DECRETO Nº 49.265, DE 6 DE AGOSTO DE 2020.

Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais).

O GOVERNADOR DO ESTADO, no uso das atribuições que lhe são conferidas pelos incisos II e IV do art. 37 da Constituição Estadual,

CONSIDERANDO que os dados pessoais integram o âmbito de proteção dos direitos fundamentais de liberdade, de privacidade, de intimidade e do livre desenvolvimento da personalidade da pessoa natural ou jurídica;

CONSIDERANDO a promulgação da Lei Federal nº 13.709, de 14 de agosto de 2018, que estabeleceu a Lei Geral de Proteção de Dados Pessoais – LGPD;

CONSIDERANDO que, nos termos do parágrafo único do art. 1º da Lei Geral de Proteção de Dados Pessoais, as normas de proteção relativas ao tratamento de dados pessoais são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios,

DECRETA:

CAPÍTULO I
DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída a Política Estadual de Proteção de Dados Pessoais – PEPDP, conjunto de diretrizes, normas e ações para o desenvolvimento e a adaptação da ação governamental à Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito da Administração Pública Estadual direta, autárquica e fundacional do Poder Executivo Estadual.

Parágrafo único. A Política Estadual de Proteção de Dados Pessoais observará a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

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

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

IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; e

X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Art. 2º São diretrizes da Política Estadual de Proteção de Dados Pessoais:

I - as regras de boas práticas e governança estabelecidas pelo controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular;

II - alinhamento às políticas de segurança da informação do Estado de Pernambuco;

III - o atendimento simplificado e eletrônico das demandas do cidadão;

IV - o alinhamento e o equilíbrio com a promoção da transparência pública, em específico com a Lei nº 14.804, de 29 de outubro de 2012;

V - o estabelecimento da proporcionalidade das medidas acerca de proteção de dados, privacidade e segurança da informação;

VI - o desenvolvimento do nível de maturidade dos tratamentos dos dados;

VII - a manutenção da segurança jurídica dos instrumentos firmados;

VIII - a economicidade das ações;

IX - o alinhamento ao planejamento estratégico do Estado; e

X - a aderência à Política de Tecnologia da Informação e Comunicação do Estado, instituída pela Lei nº 12.985, de 2 de janeiro de 2006.

Art. 3º Para fins deste Decreto, considera-se:

I - dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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;

III - 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;

IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;

V - titular: pessoa natural a quem se referem os dados pessoais que são objetos de tratamento;

VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

VIII - encarregado: pessoa indicada pelo controlador e operador corporativo para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX - agentes de tratamento: o controlador e o operador; e

X - tratamento: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

CAPÍTULO II
DAS POLÍTICAS DE ATUAÇÃO CONJUNTA

Art. 4º A Política Estadual de Proteção de Dados Pessoais – PEPDP será implementada através do Plano Quadrienal Estratégico de Proteção de Dados Pessoais – PPDP que estabelecerá as prioridades estaduais quanto à adequação à Lei Federal nº 13.709, de 2018, contribuindo para aumentar a efetividade na integração das ações e a conformidade da ação governamental.

§ 1º O Plano Quadrienal de que trata o *caput* será executado pelos órgãos e entidades da Administração Pública Estadual direta, autárquica e fundacional e terá acompanhamento anual de indicadores de desempenho.

§ 2º As empresas públicas e as sociedades de economia mistas estabelecerão suas políticas de proteção de dados pessoais por ato próprio aprovado pelos seus respectivos conselhos de administração.

Art. 5º A Política Estadual de Proteção de Dados Pessoais e o Plano Quadrienal Estratégico de Proteção de Dados Pessoais não alcançam tratamentos relacionados a:

I - segurança pública;

II - defesa nacional;

III - segurança do Estado;

IV - atividades de investigação e repressão a infrações penais; ou

V - origem de fora do território nacional e que 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 Federal nº 13.709, de 2018.

Art. 6º Os órgãos e as entidades da Administração Pública Estadual direta, autárquica e fundacional deverão estabelecer suas respectivas Políticas de Proteção de Dados Pessoais Locais – PPDPL a serem aprovadas pelo dirigente máximo.

§ 1º As Políticas de Proteção de Dados Pessoais Locais – PPDPL deverão considerar as prioridades previstas no Plano Quadrienal Estratégico de Proteção de Dados Pessoais – PPDP e deverão estabelecer, no mínimo:

I - princípios, diretrizes e prioridades locais da proteção de dados pessoais;

II - responsabilidades e papéis pela proteção de dados pessoais;

III - processo de gerenciamento de riscos;

IV - controles internos de proteção de dados pessoais; e

V - ações mitigadoras dos riscos identificados.

§ 2º Os dirigentes máximos agregarão objetivos e metas próprias de acordo com a maturidade e capacidade operacional do ente público.

CAPÍTULO III
DA GOVERNANÇA DA POLÍTICA ESTADUAL DE PROTEÇÃO DE DADOS PESSOAIS

Art. 7º Compete ao Comitê Executivo de Governança Digital – CEGD, instituído pelo art. 2-B da Lei nº 12.985, de 2 de janeiro de 2006:

I - aprovar normas de proteção de dados pessoais a serem regulamentadas por portaria do Secretário da Controladoria-Geral do Estado;

II - aprovar o Plano Quadrienal Estratégico de Proteção de Dados Pessoais; e

III - aprovar o parecer sobre os resultados da auditoria interna sobre a adequabilidade dos órgãos e entidades quanto à aderência à Política Estadual de Proteção de Dados Pessoais.

Art. 8º Compete ao Comitê Técnico de Governança Digital – CTGD, instituído pelo art. 2-D da Lei nº 12.985, de 2006:

I - monitorar o desempenho e riscos produzidos pela Política de Proteção de Dados Pessoais Locais para que os tratamentos adotem as lições aprendidas no ciclo anual e alcancem a padronização, a redução do custeio, a automação e a celeridade necessária às mudanças da legislação e ao cenário das ameaças cibernéticas;

II - assessorar a Secretaria da Controladoria-Geral do Estado no acompanhamento da Política Estadual de Proteção de Dados Pessoais com informações que apoiem decisões e orientem ações estratégicas;

III - deliberar a adoção de padrões para serviços e produtos que apoiem os controladores nas decisões referentes ao tratamento de dados pessoais;

IV - decidir sobre as questões de integração e de articulação entre os diversos órgãos e entidades da Administração Pública Estadual para o desenvolvimento e a operacionalização das ações de adequação à Lei Federal nº 13.709, de 2018;

V - apoiar a promoção da proteção dos dados pessoais com a divulgação de ações entre os seus membros e a criação de grupos de estudos sobre boas práticas em política de proteção de dados; e

VI - aprovar a padronização de cláusulas contratuais técnicas para fins de compartilhamento e tratamento de dados pessoais.

Art. 9º Compete à Secretaria da Controladoria-Geral do Estado:

I - coordenar e orientar a rede de encarregados responsáveis pela implementação da PEPD;

II - elaborar o Plano Quadrienal Estratégico de Proteção de Dados Pessoais, considerando a inclusão de objetivos e de metas comuns aos controladores públicos;

III - consolidar os resultados e apoiar o monitoramento da Política Estadual de Proteção de Dados Pessoais;

IV - disponibilizar canal de atendimento ao titular, considerando as atividades desempenhadas pela Ouvidoria-Geral do Estado;

V - coordenar a qualidade do atendimento ao titular do dado;

VI - produzir e manter atualizados manuais de implementação das Políticas de Proteção de Dados Pessoais Locais e modelos de documentos, bem como capacitações para os agentes públicos; e

VII - estabelecer sistemática de auditoria interna com vistas a aumentar e proteger o valor organizacional do Estado, fornecendo avaliação, assessoria e conhecimento objetivos baseados em riscos.

Art. 10. Compete à Agência de Tecnologia da Informação – ATI:

I - orientar a aplicação de soluções de TIC relacionadas à proteção de dados pessoais;

II - adequar as arquiteturas e as operações compartilhadas de TIC hospedadas no datacenter e na rede corporativa às exigências da Lei Federal nº 13.709, de 2018; e

III - propor padrões de desenvolvimento de novas soluções de TIC, considerando a proteção de dados pessoais, desde a fase de concepção do produto e serviço até a sua execução.

Parágrafo único. As arquiteturas e as operações de que trata o inciso II poderão ter seu escopo alterado por meio de acordo entre as partes responsáveis pelo compartilhamento.

Art. 11. Compete à Procuradoria-Geral do Estado:

I - disponibilizar aos agentes de tratamento e ao encarregado consultoria jurídica para dirimir questões e emitir pareceres do significado e alcance da Lei Federal nº 13.709, de 2018;

II - disponibilizar modelos de contratos, convênios e acordos de cooperação internacional aderentes à Lei Federal nº 13.709, de 2018, a serem utilizados pelos agentes de tratamento; e

III - disponibilizar modelo de termo de uso de sistema de informação da Administração Pública.

Art. 12. Compete ao controlador de cada órgão e entidade:

I - aprovar, prover condições e promover ações para efetividade da Política de Proteção de Dados Pessoais Locais;

II - nomear encarregado para conduzir a Política de Proteção de Dados Pessoais Locais, através de ato próprio;

III - elaborar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade; e

IV - fornecer aos operadores termos de uso, manuais de instruções e treinamento dos tratamentos sob sua responsabilidade.

§ 1º Os atos administrativos do controlador público são atribuídos ao cargo público de mais alta hierarquia.

§ 2º A nomeação do encarregado deverá atender prerrogativas e qualificações necessárias ao exercício dessa função.

§ 3º O encarregado deve estar subordinado diretamente ao controlador público, devendo ter experiência em gestão, com assessoria jurídica e tecnológica, e poderes para tratar questões que afetem os operadores.

Art. 13. Compete ao encarregado e sua equipe de apoio:

I - gerenciar a Política de Proteção de Dados Local para:

a) inventariar os tratamentos do controlador, inclusive os eletrônicos;

b) analisar a maturidade dos tratamentos em face dos objetivos e metas estabelecidos e do consequente risco de incidentes de privacidade;

c) avaliar 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;

d) adotar as providências cabíveis para implementar as medidas de segurança avaliadas; e

e) cumprir os objetivos e metas previstas na Política de Proteção de Dados Pessoais Locais.

II - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, em articulação com a Ouvidoria de cada órgão e entidade;

III - receber comunicações da Agência Nacional de Proteção de Dados Pessoais - ANPD e adotar providências;

IV - orientar os funcionários e os contratados no cumprimento das práticas necessárias à privacidade de dados pessoais;

V - quando provocado, entregar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade;

VI - atender às normas complementares da Agência Nacional de Proteção de Dados Pessoais; e

VII - informar à Agência Nacional de Proteção de Dados Pessoais e aos titulares dos dados pessoais eventuais incidentes de privacidade de dados pessoais, dentro da execução de um plano de respostas a incidentes.

CAPÍTULO IV
DO ATENDIMENTO AO TITULAR

Art. 14. O atendimento ao titular do dado será prestado de forma eletrônica nos canais eletrônicos de atendimento da Ouvidoria-Geral Estado.

§ 1º A identificação do titular ou procurador deverá ser idônea, emitida por autoridade certificadora da ICP-Brasil, ou através de identidade digital expedida pelo Instituto de Identificação Tavares Buril – IITB.

§ 2º O canal de atendimento deve prover funções de registro e gerenciamento para servir ao acompanhamento dessa forma de atendimento.

Art. 15. O atendimento ao titular poderá ser prestado de forma presencial na entidade onde os dados se encontram, desde que haja a conferência de documento oficial e infraestrutura adequada.

§ 1º Quando o titular for incapaz, o atendente deve conferir a certidão de nascimento do titular e o documento de identidade de um dos pais ou responsáveis legais.

§ 2º Atestada a legitimidade do titular ou de seu procurador, o atendente coletará dados de identificação e de contato do solicitante, protocolará e transcreverá a solicitação através dos canais de atendimento da Ouvidoria-Geral do Estado.

§ 3º O atendimento presencial ao procurador ou curador somente será aceito através do instrumento de outorga.

Art. 16. A Ouvidoria-Geral Estado encaminhará o atendimento ao encarregado responsável pelos dados e acompanhará sua resolutividade.

§ 1º O encarregado deverá adotar as providências para apensar os dados solicitados ao atendimento.

§ 2º Os dados pessoais solicitados no atendimento deverão ser entregues ao titular ou seu representante legal, através de meio eletrônico protegido ou pessoalmente.

Art. 17. Em qualquer forma de atendimento, o encarregado observará que as informações pessoais produzidas pelo órgão ou entidade não devem ser providas quando estiverem vinculadas a tratamento sigiloso nos termos da legislação vigente.

Parágrafo único. O encarregado informará o fundamento legal que fundamenta o indeferimento de entrega da informação sigilosa solicitada.

CAPÍTULO V
DO TRATAMENTO DE DADOS PESSOAIS

Art. 18. O tratamento de dados pessoais deve ser restrito à sua finalidade, executado de forma adequada e pelo prazo necessário.

§ 1º A finalidade prevista no *caput* não exige a coleta do consentimento do titular, exceto quando se tratar de pessoa incapaz.

§ 2º A adequação a que se refere o *caput* deve obedecer à Política Estadual de Segurança da Informação.

§ 3º A necessidade de armazenamento dos dados pessoais observará as obrigações legais ou judiciais de mantê-los protegidos.

§ 4º Os responsáveis pelos tratamentos devem registrar as operações realizadas com dados pessoais.

§ 5º O controlador deve adotar medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis no âmbito e nos limites técnicos de seus serviços, para não serem acessados por terceiros não autorizados e, sempre que possível, proceder à sua anonimização.

CAPÍTULO VI
DO COMPARTILHAMENTO DE DADOS PESSOAIS

Art. 19. O compartilhamento de dados pessoais entre controladores públicos poderá ser realizado nas seguintes hipóteses:

I - execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres; e

II - cumprir obrigação legal ou judicial.

§ 1º O controlador deve manter o registro do compartilhamento dos dados pessoais para efeito de comprovação prevista no inciso VII do art. 18 da Lei Federal nº 13.709, de 2018.

§ 2º Os dados deverão ser mantidos em formato interoperável e estruturado.

Art. 20. O compartilhamento entre controladores públicos não poderá ser realizado quando envolver dados pessoais sensíveis referentes à saúde.

Parágrafo único. Excetuam-se as hipóteses relativas à prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, desde que observado o § 5º do art. 11 da Lei Federal nº 13.709, de 2018, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados.

Art. 21. O compartilhamento entre controladores públicos e privados autorizados pela legislação vigente deve ser comunicado à Autoridade Nacional de Proteção de Dados, exceto quando:

I - os dados forem acessíveis publicamente, observadas as disposições da Lei Federal nº 13.709, de 2018 e deste Decreto;

II - houver previsão legal ou a transferência for respaldada em contratos, convênios ou instrumentos congêneres;

III - objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades; ou

IV - nos casos de execução descentralizada de atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado, observado o disposto na Lei Federal nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação).

Art. 22. A Secretaria da Controladoria-Geral do Estado editará normas e procedimentos complementares para o fiel cumprimento das metas e diretrizes estabelecidas na Política Estadual de Proteção de Dados Pessoais.

Art. 23. Este Decreto entra em vigor na data de sua publicação.

Palácio do Campo das Princesas, Recife, 6 de agosto do ano de 2020, 204º da Revolução Republicana Constitucionalista e 198º da Independência do Brasil.

PAULO HENRIQUE SARAIVA CÂMARA
Governador do Estado

ÉRIKA GOMES LACET
JOSÉ FRANCISCO DE MELO CAVALCANTI NETO
ERNANI VARJAL MEDICIS PINTO