciais por parte de terceiros desconhecidos ou comportamentos que violem as políticas de segurança.

Ao aderir às diretrizes e boas práticas descritas neste manual, os servidores desempenham um papel fundamental na salvaguarda das informações confidenciais e na manutenção da confiança dos usuários de serviço público.

É essencial que todos estejam cientes dos riscos associados a violações de privacidade e se sintam capacitados para tomar ações apropriadas para prevenir incidentes de segurança.

5. RECURSOS TECNOLÓGICOS OFICIAIS DOS DIAGNÓSTICOS

A fim de mitigar riscos referentes a incidentes de segurança, é fundamental que o servidor público utilize para o exercício de suas atividades laborativas apenas softwares e hardwares previamente homologados ou autorizados pelo órgão ou entidade.

A gestão (instalação, manutenção e configuração) dos recursos tecnológicos disponibilizados é de responsabilidade exclusiva do órgão ou entidade.

6. LAI & LGPD

Dúvida constante é quanto a eventual confronto entre a LGPD e a Lei nº 12.527/2011 - Lei de Acesso à Informação (LAI). Este fato não ocorre, visto que a LGPD irá coexistir com as outras regulamentações existentes, tal como a LAI, garantindo aos cidadãos a transparência, mediante o acesso a dados públicos.

Portanto, temos, de um lado, o dever de publicização dos atos e ações como medida de transparência e controle de sua atuação; e, de outro, o dever de proteção dos dados dos titulares.

Assim, deverá haver concordância entre a LAI e a LGPD, no sentido de que as regras de transparência não ocasionem lesão a direitos e interesses de terceiros.

Com o objetivo de orientar a adequação das organizações às novas regras, a LGPD estabeleceu princípios norteadores no tratamento de dados, tais como: finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (art. 6° da LGPD).

Dessa forma, no tratamento de dados no âmbito do Poder Público, é importante ressaltar a relevância da avaliação e aplicação de critérios como finalidade, adequação, necessidade, segurança, prestação de contas e prevenção.

Assim, os entes públicos deverão coletar apenas os dados minimamente necessários para o alcance de suas finalidades, com o conhecimento de seu titular e de forma consentida, exceto nas hipóteses previstas em Lei (art. 7º da Lei nº 13.709/2018), mas sempre observando a proteção de dados.

Importante ainda destacar que o tratamento de informações deve ser realizado para fins específicos, explícitos e informados ao titular. Portanto, se modificada a finalidade, o titular deverá ser comunicado.

No caso, a preocupação é quanto a uma suposta transgressão das regras que determinam a proteção de dados pessoais quando da publicação destes.

Em síntese, a proteção aos dados do particular não é absoluta, mesmo tendo em conta o artigo 5º, inciso II, da Constituição Federal, e a Lei nº 13.709/2018, visto que o acesso, tratamento e divulgação destes são permitidos quando de algum modo guardem contato com a Administração Pública, conforme a Lei nº 12.527 de 2011.

Quanto a questão da divulgação de dados de servidores, os tribunais já se manifestaram no sentido de autorizar a publicidade dos dados. O STF , em decisão unânime, proferida em abril de 2011, concluiu que "a pessoa que decide ingressar no serviço público adere ao regime jurídico próprio da Administração pública, que prevê a publicidade de todas as informações de interesse da coletividade".

Ainda neste contexto, os números cadastrais de documentos como RG, CPF e cadastros profissionais (OAB, CRM ou CREA), mesmo que sejam dados pessoais, são necessários à exata identificação dos indivíduos que integram a Administração Pública, com ela contratando, celebrando convênios, ou, ainda, se beneficiando individualmente e voluntariamente de atos administrativos. Desta forma, fica assegurada a transparência pública.

Além do exposto, tal procedimento estaria fundamentado nos arts. 7º e 23 da LGPD, bem como no art. 6º da LAI.

Assim, observa-se a relativização do direito à privacidade frente ao dever de publicidade do poder estatal. Nesses casos, a LGPD se propõe a permitir o exercício do controle sobre a própria Administração, reduzindo assim a esfera de intimidade dos agentes públicos em geral e permitindo que o poder público adentre na esfera pessoal para exercer suas competências.

Deste modo, na geração de processos e documentos, poderá ser aplicada a descaracterização de parte dos números documentos de identificação, a fim de evitar seu uso indevido por terceiros. Essa medida prudente e razoável, observaria o dever de transparência em matéria de gestão pública e ao mesmo tempo, o dever de proteção à privacidade e segurança dos titulares dos dados.

Quanto aos procedimentos pertinentes a descaracterização, fica a cargo dos órgãos e entidades, considerando se tratar de matéria administrativa, efetuarem as adaptações necessárias para a proteção de dados pessoais, considerando as respectivas particularidades. Orienta-se ainda a configuração apropriada do nível de acesso às informações pessoais, podendo ser público, restrito ou sigiloso, conforme as hipóteses do art. 31 da Lei de Acesso à Informação.

No que se refere aos pedidos de acesso à informação envolvendo dados pessoais, o Enunciado CGU nº 04, de 10 de março de 2022, estabelece que: "Nos pedidos de acesso à informação e respectivo recursos, as decisões que tratam da publicidade de dados de pessoas naturais devem ser fundamentadas nos arts. 3º e 31 da Lei nº 12.527/2011 (Lei de Acesso à Informação - LAI), vez que: A LAI, por ser mais específica, é a norma de regência processual e material a ser aplicada no processamento desta espécie de processo administrativo; e A LAI, a Lei nº 14.129/2021 (Lei de Governo Digital) e a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) são sistematicamente compatíveis entre si e harmonizam os direitos fundamentais do acesso à informação, da intimidade e da proteção aos dados pessoais, não havendo antinomia entre seus dispositivos".

7. CANAIS DE CONTATO

Titulares de dados: As manifestações do titular de dados ou seu representante legal serão atendidas eletronicamente, por meio do **Serviço de Informação ao Cidadão – SIC**, (presencial ou eletrônico) junto à Ouvidoria-Geral da Secretaria de Segurança Pública do Restado do Amazonas.

Encarregados de dados pessoais: Os questionamentos aos encarregados de dados, no âmbito da SSP/AM, a respeito da implementação da LGPD que poderão ser realizados através do e-mail: **ouvidoriadeseguranca@ssp.am.gov.br**.

ANEXO I

Participe do **DIAGNÓSTICO ORGANIZACIONAL - LGPD**

Acesse o QR CODE abaixo e colabore com a implementação da **Lei Geral de Proteção de Dados na Secretaria de Segurança Pública do Amazonas**

AMAZONAS
GOVERNO DO ESTADO
TRABALHO QUE TRANSFORMA