ANEXO ÚNICO

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS LOCAL - PPDPL DA SECRETARIA DA CONTROLADORIA-GERAL DO ESTADO DE PERNAMBUCO

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º A Política de Proteção de Dados Pessoais Local - PPDPL-SCGE 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 da Controladoria-Geral do Estado – SCGE e será composta pelo disposto neste documento, bem como pelo Plano de Implementação de Controle.

Art. 2º A PPDPL-SCGE e suas eventuais normas complementares, metodologias, manuais e procedimentos aplicam-se a todos os setores da SCGE, abrangendo os servidores, prestadores de serviço, colaboradores, estagiários, consultores externos e quem, de alguma forma, desempenhe atividades de tratamento de dados pessoais em nome desta Secretaria.

CAPÍTULO II
DOS PRINCÍPIOS E OBJETIVOS

Art. 3º As atividades de proteção de dados pessoais no âmbito da SCGE, bem como seus instrumentos resultantes, devem se guiar pelos seguintes princípios, além dos previstos no Decreto Estadual nº 49.265, de 06 de agosto de 2020:

I - aderência à integridade e aos valores éticos no tratamento de dados pessoais;

II - adequado suporte de tecnologia da informação 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;

VI - aderência dos métodos e modelos de tratamento de dados às exigências regulatórias da LGPD.

Art. 4º A PPDPL-SCGE tem por objetivos:

I - proporcionar a adequação das atividades desenvolvidas pela SCGE à LGPD e regulamentos emitidos pela Autoridade Nacional de Proteção de Dados Pessoais - 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 no Decreto Estadual nº 40.271, de 09 de janeiro de 2014 (Código de Ética da SCGE) e a 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-SCGE:

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, implementação de melhorias de segurança e obtenção de informações sobre as origens da vulnerabilidade;

V – a disponibilização de informações ao titular primada pela atuação transparente e garantia da disponibilização do dado de forma clara, precisa e adequada, conforme legislação vigente; e,

VI - a gestão de riscos 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 Secretaria.

Art. 6º O método de priorização de processos seguirá a seguinte disposição:

I – Processos prioritários: serão avaliados imediatamente e reavaliados bianualmente;

II – Processos relevantes: serão avaliados no ano subsequente e reavaliados a cada três anos;

III – Processos não-prioritários: serão avaliados em dois anos e reavaliados a cada quatro anos.

Parágrafo único. A classificação de priorização será dada pela aprovação do Conselho Deliberativo de Gestão – CDG desta Secretaria, e terá metodologia própria.

CAPÍTULO IV
DOS INSTRUMENTOS

Art. 7º São instrumentos da PPDPL-SCGE:

I - as Instâncias de Supervisão: Secretário da Controladoria Geral do Estado;

II - a metodologia: o modelo de gestão de riscos da Secretaria deve ser estruturado com base do *Committee of Sponsoring Organizations of the Treadway Commission* - COSO e nas boas práticas produzidas pela *International Organization for Standardization*, em especial, as ISO 31000, 31010, 27001, 27002, 27004, 27005, 27701, 29100;

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

IV - as normas, manuais e procedimentos: as normas, manuais e procedimentos formalmente definidos e aprovados pelo Conselho Deliberativo de Gestão - CDG; e

V - 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. 8º A Secretaria da Controladoria-Geral do Estado é a controladora dos dados pessoais por ela tratados, nos termos das suas competências legal e institucional.

Art. 9º O Secretário da Controladoria-Geral do Estado, enquanto representante legal,

terá responsabilidade pela definição final da gestão dos riscos e controles internos quanto à adequação à LGPD na Secretaria, nos termos do art. 12 do Decreto Estadual nº 49.265, de 06 de agosto de 2020.

Art. 10. A Assessoria Técnica - AST, enquanto encarregado para fins da LGPD, terá responsabilidade pelo gerenciamento do projeto de implantação e dos riscos e controles internos quanto à adequação à LGPD na Secretaria, conforme art. 13 do Decreto Estadual nº 49.265, de 06 de agosto de 2020.

Parágrafo Único. O encarregado da SCGE será assessorado por equipe de apoio, formada pelas seguintes áreas: Gerência da Assessoria Técnica de Apoio à Procuradoria-Geral do Estado, Assessoria Especial de Controle Interno - AECI, Ouvidoria da SCGE, Diretoria de Tecnologia e Informação do Controle Interno - DTCI e Diretoria de Planejamento e Gestão - DPGE.

Art. 11. Os provedores de serviços de Tecnologia da Informação e Comunicação (TIC) e demais prestadores de serviços à Secretaria da Controladoria-Geral do Estado que tratarem dado pessoal em nome desta serão considerados operadores e deverão atender 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 SCGE;

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 emitidas pela SCGE;

V - permitir 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 SCGE, mediante solicitação;

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

VII - auxiliar, sempre que necessário, no atendimento pela SCGE de obrigações perante titulares de dados pessoais, autoridades competentes ou quaisquer outros legítimos interessados;

VIII - comunicar formalmente e de imediato à SCGE 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 SCGE 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. 12. O Conselho Deliberativo de Gestão - CDG, instituído pelo Decreto nº 49.993, de 18 de dezembro de 2020, é órgão colegiado de natureza consultiva e deliberativa, conforme seu Regimento Interno, aprovado pela Portaria SCGE nº 045, de 21 de dezembro de 2020.

Art. 13. 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. 14. Compete ao Secretário da Controladoria-Geral do Estado, enquanto representante legal:

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

II - aprovar as alterações da PPDPL-SCGE;

III - deliberar 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-SCGE;

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-SCGE;

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

X - 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.

Art. 15. Compete ao encarregado:

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

II – propor alterações da PPDPL-SCGE;

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-SCGE;

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

VI - definir o diagnóstico preliminar de controles internos;

VII - instituir e acompanhar a avaliação de controles internos;

VIII - monitorar o PPDPL-SCGE;

IX - elaborar o Plano de Gestão de Resposta a Incidentes com Dados Pessoais;

X – subsidiar a elaboração do Relatório de Impacto de Proteção aos Dados Pessoais, na forma da lei, com o apoio técnico das áreas jurídica e tecnológica da entidade;

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

XII - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências, em articulação com a Ouvidoria;

XIII - receber comunicações da Autoridade Nacional de Proteção de Dados Pessoais - ANPD e adotar providências;

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

XV - 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;

XVI - atender às normas complementares da Autoridade Nacional de Proteção de Dados Pessoais; e

XVII - informar à Autoridade 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 Gerência da Assessoria Técnica de Apoio à Procuradoria-Geral do Estado - GAP:

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-SCGE, em conjunto com a DPGE; 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 Diretoria de Tecnologia da Informação do Controle Interno - DTCI:

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 Assessoria Especial de Controle Interno - AECI e o Gestor de Processo, o diagnóstico preliminar;

IV - realizar, em conjunto com a AECI 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 instrumentos, em especial contratos e congêneres; e

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

Art. 18. Compete à Assessoria Especial de Controle Interno - AECI:

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

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

III - realizar, em conjunto com a DTCI 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 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, em conjunto com a Autoridade de Monitoramento de que trata o § 1º do artigo 20 da Lei Estadual nº 14.804, de 29 de outubro de 2012, a transparência dos tratamentos de dados pessoais sob a responsabilidade da SCGE.

Art. 20. Compete à Diretoria de Planejamento e Gestão - DPGE:

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

II – prover, em conjunto com a Escola de Controle Interno Prof. Francisco Ribeiro, a capacitação dos agentes públicos no exercício do cargo, função e emprego no conteúdo de proteção de dados pessoais;

III - elaborar os ajustes contratuais e termos de compromisso decorrentes da implementação da PPDPL-SCGE, em conjunto com a Gerência da Assessoria Técnica de Apoio à Procuradoria-Geral do Estado; e

IV - praticar outros atos de natureza técnica e administrativa necessários ao exercício de suas responsabilidades.

Art. 21. Compete aos Gestores de Processos:

I - realizar, em conjunto com a DTCI e a AECI, o diagnóstico preliminar;

II - realizar, em conjunto com a DTCI e a AECI, a avaliação de controles internos dos processos priorizados;

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 às demandas dos titulares;

VIII - cumprir as recomendações e observar as orientações emitidas pelo Secretário da Controladoria-Geral do Estado e pelo encarregado; e

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

Art. 22. Compete ao Comitê Deliberativo de Gestão - CDG:

I – colaborar para a aprovação de alterações da PPDPL-SCGE, quando for o caso;

II – acompanhar o diagnóstico preliminar de controles internos;

III – opinar sobre o Plano de Implementação de Controles Internos

IV - acompanhar, em conjunto com o Secretário, o diagnóstico preliminar de controles internos;

V – deliberar sobre a priorização de processos;

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

VII - tomar ciência do monitoramento do PPDPL-SCGE;

VIII – tomar ciência acerca do conteúdo do Inventário de Dados; e

IX – opinar sobre o Plano de Gestão de Resposta a Incidentes com Dados Pessoais e o Relatório de Impacto de Proteção aos Dados Pessoais;

CAPÍTULO VI
DO TRATAMENTO DE DADOS PESSOAIS

Art. 23. O tratamento de dados pessoais pela SCGE 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 da SCGE, aprovado pelo Decreto nº 47.667, de 1º de julho de 2019, 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. 24. Em atendimento a suas competências legais, a SCGE 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. 25. A SCGE 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. 26 Os dados pessoais tratados pela SCGE deverão ser:

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

II - mantidos disponíveis, exatos, adequados, pertinentes e atualizados, sendo retificado ou eliminado o dado pessoal mediante informação ou constatação de impropriedade ou face à solicitação de descarte, 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, sendo 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. 27. A responsabilidade da SCGE 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.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 28. Em função da complexidade e abrangência, a implementação desta Política será realizada de forma gradual e continuada através do Plano de Implementação de Controles, a ser elaborado em 120 (cento e vinte) dias, contados da publicação **da Portaria que aprovar o presente documento**, 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 do Secretário da

Controladoria-Geral do Estado, a partir da redefinição de prioridades por parte da Política Estadual de Proteção de Dados Pessoais, conforme § 1º do art.6º do Decreto Estadual nº 49.265, de 06 de agosto de 2020.

Art. 29. 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. 30. Os casos omissos ou excepcionalidades serão deliberados pelo Secretário, consultado o Conselho Deliberativo de Gestão - CDG.