SECRETARIA DA CONTROLADORIA GERAL DO ESTADO

GOVERNO DE PERNAMBUCO
ESTADO DE MUDANÇA

PORTARIA SCGE Nº 41, DE 07 DE JULHO DE 2023.

A **SECRETÁRIA DA CONTROLADORIA-GERAL DO ESTADO**, no uso de suas atribuições que lhe foram conferidas pela Lei nº 18.139, de 18 de janeiro de 2023 e em atendimento aos artigos 9º e 22 do Decreto Estadual nº 49.265, de 06 de agosto de 2020, que institui a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual,

RESOLVE:

Art. 1º Aprovar a atualização das diretrizes a serem observadas pelos órgãos da Administração Pública Estadual direta, autárquica e fundacional, no tocante ao Projeto de Adequação à Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), na forma estabelecida no anexo único desta, disponível no endereço eletrônico https://www.scge.pe.gov.br/legislacao/.

Art. 2º Fica revogada a PORTARIA SCGE nº 1, de 05 de janeiro de 2021.

Art. 3º Esta Portaria entra em vigor na data de sua publicação.

ÉRIKA GOMES LACET

Secretária da Controladoria-Geral de Pernambuco

ANEXO ÚNICO

Art. 1º Os órgãos e entidades da Administração Pública Estadual direta, autárquica e fundacional deverão desenvolver Projeto de Adequação à Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD) a ser conduzido pelo encarregado indicado pelo controlador, considerando as seguintes medidas:

I – ALINHAMENTO ESTRATÉGICO: sensibilização da alta direção do órgão ou entidade sobre a importância da adequação institucional à LGPD e sobre o papel exercido pelo encarregado de dados pessoais;

II – DIAGNÓSTICO PRELIMINAR DE PROTEÇÃO DE DADOS: avaliação que tem como objetivo fornecer à Alta Gestão dos órgãos e entidades as informações necessárias para obter uma visão sistêmica sobre a adequação do Órgão ou Entidade às regras dispostas na LGPD e, também, possibilitar a identificação e a priorização dos processos em relação às atividades de maior relevância no tocante à proteção de dados pessoais;

III – ELABORAÇÃO DO INVENTÁRIO DE DADOS PESSOAIS: registro das operações de tratamento dos dados pessoais realizados pelo Órgão ou Entidade;

IV – AVALIAÇÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE: processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, de identificação dos principais riscos enfrentados, de análise dos controles internos estabelecidos e de aferição dos níveis de risco residual expressos em termos da combinação das consequências e de suas probabilidades;

V – ELABORAÇÃO DO PLANO DE IMPLEMENTAÇÃO DOS CONTROLES: elaboração de proposta de novos controles internos, por meio da definição de atividades, planos, métodos, indicadores e procedimentos interligados para tratar a causa e/ou a consequência do evento de risco;

VI – ADEQUAÇÃO DOS INSTRUMENTOS CONTRATUAIS E CONGÊNERES: ação de adequação à LGPD dos instrumentos contratuais e parcerias dos provedores de serviços de Tecnologia da Informação e Comunicação (TIC) e demais prestadores de serviços, que vierem a tratar dado pessoal em nome do Órgão ou da Entidade;

VII – ELABORAÇÃO DE POLÍTICA DE PRIVACIDADE E TERMOS DE USO: produção dos Termos de Uso estabelecendo as obrigações e condições de uso de determinado serviço oferecido ao Titular pelo Órgão ou Entidade, e das Políticas de Privacidade, indicando ao cidadão como o Órgão ou Entidade trata seus dados pessoais ao longo de todo o ciclo de vida do dado;

VIII – ELABORAÇÃO DO PLANO DE GESTÃO DE INCIDENTES COM DADOS PESSOAIS: produção do plano de resposta a incidentes para tratar ocorrências de situações que venham a lesar a segurança de dados pessoais mantidos sob a responsabilidade do Órgão ou Entidade;

IX – FOMENTO À CULTURA DE PROTEÇÃO DE DADOS: desenvolvimento de ações institucionais de conscientização voltadas para servidores, operadores de dados, fornecedores e demais partes interessadas quanto à relevância da adequada proteção dos dados pessoais tratados pelo Órgão ou Entidade;

X – ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS: elaboração de documento contendo 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 riscos;

XI – TRANSPARÊNCIA DA PROTEÇÃO DE DADOS PESSOAIS: disponibilização das informações sobre as políticas e práticas relacionadas ao gerenciamento de dados pessoais para consulta pelos Titulares de dados;

XII – CONSTRUÇÃO DA TABELA DE RETENÇÃO DE DADOS PESSOAIS: desenvolvimento da tabela de ciclo de vida do dado pessoal associado a sua finalidade.

§1º. As medidas apresentadas no caput não devem ser consideradas em sequência e devem ser adaptadas à realidade de cada Órgão ou Entidade.

§2º. O diagnóstico preliminar a que se refere o inciso II do presente artigo, deverá considerar, em sua elaboração, aspectos qualitativos e quantitativos a serem definidos pelo Encarregado de Proteção de Dados, de modo que, ao final, os processos sejam agrupados na seguinte ordem de priorização:

I – Processos prioritários: serão avaliados imediatamente;

II – Processos relevantes: serão avaliados no ciclo de avaliação subsequente;

III – Processos não-prioritários: serão avaliados em até dois ciclos de avaliação, ou quando couber.

Art. 2º O monitoramento da efetivação da Política Estadual de Proteção de Dados Pessoais - PEPDP a ser realizado pela SCGE, será executado considerando as seguintes perspectivas:

I – CONFORMIDADE: Adequação da atividade institucional às exigências legais e normativas no tocante à proteção de dados pessoais;

II – DESEMPENHO: Avaliação qualitativa do atendimento ofertado pelo Órgão ou Entidade aos Titulares de dados pessoais, bem como a aferição da efetividade do gerenciamento dos riscos de segurança da informação e privacidade organizacionais identificados.

Art. 3º O monitoramento da PEPDP sob a pespectiva da conformidade deverá considerar a maturidade do Órgão ou Entidade em relação à maneira como é conduzida a gestão de seus processos de negócio.

§1º. O nível de maturidade da gestão de processos do Órgão ou Entidade deverá ser examinado considerando os seguintes níveis:

I – NÍVEL 1: O Órgão ou Entidade que não tem os seus processos de negócios mapeados para basear sua atuação nas competências previstas em Lei ou normativo vigente que disponha sobre a estrutura e o funcionamento do Poder Executivo estadual, ou na constatação direta das funções administrativas básicas, tais como "Gestão de Pessoas", "Compras", "Patrimônio", “Recursos Humanos;

II – NÍVEL 2: O Órgão ou Entidade que ainda não tem seus processos de negócio mapeados, contudo, as atribuições e funcionamento dos órgãos integrantes estão instituídas em regulamento próprio, conforme disposto no parágrafo único do art. 14 da Lei Complementar nº 49/2003, de 31 de janeiro de 2003;

III – NÍVEL 3: Os processos de negócio da UG encontram-se formalmente mapeados e modelados, ou seja, é possível encontrar documentos que demonstram, de forma objetiva e lógica, como o trabalho é (ou deve ser) realizado;

IV – NÍVEL 4: Os processos de negócio do Órgão ou Entidade encontram-se formalmente mapeados e são monitorados por meio de indicadores de desempenho;

V – NÍVEL 5: Os processos do Órgão ou Entidade encontram-se mapeados, são monitorados por meio de indicadores de desempenho, encontram-se automatizados e são continuamente otimizados.

Art. 4º A perspectiva de conformidade do Órgão ou Entidade será aferida semestralmente pelo Encarregado, a partir de um questionário autoavaliativo elaborado pela SCGE, que considere pontos de controle elaborados de acordo com os 5 (cinco) níveis de maturidade de gestão de processos apresentados nesta portaria.

§1º A Secretaria da Controladoria-Geral do Estado - SCGE divulgará, no seu sítio institucional, preferencialmente até o último dia útil dos meses de fevereiro e agosto de cada exercício, os pontos de controle que serão considerados na autoavaliação.

§2º As Unidades de Controle Interno, instituídas conforme o Decreto Estadual nº 47.087, de 01 de fevereiro de 2019, devem prestar apoio técnico ao Encarregado na autoavaliação da conformidade dos seus respectivos Órgãos e Entidades.

§3º Os pontos de controle e o resultado da autoavaliação previstos não isentam os Órgãos e Entidades a se adequarem às outras determinações da LGPD.

Art. 5º A perspectiva de desempenho do Órgão ou Entidade será aferida semestralmente pelo Encarregado a partir da aferição dos seguintes indicadores

gerenciais::

I – Indicadores de Atendimento aos titulares de dados:

a. Percentual de controladores que disponibilizam tratamentos com atendimentos eletrônicos;

b. Evolução do total de consultas efetuadas nos canais de atendimento da ouvidoria;

c. Principais controladores consultados;

d. Principais espécies de consulta;

e. Evolução do total detalhado das reclamações e queixas apresentados;

f. Percentual de demandas respondidas fora do prazo legal.

II – Indicadores de Risco:

a. Percentual de tratamentos com maior grau de risco;

b. Percentual de sistemas de informação que sofreram incidentes de segurança;

c. Principais espécies de incidentes de segurança, tempo de solução e medidas adotadas.

§1º. As Ouvidorias dos órgãos e entidades devem prestar apoio técnico ao encarregado na aferição dos indicadores da perspectiva de desempenho, quando cabível.

§2º. A lista apresentada neste artigo não é taxativa, de modo que a SCGE poderá elaborar outros indicadores gerenciais, quando necessário.

Art. 6º O Encarregado de cada Órgão ou Entidade deverá encaminhar à SCGE, os resultados do desenvolvimento da Política de Proteção de Dados Pessoais Local - PPDPL, sempre que solicitado, contendo:

I – Detalhamento das atividades desenvolvidas e controles implantados;

II – Status das ações mitigadoras dos riscos identificados;

III – Resultados da autoavaliação da conformidade institucional;

IV – Resultados da Perspectiva Desempenho.

Art. 7º O Encarregado de cada Órgão ou Entidade enviará à SCGE, o Relatório de Impacto de Proteção aos Dados Pessoais – RIPDP conforme modelo disponibilizado em sítio desta Secretaria.

Art. 8º O Encarregado de cada Órgão ou Entidade deverá comunicar à SCGE, a ocorrência de incidentes de segurança com dados pessoais que possam acarretar riscos ou danos relevantes aos titulares, ocorridos dentro de sua Unidade Gestora.

Art. 9º A SCGE realizará auditorias internas com objetivo de avaliar a adequabilidade das PPDPLs e dos resultados apresentados na autoavaliação de forma amostral.

Art. 10. Em razão do caráter estratégico, e por conterem vulnerabilidades que poderiam ser exploradas com a sua publicação indevida, as informações contidas nos inventários de segurança, nos relatórios executivos da governança, bem como, nos indicadores de atendimento e de riscos devem ser classificadas como sigilosas a cada ciclo de monitoramento.

Art. 11. No decorrer do ciclo anual, a SCGE disponibilizará no seu sítio institucional a relação de encarregados e os contatos institucionais.

Art. 12. O ciclo anual de monitoramento da Política Estadual de Proteção de Dados Pessoais - PEPDP terá seu início em janeiro e término em dezembro de cada ano.

Documento assinado eletronicamente por **Erika Gomes Lacet**, em 07/07/2023, às 11:24, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.pe.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **38467637** e o código CRC **A24831FF**.

SECRETARIA DA CONTROLADORIA GERAL DO ESTADO

Rua Santo Elias, 535, - Bairro Espinheiro, Recife/PE - CEP 52020-095, Telefone: 3183-0800