

## **POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS LOCAL - PPDPL DA SECRETARIA DE PLANEJAMENTO E GESTÃO DE PERNAMBUCO**

### **CAPÍTULO I DISPOSIÇÕES PRELIMINARES**

Art. 1º A Política de Proteção de Dados Pessoais Local - PPDPL tem por finalidade estabelecer os princípios, diretrizes e responsabilidades mínimas a serem observados e seguidos para a proteção dos dados pessoais aos planos estratégicos, programas, projetos e processos da Secretaria de Planejamento e Gestão de Pernambuco (Seplag/PE).

Parágrafo único. A PPDPL será composta por este instrumento normativo e pelo Plano de Implementação de Controle.

Art. 2º A PPDPL e suas eventuais normas complementares, metodologias, manuais e procedimentos aplicam-se a todos os setores da Seplag/PE, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de dados pessoais, estendendo-se àqueles que realizem tratamento de dado pessoal em nome da Seplag/PE.

### **CAPÍTULO II DOS PRINCÍPIOS E OBJETIVOS**

Art. 3º As atividades de proteção de dados pessoais no âmbito da Seplag/PE, bem como seus instrumentos resultantes, devem se guiar pelos seguintes princípios, além dos previstos no Decreto Estadual nº 49.265, de 6 de agosto de 2020:

- I - aderência à integridade e aos valores éticos no tratamento de dados pessoais;
- II - suporte de tecnologia da informação adequado para apoiar os processos de adaptação dos tratamentos de dados pessoais;
- III - disseminação de informações necessárias ao fortalecimento da cultura do tratamento de dados pessoais em respeito à Lei Federal nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais - LGPD;
- IV - realização de avaliações periódicas internas para verificar a eficácia da proteção de dados pessoais, comunicando o resultado aos responsáveis pela adoção de ações corretivas, inclusive à alta administração;
- V - estruturação do conhecimento e das atividades em metodologias, normas, manuais e procedimentos; e
- VI - aderência dos métodos e modelos de tratamento de dados às exigências regulatórias da LGPD.

Art. 4º A PPDPL tem por objetivos:

- I - proporcionar a adequação das atividades desenvolvidas pela Seplag/PE à LGPD e

regulamentos emitidos pela Autoridade Nacional de Proteção de Dados - ANPD, em consonância com o atingimento dos objetivos estratégicos;

II - produzir informações íntegras, confiáveis e completas das demandas dos titulares do dado;

III - salvaguardar o direito à proteção dos dados pessoais dos titulares;

IV - possibilitar a adequada apuração dos responsáveis, em todos os níveis, que tenham acesso inadequado aos dados pessoais, em especial aqueles considerados sensíveis, considerando o disposto na Lei Estadual nº 6.123, de 20 de julho de 1968 (Estatuto do Servidor Público Estadual);

V - reduzir os riscos relacionados a incidentes envolvendo dados pessoais, com a implantação de medidas de controle de segurança da informação; e

VI - orientar e servir de diretriz para os agentes de tratamento.

### **CAPÍTULO III DAS DIRETRIZES**

Art. 5º São diretrizes da PPDPL:

I - a gestão da integridade com a promoção da cultura ética focada na preservação da privacidade;

II - o fortalecimento da integridade institucional, a partir do diagnóstico de vulnerabilidades na segurança da informação;

III - a capacitação adequada do encarregado e sua equipe de apoio e dos agentes de tratamento;

IV - o fortalecimento dos mecanismos de comunicação de possíveis incidentes deve ser pautado pela tempestividade, pela implementação de melhorias de segurança e pela obtenção de informações sobre as origens da vulnerabilidade; e

V - a gestão de riscos será sistematizada e suportada pelas premissas de metodologias técnicas.

Parágrafo único. O modelo de gestão de gerenciamento de riscos deve seguir o método de priorização de processos, considerando sua relevância e impacto na estratégia da Seplag/PE.

### **CAPÍTULO IV DOS INSTRUMENTOS**

Art. 6º São instrumentos da PPDPL:

I - a metodologia: o modelo de gestão de riscos deve ser estruturado com base nas boas práticas produzidas pela *International Organization for Standardization*, em especial as ISO

31000, 31010, 27001, 27002, 27004, 27005, 27701, 29100;

II - a capacitação continuada: o Plano Anual de Capacitação, incluindo o eixo temático de Segurança da Informação e Proteção de Dados Pessoais;

III - a normatização: legislação, manuais e procedimentos formalmente definidos, em especial, no âmbito da Seplag/PE; e

IV - a solução tecnológica: o processo de gestão de riscos deve ser apoiado por adequado suporte de tecnologia da informação.

## **CAPÍTULO V DAS INSTÂNCIAS DE SUPERVISÃO, COMPOSIÇÃO E DAS ATRIBUIÇÕES E RESPONSABILIDADES**

### **Seção I Do Controlador, Encarregado e Operadores**

Art. 7º A Seplag/PE é a controladora dos dados pessoais por ela tratados, nos termos de suas competências legal e institucional.

Art. 8º A Secretaria Executiva de Coordenação Geral (Secoge), enquanto representante legal, terá responsabilidade pela definição final da gestão dos riscos e controles internos quanto à adequação à LGPD na Seplag/PE, nos termos do art. 12 do Decreto Estadual nº 49.265, de 2020.

Art. 9º O encarregado é responsável pelo gerenciamento do projeto de implantação e dos riscos e controles internos quanto à adequação da Seplag/PE à LGPD, conforme art. 13 do Decreto Estadual 49.265, de 2020.

Parágrafo único. Para assessorar o encarregado da Seplag/PE, as seguintes unidades devem ser consideradas como equipe de apoio: a Gerência de Assuntos Jurídicos (GAJ), a Gerência de Controle Interno (GCI), a Gerência de Tecnologia da Informação (GTI), o Instituto de Gestão Pública de Pernambuco Governador Eduardo Campos (IGPE) e a Ouvidoria.

Art. 10. Os provedores de serviços de Tecnologia da Informação e Comunicação (TIC) e demais prestadores de serviços à Seplag/PE, que vierem a tratar dado pessoal em nome desta, poderão ser considerados operadores e deverão aderir a esta Política, além de cumprir os deveres legais, contratuais e de parceria respectivos, dentre os quais se incluirão, mas não se limitarão aos seguintes:

I - assinar contrato ou termo de compromisso com cláusulas específicas sobre proteção de dados pessoais requeridas pela Seplag/PE;

II - apresentar evidências e garantias suficientes de que aplica adequado conjunto de medidas técnicas e administrativas de segurança, para a proteção dos dados pessoais, segundo a legislação, os instrumentos contratuais e de compromissos;

III - manter os registros de tratamento de dados pessoais que realizar, assim como aqueles compartilhados, com condições de rastreabilidade e de prova eletrônica a qualquer

tempo;

IV - seguir fielmente as diretrizes e instruções transmitidas pela Seplag/PE;

V - facultar acesso a dados pessoais somente para o pessoal autorizado que tenha estrita necessidade e que tenha assumido compromisso formal de preservar a confidencialidade e segurança de tais dados, devendo tal compromisso estar disponível em caráter permanente para exibição à Seplag/PE, mediante solicitação;

VI - permitir a realização de auditorias da Seplag/PE e disponibilizar toda a informação necessária para demonstrar o cumprimento das obrigações estabelecidas;

VII - auxiliar, em toda providência que estiver ao seu alcance, no atendimento pela Seplag/PE de obrigações perante Titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII - comunicar formalmente e de imediato à Seplag/PE a ocorrência de qualquer risco, ameaça ou incidente de segurança que possa acarretar comprometimento ou dano potencial ou efetivo a Titular de dados pessoais, evitando atrasos por conta de verificações ou inspeções; e

IX - descartar de forma irrecuperável, ou devolver para a Seplag/PE, todos os dados pessoais e as cópias existentes, após a satisfação da finalidade respectiva ou o encerramento do tratamento por decurso de prazo ou por extinção de vínculo legal ou contratual.

## **Seção II Instituições**

Art. 11. O Comitê de Privacidade será designado por meio de portaria do Dirigente Máximo.

Art. 12. O Gestor de Processos corresponde a todo e qualquer responsável pela unidade de execução de um determinado processo de trabalho, inclusive sobre a gestão de riscos.

## **Seção III Das Atribuições e Responsabilidades**

Art. 13. Compete à Secoge, enquanto representante legal:

I - aprovar práticas e princípios de conduta e padrões de tratamento de dados pessoais;

II - aprovar as alterações da PPDPL;

III - decidir sobre o Plano de Implementação de Controles Internos;

IV - aprovar a estrutura, extensão e conteúdo do Inventário de Dados;

V - realizar os ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL;

VI - acompanhar o diagnóstico preliminar de controles internos;

VII - tomar conhecimento do andamento e resultados da avaliação de controles internos;

VIII - tomar ciência do monitoramento do PPDPL;

IX - aprovar e promover o Plano de Tratamento de Incidentes com Dados Pessoais; e

X - aprovar o Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica do órgão.

Art. 14. Compete ao Comitê de Privacidade:

I - apoiar a promoção da disseminação da cultura de proteção de dados pessoais; e

II - apoiar e monitorar o Plano de Implementação de Controles Internos.

Art. 15. Compete ao encarregado:

I - propor práticas e princípios de conduta e padrões de tratamento de dados pessoais;

II - elaborar alterações da PPDPL;

III - consolidar propostas de ações, avaliar e elaborar o Plano de Implementação de Controles Internos;

IV - elaborar a estrutura, extensão e conteúdo do Inventário de Dados;

V - promover a aderência às regulamentações, leis, códigos, normas e padrões na condução da PPDPL;

VI - recomendar ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL;

VII - definir o diagnóstico preliminar de controles internos;

VIII - instituir e acompanhar a avaliação de controles internos;

IX - monitorar a PPDPL;

X - elaborar o Plano de Tratamento de Incidentes com Dados Pessoais;

XI - 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;

XII - cumprir os objetivos e metas previstas na Política de Proteção de Dados Pessoais Local;

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

XIV - receber comunicações da ANPD e adotar providências;

XV - orientar os funcionários e os operadores no cumprimento das práticas necessárias à proteção de dados pessoais;

XVI - 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;

XVII - atender às normas complementares da ANPD; e

XVIII - 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 Tratamento de Incidentes com Dados Pessoais.

Art. 16. Compete à GAJ:

I - prestar orientação jurídica ao encarregado e aos operadores sobre aplicação da LGPD e dos normativos dela decorrentes;

II - elaborar os ajustes contratuais e de termos de compromisso decorrentes da implementação da PPDPL, em conjunto com o gestor do contrato; e

III - prestar consultoria jurídica na elaboração de normativos e instrumentos internos, em especial Termos de Uso e Termos de Consentimento, quanto à proteção de dados pessoais.

Art. 17. Compete à GTI:

I - prestar orientação técnica ao encarregado e aos operadores sobre questionamentos e boas práticas em segurança da informação;

II - apoiar as ações de capacitação nas áreas de Segurança da Informação e Proteção de Dados Pessoais;

III - realizar, em conjunto com a GCI, o IGPE e o Gestor de Processo, o diagnóstico preliminar;

IV - realizar, em conjunto com a GCI, o IGPE e o Gestor de Processo, a avaliação de controles internos dos processos priorizados;

V - apoiar, com propostas técnicas de segurança da informação, a elaboração do Plano de Tratamento de Incidentes com Dados Pessoais;

VI - apoiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais;

VII - extrair estrutura e conteúdo de dados pessoais em sistemas informatizados para elaboração do Inventário de Dados;

VIII - extrair conteúdo de dados pessoais em sistemas informatizados para atendimentos das demandas dos titulares;

IX - apoiar, com propostas técnicas de segurança da informação, a elaboração de instrumentos, em especial contratos e congêneres; e

X - apoiar a elaboração do Plano de Implementação de Controles Internos.

Art. 18. Compete à GCI:

I - propor melhorias metodológicas no gerenciamento dos riscos associados à proteção de dados pessoais;

II - realizar, em conjunto com a GTI, o IGPE e o Gestor de Processo, o diagnóstico preliminar;

III - realizar, em conjunto com a GTI, o IGPE e o Gestor de Processo, a avaliação de controles internos dos processos priorizados;

IV - apoiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais; e

V - apoiar a elaboração do Plano de Implementação de Controles Internos.

Art. 19. Compete à Ouvidoria:

I - apoiar no recebimento de manifestações e comunicações dos titulares de dados pessoais;

II - realizar a interlocução do titular de dados pessoais com o encarregado;

III - mapear as principais possíveis demandas do titular de dado pessoal, considerando o Inventário de Dados;

IV - apoiar o encarregado na propositura de ações que facilitem o atendimento às demandas dos titulares de dados pessoais; e

V - promover a transparência dos tratamentos de dados pessoais sob a responsabilidade da Seplag/PE.

Art. 20. Compete ao IGPE:

I - prover a capacitação dos agentes públicos no exercício do cargo, função e emprego no conteúdo de proteção de dados pessoais;

II - mapear processos e propor melhorias contínuas; e

III - propor o desenvolvimento de soluções tecnológicas para melhoria do tratamento de dados pessoais e segurança da informação em conjunto com a GTI.

Art. 21. Compete aos Gestores de Processos:

I - realizar, em conjunto com a GTI, a GCI e IGPE, o diagnóstico preliminar;

II - realizar, em conjunto com a GTI, a GCI e IGPE, a avaliação de controles internos dos processos prioritizados;

III - elaborar propostas de ação ao Plano de Implementação de Controles dos processos sob sua responsabilidade;

IV - cumprir os objetivos e as prioridades estabelecidas pelo Plano de Implementação de Controles;

V - gerenciar as ações do Plano de Implementação de Controles e avaliar os seus resultados dos processos sob sua responsabilidade;

VI - disponibilizar o conteúdo de dados pessoais para elaboração do Inventário de Dados;

VII - disponibilizar conteúdo de dados pessoais para atendimentos das demandas dos titulares;

VIII - cumprir as recomendações e observar as orientações emitidas pela Secoge e pelo encarregado; e

IX - adotar princípios de conduta e padrões de comportamento no âmbito da sua estrutura organizacional.

## **CAPÍTULO VI DO TRATAMENTO DE DADOS PESSOAIS**

Art. 22. O tratamento de dados pessoais pela Seplag/PE será realizado para o atendimento de sua finalidade pública, na persecução do interesse público, com o objetivo de executar suas competências legais e de cumprir as atribuições legais do serviço público.

Parágrafo único. O Regulamento (Decreto nº 30.433, de 15 de maio de 2007) da Seplag/PE e demais normas de organização definem as funções e atividades que constituem as finalidades e balizadores do tratamento de dados pessoais para fins desta Política.

Art. 23. Em atendimento a suas competências legais, a Seplag/PE poderá, no estrito limite de suas atividades, tratar dados pessoais com dispensa de obtenção de consentimento pelos respectivos titulares.

Parágrafo único. Eventuais atividades que transcendam o escopo da função institucional estarão sujeitas à obtenção de consentimento dos titulares dos dados pessoais a serem objeto de tratamento.

Art. 24. A Seplag/PE manterá contratos com terceiros para o fornecimento de produtos ou a prestação de serviços necessários a suas operações, os quais poderão, conforme o caso, importar em disciplina própria de proteção de dados pessoais, a qual deverá estar disponível e ser consultada pelos interessados.

Art. 25. Os dados pessoais tratados pela Seplag/PE são:

I - protegidos por procedimentos internos para registrar autorizações e utilizações;

II - mantidos disponíveis, exatos, adequados, pertinentes e atualizados, devendo ser retificado ou eliminado o dado pessoal mediante informação, constatação de impropriedade ou solicitação de remoção, devendo a neutralização ou descarte do dado observar as condições e períodos da tabela de temporalidade de retenção de dados;

III - compartilhados somente para o exercício das funções institucionais ou para atendimento de políticas públicas aplicáveis; e

IV - revistos em periodicidade mínima bianual, devendo ser de imediato eliminados aqueles que já não forem necessários, por terem cumprido sua finalidade ou por ter se encerrado o seu prazo de retenção.

Art. 26. A responsabilidade da Seplag/PE pelo tratamento de dados pessoais estará circunscrita ao dever de se ater ao exercício de sua competência legal e institucional e de empregar boas práticas de governança e de segurança.

### **DAS DISPOSIÇÕES FINAIS**

Art. 27. Em função da complexidade e abrangência, a implementação desta Política será realizada de forma gradual e continuada por meio do Plano de Implementação de Controles, a ser elaborado em 120 (cento e vinte) dias a contar da publicação desta Política, com prazo de conclusão de 48 (quarenta e oito meses).

Parágrafo único. O Plano de Implementação de Controles deverá ser revisado anualmente e poderá sofrer alterações de ofício, após validação da Secoge, a partir da redefinição de prioridades por parte da Política Estadual de Proteção de Dados Pessoais, conforme § 1º do art. 6º do Decreto Estadual 49.265, de 2020.

Art. 28. O Plano de Implementação de Controles aprovado pelo Secretário deverá ser inserido e gerenciado na solução tecnológica de gestão de riscos com adequado suporte do setor responsável.

Art. 29. Os casos omissos ou excepcionalidades serão deliberados pela Secoge, consultado o Comitê de Privacidade.