MAPA - GUIA DE PONTOS DE CONTROLE

NÍVEL 1

Secretaria da Controladoria Geral do Estado

GOVERNO DO ESTADO
PERNAMBUCO
MAIS TRABALHO, MAIS FUTURO.

LGPD Pernambuco

EXPEDIENTE

GOVERNO DO ESTADO DE PERNAMBUCO

PAULO HENRIQUE SARAIVA CÂMARA
Governador do Estado

LUCIANA BARBOSA DE OLIVEIRA SANTOS
Vice-Governadora do Estado

MARCONI MUZZIO PIRES DE PAIVA FILHO
Secretário da Controladoria-Geral do Estado
Ouvidor-Geral do Estado

FILIPE CAMELO DE CASTRO
Secretário-Executivo da Controladoria-Geral do Estado

CARMEN RAQUEL NUNES SILVA
Diretora de Tecnologia da Informação do Controle Interno – DTCI

RENATO BARBOSA CIRNE
Coordenador de Proteção de Dados

FLÁVIO ROBERTO DOS SANTOS PEREIRA
Diretor de Auditoria - DAUD

Elaboração:

RENATO BARBOSA CIRNE
Gestor Governamental - Controle Interno

KARLOS GUSTAVO ARAGÃO BUNGENSTAB
Gestor Governamental - Controle Interno

LEANDRA SOUZA LEÃO DE AGUIAR
Gestora Governamental - Controle Interno

www.scge.pe.gov.br | www.transparencia.pe.gov.br
www.ouvidoria.pe.gov.br | www.lai.pe.gov.br
instagram: @scge_pe

SECRETARIA DA CONTROLADORIA-GERAL DO ESTADO
Rua Santo Elias, 535 - Espinheiro - Recife - PE - CEP.: 52020-095
Telefone: (081) 3183-0800

SUMÁRIO

APRESENTAÇÃO

A Lei Geral de Proteção de Dados - LGPD, Lei nº 13.709/18, é a legislação federal que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado. A LGPD tem como objetivo dar poderes à pessoa natural quanto ao tratamento dos seus dados pessoais, e para isso, apresenta regramentos específicos em sinergia com normativos internacionais de proteção de dados pessoais.

Como é um tema complexo e recente, algumas matérias da Lei necessitam de complementação através de regulamentação ou serão objeto de opiniões técnicas ou recomendações. Para efetivação do cumprimento da LGPD, o estado de Pernambuco instituiu o Decreto Estadual n° 49.265/2020, que atribuiu à Secretaria da Controladoria-Geral do Estado (SCGE) o papel de produzir e manter atualizados manuais e cartilhas de implementação das Políticas de Proteção de Dados Pessoais Locais e modelos de documentos, bem como de capacitar os agentes públicos e de coordenar a qualidade do atendimento ao titular do dado.

Para viabilizar a aplicação da Política Estadual de Proteção de Dados Pessoais, foram criados documentos de autoavaliação institucional, sendo um deles o Mapa de Pontos de Controle, material utilizado para a avaliação da conformidade com as exigências legais e normativas de proteção de dados. O Mapa considera 5 (cinco) níveis de maturidade de gestão de processos, dado os seguintes objetos de Avaliação de Controles, previstos no inciso III do art. 1° da Portaria SCGE nº 01, de 05 de janeiro de 2021, vide:

- Nível 1: competências estabelecidas na lei vigente que dispõe sobre a estrutura e o funcionamento do Poder Executivo e funções administrativas básicas, tais como Gestão de Pessoas, Compras, Patrimônio e Tecnologia da Informação;

• Nível 2: atribuições instituídas em regulamento, conforme parágrafo único do art. 14 da Lei Complementar nº 49, de 31 de janeiro de 2003;

• Nível 3: processos modelados, ou seja, uma visão lógica das atividades que demonstre, de forma simples e intuitiva, como o trabalho é (ou deve ser) realizado;

• Nível 4: processos com indicadores de desempenho;

• Nível 5: processos otimizados e automatizados.

Este Guia apresenta os controles de Nível 1, demonstrando os detalhes de cada ponto de controle, além de referenciar cada ponto com normas de padrão internacional (como a ISO) e normativos nacionais. Adicionalmente são destacadas as evidências de auditoria, que apresentam quais documentos são objeto de verificação para cumprimento dos pontos de controle. O material é recomendado para encarregados, equipe de controle interno e demais servidores interessados em proteção de dados pessoais.

LISTA DE SIGLAS

SIGLA	DESCRIÇÃO
ABPMP	*Association of Business Process Management Professionals*
ANPD	Autoridade Nacional de Proteção de Dados
BPM	*Business Process Management*
DP	Dado Pessoal
LAI	Lei de Acesso à Informação
SI&P	Segurança da Informação e Privacidade
LGPD	Lei Geral de Proteção de Dados Pessoais
PEPDP	Política Estadual de Proteção de Dados Pessoais
PPDPL	Política de Proteção de Dados Pessoais Local
SCGE	Secretaria da Controladoria-Geral do Estado

Detalhamento dos pontos de controle contidos na autoavaliação institucional - Nível 1

A seguir, serão apresentados os detalhamentos dos pontos de controle atualmente vigentes para realização da autoavaliação institucional, indicando as boas práticas, os requisitos e evidências aplicáveis ao nível 1 de monitoramento.

1. Já existe um encarregado de proteção de dados designado por Portaria?

A indicação do encarregado de proteção de dados é uma das ações primordiais para a adequação do órgão público à LGPD.

Dentre as principais funções do encarregado, destacam-se a de apoiar a política de proteção de dados, promover a orientação dos servidores nas questões de privacidade e proteção de dados e implementar o inventário de dados para determinar como os dados pessoais são utilizados pela organização.

Outra característica relevante é o papel de comunicação, atribuição que pode ser vislumbrada na própria definição da LGPD ao encarregado, vide: o encarregado é a pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador/operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD) (art. 5º, VIII, LGPD). A mesma Lei determina que a indicação de encarregado é um requisito para as pessoas jurídicas de direito público realizarem o tratamento de dados (art. 23, III, LGPD).

Pelos deveres significativos para a proteção de dados, o encarregado precisa ser designado formalmente no órgão/entidade e deve ter apoio das áreas de tecnologia da informação e jurídica. Adicionalmente, é necessário que o encarregado tenha o patrocínio da gestão estratégica do órgão para possibilitar o desenvolvimento efetivo da política de proteção de dados. Conforme inciso II do art. 12 do Decreto Estadual nº 49.265/2020, a designação do encarregado deverá ser feita por ato próprio do dirigente máximo. Ou seja, a designação deverá ser dada por Portaria do dirigente máximo de cada órgão ou entidade.

A SCGE disponibiliza o Modelo de Portaria de Designação de Encarregado no seu site institucional.

Requisito: Parte do Item 5.5.1 e itens 6.3.1.3 e 6.3.1.4 e Controles A.6.1.3 e A.6.1.4 da ISO 27001/2013; Item 7.1 da ISO 27001/2013; e, Inciso II do art. 12 do Decreto Estadual nº 49.265/2020

Evidência: Portaria de Designação.

2 - O encarregado de proteção de dados possui os conhecimentos especializados da LGPD?

Dentre as atribuições do encarregado previstas na LGPD, a de maior impacto na organização é a de orientar os funcionários e os contratados da entidade a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

Para ajudar o encarregado nessa missão, a SCGE promove curso ativo no Centro de Formação dos Servidores e Empregados Públicos do Estado de Pernambuco – CEFOSPE, denominado de Introdução à Lei Geral de Proteção de Dados (LGPD), assim como a Escola Nacional de Administração Pública - Enap

É de suma importância que o encarregado visite regularmente o site da Autoridade Nacional de Proteção de Dados (ANPD), pois lá são lançados guias orientativos e instruções técnicas sobre proteção de dados, a exemplo, do Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado, que esclareceu pontos ausentes na LGPD acerca das obrigações com os operadores, além de reforçar o entendimento sobre Controladoria Conjunta, tema retratado de maneira insuficiente na Lei.

Para além dos cursos acima mencionados, o acompanhamento dos boletins e informativos da SCGE e do site da ANPD, é recomendável a realização de outras capacitações, a fim de complementar os requisitos fundamentais de conformidade com a LGPD. Neste sentido, é de fundamental importância que o encarregado aprimore os seus conhecimentos sobre a Lei de Acesso à Informação (LAI), Marco Civil da Internet, noções de gestão de riscos e processos e à segurança da informação e da privacidade.

Aconselha-se que o encarregado ainda tenha conhecimento das normas técnicas e controles da *International Organization for Standardization* (ISO), em especial àquelas referentes a riscos, segurança da informação, tratamento de dados pessoais e privacidade:

- ISO 27001 - Sistemas de Segurança da Informação - Requisitos
- ISO 27002 - Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação
- ISO 27004 - Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação
- ISO 27005 - Tecnologia da informação - Técnicas de segurança - Gerenciamento de risco de segurança da informação
- ISO 27701 - Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes
- ISO - 29100 - Tecnologia da informação — Técnicas de segurança — Estrutura de privacidade
- ISO 31000 - Gestão de Riscos
- ISO 31010 - Avaliação de Riscos

A lista acima não é exaustiva e a LGPD como tema atual deverá passar por modificações, o que requer atualização constante do encarregado.

Requisito: Item 5.5.2 da ISO 27701/2019 e Item 7.2.b e c da ISO 27001/2013; e, Inciso IV do art. 12 do Decreto Estadual nº 49.265/2020.

Evidência: Declaração de experiência profissional, certificações, diplomas.

3 - O encarregado de proteção de dados está vinculado diretamente ao dirigente máximo?

Compete ao encarregado funções que requerem amplo acesso à estrutura organizacional para possibilitar uma avaliação sistêmica da conformidade do órgão ou entidade com a LGPD.

Cabe à alta administração garantir que o encarregado detenha liberdade para executar as suas funções, orientar as partes interessadas e determinar as ações necessárias no desempenho da LGPD. Ademais, a gestão estratégica precisa providenciar suporte de infraestrutura, recursos financeiros, cursos de aprendizado e acompanhar em períodos programados a adequação do órgão ou entidade à LGPD.

Requisito: §§ 2º e 3º do art. 12 do Decreto Estadual nº 49.265/2020.
ISO 27701 - Requisito 6.3.1.1 - Responsabilidades e papéis da segurança da informação.

Evidência: Organograma, regulamento, manual de serviços ou documento oficial similar que contenha as atribuições do encarregado.

4 - O encarregado de proteção de dados foi designado para as tarefas atribuídas pelo Decreto Estadual nº 49.265/20?

É recomendável que o órgão ou entidade insira as atribuições do encarregado, previstas no Decreto Estadual nº 49.265/20, nas suas respectivas Política de Proteção de Dados Pessoais Local. O propósito de correlacionar tais funções na política local do órgão é garantir a adoção de procedimentos fundamentais para viabilizar a conformidade com a LGPD, além de demonstrar as principais ações requeridas de um encarregado, uma vez que as suas responsabilidades compreendem a maioria das atividades necessárias à proteção de dados pessoais.

Ademais, a depender da estrutura e funcionamento do órgão ou entidade, atribuições específicas ou complementares podem ser adicionadas ao rol de competências instituídas no Decreto Estadual abaixo relacionadas:

- Inventariar os tratamentos do controlador, inclusive os eletrônicos
- Analisar a maturidade dos tratamentos em face dos objetivos e metas estabelecidos e do consequente risco de incidentes de privacidade.
- 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.
- Orientar as providências cabíveis para implementar as medidas de segurança avaliadas.
- Cumprir os objetivos e metas previstas na Política de Proteção de Dados Pessoais Locais.

Requisito: Item 5.5.2 da ISO 27701/2019, Item 7.2.a e Controle A.6.1 da ISO 27001/2013.

Evidência: Regulamento, manual de serviços ou documento oficial similar que contenha as atribuições do Encarregado. Além da designação podem ser verificados na prática se o encarregado está responsável por essas atividades.

5 - O envio da autoavaliação cumpre o prazo estabelecido no §2º do art. 4º da Portaria SCGE nº 01/2021?

A SCGE, através da Portaria SCGE nº 1, de 05 de janeiro de 2021, disciplinou o monitoramento da Política Estadual de Proteção de Dados Pessoais (PEPDP) e estabeleceu a exigência da autoavaliação de conformidade por parte de todos os órgãos e entidades inseridos na Política Estadual. Portanto, os encarregados devem se atentar para os procedimentos e prazos requeridos na Portaria, em especial ao disposto no art. 4º:

> Art. 4º - A perspectiva de conformidade será aferida semestralmente pelo órgão ou entidade a partir da autoavaliação considerando os pontos de controle atribuídos ao nível de maturidade de gestão de processos.
>
> (...)
>
> §2º - Os resultados da autoavaliação serão enviados a esta Secretaria pelo encarregado em até 30 dias após o fechamento de cada semestre.

A autoavaliação trata-se da análise de controles implementados pelo órgão ou entidade, dividida em 5 níveis de maturidade de gestão de processos.

Este documento apresenta os controles do nível I de maturidade. Os demais podem ser verificados no site da Secretaria da Controladoria-Geral do Estado - seção - LGPD Monitoramento.

É oportuno que o encarregado responda antecipadamente o questionário de autoavaliação por e-mail com envio de um token específico de acesso à ferramenta. A ferramenta permite salvar as suas respostas parcialmente, para envio posterior, porém, só serão registradas as respostas após a conclusão do questionário.

Requisito: §2º do art. 4º da Portaria SCGE nº 01/2021.

Evidência: Envio, no prazo (até 30 de julho - referente ao 1º semestre e até 30 de janeiro - referente ao 20 semestre), da autoavaliação de conformidade à SCGE através do link enviado por e-mail.

6 - O envio dos resultados de desempenho cumpre o prazo estabelecido no Parágrafo Único do Art. 5º da Portaria SCGE nº 01/2021?

Igualmente ao item 5, os encarregados devem atentar para os procedimentos e prazos requeridos na Portaria SCGE nº 01/2021, em especial ao disposto no art. 5º.

O monitoramento da perspectiva desempenho dos órgãos e entidades será realizado a partir da aferição dos seguintes indicadores:

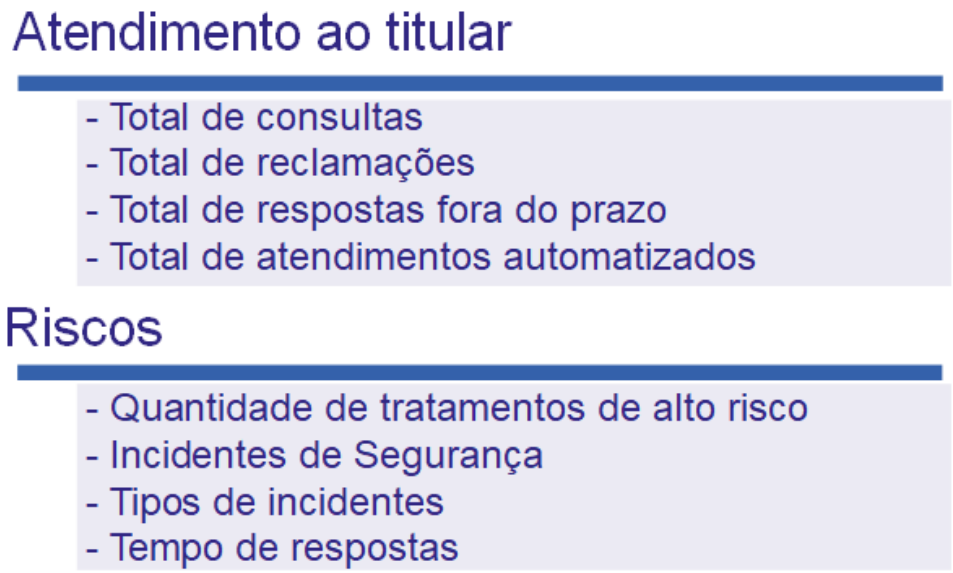

Figura 7 - Indicadores de desempenho do monitoramento da PEPDP.

Conforme Parágrafo Único do art. 5º, o encarregado de cada órgão e entidade deverá enviar até 30 de julho e 30 de janeiro de cada ano os resultados da perspectiva de desempenho.

Para os indicadores de atendimento, primeiramente, o encarregado deve articular com a ouvidoria a disponibilização de canal de suporte ao titular de dados, em seguida providenciar o recebimento e a quantificação desses resultados - para facilitar o trabalho do encarregado, a mensuração desses resultados pode ser preparada pela ouvidoria ou adotar-se mecanismos para que os resultados sejam calculados automaticamente.

De igual modo, para efetuar o tratamento de riscos, o encarregado deve definir os critérios de avaliação de riscos de segurança da informação e da privacidade, a identificação, análise e avaliação dos riscos. Portanto,

a quantificação dos tratamentos de riscos só será possível após desenvolvimento de gestão de avaliação de riscos e com a elaboração dos respectivos controles. **Destaca-se que a gestão e o tratamento de riscos são fases subsequentes entre os procedimentos de proteção de dados pessoais, por isso será comum a unidade ainda não ter desenvolvido esses procedimentos e não pontuar nas primeiras avaliações nos indicadores de riscos.**

Requisito: Parágrafo único do art. 5º da Portaria SCGE nº 01/2021.

Evidência: Envio, no prazo (até 30 de julho - referente ao 1º semestre e até 30 de janeiro - referente ao 20 semestre), da dos resultados de desempenho à SCGE através do link enviado por e-mail.

7 - Foram identificados os fins específicos dos dados pessoais dos processos/atribuições estratégicos?

Os propósitos dos tratamentos de dados pessoais devem estar direcionados para o atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Pode-se dizer que a observação da finalidade é o princípio mais relevante do tratamento de dados pessoais. A coleta de dados pessoais sem finalidade específica, a coleta em excesso, o armazenamento por tempo indefinido, a ausência de política de descarte de dados, essas e outras práticas não são mais aceitas com a chegada da LGPD. **O tratamento de dados pessoais precisa ter propósitos legítimos, específicos e explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.**

Ademais, outros princípios como o da adequação e o da necessidade alicerçam o campo de aplicação conforme a finalidade, vide texto art. 6º, II e III da LGPD, que descrevem tais princípios:

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

- 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.

Verifica-se que não há possibilidade de tratamento de dados com

finalidade genérica, o que era prática comum antes da implementação da LGPD.

A documentação da finalidade deve ser realizada de maneira clara e suficiente e envolver os processos estratégicos do órgão ou entidade, facilitando assim o cumprimento de outra exigência legal que é o atendimento ao titular sobre as informações referentes aos seus dados.

A título de sugestão foi disponibilizado pela SCGE um modelo de diagnóstico preliminar, que pode dar suporte à identificação das finalidades dos tratamentos (vide questões 11 a 14 do referido documento), que, também, devem ser registradas durante a realização do inventário de dados.

Adicionalmente à finalidade, precisa-se relacionar o tratamento de dados pessoais com as respectivas bases legais que justifiquem a operação (vide próximo ponto).

Requisito: Controle A.7.2.1 da ISO 27701/2019.

Evidência: Documento que determina explicitamente a finalidade para a qual os dados pessoais serão processados (limitações de finalidade).

8 - O órgão conscientizou a(s) área(s) envolvida(s) com tratamento de dados pessoais em quais hipóteses a administração pública pode efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas?

No processo de transparência da proteção de dados pessoais não basta apontar a finalidade do tratamento, é preciso associá-lo a uma das hipóteses de permissão de tratamento previstas na LGPD. Também conhecidas como bases legais, a identificação das hipóteses de tratamento permite justificar o tratamento de dados pessoais e identificam a sua adequabilidade com a Lei. É o caso, por exemplo, de um órgão público que coleta dados de identificação pessoal com a finalidade de cadastro para a concessão de benefício de assistência social. Para que o titular exerça seu direito à transparência, é importante que saiba que a coleta dos seus dados pessoais está sustentada por uma **obrigação legal** ou é

necessária para a **execução de uma política pública**.

Tem-se que as hipóteses de tratamento estão divididas, a depender do tipo de dado pessoal, da seguinte forma:

I. Dados pessoais em geral (art. 7º);

II. Dados pessoais sensíveis (art. 11)

O Manual de Proteção de Dados Pessoais de Pernambuco, disponível em LGPD – Manuais e Cartilhas – SCGE elenca e detalha todas as hipóteses legais que justificam o tratamento de dados, apresentando exemplos que servirão de apoio na associação dos tratamentos de dados pessoais às bases legais.

Assim, espera-se que o encarregado e equipe técnica envolvida promova momentos de orientação, treinamentos e divulgação das bases legais envolvidas em seus órgãos, a fim de conscientizar a correta associação. A precaução é para evitar que dados pessoais sejam tratados sem uma hipótese adequada, o que tornaria o tratamento de dados em desconformidade com a LGPD.

Requisito: Item 5.5.3 da ISO 27701/2019, Item 7.3 da ISO 27001/2013, Controle A.7.2.2 da ISO 27001/2013 e Controle A.6.4.2.2 da ISO 27701/2019.

Evidência: Ata de presença dos cursos, palestras ou seminários ofertados pela instituição direcionados a formação e conscientização das pessoas na área de segurança da informação e privacidade, avaliação do entendimento das pessoas conduzida no final do curso de conscientização, educação ou treinamento para testar a transferência de conhecimento, materiais de publicidade e divulgação interna da política de segurança da informação e privacidade, entrevista com os servidores, a fim de verificar o quanto as pessoas estão familiarizadas com a Política de Proteção de Dados Pessoais Local.

9 - Já existe por parte da alta direção da organização entendimento sobre os efeitos de implementação da LGPD em qualquer tratamento de dados pessoais realizado?

A gestão estratégica da organização deve ter uma participação efetiva no processo de adequação do órgão ou entidade à LGPD. Desde a correta designação do encarregado, assim como com a aprovação da Política de Proteção de Dados Pessoais Local, a alta direção deve promover condições e recursos para que o processo seja exitoso. Para tanto, é essencial que a alta direção tenha conhecimentos básicos sobre sua responsabilidade e os efeitos da LGPD nos seus processos de negócios.

Desse modo, a SCGE, através da Portaria SCGE nº 01/2021, prevê a existência da etapa "Alinhamento Estratégico" no projeto de adequação à LGPD. Nesse momento será realizada uma apresentação para a alta direção do órgão ou entidade das exigências da LGPD e do papel exercido pelo encarregado.

A fim de apoiar a execução da referida etapa, a SCGE disponibiliza uma apresentação modelo (Exemplo de Alinhamento Estratégico) que deve ser adaptada à realidade de cada órgão ou entidade.

Somado a essas medidas iniciais, deve a alta direção do órgão ou entidade demonstrar sua liderança e comprometimento em relação ao sistema de gestão da segurança e privacidade através de avaliações periódicas.

Além da etapa do projeto de adequação "Alinhamento Estratégico", é recomendável que o órgão ou entidade considere outras situações de participação da alta direção, como:

- Alterações do contexto interno e externo da organização que produzam efeitos no tratamento de dados pessoais, a exemplo de novas atribuições do órgão;
- Resultados das avaliações e tratamento de riscos;
- Avaliações sobre ações tomadas anteriormente sobre análises críticas da direção.

Requisito: Item 5.3.1 da ISO 27701/2019 e Item 5.1 da ISO 27001/2013.

Evidência: Planejamento estratégico alinhado às políticas de segurança da informação e privacidade, ações de conscientização/capacitação que demonstrem que a Alta Administração é o principal apoiador/disseminador/motivador das políticas de segurança da informação e privacidade, indicações de que a gestão das políticas de segurança da informação e privacidade são tratadas à nível de diretoria, ata de reunião ou documento similar que demonstre que a Alta Administração foi a responsável por estabelecer a Política de Proteção de Dados Pessoais Local.

10 - Há Políticas de Privacidade definidas e mantidas para os serviços digitais?

Primeiramente é necessário definir o que é uma Política de Privacidade. No Brasil esse termo foi interpretado de diferentes maneiras, inclusive divergindo do que é adotado por padrões técnicos internacionais.

A Política de Privacidade comumente utilizada no Brasil se refere ao documento que apresenta os procedimentos utilizados aos dados pessoais tratados pela organização. Ou seja, é um instrumento essencial

de transparência.

Já a *International Organization for Standardization* (ISO) considera que a Política de Privacidade é orientada para o contexto interno da organização, e seria as diretrizes da entidade às questões relacionadas à privacidade e aplicadas aos seus colaboradores.

Em Pernambuco, este documento é equivalente à Política de Proteção de Dados Pessoais Local de cada órgão ou entidade. Por outro lado, a ISO define que a comunicação externa aos titulares de dados sobre como seus dados pessoais são tratados pela organização recebe o nome de Aviso de Privacidade.

Entretanto, é válido reforçar que essa definição pode ser objeto de regulamentação ou padronização por parte da ANDP e ter seu conteúdo alterado.

Portanto, a Política de Privacidade é um documento informativo pelo qual o prestador de serviço transparece ao usuário a forma como realiza o tratamento dos dados pessoais e como ele fornece privacidade ao usuário. Esse documento tem por objeto dar transparência ao tratamento de dados pessoais, elucidando como essas informações serão utilizadas pela organização, se são compartilhadas com terceiros, qual a finalidade para o tratamento, dentre outros aspectos.

Como ação de apoio à produção de tais documentos, a SCGE disponibiliza modelo de Política de Privacidade para ser adaptado a cada serviço digital.

Requisito: Inc. VI do art. 1º da Portaria SCGE nº 01/2021, Itens 5.3.2 e 6.2.1.1 da ISO 27701/2019, Item 5.2 e Controle A.5.1.1 da ISO 27001/2013; ISO 27701/2019 - 7.3.9

Evidência: Políticas de Privacidade nas plataformas digitais governamentais.

11 - Existem recursos (técnicos e humanos) disponíveis ao encarregado de proteção de dados para este realizar as tarefas exigidas, bem como o acesso a dados pessoais, operações de processamento e para manter o seu conhecimento especializado e atualizado?

Nos itens anteriores foram apresentadas as atribuições do encarregado na Política Estadual. Dentre elas, destacam-se duas: a orientação dos gestores e a elaboração do inventário de dados. Ambas as atribuições

demandam livre acesso aos setores da organização que tratam de dados pessoais e exigem experiência e conhecimentos específicos como: segurança da informação, gestão de processos e direito digital.

Resta claro que são necessários recursos relevantes para garantir o trabalho do encarregado. Portanto, o investimento deve ser proporcional ao tamanho do órgão e à complexidade do tratamento de dados.

Neste sentido, a direção estratégica de cada órgão ou entidade deve garantir que o encarregado tenha suporte das seguintes áreas (caso disponível no órgão ou entidade pública):

- TI: para implementação de controles de segurança da informação, atualizações nas plataformas de serviço digital do órgão, etc;
- Ouvidoria: para estabelecer o canal de comunicação com o titular e o repasse de demandas que tratam de proteção de dados;
- Controle Interno: acompanhamento de notas técnicas, implementação da LGPD, verificação de conformidade e regulamentos específicos sobre proteção de dados pessoais;
- Departamento Jurídico: para verificação das atualizações contratuais necessárias à LGPD, modificações de contratos com operadores, terceirizados, cláusulas de trabalho com contratados que atuarão com dados pessoais, etc.

Requisito: Parte do Item 5.5.1 da ISO 27701/2019 e Item 7.1 da ISO 27001/2013.

Evidência: Entrevista com o encarregado, para verificar a real disponibilidade de recursos necessários à execução Política de Proteção de Dados Pessoais Local, observação da rotina de trabalho do Encarregado e sua equipe de apoio, atos de nomeação e designação de pessoal para dar suporte à execução Política de Proteção de Dados Pessoais Local, criação de setor específico, preferencialmente com status de assessoria, responsável por gerenciar a Política de Proteção de Dados Pessoais Local.

12 - São feitas campanhas de conscientização quanto ao uso responsável da informação/internet?

Uma vez que a adequação da organização à LGPD depende de um esforço coletivo de todos envolvidos, é imprescindível promover a cultura organizacional de proteção de dados pessoais. A atitude dos colaboradores e parceiros pode ser decisiva na redução de riscos associados ao uso desconforme ou acesso indevido aos dados pessoais de posse de uma organização.

Além das boas práticas de segurança, é interessante que as campanhas

exponham aspectos básicos da LGPD: a indicação da finalidade do tratamento de dados, das bases legais, dos princípios, a diferença entre dados pessoais e dados pessoais sensíveis.

Assim que o órgão ou entidade detiver uma Política de Dados Pessoais Local é fundamental para a sua efetivação o envolvimento e apoio da gestão estratégica para divulgação e implementação das ações de adequações necessárias.

Tais ações devem ser registradas para comprovação de que o órgão ou entidade está empenhado no cumprimento de suas obrigações para com a LGPD. Adicionalmente se faz necessário que as campanhas de conscientização sejam oportunas às alterações provenientes de normas técnicas e regulamentares da Autoridade Nacional de Proteção de Dados, atualizações legais e orientações da SCGE.

O programa de conscientização deve levar em conta novos colaboradores, estagiários, parceiros, terceirizados e considerar as diferentes formas de aplicação: cursos à distância, palestras, cartilhas e boletins. Complementarmente, onde aplicável, deve incluir as responsabilidades de agentes externos (operadores ou no caso de o controle de dados pessoais ser compartilhado com outro órgão - caso de controladoria conjunta).

Deve ficar evidente que o comando do órgão ou entidade da Administração Pública endossa o treinamento. Assim como, devem ser notórias as implicações que possam ocorrer por negligência ou mau uso de dados.

Como material de apoio para campanhas, recomendamos os fascículos informativos da Autoridade Nacional de Proteção de Dados - ANPD, que são:

1. Proteção de Dados
2. Vazamento de dados
3. Como Proteger seus Dados Pessoais

Cumpre destacar que a ANPD publicou um Guia[1] de Segurança com algumas recomendações que devem ser consideradas em campanhas de conscientização, vide:

- como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário;

[1] Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.

• como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;

• manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas;

• não compartilhar logins e senhas de acesso das estações de trabalho;

• bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros;

• seguir as orientações da política de segurança da informação.

Por fim, a ANPD recomenda criar um ambiente organizacional que incentive usuários de sistemas da empresa, tanto clientes quanto funcionários, a informar incidentes e vulnerabilidades detectadas.

Requisito: Item 5.5.3 e Diretriz 6.4.2.2 da ISO 27701/2019 e Item 7.3 e Controle A.7.2.2 da ISO 27001/2013.

Evidência: Ata de presença dos cursos ofertados pela instituição direcionados a formação e conscientização das pessoas na área de segurança da informação e privacidade, avaliação do entendimento das pessoas conduzida no final do curso de conscientização, educação ou treinamento para testar a transferência de conhecimento, materiais de publicidade e divulgação interna da política de segurança da informação e privacidade, entrevista com os servidores, a fim de verificar o quanto as pessoas estão familiarizadas com a Política de Proteção de Dados Pessoais Local.

13 - A organização dispõe de uma lista de todos seus operadores de modo estruturado?

A LGPD, em seu art. 39, estabelece que o operador deverá realizar o tratamento segundo as orientações fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. Portanto, o levantamento de informações sobre os operadores de dados pessoais é ação primordial para garantir o processo de adequação dos instrumentos contratuais, de instrução aos operadores e para realização de monitoramento.

A lista deve incluir:

• os tipos de dados pessoais que são compartilhados com o operador;

• identificação do processo em que o operador trata dados pessoais;

• as informações contratuais.

Neste contexto, a SCGE disponibiliza no site institucional o modelo de Mapa de Identificação de Operadores para apoiar o processo de adequação dos instrumentos contratuais às exigências da LGPD e às cláusulas padrões estabelecidas pela Procuradoria-Geral do Estado de Pernambuco (PGE-PE).

Requisito: Art. 39 da Lei nº 13.709/ 2018; e, Item 7.2.6 e Anexo B da ISO 27701/2019 (por similaridade)

Evidência: Lista/Mapa de todos os operadores (pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador), que contenha informações mínimas acerca das condições de tratamento de dados pessoais realizados pelos operadores, inventário de dados.

14 - Existem medidas de promoção organizacional para capacitar os funcionários sobre as exigências da LGPD?

É recomendado que o órgão disponibilize treinamento sobre proteção de dados pessoais para todos os servidores e demais colaboradores. Além de um treinamento geral, devem ser consideradas capacitações proporcionais às atividades de tratamento realizadas pelo órgão e treinamentos pontuais para pessoal transferido recentemente a setor que lide com tratamento de dados.

Como temática nova, a legislação e os procedimentos de proteção de dados devem ser atualizados e comunicados oportunamente. Além disso, outros fatores que devem ser considerados na gestão dos treinamentos:

- Apoio da gestão estratégica para reforçar as políticas de treinamento sobre proteção de dados e de privacidade;
- Comunicação dos impactos negativos por atos de negligência ou omissões referentes ao tratamento de dados;
- Treinamentos específicos como políticas de segurança da informação e privacidade, controle de acesso a sistemas, elaboração de senhas com nível alto de proteção e troca periódica, informações sobre malwares (códigos maliciosos);
- Apresentação do encarregado de dados e de demais servidores que se disponibilizaram para prestar orientações.

Requisito: Item 5.5.3 e Controle A.6.4.2.2 da ISO 27701/2019 e Item 7.3 e Controle A.7.2.2 da ISO 27001/2013.

Evidência: Plano de treinamento, indicadores de desenvolvimento individual, ata de presença dos cursos, palestras ou seminários ofertados pela instituição direcionados a formação e conscientização das pessoas na área de segurança da informação e privacidade, avaliação do entendimento das pessoas conduzida no final do curso de conscientização, educação ou treinamento para testar a transferência de conhecimento, entrevista com os servidores, a fim de verificar o quanto as pessoas estão familiarizadas com a Política de Proteção de Dados Pessoais Local.

15 - As partes envolvidas com a implementação da LGPD realizaram a leitura do Manual da Lei Geral de Proteção de Dados (LGPD) em PE produzido pela SCGE?

Conforme preconizado pelo Decreto Estadual nº 49.265/20, que estabelece a Política Estadual de Proteção de Dados Pessoais do Poder Executivo Estadual à SCGE tem a missão de 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. Em vista dessa competência foi produzido um material que além de garantir noções e referências sobre a temática de proteção de dados pessoais, assegura um maior nível de aplicabilidade pela administração pública dos procedimentos de adequação à proteção de dados pessoais, o Manual da Lei Geral de Proteção de Dados (LGPD) de Pernambuco.

No manual são apresentadas matérias que retratam o contexto histórico da LGPD, conceitos sobre controlador e operador alinhados com a atualização promovida pela Autoridade Nacional de Proteção de Dados (ANPD), são detalhadas as hipóteses de tratamento de dados, além de indicações de materiais produzidos pelo Estado de Pernambuco.

Requisito: Item 5.5.3 e Controle A.6.4.2.2 da ISO 27701/2019 e Item 7.3 e Controle A.7.2.2 da ISO 27001/2013.

Evidência: Ata de presença dos cursos ofertados pela instituição direcionados a formação e conscientização das pessoas na área de segurança da informação e privacidade, avaliação do entendimento das pessoas conduzida no final do curso de conscientização, educação ou treinamento para testar a transferência de conhecimento, entrevista com as partes envolvidas, a fim de verificar o quanto as pessoas estão familiarizadas com a Política de Proteção de Dados Pessoais Local e o Manual da Lei Geral de Proteção de Dados (LGPD), elaborar quiz para medir o grau de entendimento do Manual da Lei Geral de Proteção de Dados (LGPD) em PE.

16 - A organização tem um setor específico responsável por Tecnologia da Informação?

A Lei Geral de Proteção de Dados Pessoais abrange o tratamento de dados pessoais nos meios digitais e físicos. Pelo uso cada vez mais comum de plataformas governamentais digitais, de serviços prestados através de websites, de armazenamento de informações em bancos de dados digitais, contar com um setor de Tecnologia da Informação (TI) auxilia em

procedimentos técnicos de segurança da informação e privacidade.

O setor de TI, conforme Lei Estadual nº 12.985, de janeiro de 2006, também denominados de Núcleos Setoriais de Informática (NSI), são responsáveis por desenvolver, manter, dar suporte e gerenciar, direta ou indiretamente, os ativos, serviços, sistemas e aplicativos setoriais de Tecnologia da Informação e Comunicação.

Portanto, o NSI poderá apoiar na implementação dos controles previstos nas seguintes áreas de segurança da informação (ISO 27.001/2013):

- **Gestão de mídias e de ativos informáticos:** de acordo com o nível de confidencialidade das informações devem ser implementados procedimentos de gestão de mídias, incluindo controles específicos para o descarte seguro e políticas de transferência de dados com recursos de proteção para impedimento à acesso não autorizado.

- **Controle de acesso:** gerenciamento de acesso ao usuário: garantir acesso ao usuário devidamente cadastrado para determinadas operações e viabilizar mecanismos de proteção ao acesso não autorizado.

- **Criptografia:** desenvolvimento de controles de criptografia para garantir a segurança da informação e da privacidade.

- **Manutenção de equipamentos:** o setor de TI geralmente opera para propiciar atualizações necessárias das máquinas utilizadas no processamento e armazenamento de dados. Com a devida atualização são reduzidas as vulnerabilidades dos sistemas

- **Controle de instalação de *softwares:*** devem ser definidos controles para a instalação de programas para evitar perdas da informação e operação das máquinas para garantir a disponibilidade e integridade da informação.

- **Proteção contra *malwares:*** códigos maliciosos são programas elaborados para executar ações prejudiciais a um computador, alguns exemplos são vírus, worms, spyware, cavalo de troia. O setor de TI deve considerar ações de prevenção, detecção e recuperação de dados para garantir a proteção, confidencialidade, disponibilidade e integridade dos dados pessoais.

Requisito: Lei 12.985/06, Item 5.3 e Controles A.6.1.1 e A.6.1.2 da ISO 27001/2013 e item 6.3.1.2 da ISO 27701/2019.

Evidência: Organograma, regulamento, manual de serviços ou documento oficial similar que contenha as atribuições do Núcleos Setoriais de Informática/Departamento de informática.

17 - Existe pessoal dedicado especificamente à Segurança da Informação?

A segurança da informação e da privacidade deve garantir a conformidade com a LGPD e é um instrumento para otimizar os processos da organização. Segundo a ANPD[2]: *"a segurança da informação pode ser definida como o conjunto de ações que visam à preservação da confidencialidade, integridade e disponibilidade da informação. esse conjunto de ações impacta todo o ambiente institucional das empresas, com objetivo de prevenir, detectar e combater as ameaças digitais".*

Como verificado, a segurança da informação resulta em fatores que influenciam de forma geral a entidade, portanto considerar pessoal dedicado para atuar com segurança da informação e privacidade pode ser fundamental a depender do nível de complexidade e do volume do tratamento de dados.

É importante destacar atribuições de unidades para lidar com segurança da informação, com profissionais capacitados que garantam uma maior efetividade do trabalho e, assim, evitar possíveis conflitos de interesses nas atividades. O time que atuará com segurança da informação e privacidade deve ser apoiado pela gestão estratégica para garantir as atribuições de responsabilidade e autoridade necessárias para que as atividades com segurança da informação e privacidade sejam efetivas e em conformidade com a LGPD. Os profissionais destacados devem reportar à gestão estratégica os indicadores de desempenho das operações de segurança e privacidade.

Requisito: Lei 12.985/06, Item 5.3 e Controles A.6.1.1 e A.6.1.2 da ISO 27001/2013 e item 6.3.1.2 da ISO 27701/2019.

Evidência: Organograma, regulamento, manual de serviços ou documento oficial similar que contenha as atribuições do pessoal dedicado à segurança da informação.

18 - A página da LAI da organização inseriu as Políticas de Privacidade e Termos de Uso dos seus serviços digitais?

Os dois documentos originam-se da responsabilidade de os agentes de tratamento de dados serem transparentes com o titular de dados e

[2] Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte.

informarem como as atividades de tratamento de dados atendem os princípios dispostos no art. 6º da LGPD. Nesse contexto, como estrutura permanente de transparência ativa, o estado de Pernambuco desenvolveu o Portal da Lei de Acesso à Informação (www.lai.pe.gov.br) para inserção de documentos relevantes para a transparência.

- Termos de Uso: documento que estabelece obrigações e condições de uso de determinado serviço oferecido ao titular pelo órgão e entidade.

- Políticas de Privacidade: documento que indica ao cidadão como o órgão ou entidade trata seus dados pessoais ao longo de todo o ciclo de vida do dado.

A fim de orientar os órgãos e/ou entidades no processo de concepção das Políticas de Privacidade e Termos de Uso a União lançou o Guia de elaboração de Termo de Uso e Política de Privacidade para serviços públicos, disponível em :guia_tupp.pdf (www.gov.br).

Nesse contexto, a SCGE disponibiliza o Modelo de Política de Privacidade e Modelo de Política de Termo de Uso no seu site institucional para apoiar a elaboração dos documentos.

Requisito: Inciso XI do art. 1º da Portaria SCGE nº 01/2021 e inciso VI do art. 60 da Lei nº 13.709/2018.

Evidência: Link de publicação da Política de Privacidade e Termos de Uso.

19 - Os contatos do encarregado de proteção de dados foram publicados na página da LAI da organização?

Os princípios de livre acesso e transparência são formas de assegurar ao titular de dados consulta facilitada e gratuita sobre a forma e duração do tratamento de dados, garantindo de igual modo que as informações sejam claras, precisas e facilmente acessíveis.

Em continuidade com as determinações acima, o art. 41 da LGPD define que a identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador. Nesse contexto, como estrutura permanente de transparência ativa, o estado de Pernambuco desenvolveu o Portal da Lei de Acesso à Informação (www.lai.pe.gov.br) para inserção de documentos relevantes para a transparência, onde deverão apresentar a identificação do encarregado de dados.

Requisito: Art. 41, § 1º da Lei nº 13.709/2018 e inciso XI do art. 1º da Portaria SCGE nº 01/2021.

Evidência: Link de publicação dos contatos do Encarregado.

20 - O encarregado está disponível para ser contatado por titulares de dados?

Como verificado no item 19, os dados do encarregado devem ser publicizados na página da LAI do respectivo órgão público. Além de garantir o canal de comunicação para assuntos relacionados à LGPD, deve o órgão dar liberdade, autonomia, acesso aos processos que tratam dados pessoais, treinamentos, tempo para a realização dessas atividades e **assegurar que o encarregado esteja à disposição do titular de dados**.

Conforme art. 6º da LGPD, as atividades de tratamento de dados pessoais deverão dar garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento. No mesmo sentido, a LGPD, em seu art. 9º estabelece que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso.

Portanto, a disponibilidade do encarregado torna-se essencial para o cumprimento do princípio livre acesso, se considerarmos a atribuição prevista no art. 41, § 2º, I da LGPD de aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências.

Requisito: Inciso II do art. 13 do Decreto Estadual nº 49.265/2020; e, Controle 7.3.1 da ISO 27701/2019.

Evidência: Link de publicação dos contatos do Encarregado, realizar tentativa de contato (telefônico, e-mail) com o encarregado através das informações disponíveis na página da LAI e avaliar o tempo de resposta.

21 - A Política de Proteção de Dados Pessoais Local foi aprovada pelo dirigente máximo e encontra-se publicada na página da LAI da organização?

A Lei exige por parte do poder público a instituição de processos e políticas internas, visando a adequação dos serviços públicos à cultura de proteção de dados pessoais. Em especial, a LGPD prevê que os agentes de tratamento, no âmbito de suas competências, poderão formular regras de boas práticas e de governança que estabeleçam condições

de organização, o regime de funcionamento, os procedimentos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

Adicionalmente, a LGPD estabelece (art. 50, §2º) que o controlador deverá implementar programa de governança em privacidade que demonstre o seu comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais sob seu controle. A Lei espera que o programa seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados, assim como, seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

Portanto, o programa de governança visa estabelecer o modelo de implantação, comunicação e de gerenciamento dos riscos associados à proteção de dados. Assim, todas as atividades poderão ser dirigidas, monitoradas e incentivadas, envolvendo as principais partes interessadas e promovendo a adoção das medidas mitigadoras dos riscos identificados.

O art. 6º do Decreto determina que 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 e deverão estabelecer, no mínimo:

1. princípios, diretrizes e prioridades locais da proteção de dados pessoais;

2. responsabilidades e papéis pela proteção de dados pessoais;

3. processo de gerenciamento de riscos;

4. controles internos de proteção de dados pessoais.

Como orientação, encontra-se disponível o modelo de Política de Proteção de Dados Pessoais Local no site da SCGE. Cumpre destacar que o conteúdo deve ser adaptado à realidade de cada órgão e entidade.

Nesse contexto, como estrutura permanente de transparência ativa, o estado de Pernambuco desenvolveu o Portal da Lei de Acesso à Informação (www.lai.pe.gov.br) para inserção de documentos relevantes para a transparência.

Requisito: Inciso I do art. 12 do Decreto Estadual nº 49.265/2020.

Evidência: Link de publicação da Política de Proteção de Dados Pessoais Local, Documento oficial de publicação da PPDPL assinado pelo dirigente máximo.

22 - O órgão, ao efetuar o tratamento de dados pessoais no exercício de suas competências legais ou execução de políticas públicas, dá publicidade sobre a finalidade e a forma como o dado será tratado na página da LAI da organização?

Segundo o art. 23 da LGPD, o tratamento de dados pessoais pelas pessoas jurídicas de direito público deverá ser realizado desde que sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

Nesse contexto, como estrutura permanente de transparência ativa, o estado de Pernambuco desenvolveu o Portal da Lei de Acesso à Informação (www.lai.pe.gov.br) para inserção de documentos relevantes para a transparência.

O órgão deve atentar para as informações que são excepcionalizadas pela LGPD, especialmente àquelas que deverão ter impacto em âmbito público, a exemplo de tratamento de dados realizados para as seguintes finalidades:

- acadêmicas, considerando as hipóteses de tratamento de dados.
- segurança pública, defesa nacional, segurança do Estado e para atividades de investigação ou repressão de infrações penais.

Como modelo prático, seguem 2 processos realizados pela Secretaria da Controladoria-Geral do Estado, onde são apresentados o processo, a categoria de dados - com detalhamento dos tipos de dados, a finalidade do tratamento e a respectiva base legal. Vide que a quantidade de dados para realização de auditoria de pessoal é extensa, já para o cadastro em cursos, limitada.

Tabela 1 - Demonstrativo de Tratamento de Dados para Portal LAI da SCGE

Processo	Conjunto de Dados Pessoais	Finalidade do Tratamento de dados pessoais	Hipóteses de Permissão de Tratamento de Dados
DOGI - Capacitações (Cursos, Oficinas e Palestras) nas modalidades presencial e/ou EAD - Público Externo	Dados Cadastrais (Estado civil, identidade, dados de identificação...), Dados de conexão (endereço IP, logs etc.), Dados de contato pessoal (e-mail, telefone celular, telefone residencial...)	Inscrição em capacitações da ECI por participantes de outros órgãos; validação e pagamento de instrutoria.	para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres
DAUD - Auditoria de Pessoal	Dados Cadastrais (Estado civil, identidade, dados de identificação,...), Vida pessoal (estilo de vida, situação familiar, etc.), Informações econômico-financeiras (receita, situação financeira, situação tributária etc.), Dados de localização (movimentos, dados de GPS, GSM, etc.), Dados da Seguridade Social e Trabalhistas (PIS, PASEP, Seguro-Desemprego, Programa de Assistência Social, vínculos trabalhistas, etc.), Dados revelando associação sindical, Dados biométricos com o objetivo de identificar exclusivamente uma pessoa singular, Dados relativos à saúde, Dados relativos a condenações e infrações penais	Os dados e informações pessoais dos servidores/agentes públicos são imprescindíveis para a obtenção de evidências suficientes e adequadas à conclusão do objeto da auditoria	para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres

Fonte: produzido por SCGE

Requisito: Inciso XI do art. 1º da Portaria SCGE nº 01/2021 e inciso VI do art. 60 da Lei nº 13.709/2018.

Evidência: Link de publicação da Política de Privacidade e Termos de Uso.