ANEXO XIII
NORMA DE PROTEÇÃO DE DADOS PESSOAIS

Normativos relacionados:

Ato normativo	Capítulo / Seção / Artigo
Resolução-GP nº 5/2024	

Versionamento:

Versão:	2.0
Data:	22/04/2024
Criada por:	Grupo de Trabalho Técnico (GTT) do CGSI
Aprovada por:	Comitê de Governança de Segurança da Informação (CGSI)
Aprovada em:	22/04/2024

Histórico de mudanças:

Data	Versão	Alterado por	Descrição das alterações
14/08/2023	1.0		
22/04/2024	2.0	GTT do CGSI	Conforme arquivo de registro de alterações (changelog).

1. INTRODUÇÃO

A Norma de Proteção de Dados Pessoais complementa a Política de Segurança da Informação (PSI) estabelecendo princípios que deverão nortear o tratamento de dados pessoais, físicos e digitais, no âmbito do Poder Judiciário do Estado do Maranhão (PJMA), a fim de garantir a proteção de dados e a privacidade de titulares.

Para fins desta norma aplica-se a lista de termos do glossário com suas respectivas definições, conforme descrito no ANEXO I - Glossário da PSI.

As orientações da Norma de Proteção de Dados Pessoais são baseadas nos princípios da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) e seguem as diretrizes que constam na Resolução-GP nº 05/2024 - TJMA ou posterior que a substitua.

2. OBJETIVO

Assegurar o cumprimento dos requisitos legais, estatutários, regulamentares e contratuais relacionados aos aspectos de segurança da informação e da proteção de dados pessoais.

3. DIRETRIZES

Orientações da Norma de Proteção de Dados Pessoais.

3.1 Princípios de Proteção de Dados Pessoais

Esta seção descreve os princípios que deverão ser observados no tratamento de dados pessoais pelo Poder Judiciário do Estado do Maranhão, atendendo aos padrões de proteção de dados no âmbito institucional.

3.1.1 Legalidade, Transparência e Não Discriminação

O Poder Judiciário do Estado do Maranhão (PJMA) trata os dados pessoais de forma transparente, justa, em conformidade com legislação e regulamentação aplicáveis e sempre vinculado a finalidade do tratamento às hipóteses legais permitidas, abaixo elencadas, sendo obrigatório informar aos(às) titulares dos dados a razão e a forma, pela qual seus dados estarão sendo tratados:

I - mediante o fornecimento de consentimento pelo(a) titular;

II - cumprimento de obrigação legal ou regulatória, ao qual o PJMA está sujeito;

III - para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

IV - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o(a) titular, a pedido do(a) titular dos dados;

V - quando necessário para atender aos interesses legítimos do PJMA ou de terceiro(a), exceto no caso de prevalecerem direitos e liberdades fundamentais do(a) titular que exijam a proteção dos dados pessoais;

VI - para tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

VII - para a proteção da vida ou da incolumidade física do(a) titular ou de terceiro(a);

VIII - para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres.

O consentimento dos(as) titulares para o tratamento de seus dados pessoais deverá ser obtido de forma específica, voluntária, inequívoca e informada.

O PJMA, através das unidades administrativas e/ou judiciais, deverá coletar, armazenar e gerenciar as respostas de consentimento de maneira organizada e acessível, para que sua comprovação possa ser fornecida pelo(a) Encarregado(a), quando necessário.

Para quaisquer hipóteses em que os dados se tornem manifestamente públicos pelo(a) seu(sua) titular será dispensada a exigência de consentimento, ficando resguardados os direitos dos(as) titulares e os princípios previstos na Política Geral de Privacidade e Proteção de Dados Pessoais do PJMA, na legislação e/ou nesta norma.

As atividades de tratamento de dados pessoais deverão observar o princípio da não discriminação, proibindo qualquer forma de tratamento que tenha como finalidade a discriminação ilícita ou abusiva dos(as) titulares dos dados.

O PJMA poderá tratar dados pessoais sensíveis, quais sejam:

I - relacionados à saúde ou à vida sexual;

II - relacionado a dado genético ou biométrico, quando vinculado a uma pessoa natural;

III - que evidenciem a origem racial ou étnica;

IV - referente a convicção religiosa;

V - referente a opinião política;

VI - referente à filiação a sindicato ou a organização de caráter religioso, filosófico ou político.

O tratamento de dados pessoais sensíveis, só poderá ocorrer nos casos específicos descritos abaixo, devendo observar padrões de segurança mais robustos do que aos demais dados:

I - quando o(a) titular ou seu(sua) responsável legal consentir, de forma específica e destacada, para finalidades específicas;

II - sem fornecimento de consentimento do(a) titular, nas hipóteses em que for indispensável para:

a) cumprimento de obrigação legal ou regulatória pelo PJMA;

b) tratamento e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral;

d) proteção da vida ou da incolumidade física do(a) titular ou de terceiro(a);

e) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;

f) garantia da prevenção à fraude e à segurança do(a) titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos previstos do(a) titular em legislação específica, exceto nos casos de prevalecerem direitos e liberdades fundamentais do(a) titular que exijam a proteção dos dados pessoais.

3.1.2 Limitação e Adequação da Finalidade

O tratamento de dados pessoais deverá ser realizado de maneira compatível com a finalidade original para qual os dados foram coletados, ou seja, somente poderão ser utilizados para o propósito para o qual foram solicitados inicialmente, vedando-se a coleta com uma finalidade e utilização para outra sem o consentimento específico do(a) titular, garantindo assim a proteção dos direitos e da privacidade dos(as) titulares.

O tratamento deverá ser limitado ao mínimo necessário para o cumprimento da finalidade específica, não podendo ser excessivo ou desproporcional. Portanto, deverão ser priorizados os modos de tratamento menos invasivos/abusivos à privacidade dos(as) titulares de dados pessoais.

O compartilhamento de dados pessoais com outra área, empresa ou órgão, somente será possível dentro das hipóteses legais.

3.1.3 Princípio da Necessidade (Minimização dos Dados)

O Poder Judiciário do Estado do Maranhão (PJMA) somente poderá tratar dados pessoais, limitando-se 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.

3.1.4 Exatidão (Qualidade dos Dados)

O Poder Judiciário do Estado do Maranhão (PJMA) deverá adotar medidas razoáveis para assegurar que os dados pessoais em sua posse sejam mantidos precisos e atualizados em relação às finalidades para as quais foram coletados. Dessa forma, será disponibilizado ou facilitado ao(à) titular dos dados pessoais canais para requerimento de correção dos dados imprecisos ou desatualizados.

3.1.5 Retenção e Limitação do Armazenamento de Dados

O Poder Judiciário do Estado do Maranhão (PJMA) deverá ter conhecimento de suas atividades de tratamento, períodos de retenção estabelecidos e processos de revisão periódica, não podendo manter os dados pessoais por prazo superior ao necessário para atender as finalidades pretendidas.

A retenção da informação, no que couber, deverá observar os prazos definidos no Plano de Classificação e Tabelas de Temporalidade do PJMA, que constam na Resolução-GP nº 31/2015 - TJMA ou posterior que a substitua.

3.1.6 Livre Acesso, Prevenção e Segurança

As atividades de tratamento de dados pessoais deverão observar:

I - livre acesso: garantia, aos(às) titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a plenitude de seus dados pessoais;

II - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

III - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

Dentre algumas técnicas, no que refere-se às questões de proteção de dados pessoais, poderão ser utilizadas:

I - a anonimização;

II - a pseudonimização.

3.1.7 Responsabilização e Prestação de Contas

O Poder Judiciário do Estado do Maranhão (PJMA) é responsável e deverá demonstrar o cumprimento desta norma, assegurando a implementação de diversas medidas que incluem, mas não se limitam, a:

I - garantia de que os(as) titulares dos dados pessoais poderão exercer os seus direitos;

II - registro de dados pessoais, incluindo:

a) registros de atividades de tratamento de dados pessoais, com a descrição dos propósitos/finalidades, os(as) destinatários(as) do compartilhamento dos dados e os prazos pelos quais o PJMA deverá retê-los;

b) registros de incidentes e violações de dados pessoais.

III - garantia de que os(as) prestadores(as) de serviços terceirizados que sejam operadores(as) de dados pessoais estejam agindo em conformidade com esta norma e com a legislação e regulamentação aplicáveis;

IV - garantia de que o PJMA cumpre as exigências e solicitações de qualquer autoridade de supervisão à qual esteja sujeita.

3.2 Padrões de Segurança

O Poder Judiciário do Estado do Maranhão (PJMA) está comprometido em garantir a segurança da informação e a proteção de dados pessoais, respeitando o direito fundamental do indivíduo à autodeterminação da informação.

Os(As) agentes de tratamento deverão adotar medidas de segurança técnicas e administrativas capazes de proteger os dados pessoais contra acessos não autorizados, assim como contra situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado.

Os(As) usuários(as) deverão observar as boas práticas de proteção de dados a seguir:

I - observar as normas, políticas e orientações aplicáveis adotadas pelo PJMA, ANPD e CNJ;

II - utilizar apenas meios seguros para realizar o tratamento de dados pessoais, reduzindo o risco relacionado à segurança da informação;

III - evitar o tratamento de informações desnecessárias ou em excesso ao estrito cumprimento de sua tarefa (princípio da necessidade);

IV - atentar para e-mails contendo dados pessoais, evitando o envio de informações excessivas e destinando-os apenas às pessoas necessárias;

V - não deixar documentos que contenham dados pessoais expostos na impressora, copiadora ou na mesa de trabalho;

VI - não expor a tela do monitor do computador ao tratar dados pessoais, se não estiver em uso;

VII - certificar-se de que existam salvaguardas contratuais adequadas, caso seja necessário compartilhar dados pessoais com terceiros (pessoas ou organizações);

VIII - não fotografar, filmar ou divulgar documentos que contenham dados pessoais;

IX - assegurar o direito dos(as) titulares de revisarem seus dados e, caso detectem não-conformidades, corrigir ou permitir que o(a) usuário(a) faça os ajustes necessários;

X - armazenar os dados pessoais apenas pelo prazo necessário para a finalidade para a qual foram captados, eliminando-os da forma adequada, após decorrido esse prazo;

XI - explicar com clareza aos(às) titulares a forma de utilização e de tratamento dos dados pessoais.

3.2.1 Garantir a Segurança dos Dados Pessoais

A confidencialidade, integridade e disponibilidade, bem como autenticidade, responsabilidade e não-repúdio, deverão ser observados para a segurança dos dados pessoais tratados pelo PJMA.

A Autoridade Nacional de Proteção de Dados Pessoais (ANPD) poderá solicitar ao Poder Judiciário do Estado do Maranhão (PJMA) a publicação de relatórios de impacto à proteção de dados pessoais e sugerir a adoção de padrões e de boas práticas para os tratamentos de dados pessoais.

3.2.2 Obrigação do Sigilo de Dados Pessoais

Todos(as) os(as) servidores(as), prestadores(as) de serviço, colaboradores(as), terceirizados(as), agentes públicos(as) externos(as) e estagiários(as) com acesso a dados pessoais estarão obrigados(as) aos deveres de manter a confidencialidade dos dados pessoais tratados.

3.2.3 Privacidade de Dados Pessoais por Concepção (privacy by design) e por Padrão (privacy by default)

Ao implementar novos processos, procedimentos ou sistemas que envolvam o tratamento de dados pessoais, o Poder Judiciário do Estado do Maranhão (PJMA) deverá adotar medidas para garantir a aplicação das regras de privacidade e proteção de dados durante todo o ciclo de vida do tratamento (coleta, armazenamento, uso, manutenção e descarte).

3.2.4 Direito dos(as) Titulares de Dados Pessoais

O Poder Judiciário do Estado do Maranhão (PJMA) deverá estar comprometido com os direitos dos(as) titulares de dados pessoais, os quais incluem:

I - confirmação da existência de tratamento de seus dados;

II - o acesso aos dados pessoais que o PJMA detenha sobre eles(as);

III - a correção de seus dados pessoais se estiverem incompletos, inexatos ou desatualizados;

IV - a anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade. Isso poderá incluir, mas não se limita a, circunstâncias em que não é mais necessário que o PJMA retenha seus dados pessoais para os propósitos para os quais foram coletados;

V - a eliminação dos dados pessoais após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades:

a) cumprimento de obrigação legal ou regulatória pelo PJMA;

b) transferência a terceiro(a), desde que respeitados os requisitos de tratamento de dados dispostos na LGPD; ou

c) uso exclusivo do PJMA, vedado seu acesso por terceiro(a), e desde que anonimizados os dados.

VI - informação das entidades públicas e privadas com as quais o PJMA realizou o uso compartilhado de dados;

VII - a revogação do consentimento a qualquer momento, se o tratamento dos dados pessoais se basear no consentimento do indivíduo para um propósito específico;

VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.

3.2.5 Operadores

Os operadores do Poder Judiciário do Estado do Maranhão (PJMA) estarão sujeitos às obrigações estabelecidas pela legislação e regulamentação vigentes de proteção de dados pessoais.

O PJMA deverá garantir que o contrato de prestação de serviços inclua cláusulas de privacidade e proteção de dados, exigindo que o operador implemente medidas de segurança adequadas. Além disso, deverá assegurar controles técnicos e administrativos apropriados para garantir a confidencialidade, a integridade e a segurança dos dados pessoais e especificar no contrato que o operador está autorizado a tratar dados pessoais apenas mediante solicitação formal do PJMA.

Nos casos em que o operador estiver localizado fora do país em que o dado pessoal é tratado, cláusulas contratuais deverão ser incluídas no contrato de proteção de dados pessoais como um anexo para garantir que as devidas salvaguardas exigidas pela legislação e regulamentação aplicáveis de proteção de dados sejam atendidas.

3.2.6 Gerenciamento de Violação de Dados

Os(As) usuários(as) deverão estar cientes de suas responsabilidades pessoais de encaminhar e escalonar possíveis problemas, bem como de denunciar violações ou suspeitas de violações de dados pessoais assim que as identificarem. No momento em que um incidente ou violação real for descoberto, é essencial que os incidentes sejam informados e formalizados de forma tempestiva.

As violações de dados pessoais incluem, mas não se limitam a, qualquer perda, exclusão, roubo ou acesso não autorizado de dados pessoais tratados pelo Poder Judiciário do Estado do Maranhão (PJMA).

O PJMA deverá comunicar à Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e ao(à) próprio(a) titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos(às) titulares.

Quando houver infração à LGPD em decorrência do tratamento de dados pessoais realizados pelo PJMA, a ANPD poderá enviar informe com medidas cabíveis para fazer cessar a violação.

A comunicação à ANPD será realizada em prazo razoável, conforme detalhado no ANEXO VII - Norma de Gestão de Incidentes de Segurança da Informação da Política de Segurança da Informação, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os(as) titulares envolvidos(as);

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, caso a comunicação não seja imediata;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

Na impossibilidade de comunicação individual ao(à) titular de dados pessoais, o PJMA providenciará publicação em mídias de massa, com o propósito de garantir minimamente condições de que os(as) afetados(as) sejam notificados(as) do vazamento.

3.2.7 Auditorias de Proteção de Dados

O Poder Judiciário do Estado do Maranhão (PJMA) deverá garantir que existam revisões periódicas a fim de confirmar que as iniciativas de privacidade, seus sistemas, medidas, processos, precauções e outras atividades incluindo o gerenciamento de proteção de dados pessoais são efetivamente implementados e mantidos e estão em conformidade com a legislação e regulamentação aplicáveis.

4. PAPÉIS E RESPONSABILIDADES

Papéis e responsabilidades no contexto desta norma.

4.1 Comitê Gestor de Proteção de Dados Pessoais

São responsabilidades do Comitê Gestor de Proteção de Dados Pessoais (CGPD):

I - avaliar os mecanismos de tratamento e proteção dos dados existentes e propor políticas, estratégias e metas para a conformidade do PJMA, com as disposições da LGPD;

II - formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação;

III - supervisionar a execução dos planos, dos projetos estratégicos e ações aprovadas para viabilizar a implantação das diretrizes previstas na LGPD;

IV - prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com diretrizes estabelecidas na LGPD e nas normas internas;

V - promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos;

VI - sugerir medidas de transparência do tratamento de dados;

VII - analisar a disponibilização no sítio eletrônico do PJMA de fácil acesso aos(às) usuários(as), informações básicas sobre aplicação da LGPD, incluindo os requisitos para o tratamento legítimo de dados, as obrigações dos controladores de dados e os direitos dos(as) titulares;

VIII - analisar o plano de ação para adequação da LGPD;

IX - apresentar proposta de disponibilização pública dos registros de tratamentos de dados pessoais;

X - orientar os(as) usuários(as) do PJMA, a respeito das práticas a serem tomadas em relação à proteção de dados pessoais.

4.2 Encarregado(a) pelo Tratamento de Dados Pessoais

São responsabilidades do(a) Encarregado(a) pelo tratamento de dados pessoais:

I - aceitar reclamações e comunicações dos(as) titulares de dados pessoais, prestar esclarecimentos e adotar as providências necessárias;

II - receber comunicações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e adotar as providências necessárias;

III - atender outras atribuições determinadas pelo PJMA ou estabelecidas em normas complementares;

IV - apoiar a implementação e a manutenção de práticas de conformidade do PJMA à legislação sobre o tratamento de dados pessoais;

V - identificar e avaliar as principais ameaças à proteção de dados, bem como propor e, quando aprovado, apoiar a implantação de medidas corretivas para mitigação dos riscos;

VI - tomar as ações cabíveis para se fazer cumprir os termos desta norma;

VII - apoiar a gestão das violações de dados pessoais, garantindo tratamento adequado e comunicando, em prazo razoável, a ANPD e os(as) titulares afetados(as) pela violação sempre que esta representar risco ou dano relevante aos(às) titulares.

4.3 Diretoria de Informática e Automação

São responsabilidades da Diretoria de Informática e Automação (DIA):

I - adotar medidas de segurança, técnicas e/ou administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado, conforme padrões mínimos recomendados pela Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e em conformidade com a legislação vigente de proteção de dados.

4.4 Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação

São responsabilidades da Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação (ETIR):

I - realizar o tratamento de incidentes de segurança da informação que envolvam o tratamento de dados pessoais, garantindo sua detecção, contenção, eliminação e recuperação;

II - apoiar o(a) Encarregado(a) pelo tratamento de dados pessoais na comunicação à Autoridade Nacional de Proteção de Dados Pessoais (ANPD) e ao(à) titular dos dados em casos de ocorrência de incidentes de segurança que possam acarretar riscos ou danos relevantes aos(às) titulares, seguindo

os procedimentos estabelecidos e os prazos determinados pela legislação e regulamentação vigentes.

4.5 Usuários(as)

São responsabilidades dos(as) usuários(as) do Poder Judiciário do Estado do Maranhão (PJMA):

I - encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento ao(à) Encarregado(a) pelo tratamento de dados pessoais ou, quando pertinente, ao Comitê Gestor de Proteção de Dados Pessoais (CGPD);

II - comunicar ao(à) Encarregado(a) qualquer evento que coloque em risco os dados pessoais tratados pelo PJMA, garantindo a pronta notificação de incidentes de segurança ou outras irregularidades que possam comprometer a proteção de dados pessoais;

III - responder pela inobservância das diretrizes da segurança da informação e da proteção de dados pessoais, assegurado o contraditório e a ampla defesa.

Os(As) usuários(as) poderão ser responsabilizados(as) por condutas ilícitas relacionadas ao tratamento de dados pessoais e acesso à informação quando:

I - recusar a fornecer a informação requerida nos termos da lei, retardar deliberadamente seu fornecimento ou fornecê-la intencionalmente de forma incorreta, incompleta ou imprecisa;

II - utilizar indevidamente, bem como subtrair, destruir, inutilizar, desfigurar, alterar ou ocultar, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenha acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;

III - agir com dolo ou má-fé na análise das solicitações de acesso à informação;

IV - divulgar ou permitir a divulgação ou acessar ou permitir acesso indevido à informação sigilosa ou informação pessoal;

V - impuser sigilo à informação para obtenção de proveito pessoal ou de terceiro, ou para fins de ocultação de ato ilegal cometido por si ou por outrem;

VI - ocultar da revisão de autoridade superior competente informação sigilosa para beneficiar a si ou a outrem, ou em prejuízo de terceiros;

VII - destruir ou subtrair, por qualquer meio, documentos concernentes a possíveis violações de direitos humanos por parte de agentes do Estado;

VIII - agir em desacordo com disposto na Lei Geral de Proteção de Dados Pessoais (LGPD).

5. INFRAÇÕES E PENALIDADES

As infrações e penalidades serão aplicadas conforme previsto na Política de Segurança da Informação.

6. REVISÕES

Esta norma será alterada mediante necessidade de atualização, com apreciação e aprovação do Comitê de Governança de Segurança da Informação (CGSI).

7. APROVAÇÃO

A norma foi aprovada pelo Comitê de Governança de Segurança da Informação (CGSI), revogando-se todas as disposições em contrário.