

PLANO DE ADEQUAÇÃO



**CONTROLADORIA-GERAL DO ESTADO
DE MATO GROSSO DO SUL**

Carlos Eduardo Girão de Arruda

Controlador-Geral do Estado

Marina Hiraoka Gaidarji

Controladora-Geral do Estado Adjunta

Juris Jankauskis Junior

Assessor de Governança e Comunicação

Elaboração: Rosely Pereira Maia
Auditora do Estado
Encarregada pelo Tratamento dos Dados Pessoais

Sumário

1.	Apresentação.....	5
2.	Conceitos Relevantes.....	6
2.1	Aplicação da LGPD	7
2.2	Conceito de Plano de Adequação.....	7
2.3	Objetivo geral do Plano de Adequação.....	8
2.4	Objetivos específicos do Plano de Adequação.....	8
2.5	Tratamento de Dados Pessoais.....	9
2.5.1	Categorias de Dados Pessoais.....	9
2.6	Princípios da LGPD	10
2.7	Hipóteses de Tratamento da LGPD.....	11
2.8	Participantes da Lei Geral de Proteção de Dados Pessoais.....	12
2.8.1	Agentes de Tratamento de Dados Pessoais.....	12
2.8.2	Encarregado pelo Tratamento de Dados Pessoais.....	15
2.8.3	Titular dos dados pessoais.....	16
2.8.4	Autoridade Nacional de Proteção de Dados – ANPD.....	17
2.9	Compartilhamento de dados.....	17
2.10	Responsabilização.....	19
3.	Etapas para adequação da CGE à LGPD.....	20
3.1	Treinamento/Capacitação.....	21
3.2	Designação de Encarregado pelo Tratamento de Dados Pessoais.....	22
3.3	Comitê de Proteção de Dados Pessoais.....	23
3.4	Publicidade de informações relativas ao tratamento de dados pessoais.....	24
3.5	Revisão e adequação de Contratos administrativos, Convênios, Parcerias e Congêneres.....	25
3.6	Adequação do Regimento Interno e do Código de Conduta Ética.....	25
3.7	Mapeamento de Dados Pessoais.....	26
3.8	Mapeamento do fluxo de dados.....	27
3.9	Levantamento de Riscos.....	27
3.10	Ações mitigadoras de Riscos.....	27
3.11	Atualização de sistemas	29
3.12	Política de Segurança da Informação.....	30
3.13	Política de Privacidade / Notificação de Cookies.....	30
3.14	Processos internos de atendimento às solicitações dos titulares.....	31
3.15	Procedimentos de resposta a incidentes de segurança.....	31
3.16	Relatório de Impacto à Proteção de Dados Pessoais –RIPD.....	32
3.17	Monitoramento.....	32
3.18	Cronograma de implementação das ações.....	33



1. APRESENTAÇÃO

Apresentação

O presente Plano de Adequação tem como objetivo consolidar o planejamento das ações e atividades a serem desenvolvidas pela Controladoria-Geral do Estado, no que tange à implementação da Lei Geral de Proteção de Dados Pessoais.

A LGPD foi sancionada em 2018 e entrou em vigor em setembro de 2020. A lei é considerada um marco histórico na regulamentação sobre o tratamento de dados pessoais no Brasil, tanto em meios físicos quanto em digitais.

Nesse contexto, a CGE possui o dever de atender aos preceitos normativos, no que se refere ao tratamento de dados pessoais, sejam eles digitais ou não, razão pela qual torna-se relevante publicizar as ações que serão efetivadas.

A implementação de uma estratégia para atuar preventivamente tem o intuito de estimular a cultura de proteção de dados, por meio de ações que facilitem o processo de adequação à LGPD, minimizando os riscos e priorizando melhorias na segurança da informação.

A **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022, alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, além de fixar a competência privativa da União para legislar sobre esse tema. Este fato, por si só, tornou a proteção de dados pessoais cláusula pétrea, ou seja, dispositivo que não pode ser abolido, mas apenas alterado para ampliar e resguardar direitos.

Esta medida consolida o papel da Lei Geral de Proteção de Dados Pessoais no cenário brasileiro, reforçando sua relevância.

Por fim, o Plano de Adequação objetiva o *compliance*, ou seja, garantir o tratamento dos dados pessoais com segurança e privacidade, evitando exposição indevida.

Versão: abril/2022



2.1 Aplicação da LGPD

A LGPD se aplica a qualquer pessoa, tanto física quanto jurídica, sendo pública ou privada, que faça o tratamento de dados pessoais, em meio físico ou digital, inclusive daqueles que foram coletados antes da lei ser criada e passar a vigorar.

O principal foco da LGPD é proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.2 Conceito de Plano de Adequação à LGPD

A LGPD foi sancionada em 2018 para determinar regras sobre **coleta, tratamento, armazenamento e compartilhamento de dados pessoais**. A lei já está em vigor desde setembro de 2020, sendo que as sanções administrativas são passíveis de aplicação desde 1º de agosto de 2021.

Após a publicação do “*Guia de Boas Práticas para implementação e adequação da LGPD na Administração Pública Estadual*”, disponível no link www.lgpd.ms.gov.br/materiais-disponiveis/, iniciou-se a elaboração do Plano de Ação com o objetivo de fomentar a cultura de proteção de dados necessária à adequação da lei na Controladoria-Geral do Estado (CGE/MS).

O Decreto Estadual nº 15.572/2020, atualizado pelos Decretos Estaduais nº 15.646 e nº 15.723, ambos de 2021, estabelece que:

“Art. 2º, parágrafo único. Será adotado, ainda, como **conceito de Plano de Adequação** o conjunto de regras de boas práticas e de governança de dados pessoais, estabelecidas pelos Controladores e Operadores, no âmbito de suas competências, que visem à implantação da LGPD pelos órgãos da Administração Direta, pelas autarquias e pelas fundações do Poder Executivo Estadual e que estabeleçam as **condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos** relacionados ao tratamento de dados pessoais.”

E mais:

“Art. 6º. Os **planos de adequação** devem observar, no mínimo, o seguinte:

I - **publicidade das informações relativas ao tratamento de dados** em veículos de fácil acesso, preferencialmente nas páginas dos órgãos da Administração Direta, das autarquias e das fundações do Poder Executivo Estadual na internet, bem como no Portal da Transparência, em seção específica a que se refere o § 1º do art. 3º deste Decreto;

II - **atendimento das exigências que vierem a ser estabelecidas pela Autoridade Nacional de Proteção de Dados**, nos termos do art. 23, § 1º, e do art. 27, parágrafo único da Lei Federal nº 13.709, de 2018;

III - manutenção de dados em formato interoperável e estruturado para o uso compartilhado de dados com vistas à **execução de políticas públicas**, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.”

Como qualquer iniciativa, depreende-se que é necessário o **apoio dos dirigentes do órgão e a demonstração de comprometimento dos mesmos** aos esforços destinados à adequação da CGE/MS à LGPD.

2.3 Objetivo geral do Plano de Adequação

Orientar a implementação das medidas destinadas à aplicação da Lei Federal nº 13.709/18, Lei Geral de Proteção de Dados Pessoais, e do Decreto Estadual nº 15.572/2020, no âmbito da Controladoria-Geral do Estado de Mato Grosso do Sul.

2.4 Objetivos específicos do Plano de Adequação

- ✓ Possibilitar que os dados pessoais sejam tratados com segurança e privacidade, evitando acesso ou exposição indevidas;

-
- ✓ Definir as atividades fundamentais a serem desenvolvidas para o atendimento das disposições da LGPD;
 - ✓ Apresentar algumas das medidas necessárias para a adequada implementação da LGPD na CGE/MS;
 - ✓ Promover a cultura de proteção de dados pessoais na CGE/MS.

2.5 Tratamento de Dados Pessoais

O inciso X do art. 5º da LGPD considera tratamento “*toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração*”.

2.5.1 Categorias de Dados Pessoais

Objetivando simplificar a identificação de termos utilizados na LGPD, indicamos os conceitos abaixo:

- ✓ **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável (art. 5º, I, LGPD);
- ✓ **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (art. 5º, II, LGPD);
- ✓ **Dado pessoal de criança e adolescente:** o tratamento de dados pessoais de crianças (até 12 anos incompletos) e adolescentes (12 a 18 anos) deverá ser realizado com consentimento e específico e em destaque, por, pelo menos, um dos pais ou responsável legal, mesmo que se trate de execução de políticas públicas, havendo exceções para tratamento sem consentimento;
- ✓ **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento (art. 5º, III, LGPD);

-
- ✓ **Dado pseudonimizado:** dado submetido a tratamento no qual perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (art. 13, §4º, LGPD);
 - ✓ **Dado pessoal de acesso público:** dado que deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização (art. 7º, §3º, LGPD);
 - ✓ **Dado pessoal tornado manifestamente público pelo titular:** dado pessoal publicado e compartilhado pelo próprio titular (art. 7º, §4º, LGPD), o que dispensa a exigência do consentimento;

2.6 Princípios da LGPD

A aplicação das regras previstas na LGPD deve observar os **10 princípios** estabelecidos pelo art. 6º da lei, sendo que a **boa-fé** é destacada no *caput*.

A LGPD dispõe de base principiológica bem específica, contendo uma sucessão de princípios que visam maior proteção à privacidade do cidadão e integram um grupo de elementos de cumprimento obrigatório.

O tratamento dos dados pessoais realizado na CGE/MS deve ser orientado pelos princípios dispostos na LGPD, cujos princípios devem ser observados:

Objetivando limitar o uso dos dados, o legislador lançou mão dos princípios da:

- ✓ **Finalidade**, cujo tratamento deve ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular;
- ✓ **Adequação**, para que haja compatibilidade do tratamento com as finalidades informadas ao titular;
- ✓ **Necessidade**, para que haja limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

O legislador, para garantir aos titulares o acesso às informações relativas ao uso de seus dados, evidenciou os princípios da (o):

- ✓ **Qualidade dos dados**, com garantia de exatidão, clareza, relevância e atualização dos dados;
- ✓ **Transparência**, com garantia de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento;
- ✓ **Livre acesso**, propiciando consulta facilitada e gratuita sobre a forma e duração do tratamento.

Para assegurar a proteção dos dados, o legislador efetivou os seguintes princípios:

- ✓ **Segurança**, para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas;
- ✓ **Prevenção**, com adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
- ✓ **Não-discriminação**, que veda a realização do tratamento para fins discriminatórios ilícitos ou abusivos.

E, finalmente, para salvaguardar a aplicação da LGPD, foi editado o princípio da **Responsabilização e prestação de contas**, que dispõe sobre a demonstração, pelo agente, da adoção de medidas comprovadamente eficazes e capazes de atestar a observância e o cumprimento das normas de proteção de dados pessoais.

2.7 Hipóteses de Tratamento da LGPD

As bases legais da LGPD se fundamentam nas hipóteses que autorizam o tratamento de dados. São elas as **condições** determinadas pela Lei Geral de Proteção de Dados que possibilitam a **coleta de dados pessoais e o tratamento deles**.

Essas hipóteses de tratamento estão previstas nos artigos 7º e 11 da LGPD e não têm dependência ou preponderância entre si. São alusivas ao tratamento dos **dados pessoais e dos dados pessoais sensíveis**, respectivamente:

HIPÓTESES DE TRATAMENTO		FUNDAMENTO LEGAL	
		DADOS PESSOAIS	DADOS PESSOAIS SENSÍVEIS
1	<i>Mediante consentimento do titular</i>	LGPD, art. 7º, I	LGPD, art.11, I
2	<i>Para o cumprimento de obrigação legal ou regulatória</i>	LGPD, art. 7º, II	LGPD, art. 11, II, "a"
3	<i>Para a execução de políticas públicas</i>	LGPD, art. 7º, III	LGPD, art. 11, II, "b"
4	<i>Para a realização de estudos por órgão de pesquisa</i>	LGPD, art. 7º, IV	LGPD, art. 11, II, "c"
5	<i>Para a execução ou preparação de contrato</i>	LGPD, art. 7º, V	Não se aplica
6	<i>Para o exercício de direitos em processo judicial, administrativo ou arbitral</i>	LGPD, art. 7º, VI	LGPD, art. 11, II, "d"
7	<i>Para a proteção da vida ou da incolumidade física do titular ou terceiro</i>	LGPD, art. 7º, VII	LGPD, art. 11, II, "e"
8	<i>Para a tutela da saúde do titular</i>	LGPD, art. 7º, VIII	LGPD, art. 11, II, "f"
9	<i>Para atender interesses legítimos do controlador ou de terceiro</i>	LGPD, art. 7º, IX	Não se aplica
10	<i>Para proteção do crédito</i>	LGPD, art. 7º, X	Não se aplica
11	<i>Para a garantia da prevenção à fraude e à segurança do titular</i>	Não se aplica	LGPD, art. 11, II, "g"

A LGPD dedicou o Capítulo IV para o tratamento de dados pessoais pelo Poder Público, sendo que está circunscrito à Administração Pública 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*”.

Entretanto, muitas outras hipóteses podem ser utilizadas pelo Poder Público, a depender do tratamento de dados pessoais que será realizado, a saber:

- cumprimento de obrigação legal ou regulatória;
- execução ou preparação de contrato;
- exercício de direitos em processo judicial, administrativo ou arbitral;
- tutela da saúde do titular;
- legítimo interesse do controlador, entre outros.

Da mesma forma, o art. 12 do Decreto Estadual nº 15.572/2020 dispõe que “*o tratamento de dados pessoais pelos órgãos da Administração Direta, pelas autarquias e pelas fundações do Poder Executivo Estadual, observado o disposto no Capítulo IV da LGPD, será realizado para atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.*”

Não se aplicam as normas da LGPD quando o tratamento de dados pessoais ocorrer para fins de segurança nacional, de defesa nacional e de segurança do Estado, bem como para finalidade de investigação e de repressão de infrações penais (art. 4º, III, “a” a “d”, LGPD).

2.8 Participantes da Lei Geral de Proteção de Dados Pessoais

2.8.1 Agentes de Tratamento de Dados Pessoais

Os agentes de tratamento são o Controlador e o Operador, responsáveis pelo tratamento dos dados pessoais, sujeitos às regras da LGPD e, conseqüentemente, à fiscalização da Autoridade Nacional de Proteção de Dados - ANPD.

O Controlador é quem toma as decisões referentes ao tratamento de dados pessoais e o Operador, é o que realiza, em nome do Controlador, o tratamento de dados pessoais (art. 5º, VI, VII e IX, LGPD).

Nos termos do Decreto Estadual nº 15.572/2020, constam as respectivas definições:

“Art.3º, I - **Controlador**: o Estado de Mato Grosso do Sul por intermédio dos Secretários de Estado, do **Controlador-Geral**, do Procurador-Geral do Estado e dos dirigentes das entidades da Administração Indireta, respeitadas suas respectivas competências e campos funcionais;

II- **Operador**: o(s) agente(s) público(s), no sentido amplo, que exerça(m) o tratamento de dados, bem como pessoa(s) jurídica(s) diversa(s) daquela representada pelo Controlador, que exerça(m) atividade de tratamento no âmbito de contrato ou de instrumento congêneres.”

As atribuições desses agentes de tratamento foram explicitamente definidas pelo Decreto Estadual nº 15.572/2020:

“Art. 7º São **atribuições do Controlador** de dados pessoais a que se refere o inciso VI do art. 5º da LGPD:

I - designar, por ato próprio, o(s) **encarregado(s)** de proteção de dados pessoais do respectivo órgão da Administração Direta, da autarquia ou da fundação;

II - **manter registro das operações de tratamento de dados pessoais** que realizar, especialmente quando baseado no legítimo interesse;

III - elaborar o **relatório de impacto à proteção de dados pessoais, quando determinado pela Autoridade Nacional de Proteção de Dados**;

IV - verificar a **observância, pelo Operador, das instruções** dadas para o tratamento de dados pessoais e das normas sobre a matéria;

V - adotar **medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;

VI - dar cumprimento, no âmbito dos respectivos órgãos da Administração Direta, das autarquias e das fundações, às **orientações e às recomendações do encarregado** de proteção de dados pessoais;

VII - atender às solicitações encaminhadas pelo encarregado de proteção de dados pessoais, no sentido de **fazer cessar** uma afirmada **violação** à Lei Federal nº 13.709, de 2018, ou apresentar as justificativas pertinentes;

VIII - **encaminhar ao encarregado**, no prazo por este fixado:

a) **informações sobre o tratamento de dados pessoais** que venham a ser solicitadas pela Autoridade Nacional de Proteção de Dados, nos termos do art. 29 da Lei Federal nº 13.709, de 2018;

b) **relatórios de impacto à proteção de dados pessoais**, ou informações necessárias à elaboração de tais relatórios, nos termos do art. 32 da Lei Federal nº 13.709, de 2018.

IX - assegurar que o **encarregado seja informado, de forma adequada e em tempo útil, de todas as questões relacionadas com a proteção de dados pessoais** no âmbito do respectivo órgão da Administração Direta, da autarquia ou da fundação do Poder Executivo Estadual;

X - exercer outras atribuições correlatas.

Art. 8º São atribuições do **Operador de dados pessoais** de que trata o inciso VII do art. 5º da LGPD:

I - **manter registro das operações de tratamento de dados pessoais** que realizar, especialmente quando baseado no legítimo interesse;

II - **realizar o tratamento de dados segundo as instruções fornecidas pelo Controlador** e de acordo com as normas aplicáveis;

III - **adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito;

IV - **subsidiar o Controlador** no intuito de dar cumprimento às solicitações, orientações e às recomendações do Encarregado;

V - executar outras atribuições correlatas.

2.8.2. Encarregado pelo Tratamento de Dados Pessoais

O Encarregado pelo tratamento de dados pessoais é o agente público designado para fazer a mediação entre o Controlador, os titulares dos dados pessoais e a Autoridade Nacional de Proteção de Dados – ANPD (art. 5º, VIII, LGPD), sendo que deve possuir “*conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos a gestão de riscos e governança de dados, com assessoria jurídica e tecnológica, e poderes para tratar questões que afetem os operadores*” (art.3º, §3º Decreto Estadual nº 15.572/2020).

O art. 9º do Decreto Estadual nº 15.572/2020 estabelece as atribuições do Encarregado, quais sejam:

- “I - **receber reclamações e comunicações dos titulares**, prestar esclarecimentos e adotar providências;
- II - **receber comunicações da Autoridade Nacional de Proteção de Dados** e adotar providências;
- III - **orientar os funcionários e os contratados** do órgão da Administração Direta, da autarquia ou da fundação a respeito das práticas a serem adotadas em relação à proteção de dados pessoais;
- IV - submeter à **Comissão Mista de Avaliação de Informações Classificadas, ao Comitê Encarregado de Editar Diretrizes do Plano de Adequação e ao Comitê Estratégico de Tecnologia da Informação**, sempre que julgar necessário, no que couber, matérias atinentes a este Decreto;
- V - **decidir sobre as sugestões formuladas pela Autoridade Nacional de Proteção de Dados** a respeito da adoção de padrões e de boas práticas para o tratamento de dados pessoais, nos termos do art. 32 da Lei Federal nº 13.709, de 2018;
- VI - **providenciar, quando solicitados pela Autoridade Nacional de Proteção de Dados, a publicação dos relatórios de impacto à proteção de dados pessoais previstos** pelo art. 32 da Lei Federal nº 13.709, de 2018;
- VII - adotar providências, quando do recebimento de informe da Autoridade Nacional de Proteção de Dados nos termos do art. 31 da Lei nº 13.709, de 2018, visando a **cessar violação à referida Lei**, em decorrência do tratamento de dados pessoais por parte do respectivo

órgão da Administração Direta, da autarquia ou da fundação, fixando prazo para atendimento à solicitação ou à apresentação de justificativas pertinentes;

VIII - **avaliar as justificativas** apresentadas nos termos do inciso VII deste artigo, para o fim de:

a) caso avalie ter havido a violação, determinar a adoção das medidas solicitadas pela Autoridade Nacional de Proteção de Dados;

b) caso avalie não ter havido a violação, apresentar as justificativas pertinentes à Autoridade Nacional de Proteção de Dados, segundo o procedimento cabível;

IX - executar as demais atribuições estabelecidas em normas complementares”.

Por dever de ofício, o Encarregado pelo tratamento dos dados pessoais está vinculado à obrigação de sigilo ou confidencialidade no exercício das funções inerentes às atividades (art.9º, parágrafo único, Decreto Estadual nº 15.572/2020).

2.8.3. Titular dos dados pessoais

O titular é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. A edição da LGPD veio para assegurar direitos para os titulares de dados pessoais, uma vez que eles têm que ser informados sobre como vão ser utilizados os seus dados, tendo o direito de obstar qualquer uso futuro que não esteja compreendido nas finalidades apresentadas no momento da coleta.

Os direitos dos titulares de dados pessoais estão especificados no Capítulo III, dos artigos 17 ao 22, da LGPD, quais sejam:

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 na LGPD

Portabilidade dos dados a outro fornecedor de serviço ou produto

Eliminação dos dados pessoais tratados com o consentimento do titular

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 consequências da negativa

Revogação do consentimento

Direito de peticionar com relação aos seus dados contra o controlador

Opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento

Solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses (...)

2.8.4. Autoridade Nacional de Proteção de Dados - ANPD

A Autoridade Nacional de Proteção de Dados (ANPD) é o “*órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional*” (art. 5º, XIX).

O art.55-J da LGPD elenca várias atribuições da ANPD, sendo destacadas as abaixo elencadas: zelar pela proteção dos dados pessoais; elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade; fiscalizar e aplicar sanções em caso de violação da lei; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais; editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, entre outras.

Dotada de autonomia técnica e decisória, a ANPD foi criada pela Lei 13.853, de 08/07/2019 e sua estrutura foi definida pelo Decreto 10.474, de 26/08/2020. Desde então, a ANPD tem divulgado Guias Orientativos que estão publicados no portal www.lgpd.ms.gov.br.

2.9. Compartilhamento de dados

O compartilhamento de dados pessoais já era atividade comum e corriqueira mesmo antes da LGPD. Porém, não era perceptível a relevância da proteção aos dados pessoais, visto que a lei ainda não estava em vigor.

O compartilhamento dentro da administração pública no âmbito da execução de políticas públicas é previsto na LGPD (art.26) e dispensa o consentimento específico. O órgão que coleta deve informar claramente com quem o dado será compartilhado. Do outro lado, o órgão que solicita receber o compartilhamento precisa justificar esse acesso com base na execução de uma política pública específica. Informações protegidas por sigilo seguem protegidas e sujeitas a normativos e regras específicas.

O compartilhamento de dados entre órgãos públicos e a transferência de dados a terceiro fora do setor público, no âmbito do Poder Executivo Estadual, estão previstos no Decreto Estadual nº 15.572/2020.

O art. 13 do normativo estadual autoriza o compartilhamento de dados pessoais para atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios da LGPD e observadas algumas diretrizes:

- I – assunção, pelo recebedor dos dados, dos deveres de sigilo e auditabilidade;
- II – os mecanismos de compartilhamento sejam para facilitar a execução de políticas públicas orientadas por dados;
- III – haja colaboração dos órgãos/entidades para redução dos custos de acesso a dados;
- IV – sejam observados o direito à preservação da intimidade e da privacidade da pessoa natural, a proteção dos dados e as normas e os procedimentos previstos na legislação;
- V – o tratamento e o compartilhamento de dados sejam realizados nos termos do art. 23 da LGPD (finalidade pública, interesse público, com objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público).

Em que pese o Decreto Estadual, no parágrafo único do art. 13, não obrigar a elaboração de **ato formal**, é importante que, **caso o órgão que esteja deferindo o compartilhamento seja a CGE, emita “decisão administrativa” do Controlador-Geral do Estado** autorizando o acesso aos dados e estabelecendo os requisitos para o compartilhamento, conforme consta no Guia Orientativo Tratamento de Dados Pessoais pelo Poder Público (ANPD).

Consta, também, no portal www.lgpd.ms.gov.br, o Parecer PGE/PAA/MS 49/2021 sobre compartilhamento de dados.

A transferência de dados pessoais do Poder Público para entidades privadas é **vedada (art.14 do Decreto Estadual nº 15.572/2020)**, exceto nos casos:

- I – de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado;
- II - em que os dados forem acessíveis publicamente;

III - quando houver previsão legal ou cláusula específica em contratos, convênios ou congêneres, sendo que a celebração deverá ser informada pelo responsável ao encarregado para comunicação à ANPD;

IV - de a transferência dos dados objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados.

2.10. Responsabilização

O tratamento de dados pessoais está centralizado em dois agentes, o controlador e o operador, sendo que os operadores devem realizar o tratamento de dados conforme as instruções fornecidas pelo controlador, que detém o **poder de decisão**.

A Lei Geral de Proteção de Dados, em seu artigo 42, estabelece que a responsabilidade por qualquer dano ou violação referente ao tratamento de dados pessoais é de **responsabilidade solidária** entre o **controlador** e **operador** de dados pessoais.

Esta disposição legal faz com que seja importante que, no momento da celebração de contratos, haja observação de cláusulas contratuais e disposições delimitando as **responsabilidades** de cada pessoa jurídica contratante relativo ao tratamento de dados pessoais presente no fluxo de informações para execução daquele determinado processo.



3. ETAPAS PARA ADEQUAÇÃO DA CGE/MS À LGPD

A LGPD envolve aspectos que não estão restritos a um conhecimento técnico específico, restando claro que para implementá-la será necessário um esforço de todo o corpo funcional da Controladoria-Geral do Estado, haja vista que diferentes profissionais se complementarão.

Considera-se complexa a atuação que proteja a privacidade e os dados pessoais, demandando esforços conjuntos de diversas partes interessadas. Por conta dessa diversidade é que o caráter multidisciplinar da equipe deverá ser destacado.

Sabendo que a LGPD se aplica a toda atividade que envolva utilização de dados pessoais, inclusive nos meios digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade, destacamos abaixo os principais passos para sua implementação:

3.1 Treinamento/Capacitação

A construção de uma cultura de privacidade é fundamental para a implementação da LGPD e o bom desenvolvimento dessa prática exige a conscientização da equipe.

Para isso, é necessário potencializar uma atuação integrada e coordenada com toda a equipe, de forma que haja a proteção dos dados pessoais e informações privadas em poder do órgão público, no caso, desta CGE/MS.

Desta forma, a primeira medida diz respeito à **disponibilização de treinamento e capacitação** para os servidores e demais colaboradores, já que a coleta de dados – etapa inicial do ciclo de tratamento dos dados pessoais - está presente desde um simples cadastro até a celebração de um contrato, por exemplo.

Neste sentido, propõe-se que servidores que lidam com dados pessoais procedam a cadastramento no site da Escola Nacional de Administração Pública – ENAP, no endereço eletrônico <http://www.enap.gov.br>, para participação nos cursos à distância “Introdução à Lei Brasileira de Proteção de Dados Pessoais”, “Proteção de Dados Pessoais no Setor Público”, “*Fundamentos da Lei Geral de Proteção de Dados*”, sendo este último opcional.

Recomenda-se a leitura do “*Guia de Boas Práticas para implementação e adequação da LGPD na Administração Pública Estadual*” (www.lgpd.ms.gov.br/materiais-disponiveis/), bem como da “*Cartilha LGPD*” (https://www.lgpd.ms.gov.br/wp-content/uploads/2021/11/Cartilha_LGPD-com-links.pdf), para fins de consulta, caso necessário.

Importante, ainda, a participação em cursos específicos sobre proteção de dados pessoais, a exemplo dos oferecidos pelo SERPRO, quais sejam:

-
- G02 - Adequação da Organização à Privacidade e Proteção e Dados Pessoais;
 - G03 - Auditoria e Avaliação de Riscos de Privacidade e Proteção de Dados;
 - G05 - Segurança da informação e Privacidade de Dados Pessoais.

Conveniente mencionar que é necessário continuidade de investimento em cursos neste tema, objetivando que haja o repasse de informações para servidores da CGE e de outros órgãos interessados.

Oportuno destacar, também, que deve ser intensificada a pesquisa referente a **cursos gratuitos, na área de LGPD**.

3.2 Designação de Encarregado pelo Tratamento de Dados Pessoais

Nos termos do art. 41 da LGPD, o controlador deverá indicar encarregado pelo tratamento dos dados pessoais, publicando-se a designação em Diário Oficial do Estado, em atendimento ao princípio da publicidade.

A CGE, em cumprimento ao estabelecido pelo Decreto Estadual nº 15.572/2020, designou a encarregada de dados, por meio da Resolução “P” CGE Nº 45, de 27 de julho de 2021, publicada no D.O.E. nº 10587, de 28/07/2021.

O § 1º do art. 3º do Decreto Estadual se refere especificamente à figura do **encarregado de dados**, cuja identidade e informações de contato “*devem ser divulgadas publicamente, de forma clara e objetiva, no Portal da Transparência, em seção específica sobre tratamento de dados pessoais, como também na página do órgão da Administração Direta, da autarquia ou da fundação do Poder Executivo Estadual na internet*”.

Assim, as informações de contato estão divulgadas no portal www.lgpd.ms.gov.br, bem como no Portal da Transparência (www.transparencia.ms.gov.br) e no sítio eletrônico da CGE/MS (www.cge.ms.gov.br).

Conveniente mencionar que, em atendimento às disposições contidas no Decreto Estadual nº 15.572/2020, com relação a orientar servidores quanto às práticas de proteção de dados pessoais, o encarregado pelo tratamento de dados da CGE pode proceder à elaboração de materiais educativos, com foco nessas questões.

Esta atividade tanto pode ser efetuada de forma autônoma, ou por intermédio de Colegiado, a exemplo do Comitê para implementação de Diretrizes e Plano de Adequação sobre a Lei Geral de Proteção de Dados Pessoais, instituído pela Resolução “P” Conselho de Governança nº 01, de 24 de fevereiro de 2021, e presidido por servidora desta CGE, que elaborou, juntamente com seus pares, **Cartilha** explicativa sobre conceitos, princípios, hipóteses de tratamento referentes à LGPD, bem como a forma de adequação de cada servidor à nova lei.

A Cartilha, disponível no portal www.lgpd.ms.gov.br, desde sua elaboração, tem sido divulgada aos servidores da CGE e de outros órgãos, pela encarregada de dados da CGE, conforme abaixo:

PALESTRAS SOBRE CARTILHA LGPD NO ANO DE 2021			
CGE	05/11/2021	Auditório SEDHAST	25 servidores
SAD	23/11/2021	Sala de reuniões	09 servidores
AGEPREV	30/11/2021	Sala de reuniões	23 servidores
SES	01/12/2021	Encontro Estadual de Auditores de Saúde	120 servidores on line
SEDHAST	03/12/2021	Auditório SEDHAST	50 servidores
PGE	06/12/2021	Auditório PGE	50 servidores
AEMS	07/12/2021	Auditório AEMS	30 servidores
Total			309 servidores

PALESTRAS SOBRE CARTILHA LGPD NO ANO DE 2022			
JANEIRO			
MSGÁS	19/01/2022	Microsoft Teams	80 servidores
FEVEREIRO			
SEDHAST	21/02/2022	Canal Youtube CGE MS	1.690 visualizações (até 31/03/2022)
REDE HEMOSUL	21/02/2022	Canal Youtube CGE MS	638 visualizações (até 31/03/2022)
IAGRO	21/02/2022	Plataforma Cisco Webex	451 servidores
SAD	24/02/2022	Auditório IMASUL	35 servidores
Total			566 servidores e mais 2.328 visualizações

3.3 Comitê de Proteção de Dados Pessoais

O Decreto Estadual (art. 3º, §3º) estabelece que o encarregado pelo tratamento dos dados pessoais deve possuir “*conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente, os relativos a gestão de riscos e governança de dados, com assessoria jurídica e tecnológica*”.

O Guia Orientativo para definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, elaborado pela Autoridade Nacional de Proteção de Dados – ANPD (<https://www.lgpd.ms.gov.br/wp-content/uploads/2021/08/Guia-Agentes-de-Tratamento-LGPD.pdf>) destaca que a LGPD “*não proíbe que o encarregado seja apoiado por uma equipe de proteção de dados*”. Pelo contrário, em atendimento às boas práticas, considera-se que o encarregado disponha de recursos adequados (recursos humanos, infraestrutura, operacionais) para a realização de suas atividades.

Neste sentido, é recomendado que a CGE institua um Comitê, que pode ter caráter permanente, com objetivo de **definir as estratégias e diretrizes de proteção de dados pessoais no órgão**.

O Comitê permanente pode ser presidido pela Controladora-Geral Adjunta, coordenado pela encarregada pelo tratamento de dados pessoais e composto por representantes das demais áreas da CGE/MS.

3.4 Publicidade de informações relativas ao tratamento de dados pessoais

Em atendimento ao Decreto Estadual nº 15.572/2020 (art. 6º, I), é necessário publicar as informações relativas ao tratamento de dados pessoais efetuado pelo Poder Público, dispositivo este originário da LGPD, que estabelece que os órgãos e entidades forneçam “*informações claras e atualizadas sobre a previsão legal, finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades*” (art. 23, I).

O parágrafo 1º do art. 23, LGPD informa que a Autoridade Nacional de Proteção de Dados (ANPD) poderá dispor sobre as formas de publicidade das operações de tratamento.

Nos termos do art. 6º, I, do Decreto Estadual nº 15.572/2020, essas informações devem constar “*preferencialmente nas páginas dos órgãos da Administração Direta, das autarquias e das fundações do Poder Executivo Estadual na internet, bem como no Portal da Transparência, em seção específica a que se refere o § 1º do art. 3º deste Decreto*”.

Desta forma, com relação ao Plano de Adequação, no tocante à **publicidade das informações**, conforme estabelece o art. 6º do Decreto estadual nº 15.572/2020, a identidade e os dados de contato do encarregado devem ser divulgados “*publicamente, de forma clara e objetiva, no Portal da Transparência, em seção específica sobre tratamento de dados pessoais, como também na página do órgão da Administração Direta, da autarquia ou da fundação do Poder Executivo Estadual na internet*” (art. 3º, §1º Decreto Estadual nº 15.572/2020).

Nesse sentido, constitui uma boa prática a disponibilização dessas informações em documentos como a **política de privacidade** ou similar.

Ainda com relação à publicidade no setor público, o art. 6º, inciso III do Decreto Estadual nº 15.572/2020 prevê que os dados devem ser mantidos em “*formato interoperável e estruturado para o uso compartilhado de dados com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral*”.

3.5 Revisão e adequação de Contratos administrativos, Convênios, Parcerias e congêneres

A LGPD estabelece regras para o tratamento de dados pessoais, envolvendo uma série de princípios e procedimentos que devem ser seguidos pelos que realizam coleta de dados pessoais, regras essas que devem ser observadas no momento da contratação, bem como adicionadas às celebrações já efetuadas.

Assim, a revisão e a adequação dos Contratos administrativos, Convênios, Parcerias e congêneres têm caráter imprescindível, já que são responsáveis por nortear as relações com fornecedores e prestadores de serviço em geral, por exemplo.

Uma vez que os dados pessoais são toda e qualquer informação relacionada à pessoa natural identificada ou identificável, sendo que no contrato e congêneres, entre duas pessoas jurídicas, constam os dados pessoais dos representantes, então esses dados devem ser preservados.

É importante que se inicie o processo de adequação desses instrumentos com o mapeamento completo dos contratos que já estejam em vigor. Processo que pode ser trabalhoso, mas é extremamente útil, não só para a LGPD, como para as práticas de *compliance* também.

Neste sentido, a Procuradoria-Geral do Estado - PGE elaborou as Minutas-Padrão de Termo Aditivo e cláusulas gerais para inserção em todos os instrumentos firmados e a serem celebrados pela Administração Pública Estadual, por meio da Resolução PGE/MS 346, de 08/11/2021, contida no link <https://www.lgpd.ms.gov.br/wp-content/uploads/2021/11/Resolucao-PGE-MS-n.346-2021-Minuta-Padrao-Termo-Aditivo-LGPD.pdf>.

3.6 Adequação do Regimento Interno e do Código de Conduta Ética

A Resolução CGE/MS nº 10, de 02 de janeiro de 2019, instituiu o Código de Conduta Ética, instrumento que estabelece diretrizes para adoção de padrões de conduta e comportamento ético, norteados a execução das atividades dos Auditores do Estado e demais servidores em exercício na Controladoria-Geral do Estado – CGE/MS.

A Resolução CGE/MS nº 60, de 03 de fevereiro de 2022, aprovou o Regimento Interno e respectivo organograma da CGE/MS.

Importante observar que os dois normativos necessitam de adequação, com a consequente inserção de dispositivos que estejam em consonância com as orientações da Lei Geral de Proteção de Dados Pessoais – LGPD.

3.7 Mapeamento de Dados Pessoais

Um dos principais passos para adequação à LGPD se dá por meio da análise de todas as operações desenvolvidas pelo órgão, sendo que o mapeamento dos dados pessoais visa identificar:

- ✓ quais dados são coletados;
- ✓ como, quando e por que são coletados;
- ✓ qual é o ciclo de vida dessas informações;
- ✓ qual a hipóteses de tratamento dos dados pessoais;
- ✓ quais os envolvidos no processo;
- ✓ onde e por quanto tempo são armazenados os dados pessoais;
- ✓ como são protegidos os dados;
- ✓ se os dados são compartilhados com terceiros e onde estão localizados esses terceiros;
- ✓ quais os protocolos de segurança para as transferências dos dados.

O mapeamento permite o conhecimento de como os dados pessoais são coletados e que trilha percorrem dentro do órgão/entidade.

Todas as informações coletadas possibilitam a elaboração do **Inventário de Dados Pessoais (IDP)**, que é uma das maneiras de atender ao estabelecido pelo art. 37 da LGPD, a saber: “*o controlador e o operador devem **manter registro** das operações de tratamento de dados pessoais que realizarem (...)*”.

Assim, por meio do Inventário, é analisado o caminho que o dado pessoal percorre desde quando é coletado até o término do tratamento.

O Inventário de Dados Pessoais do Poder Executivo Estadual foi elaborado pelo Comitê para implementação de Diretrizes e Plano de Adequação sobre a Lei Geral de Proteção de Dados Pessoais.

A partir da aprovação, será providenciado o **agendamento de reunião** com as áreas da CGE, objetivando a explicação do IDP, visto que cada área terá que proceder à elaboração do seu. Está prevista, também, a **gravação de um vídeo explicativo** para divulgação da atividade para os órgãos e entidades.

3.8 Mapeamento do fluxo de dados

O entendimento de quais dados pessoais e dados pessoais sensíveis são coletados, armazenados, utilizados, compartilhados e eliminados pelo órgão/entidade propicia a identificação do **fluxo de dados** e o conseqüente conhecimento de suas particularidades.

Assim, é possível reconhecer que dados são manipulados e por onde transitam dentro do órgão/entidade, compondo o ciclo de vida dos dados pessoais, sendo esta uma das etapas de adequação à LGPD.

3.9 Levantamento de Riscos

A realização do Inventário de Dados Pessoais viabiliza a constatação a quais riscos o órgão/entidade está exposto. É relevante a identificação de riscos naturais, tais como humanos, tecnológicos, operacionais, etc). Devem ser analisadas vertentes distintas, abordando aspectos de operacionalização, sistema e privacidade.

Quanto à operacionalização, podem ser identificados, por exemplo, o tratamento irregular de dados, a coleta desnecessária de dados pessoais ou armazenamento inseguro de dados pessoais em meio físico, a contratação de terceiros, entre outros.

Os riscos de segurança e privacidade estão relacionados à vulnerabilidade de sistema, abrangendo temas como controles de acesso lógico, utilização de sistemas de armazenamento suscetíveis à invasão, violação do sistema de segurança, entre outras questões.

Os riscos são analisados de acordo com a **probabilidade** de que venham a acontecer e, em ocorrendo, qual o **impacto** podem causar, podendo ser classificados em grau alto, moderado ou baixo.

3.10 Ações Mitigadoras de Riscos

A LGPD foi instituída com o objetivo de garantir aos titulares maior nível de proteção com referência aos seus dados pessoais. Nestes termos, será exigido dos agentes de tratamento melhor controle e comprometimento na observância dos princípios que regem a lei, além de plena transparência e segurança aos dados pessoais que estão disponibilizados para tratamento.

Importante ressaltar que, ainda que os próprios titulares devam se valer de medidas que diminuam riscos de vazamentos de seus dados, a responsabilidade maior nessa proteção é daqueles que os coletam para realizar o tratamento, ou seja, neste caso, o Poder Público.

Assim, após a elaboração do Inventário de Dados Pessoais e análise dos riscos a que os dados pessoais sob responsabilidade do Poder Público estão expostos, é necessária a correção das vulnerabilidades detectadas.

Um ponto essencial a considerar é a importância de se observar a legislação, de forma que seja fornecida ao titular a segurança que ele espera, com a consequente adoção de mecanismos e procedimentos internos que sejam capazes de minimizar possíveis danos.

Medidas de prevenção e segurança têm papel relevante dentro do contexto da proteção de dados pessoais, uma vez que podem evitar danos ao titular dos dados.

Desta forma, o art. 44 da LGPD julga irregular o tratamento que deixar de cumprir a legislação ou que não levar em consideração, dentre outros aspectos, “*as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado*”.

Porém, a par das **medidas técnicas**, abrangendo aspectos de confidencialidade, integridade e disponibilidade, também deverão ser implementadas **medidas administrativas** tendentes a proteger os dados pessoais de acessos não autorizados e situações causadoras de “*destruição, perda, alteração, comunicação ou difusão.*”

Abaixo constam alguns exemplos de medidas administrativas e técnicas que a CGE/MS poderá adotar para o processo de adequação à LGPD, após análise da área de Tecnologia da Informação:

Medidas administrativas	Medidas técnicas
Conscientização e Treinamento	Controle de acesso, baseado na necessidade de acesso aos dados pessoais
Política de Segurança da Informação	Não compartilhamento de senha entre servidores
Gerenciamento de contratos (termos de confidencialidade)	Minimização da coleta dos dados; não utilização de HD externo ou <i>pendrives</i> ; utilização de cópias de segurança (backup) e uso de criptografia nos dados armazenados
Indicação de Encarregado de Dados	Utilização de protocolos de comunicação seguros – como HTTPS; Utilização de tecnologias de proteção de tráfego, como sistema de firewall, antivírus, <i>antispyware</i> e AntiSpam
	Sistemas e aplicativos sempre atualizados

3.11 Atualização e/ou implementação de sistemas

A LGPD menciona expressamente, no art. 49, que “*os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares*”. Desta forma, sistemas, por conta de possíveis vulnerabilidades, devem manter programas atualizados.

Ademais, considerando que a LGPD prevê vários direitos para os titulares dos dados pessoais, notadamente no **art.18**, é importante que os sistemas sejam adequados de forma a cumprir os requisitos estabelecidos pela lei.

Assim, objetivando o cumprimento da lei, é importante que a CGE/MS providencie a atualização e/ou implementação de sistema ou rotina que possibilite:

- confirmação da existência de tratamento, por intermédio de funcionalidade que propicie a busca de dados pessoais no sistema pelo nome ou CPF, por exemplo;
- acesso aos dados, por meio da geração de relatório, por exemplo, que apresente cópia completo dos dados pessoais de um determinado titular;
- correção de dados, objetivando verificar se o sistema permite atualizar os dados pessoais armazenados;
- anonimização, bloqueio ou eliminação de dados que não estejam de conformidade com a lei, visto que, inclusive, essa atividade pode ser decorrente de determinação da Autoridade Nacional de Proteção de Dados – ANPD;
- portabilidade dos dados pessoais do titular;
- eliminação dos dados pessoais do titular, atendido o interesse público e quando for o caso.

É importante que haja atualização dos sistemas utilizados, de forma a se proteger contra as vulnerabilidades para que os riscos sejam minimizados.

3.12 Política de Segurança da Informação

Política de Segurança da Informação é um documento que contém os padrões, as normas e diretrizes que devem ser seguidas por todos que utilizam a infraestrutura de TI do órgão/entidade, sendo que objetiva a garantia da proteção das informações corporativas contra possíveis ameaças que possam causar qualquer tipo de dano neste sentido.

A Deliberação CETI nº 02, de 24 de fevereiro de 2022, publicada no Diário Oficial do Estado nº 10.767, de 25 de fevereiro de 2022, aprova a **Política de Segurança da Informação do Estado de Mato Grosso do Sul**.

3.13 Política de Privacidade/Notificação de Cookies

Política de privacidade é um documento que informa ao usuário sobre os dados coletados de forma direta ou indireta durante o acesso a um *site*, aplicativo ou sistema.

Esse documento legal divulga as formas de como uma parte coleta, utiliza, divulga e gerencia os dados dos titulares.

A política de privacidade deve conter, basicamente:

- descrição do tratamento dos dados pessoais;
- direitos do titular;
- medidas de segurança;
- responsabilidades da instituição e do titular;
- término do tratamento dos dados pessoais.

Conveniente observar que esse instrumento será providenciado pela Superintendência de Gestão da Informação –SGI, responsável pela coordenação das atividades relativas à Tecnologia da Informação, no que se refere à sistemática, modelos, técnicas e ferramentas utilizadas pelo Estado de Mato Grosso do Sul.

Os **cookies** são pequenos arquivos de texto, utilizados pelos *sites*, principalmente para identificar e armazenar informações sobre os usuários visitantes. Os cookies, por tornar pessoas identificáveis por meio de informações coletadas durante a navegação *online*, até podem, segundo a doutrina, ser considerados como dados pessoais.

Com relação aos **cookies**, estes já foram devidamente providenciados pela Superintendência de Gestão da Informação – SGI e se encontram implantados em todos os portais do Governo do Estado, exceto em sistemas específicos, que sejam geridos por Unidade de Tecnologia da Informação e Comunicação (UTIC) própria do órgão/entidade.

3.14 Processos internos de atendimento às solicitações dos Titulares de Dados Pessoais

O artigo 18 da Lei Geral de Proteção de Dados Pessoais estabeleceu a necessidade de criar processos internos para atendimento do titular, visto que este tem direito a obter do Controlador informações sobre o tratamento de seus dados pessoais.

Nesse contexto, o Decreto Estadual nº 15.572/2020 destinou o Capítulo IV ao atendimento do titular dos dados pessoais. Assim, o art.16 definiu que o apoio será efetuado por meio dos canais de atendimento da Ouvidoria-Geral do Estado ou das Unidades Setoriais e Seccionais de Controle Interno, sendo quem, inclusive, foi inserido o tema “LGPD”, nas opções disponibilizadas aos titulares, em fevereiro/2022.

O acesso pode ser tanto pelo endereço eletrônico www.ouvidorias.ms.gov.br, quanto pelo Portal da Transparência (www.transparencia.ms.gov.br).

No recebimento de demanda por parte do titular, o Ouvidor-Geral do Estado ou o responsável pela Unidade Setorial ou Seccional do órgão/entidade, deve encaminhar ao encarregado do órgão, responsável pelos dados, que acompanhará sua resolutividade.

Desta forma, o encarregado deverá apensar os dados solicitados ao atendimento, sendo que os dados pessoais solicitados deverão ser entregues ao titular ou seu representante legal, por meio eletrônico protegido ou pessoalmente.

3.15 Procedimentos de resposta a incidentes de segurança

O art.46 da LGPD estabelece que “*os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito*”.

A doutrina cita alguns exemplos de incidentes de segurança, quais sejam: acesso a dados pessoais ou sistemas por pessoa não autorizada; exposição acidental de dados pessoais em sites ou comunicados; vazamento ou sequestro de dados pessoais (*ransomware*) após um ataque hacker; eliminação indesejada de dados pessoais; alteração indevida de dados pessoais, por responsabilidade de servidor/colaborador; falhas no sistema que impedem acesso autorizado; desrespeito à política de segurança do órgão, entre outros.

Considerando que a ocorrência de incidente de segurança deve ser comunicada à Autoridade Nacional de Proteção de Dados (ANPD) em prazo razoável e munida de conteúdo mínimo, é imprescindível que a CGE, para garantir a conformidade à LGPD, estabeleça um **Plano de Resposta** que permita lidar com a situação e minimizar os prejuízos aos titulares dos dados, desenvolvendo medidas para solucionar eventuais vazamento de dados.

3.16 Relatório de Impacto à Proteção de Dados Pessoais - RIPD

O **Relatório de Impacto à Proteção de Dados Pessoais – RIPD** é a documentação do Controlador que contém a descrição dos processos de tratamento de dados pessoais que podem causar “*riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco*” (art. 5º, XVII, LGPD).

O art. 38 da LGPD estabelece que 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”.

O Decreto Estadual nº 15.572/2020 (art. 7º, III) informa que a elaboração do RIPD constitui uma das atribuições do Controlador, quando for solicitada pela Autoridade Nacional de Proteção de Dados – ANPD.

3.17 Monitoramento

À medida que as ações forem desenvolvidas, é importante que seja realizado o monitoramento, de forma a verificar o andamento da adequação da CGE/MS às disposições contidas na LGPD e no Decreto Estadual nº 15.572/2020.

3.18 Cronograma de implementação das ações

CRONOGRAMA PLANO DE ADEQUAÇÃO LGPD	
TREINAMENTO/CAPACITAÇÃO	
Cursos ENAP	
ATIVIDADE	PRAZO ATÉ
Introdução à Lei Brasileira de Proteção de Dados Pessoais	maio/2022
Proteção de Dados Pessoais no Setor Público	junho/2022
Fundamentos da Lei Geral de Proteção de Dados (opcional)	dezembro/2022
Cursos SERPRO	
Adequação da Organização à Privacidade e Proteção e Dados Pessoais	a depender de disponibilidade financeira
Auditoria e Avaliação de Riscos de Privacidade e Proteção de Dados	julho/2022
Segurança da informação e Privacidade de Dados Pessoais.	julho/2022
DESIGNAÇÃO DE ENCARREGADO PELO TRATAMENTO DE DADOS PESSOAIS	
Designar o Encarregado de dados da CGE/MS	atendido em 27/07/2021
COMITÊ DE PROTEÇÃO DE DADOS PESSOAIS	
Instituir o Comitê de Proteção de Dados Pessoais na CGE/MS	maio/2022

PUBLICIDADE DE INFORMAÇÕES RELATIVAS AO TRATAMENTO DE DADOS PESSOAIS	
Dar publicidade às informações sobre o tratamento dos dados pessoais realizado pela CGE/MS	agosto/2022 a junho/2023 (depende da instituição da Política de Privacidade)
REVISÃO E ADEQUAÇÃO DE CONTRATOS ADMINISTRATIVOS, CONVÊNIOS, PARCERIAS E CONGÊNERES	
Proceder à adequação dos contratos administrativos da CGE/MS	atividade já iniciada, com previsão de continuidade em 2022
ADEQUAÇÃO DO REGIMENTO INTERNO E DO CÓDIGO DE CONDUTA ÉTICA	
Proceder à adequação do Regimento Interno e Código de Conduta da CGE/MS	junho a outubro/2023
MAPEAMENTO DOS DADOS PESSOAIS	
Agendar reunião com áreas da CGE/MS	maio/2022
Providenciar vídeo explicativo sobre o Inventário de Dados Pessoais	maio a junho/2022
Realizar o Inventário de Dados Pessoais da CGE/MS	maio a dezembro/2022
MAPEAMENTO DO FLUXO DE DADOS	
Mapear o fluxo de dados pessoais/dados pessoais sensíveis da CGE/MS, observado o ciclo de vida dos dados	janeiro a junho/2023
LEVANTAMENTO DE RISCOS	
Identificar riscos relacionados à proteção dos dados pessoais (naturais, humanos, tecnológicos, operacionais, etc)	junho a dezembro/2023
AÇÕES MITIGADORAS DE RISCOS	
Mitigar riscos identificados e propor ações corretivas para sanar falhas referentes à proteção de dados pessoais	dezembro/2023 a abril/2024
ATUALIZAÇÃO DE SISTEMAS	
Atualizar e/ou implementar sistemas ou rotinas, objetivando atendimento titular dos dados pessoais	abril/2024 a outubro/2024
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	
Instituir Política de Segurança da Informação	instituída pela Superintendência de Gestão da Informação – SGI, para todos os órgãos, em março/2022.
POLÍTICA DE PRIVACIDADE / NOTIFICAÇÃO DE COOKIES	
A Política de privacidade será elaborada pela SGI para todos os órgãos. Notificação de cookies foi devidamente implantada pela Superintendência de Gestão da Informação - SGI, para todos os órgãos, de forma preliminar.	agosto/2022 a junho/2023; atendido em janeiro/2022
PROCESSOS INTERNOS DE ATENDIMENTO ÀS SOLICITAÇÕES DOS TITULARES	
Canais de atendimento ao titular, por intermédio do sítio eletrônico www.ouvidorias.ms.gov.br (inserção ícone LGPD)	atendido em fevereiro/2022
PROCEDIMENTOS DE RESPOSTA A INCIDENTES DE SEGURANÇA	
Elaborar plano de resposta e divulgação para o caso de incidentes de segurança (vazamento ou uso irregular) de dados pessoais	dezembro/2023 a abril/2024
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD	

Elaborar RIPD, quando solicitado pela ANPD, ou quando detectada a necessidade	abril a outubro/2024
MONITORAMENTO	
Acompanhar e reportar ao Controlador da CGE/MS	ano de 2022 em diante

Nos termos do art. 5º, inciso VI da Lei Geral de Proteção de Dados Pessoais, na qualidade de Controlador da Controladoria-Geral do Estado, e em atendimento ao inciso III do art. 5º do Decreto Estadual, aprovo o presente **Plano de Adequação da CGE/MS** e o respectivo cronograma

Campo Grande/MS, 27 de abril de 2022.

Carlos Eduardo Girão de Arruda
Controlador-Geral do Estado de MS