Boletim n.º 028/2020

Secretaria da Controladoria Geral do Estado

GOVERNO DO ESTADO PERNAMBUCO MAIS TRABALHO, MAIS FUTURO.

Decreto nº 49.265/20 - Institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709/18 (Lei de Proteção de Dados Pessoais).

Data: 27/08/2020

Política de Proteção de Dados Pessoais – Aspectos Gerais e Política de Governança

A Secretaria da Controladoria-Geral do Estado – SCGE, através da Diretoria de Orientação ao Gestor e Informações Estratégicas – DOGI/ Coordenadoria de Orientação e Contas do Governo (COR), no exercício de sua função, vem, por meio deste boletim, esclarecer a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual em consonância com a Lei Federal nº 13.709/18, instituída pelo Decreto nº 49.265/20, **no que tange às disposições preliminares, políticas de atuação conjunta e governança da política estadual de proteção de dados**.

Inicialmente, a Política Estadual de Proteção de Dados Pessoais (PEPDP) aplica-se à **Administração Direta, Autarquias e Fundações** do Poder Executivo Estadual, no qual se 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. (Grifei).

Em consonância a tais princípios, em seu artigo 2º, o referido Decreto lista as 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. (grifos nossos).

DAS POLÍTICAS DE ATUAÇÃO CONJUNTA

A Política Estadual de Proteção de Dados Pessoais – PEPDP será implementada através do **Plano Quadrienal Estratégico de Proteção de Dados Pessoais – PPDP**, o qual deverá estabelecer as prioridades estaduais em relação à adequação à Lei Federal nº 13.709, de 2018, no intuito de contribuir para aumentar a efetividade na integração das ações e a conformidade da ação governamental.

O **Plano Quadrienal** terá acompanhamento anual de indicadores de desempenho, ficando a sua execução sob a responsabilidade dos órgãos e entidades da Administração Pública Estadual direta, autárquica e fundacional. Noutra parte, caberá às **empresas públicas e as sociedades de economia mista** estabelecerem suas políticas de proteção de dados pessoais por **ato próprio aprovado** pelos seus respectivos **Conselhos de Administração**.

Da mesma forma, 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**, no qual serão definidas, no mínimo, as seguintes diretrizes:

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**. (Grifei)

DA GOVERNANÇA DA POLÍTICA ESTADUAL DE PROTEÇÃO DE DADOS PESSOAIS

No âmbito da Governança da Política Estadual de Proteção de Dados pessoais, destacam-se as seguintes estruturas:

I - Comitê Executivo de Governança Digital – CEGD;

II - Comitê Técnico de Governança Digital – CTGD;

III - Secretaria da Controladoria-Geral do Estado - SCGE;

IV - Agência de Tecnologia da Informação – ATI;

V - Procuradoria-Geral do Estado - PGE;

VI - Controlador de cada órgão e entidade;

VII - Encarregado e sua equipe de apoio.

O **CEGD** tem a competência de aprovar normas de proteção de dados pessoais a serem regulamentadas pela SCGE; aprovar o Plano Quadrienal Estratégico de Proteção de Dados Pessoais; bem como 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.

Já a **CTGD**, dentre outras, compete 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; deliberar a **adoção de padrões para serviços e produtos** que apoiem os Controladores nas decisões referentes ao tratamento de dados pessoais; bem como 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.

A **SCGE**, dentre outras, tem a competência de **coordenar e orientar a rede de Encarregados** responsáveis pela implementação da PEPD; elaborar o Plano Quadrienal Estratégico de Proteção de Dados Pessoais; disponibilizar **canal de atendimento ao titular**[1], considerando as atividades desempenhadas pela Ouvidoria-Geral do Estado e estabelecer sistemática de auditoria interna com vistas a aumentar e proteger o valor organizacional do Estado, fornecendo **avaliação, assessoria e conhecimentos objetivos baseados em**

1 pessoa natural a quem se referem os dados pessoais que são objetos de tratamento.

riscos.

A **ATI** tem a prerrogativa de orientar a aplicação de soluções de TIC relacionadas à proteção de dados pessoais; adequar as arquiteturas e as operações compartilhadas de TIC hospedadas no datacenter e na rede corporativa; e **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.

Quanto à **PGE** compete-lhe disponibilizar aos agentes de tratamento e ao encarregado consultoria jurídica para dirimir questões e emitir pareceres do significado e alcance da Lei Federal nº 13.709/18; disponibilizar **modelos de contratos, convênios e acordos de cooperação internacional** aderentes à Lei Federal nº 13.709/18, a serem utilizados pelos agentes de tratamento; e disponibilizar modelo de termo de uso de sistema de informação da Administração Pública.

Ao **Controlador[2] de cada órgão e entidade**, dentre outras, compete aprovar, prover condições e promover ações para efetividade da Política de Proteção de Dados Pessoais Locais; bem como 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.

Por fim, ao **Encarregado[3] e sua equipe de apoio** compete gerenciar a Política de Proteção de Dados Local; receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, em articulação com a Ouvidoria de cada órgão e entidade; e orientar os funcionários e os contratados no cumprimento das práticas necessárias à privacidade de dados pessoais

Demais orientações que se façam necessárias, a DOGI/COR coloca-se à disposição através do sítio eletrônico: www.scgeorienta.pe.gov.br.

2 pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

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

3 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).

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.