PODER JUDICIÁRIO
DO ESTADO DE RORAIMA

LEI GERAL DE

PROTEÇÃO DE DADOS PESSOAIS

E SUA IMPLEMENTAÇÃO NO TRIBUNAL DE JUSTIÇA DE RORAIMA

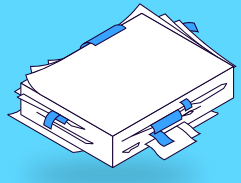
APRESENTAÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei 13.709, de 14 de agosto de 2018, entrou em vigor visando a proteção dos dados relativos a qualquer pessoa que se encontre no território brasileiro. Seguindo uma tendência global, a nova legislação objetiva proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural, promovendo o correto tratamento de dados pessoais, em meios físicos ou digitais, no âmbito das instituições públicas e privadas.

Neste contexto, o Tribunal de Justiça de Roraima desenvolveu seu Programa de Proteção de Dados Pessoais, com o fim de adequar o tratamento de dados pessoais à luz das disposições da LGPD.

OBJETIVO DA LGPD

A Lei Geral de Proteção de Dados tem como propósito disciplinar e regulamentar o tratamento de dados pessoais, ou seja, aqueles relacionados a pessoa natural, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger direitos fundamentais como liberdade, privacidade e livre desenvolvimento da personalidade da pessoa natural.



DIFERENÇA ENTRE DADO PESSOAL E DADO PESSOAL SENSÍVEL

É toda informação relacionada à pessoa natural que a identifica ou permita que ela seja identificável. Explicando melhor, o dado pessoal pode ser suficiente para identificar de imediato seu titular ou permitir que, por meio de associação a outros dados, seja possível identificá-lo.

Lado outro, dado pessoal sensível corresponde a toda informação relacionada a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, organização de caráter religioso, filosófico ou político; à saúde ou à vida sexual, dado genético ou biométrico.

É importante registrar que os dados sensíveis só devem ser solicitados ao titular quando forem imprescindíveis à operação de tratamento, pois são informações que podem causar danos mais gravosos ao titular, em caso de incidente de segurança.

O QUE É TRATAMENTO DE DADOS?

Tratamento de dados é qualquer operação realizada com dados pessoais, incluindo coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

O tratamento contempla todo o ciclo de vida do dado pessoal, desde a sua coleta até o final da operação para qual foi coletado, o que deve ser feito por agentes legalmente autorizados, de forma transparente e com respeito à intimidade, à vida privada, à honra e imagem das pessoas, bem como às liberdades e garantias individuais[1]

Para melhor compreensão do tema, seguem comentários e ilustrações constantes do Guia de Boas Práticas – Lei Geral de Proteção de Dados (LGPD) do Governo Federal[2].

• **Coleta:** obtenção, recepção ou produção de dados pessoais, independentemente do meio utilizado (documento em papel, documento eletrônico, sistema de informação etc.).

• **Retenção**: arquivamento ou armazenamento de dados pessoais, independentemente do meio utilizado (documento em papel, arquivo de pastas suspensas, documento eletrônico, banco de dados etc.).

Processamento: qualquer operação que envolva classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação de dados pessoais.

• **Compartilhamento**: qualquer operação que envolva transmissão, distribuição, comunicação, transferência, difusão e compartilhamento de dados pessoais.

[1] Art. 31 da Lei nº 12.527/11 – Lei de Acesso à Informação.

[2] <https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd>.

• **Eliminação**: qualquer operação que visa apagar ou eliminar dados pessoais, contemplando também o descarte dos ativos organizacionais, nos casos necessários ao negócio da instituição.

A tabela a seguir inserida, foi retirada do Guia de Boas Práticas do Governo Federal, em que ilustra a relação entre as fases do ciclo de vida descrito e as operações consideradas como tratamento de dados, de acordo com a LGPD.

FASE DO CICLO DE TRATAMENTO	OPERAÇÕES DE TRATAMENTO (LGPD, ART 5º, X)
COLETA	Coleta, produção e recepção
RETENÇÃO	Arquivamento e armazenamento
PROCESSAMENTO	Classificação, utilização, reprodução, processamento, avaliação ou controle da informação, extração e modificação
COMPARTILHAMENTO	Transmissão, distribuição, comunicação, transferência e difusão
ELIMINAÇÃO	Eliminação

HIPÓTESES DE TRATAMENTO DE DADOS

O art. 7º da Lei 13.709/2018 estabelece as hipóteses taxativas para tratamento de dados pessoais. Vejamos:

I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, 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, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

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

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

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

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

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

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

O tratamento de dados, para ser legítimo, necessita ter sua identificação em uma das hipóteses citadas, as quais são taxativas e podem ser cumuladas.

Convém ressaltar que a Lei Geral de Proteção de Dados não se aplica ao tratamento de dados pessoais nas seguintes hipóteses:

I - quando realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - quando realizado para fins exclusivamente jornalísticos e artísticos, ou acadêmicos;

III - quando realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação ou repressão de infrações penais;

IV - quando provenientes de fora do território nacional e não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na Lei

PRINCÍPIOS DO TRATAMENTO DE DADOS PESSOAIS

As atividades de tratamento de dados pessoais no âmbito desta Corte deverão observar, além da boa-fé, os seguintes princípios:

FINALIDADE	O tratamento de dados deverá demonstrar que tem fundamento na finalidade pública e ser realizado com propósitos legítimos, específicos, explícitos e informados.
ADEQUAÇÃO	O tratamento de dados deverá ser adequado à finalidade informada.
NECESSIDADE	O tratamento de dados deverá limitar-se ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos.
LIVRE ACESSO	O tratamento de dados deve ser pautado no livre acesso, por meio da garantia, aos titulares, do exercício de seus direitos consoante os procedimentos previstos em legislação específica, em especial na Lei 12.527/2011 (Lei de Acesso à Informação).
QUALIDADE DE DADOS	O tratamento de dados deverá ser feito com exatidão, clareza, relevância e atualização, de acordo com a necessidade e para o cumprimento de sua finalidade específica.
TRANSPARÊNCIA	O tratamento de dados deve ser realizado com transparência, por meio do fácil acesso do titular dos dados ao agente de tratamento,que deverá apresentar informações claras e precisas, mediante o procedimento previsto na Lei 12.527/11 (Lei de Acesso à Informação).

SEGURANÇA	O tratamento de dados deverá ocorrer por meio 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.
PREVENÇÃO	O tratamento de dados deverá adotar medidas de prevenção para mitigar a ocorrência de danos.
NÃO DISCRIMINAÇÃO	O tratamento de dados não poderá ser realizado para fins discriminatórios ilícitos ou abusivos.
RESPONSABILIZAÇÃO E PRESTAÇÃO DE CONTAS	O controlador, o encarregado e o operador deverão demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais.

Como podemos ver, além do enquadramento na base legal, o tratamento de dados deverá ser feito com observância aos princípios acima descritos, os agentes públicos devem verificar se a finalidade do tratamento se encontra descrita de forma precisa e clara, se os dados levantados são suficientes e necessários, se o fundamento do tratamento está adequado à finalidade apontada, se a operação está ocorrendo mediante a adoção de medidas de segurança e preventivas à ocorrência de danos e se há utilização indevida dos dados para fins discriminatórios, ilícitos ou abusivos.

TRATAMENTO DE DADOS PESSOAIS

O tratamento dos dados pessoais tem como principal fundamento o atendimento a sua finalidade pública, com o objetivo de executar competências legais, bem como o cumprimento de obrigação legal ou regulatória. Afinal, toda atividade administrativa e jurisdicional deve ter orientação obrigatória prevista na lei.

É consabido que o gestor público só pode praticar o ato amparado na lei e nos estritos limites por ela estabelecidos. Se o ato for praticado em amparo legal ou com finalidade diversa, configurará a prática do abuso de poder.

Essa orientação não é exclusiva da atividade administrativa. O Poder Judiciário, no exercício de sua atividade jurisdicional, deve, de igual modo, comportar-se de acordo com a lei.

Afora isso, a persecução do interesse público é diretriz vital para a execução das competências legais do serviço público, sob pena de desvio de finalidade. É certo que essa premissa não pode servir de instrumento para justificar o tratamento desnecessário e inadequado. Sob essa perspectiva, Francisco Gabriel Pacheco Junior alerta que uma das condutas veementemente repudiadas em todo o mundo, onde há legislação de proteção de dados, é a coleta e o armazenamento de dados pessoais, sensíveis ou não, sem a devida justificativa e simplesmente para avolumar, do ponto de vista qualitativo ou quantitativo, o banco de dados do controlador[3].

Percebe-se, portanto, que "a utilização dos dados para fins diversos daqueles atribuídos por lei aos órgãos e às entidades públicas é vedada pela LGPD e pode resultar na aplicação das sanções previstas nos arts. 52 a 54 da Lei, sem prejuízo da responsabilização nas esferas penais e cíveis"[4].

[3] O Tratamento de Dados pessoais pelo setor público e o alcance da LGPD. Coordenadores Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. São Paulo: Thomson Reuters, 2020, p. 315.

[4] LGPD e administração pública: uma análise ampla dos impactos. Coordenadores Augusto Neves Dal Pozzo e Ricardo Marcondes Martins. ão Paulo: Thomson Reuters, 2020, p. 239.

DESTINATÁRIOS

TÍTULAR DO DADO	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
CONTROLADOR	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. Em nosso contexto, é o TJRR, que tem a atribuição de editar, em seu âmbito de atuação, tais decisões.
OPERADOR	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
ENCARREGADO (DPO)	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
AUTORIDADE NACIONAL	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

AGENTES DE TRATAMENTO E ENCARREGADO NO ÂMBITO DO TJRR

CONTROLADOR

O Tribunal de Justiça do Estado de Roraima é o agente de tratamento definido como controlador, que tem o dever de tomar todas as decisões acerca do tratamento dos dados pessoais e assegurar que as ações e atividades vinculadas a seu processamento se encontrem em conformidade com a LGPD.

ENCARREGADO

As atribuições do encarregado, descritas nos incisos I a IV do § 2º do art. 41 da Lei 13.709/2018, são atualmente exercidas pelo Juiz de Direito Esdras Silva Pinto, conforme designação constante do art. 1º da Portaria GP 458/2020.

Convém assinalar as atividades do encarregado consistem em:

a) aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

b) receber comunicações da autoridade nacional e adotar providências;

c) orientar os funcionários e os contratados da entidade a respeito das práticas a serem observadas em relação à proteção de dados pessoais; e

d) executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

DIREITOS DOS TITULARES DOS DADOS

a) confirmação da existência de tratamento;

b) acesso aos dados;

c) correção de dados incompletos, inexatos ou desatualizados.

COMPARTILHAMENTO DOS DADOS PESSOAIS

O compartilhamento dos dados pessoais constantes da base de dados do TJRR deverá estar adequado a sua atribuição legal, com respeito aos princípios que regem o tratamento de dados previstos na LGPD, podendo ocorrer nas seguintes hipóteses:

a) quando os dados são acessíveis publicamente, observadas as disposições da LGPD;

b) quando houver previsão legal ou a transferência de dados for respaldada em contratos, convênios ou instrumentos congêneres;

c) quando a transferência de dados tiver como objetivo,exclusivamente, a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados.

EXERCÍCIO DOS DIREITOS PELO TITULAR

O titular do dado poderá, a qualquer momento, peticionar ao encarregado, preenchendo formulário eletrônico a ser disponibilizado no sítio eletrônico do TJRR, a fim de obter informações em relação aos dados tratados, ou diretamente à Autoridade Nacional de Proteção de Dados, pois é atribuição dessa autoridade zelar pela proteção de dados pessoais, bem como exercer a fiscalização e controle sobre o tratamento de dados pessoais realizado pelo Tribunal. O requerimento deverá conter a assinatura expressa pelo titular do dado ou seu representante legalmente constituído.

Conforme previsão do artigo 23, § 3º, da LGPD, o titular que tenha dados tratados pelo TJRR poderá exercer seu direito com base nos prazos e procedimentos dispostos em legislação específica, em especial as disposições constantes da Lei 9.507, de 12 de novembro de 1997 (Lei do Habeas Data), e da Lei 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Lei de Acesso à Informação – Lei 12.527, de 18 de Novembro de 2011

A Lei 12.527/2011 regulamenta o livre acesso às informações, bem como o procedimento e o prazo legal a serem observados para tanto. Com efeito, essa lei reservou tratamento diferenciado às informações pessoais relativas à intimidade, vida privada, honra e imagem das pessoas, conforme abaixo descrito (Lei 12.527/2011, art. 31, § 1º):

> I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 anos, a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e
>
> II - poderão ter autorizada sua divulgação ou acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa a que elas se referirem.

Como podemos ver, diversamente das informações de caráter geral, essas informações foram categorizadas como de caráter restrito, acessíveis "apenas por agentes públicos legalmente autorizados independentemente de classificação de sigilo", ou cuja divulgação tiver respaldo em previsão legal ou consentimento do titular dos dados.

Contudo, o consentimento não será exigido quando as informações forem necessárias e tiverem como substrato o atendimento ao interesse público, nas hipóteses abaixo descritas (Lei 12.527/2011, art. 31, § 3º):

I - prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico;

II - realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem;

III - cumprimento de ordem judicial;

IV - defesa de direitos humanos; ou

V - proteção do interesse público e geral preponderante.

A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá, ainda, ser invocada com o intuito de prejudicar processo de apuração de irregularidades em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância.

Procedimento e outras disposições do requerimento de informações solicitadas pelo Titular do Dado Pessoal

O titular do dado pessoal tem direito de obter, a qualquer momento e mediante requerimento, informações sobre os dados pessoais.

O pedido de acesso às informações deverá conter a identificação do requerente e a especificação da informação requerida.

O acesso à informação deverá ser imediato, se esta estiver disponível. Não sendo possível apresentar imediatamente, a administração deverá, no prazo de até 20 dias, podendo este prazo ser prorrogado por mais 10 dias, mediante justificativa expressa, adotar o seguinte procedimento:

- Comunicar a data, local e modo para se realizar a consulta, efetuar a reprodução ou obter a certidão;

- Indicar as razões de fato ou de direito da recusa, total ou parcial, do acesso pretendido; ou

- Comunicar que não possui dados do requerente e indicar, se for de seu conhecimento, o órgão ou a entidade que os detém, ou, ainda, remeter o requerimento a esse órgão ou entidade, cientificando o titular do dado da remessa de seu pedido.

As informações serão oferecidas em formato digital.
O requerimento administrativo quando formulado pelo titular do dado é gratuito, salvo nas hipóteses de reprodução de documentos pelo órgão ou entidade pública consultada, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados. Estará isento de ressarcir esses custos todo aquele cuja situação econômica não lhe permita fazê-lo sem prejuízo do sustento próprio ou da família.

Se o acesso aos dados constar de documento cuja manipulação possa prejudicar sua integridade, deverá oferecer cópia, com certificação de que esta confere com o original.

Na impossibilidade de oferecer cópias, o titular do dado poderá solicitar que, às suas expensas e sob supervisão de um servidor público, a reprodução seja feita por outro meio que não coloque em risco a conservação do documento original.

RESPONSABILIDADE DOS MAGISTRADO E SERVIDORES

Os magistrados e servidores poderão ser responsabilizados por condutas ilícitas relacionadas ao tratamento de dados pessoais e acesso à informação quando:

a) recusarem-se a fornecer a informação requerida nos termos da lei, retardarem deliberadamente seu fornecimento ou fornecerem-na intencionalmente de forma incorreta, incompleta ou imprecisa;

b) utilizarem indevidamente, bem como subtraírem, destruírem, inutilizarem, desfigurarem, alterarem ou ocultarem, total ou parcialmente, informação que se encontre sob sua guarda ou a que tenham acesso ou conhecimento em razão do exercício das atribuições de cargo, emprego ou função pública;

c) agirem com dolo ou má-fé na análise das solicitações de acesso à informação;

d) divulgarem ou permitirem a divulgação ou acessarem ou permitirem acesso indevido a informação sigilosa ou informação pessoal;

e) impuserem 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;

f) ocultarem da revisão de autoridade superior competente informação sigilosa para beneficiarem a si ou a outrem, ou em prejuízo de terceiros;

g) destruírem ou subtraírem, por qualquer meio, documentos oncernentes a possíveis violações de direitos humanos por parte de agentes do Estado; e

h) agirem em descordo com disposto na Lei de Geral de Proteção de Dados Pessoais.

A infração administrativa enseja a aplicação das sanções previstas na Lei Complementar 053/2001, que dispõe sobre o Regime Jurídico dos Servidores Públicos Civis do Estado de Roraima, e na Lei Complementar 35/1979, que dispõe sobre a Lei Orgânica da Magistratura Nacional, bem como as penalidades previstas na Lei 8.429/1992.

LGPD NO PORTAL ELETRÔNICO DO TJRR

Há no portal eletrônico do TJRR página específica concernente à Lei Geral de Proteção de Dados, onde são inseridas informações gerais sobre a aplicação da Lei, notícias, legislação e apresentação do encarregado.

CANAL DE COMUNICAÇÃO COM A OUVIDORIA E ENCARREGADO DO TJRR

Em caso de dúvidas, reclamações, elogios e sugestões referentes à política de privacidade, qualquer interessado poderá entrar em contato com a Ouvidoria, por meio dos seguintes canais de comunicação.

1. Canal online: <https://www.tjrr.jus.br/index.php/ouvidoria>;
2. Telefones funcionais: 0800 280 9551 / (95) 3198-4764;
3. Whatsapp: (95) 98402-6784;
4. Email: ouvidoria@tjrr,jus.br;
5. Sistema informatizado: Formulário eletrônico: <http://juris.tjrr.jus.br/juris/ouvidoria/public/nova-manifestacao>.
6. Atendimento presencial ou por correspondência na sede Administrativa do TJRR.

Outrossim, o canal de atendimento direto com o encarregado é por meio do correio eletrônico: encarregado.lgpd@tjrr.jus.br.

PROGRAMA DE IMPLEMENTAÇÃO DA LGPD

O Programa de Proteção de Dados Pessoais faz parte das ações de governança de privacidade do TJRR, que observa os seguintes requisitos previstos no art. 50, § 2º, I, da Lei 13.709/2018:

a) comprometimento do controlador dos dados em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) aplicação do programa a todo o conjunto de dados pessoais sob seu controle, independentemente do modo como se realizou sua coleta;

c) adaptação do programa à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;

d) estabelecimento de políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;

e) previsão de relação de confiança da organização com o titular dos dados, por meio de atuação transparente e que assegure mecanismos de sua participação;

f) previsão de que o programa esteja integrado à estrutura geral de governança da organização e que estabeleça e aplique mecanismos de supervisão internos e externos;

g) elaboração de planos de resposta a incidentes e remediação;

h) atualização permanente do programa com base em informações obtidas a partir de monitoramento contínuo e de avaliações periódicas.

Certo é, portanto, que o Programa de Proteção de Dados Pessoais do TJRR funciona como motor de aperfeiçoamento dos procedimentos internos e é fator de prevenção e redução dos riscos de desconformidades.

DA IMPLEMENTAÇÃO DO PROGRAMA DE PROTEÇÃO DE DADOS PESSOAIS NO ÂMBITO DO TJRR

INDICAÇÃO DO ENCARREGADO E CONSTITUIÇÃO DO COMITÊ GESTOR DE PROTEÇÃO E PRIVACIDADE DE DADOS (CGPPD)

O primeiro passo do programa de proteção de dados pessoais do TJRR foi a indicação do Juiz de Direito Dr. Esdras Silva Pinto, como encarregado, por meio da Portaria GP 458/2020.

Ato subsequente, constituiu-se o Comitê Gestor de Proteção e Privacidade de Dados (CGPPD), de caráter multidisciplinar, por meio da Portaria GP 547/2020, com atribuições de avaliar os mecanismos de tratamento e proteção de dados existentes e propor políticas estratégias e metas para a conformidade do Poder Judiciário do Estado de Roraima com as disposições da Lei 13.709/2018;

formular princípios e diretrizes para a gestão de dados pessoais e propor sua regulamentação; supervisionar a execução dos planos, dos projetos e das ações aprovados para viabilizar a implantação das diretrizes previstas na Lei 13.709/2018; prestar orientações sobre o tratamento e a proteção de dados pessoais de acordo com as diretrizes estabelecidas na LGPD e nas normas internas; e promover o intercâmbio de informações sobre a proteção de dados pessoais com outros órgãos. E, a nomeação dos membros que compõem o CGPPD, por meio da Portaria GP 1119/2021, atualizada.

AUTOAVALIAÇÃO E MAPEAMENTO DOS DADOS PESSOAIS

O mapeamento dos dados pessoais constitui-se como uma etapa sensível do programa de implantação da LGPD, pois é a partir dele que será apresentado o diagnóstico do tratamento de dados pessoais da instituição. Em função disso, faz-se necessário analisar os elementos e subsídios que servirão como norte para as decisões estratégicas na adoção de medidas de conformidade com a LGPD.

Essa etapa, portanto, tem o objetivo de mapear os processos de trabalho que mereçam medidas de adequação e revisões próprias, por meio do levantamento das normas, dos princípios e das possíveis incongruências com o texto da LGPD[5].

[5] Impactos da LGPD sobre a atuação da administração pública: alguns desafios e sua efetividade. Jéssica Acocella e Rodrigo Sampaio. LGPD e administração pública: uma análise ampla dos impactos. Pag. 365

Convém assinalar que merecem uma atenção quanto aos seguintes requisitos das atividades de tratamento que envolvem o ciclo de vida dos dados pessoais:

a) Base Legal e Observância dos Princípios: visa à adequação legal do processo de trabalho mapeado e ao levantamento dos princípios nos quais se apoia o tratamento de dados. Essa medida pode ensejar a publicação de novos normativos (para os casos de ausência de previsão expressa) ou adequação de normas existentes, para que estejam em consonância com a instrução do processo de trabalho, bem como a adoção de estratégias de contingenciamento no caso de inobservância do art. 6º da LGPD.

b) Processos de trabalho: visam à adequação dos processos de trabalho das unidades à LGPD. Podem representar a melhoria de fluxos, como extinção de etapas do processo ou revisão de dados coletados, adequação de formulários ou transposição de etapas ou processos que ainda ocorrem em meio físico para o digital. Tais ações podem representar grandes mudanças ou adaptações triviais, como a inserção de boas práticas e métodos de trabalho.

c) Sistemas: atividades relacionadas com o desenvolvimento de melhorias nos sistemas informatizados do Tribunal. Podem ensejar a adequação de campos ou de dados e reavaliar os requisitos relativos ao registro de dados pessoais nos projetos em desenvolvimento. Destaca-se, ainda, o estabelecimento de políticas e rotinas mais rígidas de acesso, rastreamento de usuários, armazenamento, backup, dentre outros. Salienta-se que as medidas afetas aos sistemas, dependendo da complexidade de sua implementação, podem ensejar a aceitação de riscos como, por exemplo, a definição rotinas de monitoramento em um sistema considerado mais sensível.

RISCOS E TRATAMENTO DOS DADOS PESSOAIS

Superada a fase de diagnóstico, faz-se necessário a depuração dos principais riscos dos processos e sistemas de tratamento de dados, com a adoção das medidas de contingenciamento para a revisão de processos e sua adequação às exigências da LGPD, bem como a instituição de ferramentas de controle.

ESTRUTURAÇÃO DA POLÍTICA DE PROTEÇÃO DE DADOS PESOAIS DO TJRR

O Tribunal deve estruturar políticas de proteção de dados pessoais voltadas a preservar a conformidade da organização à LGPD, o uso ético dos dados, o tratamento de ciclo de vida dos dados, a segurança da informação e a preservação da privacidade, e respostas a incidentes.

CAPACITAÇÃO E COMUNICAÇÃO

Toda implementação de uma nova política e ação, via de regra, demanda a realização de capacitação para ensinar e reforçar as melhores práticas e, também, para avaliar a retenção desse conhecimento.

A capacitação ainda é essencial para sensibilizar a equipe para o uso das ferramentas disponíveis (documentos e procedimentos operacionais padronizados e políticas próprias) e a interação com outros agentes (o titular dos dados, o controlador, o encarregado, o operador).

Notadamente, para a eficácia do engajamento de magistrados e servidores, foi elaborado um plano de capacitação, visando garantir a coerência entre as diversas fases de aprendizado.

Ainda, por se tratar de uma mudança de cultura no tratamento de dados pessoais, ressoam como vitais, para a eficácia do programa, o planejamento e a execução de um plano estratégico de comunicação para os magistrados, servidores, colaboradores, prestadores de serviços e demais usuários, com a finalidade de disseminar informações das ações implementadas e a cultura de privacidade e, sobretudo, ortalecer os comportamentos que devem ser adotados.

MONITORAMENTO

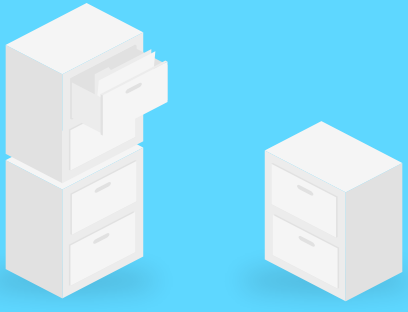
Completando o ciclo de implantação do programa de proteção de dados, passa-se à etapa de monitoramento contínuo, com ações de supervisão e operacionalização para melhorar a performance da organização. Importante destacar que a autoridade nacional poderá Solicitar, a qualquer momento, aos órgãos e às entidades do poder público, a realização de operações de tratamento de dados pessoais, informações específicas sobre o âmbito e a natureza desses dados e outros detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta da LGPD.

POLÍTICA DE PRIVACIDADE PARA NAVEGAÇÃO NO SITE DO TJRR

O TJRR adota as medidas de aperfeiçoamento e adequação à LGPD, por meio da implantação de programa de governança da privacidade, fortalecendo as ferramentas tecnológicas, as medidas de segurança técnica e administrativa, os controles, processos internos, a organização e prestação de contas.

PROCEDIMENTO DE INCIDENTES DE SEGURANÇA

O programa de proteção de dados pessoais do TJRR prevê a implantação de política relativa a incidente de segurança da informação que possa acarretar risco ou dano relevante aos titulares, com comunicação imediata à Autoridade Nacional e ao titular do dado pessoal.



DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO DO TJRR

Os agentes de tratamento do TJRR devem adotar medidas de segurança, técnicas e administrativas aptas a protegerem os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. Essas ações deverão ocorrer desde a fase de concepção do produto ou do serviço até a sua execução.

São diretrizes de segurança da informação no tratamento de dados pessoais:

Confidencialidade: propriedade de que a informação não será disponibilizada ou divulgada a indivíduos, entidades ou processos sem autorização.

Integridade: propriedade de que a informação não foi modificada ou destruída, de maneira não autorizada ou acidental, por indivíduos, entidades ou processos.

Disponibilidade: propriedade de que a informação esteja acessível e possa ser utilizada sob demanda por indivíduos, entidades ou processos.

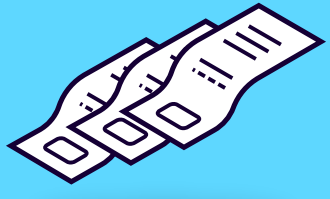
PODER JUDICIÁRIO
DO ESTADO DE RORAIMA

RELATÓRIO DE IMPACTO NA PROTEÇÃO DE DADOS PESSOAIS (RIPD)

O Relatório de Impacto na Proteção de Dados Pessoais (RIPD) é a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referentes a suas operações de tratamento de dados, consoante regulamento e observados os segredos comercial e industrial. O relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados.

A ANPD poderá editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto na proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD.



CONSIDERAÇÕES FINAIS

Como se percebe, a Lei 13.709/2018 é um marco regulatório e permite uma releitura do princípio da privacidade, estabelecendo um rol de direitos e obrigações para os órgãos e entidades públicas e privadas que irão demandar a implantação de programa de proteção de dados pessoais.

Por se tratar de programa que envolve políticas e ações permanentes, que são essenciais para manter a instituição adequada às normas da LGPD, a jornada para sua implantação tem início, mas não tem fim. A despeito de muitos desafios que serão enfrentados para a estruturação do programa, é inegável que ele representa um grande passo para a melhoria da governança em privacidade e proteção de dados pessoais do TJRR.

PODER JUDICIÁRIO
DO ESTADO DE RORAIMA