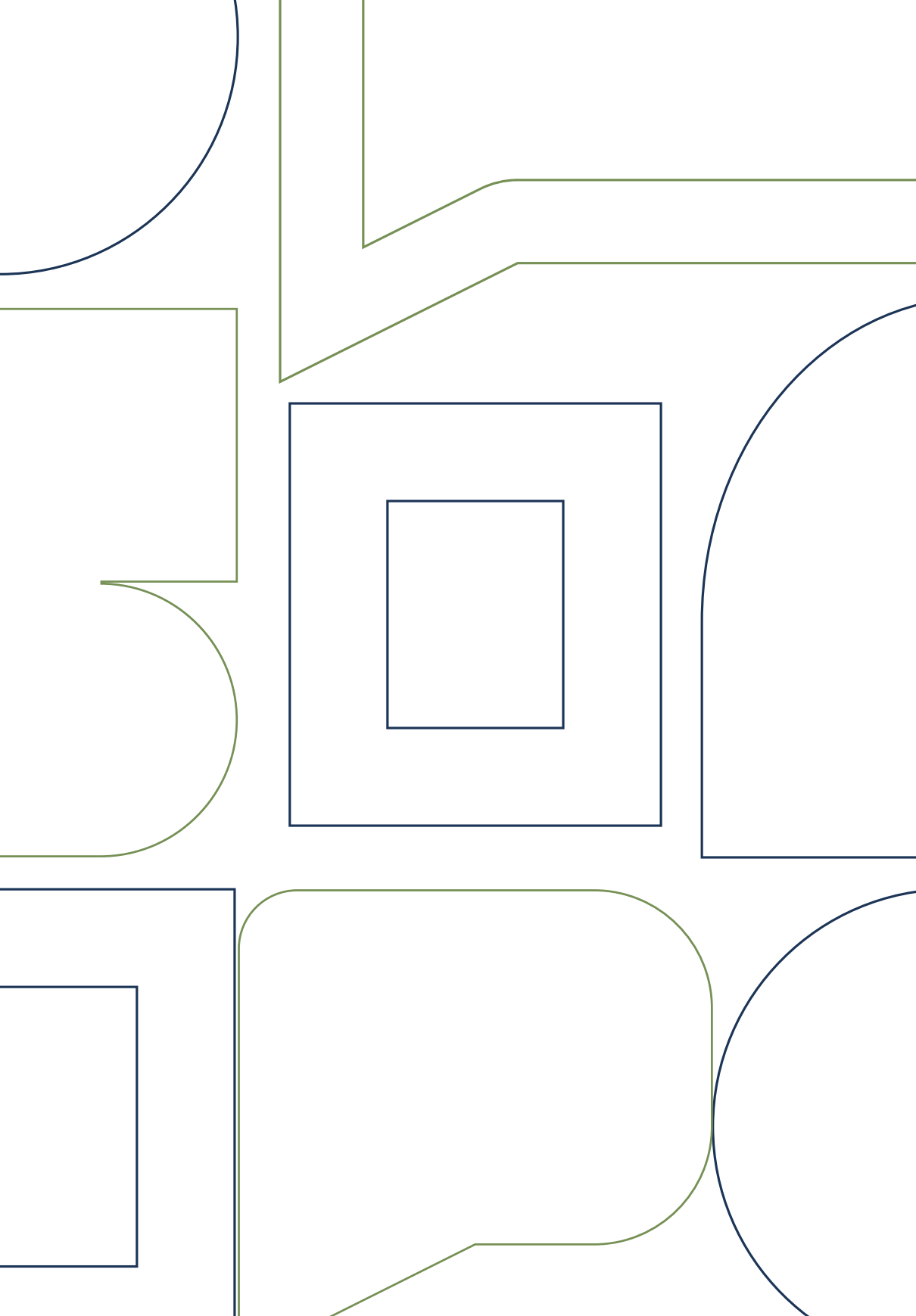
# Manual Orientativo para conformidade com a LGPD Na administração pública Estadual de São Paulo

Controladoria Geral do Estado

SÃO PAULO
GOVERNO DO ESTADO
SÃO PAULO SÃO TODOS

**VERSÃO 1**
Agosto/2025



**GOVERNO DO ESTADO DE SÃO PAULO**

**CONTROLADORIA GERAL DO ESTADO DE SÃO PAULO**

**Governador do Estado**
Tarcísio de Freitas

**Controlador Geral do Estado**
Wagner de Campos Rosário

**Controlador Geral do Estado Executivo**
Roberto Cesar de Oliveira Viegas

**Chefe de Gabinete**
Ronaldo Leite Ferreira

**Auditor Geral do Estado**
José Marcelo Castro de Carvalho

**Corregedor Geral do Estado**
Marcos Gerhardt Lindenmayer

**Ouvidor Geral do Estado**
Valmir Gomes Dias

**Subsecretário de Combate à Corrupção**
Márcio Denys Pessanha Gonçalves

**Subsecretário de Gestão Corporativa**
Daniel da Silva Lima

**Subsecretário de Integridade Pública e Privada**
Breno Barbosa Cerqueira Alves

**Coordenação e supervisão**
Ana Lúcia Moreira e Valmir Gomes Dias

**Execução**
Antonio Carlos Santa Izabel
Erika Helena Lopes Gaia Alves

**Diagramação**

Camila Mota
Daniele Pereira
Kathllen Silva

# Sumário

# 1. Apresentação

A proteção de dados pessoais tem-se demonstrado um elemento essencial da governança de dados no setor público brasileiro, especialmente no contexto da transformação digital do Estado. Embora a Administração Pública já tivesse o dever legal de proteger as informações dos cidadãos, amparado, inclusive, pela Lei de Acesso à Informação (Lei nº 12.527/2011 – LAI), a promulgação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018 – LGPD) trouxe novos fundamentos, princípios e conceitos que contribuem para a instrumentalização dessa responsabilidade, em especial ao introduzir abordagens mais robustas de gestão de riscos e governança de dados, consolidando a necessidade de tratar as informações pessoais, em todo o seu ciclo de vida, com transparência, segurança e respeito aos direitos fundamentais.

Neste cenário, o Estado de São Paulo, por meio do Decreto nº 65.347/2020, estabeleceu diretrizes específicas para a implementação da LGPD no âmbito da Administração Pública Estadual direta, autárquica e fundacional. Com base nesse marco regulatório, nas Deliberações Normativas do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP), na Lei Geral de Proteção de Dados, nas melhores práticas nacionais, considerando, também, as consultas mais recorrentes ao Encarregado de Proteção de Dados da Administração Direta estadual, foi concebido o presente Manual Orientativo.

Este Manual tem como finalidade apoiar os órgãos e entidades estaduais na estruturação e fortalecimento de seus programas de conformidade à LGPD, fornecendo orientações práticas e modelos de referência que auxiliem na adoção das medidas legais, técnicas e administrativas necessárias ao adequado tratamento de dados pessoais.

Mais do que atender a exigências legais, a proteção de dados pessoais deve ser compreendida como um instrumento primordial para garantir a privacidade e a liberdade dos indivíduos, protegendo-os contra o uso indevido e o acesso não autorizado às suas informações, fortalecendo a confiança da sociedade no serviço público e promovendo uma relação segura e transparente entre o Estado e o cidadão.

Esperamos que este material contribua para a consolidação de uma cultura institucional voltada ao adequado tratamento de dados pessoais e à segurança da informação, em plena harmonia com as diretrizes de transparência pública, promovendo uma gestão pública mais ética, moderna e eficiente.

# 2. Fundamentos da LGPD

A Lei Geral de Proteção de Dados Pessoais tem por objetivo, nos termos de seu artigo 1º, "proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural", sendo aplicável tanto ao setor público quanto ao setor privado, estabelecendo regras claras para o adequado tratamento de dados pessoais, conferindo aos indivíduos maior controle sobre suas informações.

No âmbito da atuação estatal, ao regulamentar o tratamento de dados, a LGPD busca equilibrar o interesse público e a prestação de serviços eficientes com a proteção da dignidade e da autonomia dos titulares. A lei reforça a responsabilidade dos atores envolvidos no tratamento desses dados e fomenta uma cultura de respeito à privacidade, vital para o fortalecimento da confiança entre cidadãos, governos e instituições priva-das.

Assim, a LGPD vai além da conformidade normativa: ela representa um compromisso com o respeito à pessoa humana e à construção de uma administração pública mais transparente e responsável no uso das informações que coleta e trata.

## Conceitos básicos

A compreensão de conceitos estruturais da LGPD é indispensável para que os órgãos e entidades públicas possam adequar suas práticas de tratamento de dados pessoais. Assim, apresentamos didaticamente alguns dos constantes no artigo 5º da lei:

**Dado pessoal:** qualquer informação relacionada a pessoa natural identificada ou identificável, como nome, CPF, endereço, e-mail.

**Dado pessoal sensível:** corresponde a informações de pessoa natural sobre sua origem racial ou étnica, suas convicções religiosas, opiniões políticas, filiação sindical ou à organização religiosa, filosófica ou política, sobre sua saúde ou vida sexual, bem como seus dados genéticos ou biométricos. Possui requisitos específicos para tratamento, estabelecidos na LGPD.

**Tratamento:** toda operação realizada com dados pessoais, como coleta, recepção, classificação, utilização, acesso, reprodução, armazenamento, arquivamento, eliminação, entre outras. Por exemplo: registros de acesso a instalações, preenchimento ou digitalização de formulários, alteração de dados cadastrais, análise de requerimentos, eliminação de documentos conforme tabela de temporalidade.

**Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais. No âmbito do Poder Público, a ANPD (2022) orienta que as obrigações típicas de controlador "devem ser distribuídas entre as principais unidades administrativas despersonalizadas que integram a pessoa jurídica de direito público e realizam tratamento de dados pessoais". Nesse sentido, no âmbito da Administração Direta, compete ao Estado de São Paulo esse papel, que é exercido por intermédio dos titulares das Secretarias de Estado e autoridades de nível hierárquico equivalente. Já na Administração Indireta, dada a característica de possuir natureza jurídica própria, cada autarquia, fundação pública, sociedade de economia mista e empresa pública será a controladora quando atuar com poder decisório sobre as finalidades e elementos essenciais do tratamento de dados pessoais.

O operador deve ser uma entidade distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de suas unidades.

**Operador:** pessoa natural ou jurídica, contratada ou designada para realizar o trata-mento de dados em nome do controlador. Exemplo: empresas terceirizadas que operam sistemas para órgãos públicos. Importante destacar que o operador é uma entidade distinta do controlador. Portanto, um empregado ou servidor público do quadro da própria organização não é um agente de tratamento, por estar exercendo atividades enquanto um profissional subordinado ao controlador.

**Encarregado:** pessoa indicada pelo controlador para atuar como canal de comunicação entre o órgão ou entidade, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), observado o art. 41 da LGPD. Na Administração Direta do Estado de São Paulo, esse papel é exercido pelo Ouvidor Geral do Estado, nos termos do art. 6º do Decreto nº 65.347/2020, cabendo aos dirigentes máximos das autarquias, fundações mantidas pelo Poder Público, empresas públicas e sociedades de economia mista designar o encarregado de sua respectiva entidade.

## Finalidade da LGPD no setor público

A LGPD aplica-se também ao setor público, impondo obrigações claras aos órgãos e entidades da Administração Pública. Como destacam Cristóvam et al. (2021), a lei é o marco de uma nova etapa para a governança de dados no âmbito público, voltada para a proteção dos direitos e garantias basilares de liberdade, privacidade e desenvolvi-mento da personalidade. Nesse contexto, observa-se que a lei visa assegurar que o tratamento de dados pessoais seja realizado de maneira adequada, segura e transparente, além de contribuir para a mitigação de eventuais irregularidades no tratamento de dados pessoais.

Proteger os direitos fundamentais: zelar pela privacidade, liberdade e pela proteção dos dados pessoais, enquanto direitos constitucionais dos cidadãos.

Tratamento adequado: garantir que o tratamento de dados pessoais seja realizado em conformidade com a LGPD e as demais normas aplicáveis, assegurando a legalidade e a legitimidade das ações da Administração Pública.

Promover a transparência: assegurar que os titulares saibam como seus dados são coletados, usados e compartilhados pelos órgãos públicos.

Atender a finalidade pública e ao interesse coletivo: garantir que o uso de dados pessoais pelo poder público observe o exercício de suas competências legais, a execução de políticas públicas ou a oferta de serviços de interesse social.

Promover a segurança: adotar medidas de proteção para prevenir acessos não autorizados, vazamentos e outras ameaças, assegurando a integridade e a confidencialidade das informações pessoais.

Estabelecer mecanismos de responsabilização: reforçar o dever dos agentes públicos de agir com diligência e prestar contas quanto ao uso de dados pessoais sob sua responsabilidade.

# Princípios da LGPD aplicáveis à Administração Pública

Para alcançar seu objetivo, a Lei Geral de Proteção de Dados elenca, em seu artigo 6º, relevantes princípios que devem ser necessariamente observados no tratamento de dados pessoais, inclusive por órgãos e entidades da Administração Pública.

Finalidade: o tratamento deve ocorrer para propósitos legítimos, específicos e explícitos, informados ao titular, sem possibilidade de tratamento posterior incompatível com essas finalidades.

Necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades.

Qualidade dos dados: os dados devem ser exatos, claros, relevantes e atualizados.


Segurança: adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas.

Adequação: compatibilidade do tratamento com a finalidade informada.

Livre acesso: garantia de consulta facilitada e gratuita aos titulares, em especial sobre a forma e a duração do tratamento de seus dados.

Transparência:os titulares devem ser informados de maneira clara, precisa e acessível sobre o tratamento de dados pessoais.

Prevenção: adoção de medidas para evitar danos aos titulares, em virtude do tratamento de seus dados.

Não discriminação: vedação ao tratamento de dados para fins discriminatórios, ilícitos ou abusivos.

Responsabilização e prestação de contas: o controlador deve demonstrar a adoção de medidas eficazes para assegurar a conformidade com a LGPD.

Esses princípios não apenas orientam a conduta dos órgãos e entidades públicas, mas também funcionam como base para avaliações de conformidade e responsabilização em caso de violações. Depreende-se, ainda, que tais princípios orientam para que a coleta de dados deve ser a mínima possível para o atendimento da finalidade pretendida, bem como as demais etapas de tratamento devem observar, desde a concepção, procedimentos estruturados para a aplicação de técnicas e demais medidas organizacionais de proteção de dados durante todo o ciclo de vida da informação (minimização de dados e privacidade por desenho).

Esse tratamento orientado desde a concepção também contribui para que o poder público possa melhor cumprir os deveres relacionados ao acesso à informação, ao mitigar esforços para tratamento de dados antes da disponibilização pública. Ou seja, a combinação entre privacidade por desenho e transparência por desenho, aplicada aos processos de trabalho da organização, proporciona maior eficiência estatal tanto na asseguração da proteção de dados pessoais restritos quanto na garantia da transparência pública.

## Hipóteses legais de tratamento de dados pessoais no setor público

A LGPD dedica um capítulo específico (Capítulo IV) para disciplinar as atividades de tratamento realizadas pela Administração Pública. Da leitura do mencionado capítulo, em conjunto com outros dispositivos da lei, a exemplo do art. 7º, observamos as bases legais que legitimam esse tratamento, apresentando características distintas do setor privado. Por exemplo, geralmente não é aplicável o consentimento do titular para o exercício de atividades próprias de órgãos e entidades do Administração Pública, sendo as hipóteses legais mais recorrentes as apresentadas a seguir:

**Cumprimento de obrigação legal ou regulatória:** por exemplo, o tratamento de dados de servidores para fins de folha de pagamento.

**Execução de políticas públicas** previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres: como o tratamento de dados de usuários do SUS.

**Realização de estudos por órgão de pesquisa**, garantida, sempre que possível, a anonimização dos dados pessoais.

**Proteção da vida** ou da incolumidade física do titular ou de terceiros.

**Tutela da saúde**, exclusivamente em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.

**Execução de contratos** ou de procedimentos preliminares relacionados.

**Garantia da prevenção à fraude** e à segurança do titular.

Os dados pessoais tratados pelo poder público podem ser compartilhados entre entes instituições públicas, desde que observadas as finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeita-dos os princípios de proteção de dados pessoais.

Já o compartilhamento entre o Poder Público e entidades privadas somente pode ser realizado quando observados requisitos adicionais definidos nos artigos 26 e 27 da LGPD, sendo, inclusive, prevista a necessidade de comunicação à Autoridade Nacional de Proteção de Dados.

Relevante destacar que o tratamento de dados por um operador, a exemplo de uma empresa de tecnologia contratada para desenvolvimento e suporte de sistema, não caracteriza compartilhamento de dados pessoais por si só.

## O que significa tratar dados?

Para que essas atividades sejam conduzidas em conformidade com a legislação, é importante compreender o que significa tratar dados pessoais. Segundo a LGPD (art. 5º, X), tratamento é toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência,

difusão ou extração. Assim, observa-se que o conceito de tratamento é bastante amplo, indicando a relevância da consolidação de uma cultura de privacidade na organização e impondo constante atenção de todos os agentes públicos no tratamento de informações pessoais, sendo relevante apresentar alguns exemplos de situações comuns no dia a dia de trabalho, que podem comportar riscos ao adequado tratamento de dados pessoais:

- anotação de dados pessoais de um usuário de serviço durante um atendimento telefônico, mantendo a folha utilizada em cima da estação de trabalho;
- envio de e-mail com dados pessoais copiando pessoas que não terão necessária atuação no caso;
- impressão de planilhas com informações pessoais em impressora compartilhada, sem a retirada imediata do material;
- manutenção de documentos contendo dados pessoais protegidos em processo do SEI com nível de acesso "público";
- descarte de cópias de documentos contendo dados pessoais sem sua descaracterização;
- atendimento de solicitações de informações pessoais por telefone, sem mecanismos de confirmação da identidade.
- comunicação verbal de informações pessoais de cidadãos em ambientes de circulação, como corredores ou recepções, expondo dados indevidamente.

## Cuidados no tratamento de dados pessoais

Como já observamos, o zelo no tratamento de dados pessoais deve fazer parte de nossa rotina. Assim, a adoção de cuidados em todo o ciclo de vida dos dados é fundamental, envolvendo o uso, armazenamento e descarte. O uso deve ocorrer com acesso restrito e conforme as finalidades legítimas definidas. O armazenamento requer medidas de segurança da informação, como controle de acessos e proteção contra acessos não autorizados. O

descarte, por sua vez, deve ser realizado de forma segura e apenas quando os dados deixarem de ser necessários para o interesse público ou para o cumprimento de obrigações legais, observando a legislação e as normas específicas que regulam a eliminação de documentos e informações no âmbito da Administração Pública, a exemplo da tabela de temporalidade da organização.

## Exemplos práticos

Para ilustrar a aplicação prática desses conceitos, é possível observar exemplos de tratamento adequado e inadequado:

Atualizar periodicamente os dados cadastrais de servidores com base em obrigação legal, mediante controle de acesso e registro das operações realizadas; ou fazer uso compartilhado de dados entre órgãos para execução de políticas públicas, mediante respaldo normativo e transparência dos instrumentos de compartilhamento.

Utilizar dados de cidadãos obtidos em cadastro público para envio de material publicitário ou eleitoral; armazenar informações sensíveis de saúde em planilhas abertas, sem segurança adequada; ou ainda, compartilhar dados com terceiros sem respaldo legal ou transparência quanto ao seu uso.

A conformidade com a LGPD, portanto, não se limita ao cumprimento das hipóteses legais, mas exige postura ativa de todos os integrantes dos órgãos e entidades públicas na proteção dos dados pessoais, com base em princípios claros e boas práticas de governança.

# 3. Estrutura de Governança da Privacidade no Estado de São Paulo

A conformidade com a LGPD exige a atuação coordenada de diferentes instâncias de governança, tanto em nível nacional quanto no âmbito da Administração Pública Esta-dual. Esta seção apresenta os principais atores e estruturas responsáveis por orientar, regulamentar, implementar e fiscalizar o tratamento de dados pessoais no Estado de São Paulo.

## Autoridade Nacional de Proteção de Dados Pessoais (ANPD)

A ANPD é uma autarquia de natureza especial da administração pública federal, vinculada ao Ministério da Justiça e Segurança Pública, que tem a missão de zelar pela proteção de dados pessoais, nos termos da Lei nº 13.709/2018. Dentre as competências previstas no artigo 55-J da LGPD, destacamos as seguintes:

- editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei;
- fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumpri-mento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso;
- apreciar petições de titular contra controlador após comprovada pelo titular a apresentação de reclamação ao controlador não solucionada no prazo estabelecido em regulamentação;
- promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança;

- realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização, observados os requisitos da LGPD, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluído o poder público;
- implementar mecanismos simplificados, inclusive por meio eletrônico, para o registro de reclamações sobre o tratamento de dados pessoais em desconformidade com esta Lei. (Incluído pela Lei nº 13.853, de 2019)

## Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP)

O CGGDIESP, instituído pelo Decreto nº 65.347/2020, é um órgão colegiado de caráter consultivo, normativo e deliberativo, responsável por uniformizar normas e procedimentos relacionados à política de governança de dados e informações (PGDI) no âmbito da Administração Pública estadual, incluindo a implementação da LGPD, atuando como instância central de governança em proteção de dados.

## Encarregado pelo Tratamento de Dados Pessoais

O encarregado pelo tratamento de dados pessoais é a pessoa indicada para atuar co-mo ponto de contato entre o órgão ou entidade pública, os titulares dos dados e a ANPD. Sua função é indispensável para garantir a comunicação, a transparência e o cumprimento das diretrizes da LGPD no âmbito da Administração Pública.

O encarregado deve desempenhar, entre outras, as seguintes atribuições:

- Receber reclamações e comunicações dos titulares de dados pessoais;
- Receber comunicações da ANPD e adotar medidas cabíveis;
- Orientar os agentes públicos quanto às práticas de proteção de dados;

- Adotar medidas necessárias para a publicação dos relatórios de impacto, conforme solicitado pela ANPD;

No Estado de São Paulo, a designação de encarregado de proteção de dados pessoais é realizada nos termos do Capítulo III, do Decreto nº 65.347/2020. Há um encarregado centralizado para a Administração Direta e encarregados específicos nas entidades da Indireta. Essa particularidade será detalhada no tópico "Designação do Encarregado".

Além das atribuições comuns já mencionadas, cabe ao Encarregado de Proteção de Dados da Administração Direta recomendar, aos encarregados designados pelas entidades da Administração Pública Indireta, a elaboração de propostas de adequação à Política de Proteção de Dados Pessoais (PPDP).

## Agentes de Tratamento

Embora o papel do encarregado seja relevante para viabilizar a governança de dados e a conformidade com a LGPD, vale destacar que a adequação às normas de proteção de dados pessoais não se limita à atuação desse profissional. Todo o órgão ou entidade pública, por meio de seus agentes e colaboradores, possui responsabilidades específicas e intransferíveis. A conformidade é um dever institucional que exige a atuação co-ordenada de toda a estrutura organizacional.

### O Controlador

O controlador de dados é o a pessoa natural ou jurídica, de direito público ou privado, responsável pelas decisões sobre o tratamento de dados pessoais. No setor público, a ANPD orienta que essas responsabilidades devem ser atribuídas às unidades administrativas que, de fato, realizam o tratamento de dados. No Estado de São Paulo, o papel de controlador na Administração Direta é exercido pelo próprio Estado, por meio dos titulares das Secretarias de Estado e autoridades equivalentes. Já na Administração Indireta, cada autarquia, fundação, sociedade de economia mista ou empresa pública será considerada controladora quando decidir sobre as finalidades e as regras do tratamento de dados pessoais, em razão de sua autonomia jurídica.

**O Operador**

O operador é a pessoa, física ou jurídica, contratada ou designada para realizar o tratamento de dados pessoais em nome do controlador, seguindo suas orientações e sem poder de decisão sobre as finalidades do tratamento. Um exemplo comum de operador são as empresas terceirizadas que prestam serviços de processamento de dados ou operam sistemas para órgãos públicos.

É importante destacar que o operador deve ser uma entidade distinta do controlador. Assim, empregados e servidores públicos que atuam dentro do órgão ou entidade não são considerados operadores, pois exercem suas funções como profissionais subordinados ao controlador e fazem parte da estrutura organizacional da própria Administração Pública.

**Agentes Públicos e demais colaboradores**

A boa governança de dados pessoais no âmbito do Poder Executivo estadual não depende apenas dos agentes de tratamento formalmente designados (controladores e operadores). Todos os agentes públicos e demais colaboradores que atuam nos órgãos e entidades estaduais desempenham um papel central na proteção das informações pessoais sob responsabilidade da Administração Pública.

Cada servidor, empregado público, estagiário ou colaborador terceirizado, ao lidar com dados pessoais no exercício de suas funções, torna-se corresponsável pela aplicação das diretrizes da Política Estadual de Proteção de Dados Pessoais e pelo cumprimento das normas da LGPD.

A atuação diligente e consciente desses profissionais é vital para prevenir acessos não autorizados, vazamentos e usos indevidos de dados, garantir a confidencialidade e a integridade das informações pessoais, além de contribuir para a transparência e a confiança da sociedade nas ações da Administração Pública.

Por isso, a cultura de proteção de dados deve ser incorporada no cotidiano de trabalho, reforçando que a responsabilidade pela conformidade à LGPD é coletiva e abrange to-dos os níveis da organização.

## Dos Chefes de Gabinete da Administração Direta

O artigo 11 do Decreto nº 65.347/2020 atribui relevante papel aos Chefes de Gabinete das Secretarias e órgãos de hierarquia equivalente, como pode ser observado na síntese a seguir:

- observar as recomendações e atender as requisições encaminhadas pelo encarregado;
- encaminhar ao encarregado, no prazo assinalado, informações solicitadas pela ANPD, bem como Relatório de Impacto à Proteção de Dados Pessoais - RIPD, ou informações necessárias à sua elaboração;
- assegurar que o encarregado seja informado, de forma adequada e em tempo hábil, sobre o tratamento e o uso compartilhado de dados pessoais necessários à execução de políticas públicas a cargo do órgão;
- a ocorrência de incidente de segurança que possa acarretar risco ou dano rele-vante aos titulares de dados pessoais.

## Interação entre Atores

A governança da privacidade na Administração Pública Estadual pressupõe articulação constante entre as diferentes instâncias envolvidas:

A ANPD, como entidade reguladora nacional, define os regulamentos e as diretrizes, além de fiscalizar o cumprimento da LGPD;

O CGGDIESP, no plano estadual, atua como coordenador e orientador da implementação da LGPD no âmbito da Administração Pública estadual, instituindo a Política de Proteção de Dados Pessoais da Administração Pública Estadual, que contempla a com-pilação de regras de boas práticas e de governança para tratamento de dados pessoais, bem como analisar adequações promovidas por órgãos e entidades para implementação de suas respectivas políticas;

Os encarregados são responsáveis por apoiar o processo de adequação à Lei Geral de Proteção de Dados no contexto da sua instituição, atuando como interlocutor das instâncias internas com a ANPD e com os titulares de dados pessoais.

O controlador é o responsável por tomar as decisões sobre o tratamento de dados pessoais e assegurar seu alinhamento à lei, inclusive por meio da edição de normativos internos sobre a matéria, que podem incluir a instituição de um comitê, grupo ou ponto focal interno. Especialmente no caso da Administração Direta, tais estruturas podem ser relevantes para que a Chefia de Gabinete possa bem cumprir o papel que lhe foi atribuído pelo Decreto nº 65.347/2020.

O operador é o responsável por executar o tratamento de dados pessoais de acordo com as instruções do controlador, zelando pela observância da LGPD no âmbito de suas atividades.

Importante destacar que a seção II do Capítulo VII da LGPD, a qual trata das boas práticas e da governança, incentiva que os controladores e operadores, observadas suas competências, formulem regras de boas práticas e de governança para o tratamento de dados pessoais que estabeleçam:

- as condições de organização;
- o regime de funcionamento;
- os procedimentos, incluindo reclamações e petições de titulares;
- as normas de segurança; os padrões técnicos;
- 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.

Observa-se, portanto, que a comunicação eficiente entre essas instâncias é elemento-chave para garantir a promoção de boas práticas, a troca de informações estratégicas, o alinhamento às diretrizes legais e a resposta coordenada a situações de risco, como incidentes de segurança com dados pessoais. Nesse sentido, a conscientização de todos os agentes da organização, quer sejam servidores, empregados públicos, colaboradores terceirizados, estagiários, fornecedores e usuários dos serviços prestados, é determinante para a efetiva operacionalização de sua política de proteção de dados pessoais.

# 4. Etapas para a Conformidade com a LGPD

A conformidade com a Lei Geral de Proteção de Dados Pessoais exige a adoção de medidas organizacionais, técnicas e administrativas, que devem ser implementadas de forma progressiva pelos órgãos e entidades da Administração Pública. Entre as primeiras etapas estão a designação do encarregado pelo tratamento de dados pessoais e a definição da estrutura de governança interna que será responsável pelo processo de adequação. O Encarregado exerce uma função estratégica na governança da privacidade ao atuar em conjunto com o controlador e os operadores, em especial por meio da estrutura interna que tenha atribuição para desenvolver e acompanhar ações estruturantes relacionadas ao tratamento de dados pessoais. Essa atuação colaborativa é determinante para assegurar a observância dos princípios da LGPD e promover uma gestão de dados responsável, transparente e segura.

## Designação do Encarregado

### Administração Direta

No âmbito da Administração Pública Direta do Estado de São Paulo, o encarregado da proteção de dados pessoais já está formalmente designado por força do art. 6º do De-creto Estadual nº 65.347/2020, que atribui essa função ao Ouvidor Geral do Estado. Cabe a ele atuar como canal de comunicação entre o Estado, os titulares dos dados e a Autoridade Nacional de Proteção de Dados, além de apoiar tecnicamente os órgãos na implementação da Política Estadual de Proteção de Dados Pessoais (PPDP).

Cada órgão da Administração Direta deve garantir a devida divulgação das informações de contato do encarregado em seu portal eletrônico institucional, conforme previsto na legislação, assegurando transparência e acesso aos titulares de dados pessoais. Tal providência pode ser facilmente implementada por meio do direcionamento para o menu específico da página da Controladoria Geral do Estado (Canais de Comunicação > Privacidade e Proteção de Dados > Encarregado de Dados Pessoais)

**Administração Indireta**

No caso da Administração Indireta, cada entidade, de acordo com o artigo 8º do Decreto nº 65.347/2020, deve designar seu próprio encarregado pelo tratamento de dados pessoais, por meio de um ato formal da autoridade competente.

Além disso, esses encarregados devem atuar em articulação com o Ouvidor Geral do Estado. Essa articulação busca garantir alinhamento e coerência nas ações voltadas à proteção de dados pessoais em toda a estrutura estadual.

**Perfil e competências recomendadas**

Embora a LGPD não tenha especificado o perfil ou as habilidades exigidas para o encarregado, o Guia Orientativo da ANPD - Atuação do encarregado pelo tratamento de dados, sugere que o perfil desejável seja multidisciplinar, com conhecimentos em proteção de dados, gestão de riscos, governança, compliance e segurança da informação. Esse profissional deve ter capacidade para dialogar com diferentes áreas, lidar com situações complexas e compreender as atividades principais da organização, atuando como elo entre o controlador, o operador, a ANPD e os titulares dos dados, a fim de assegurar a conformidade com a LGPD e a implementação de boas práticas de proteção de dados.

## Criação de estrutura de governança interna

Para viabilizar a implementação efetiva da LGPD no âmbito dos órgãos e entidades da Administração Pública Estadual, é primordial a definição de uma estrutura interna de governança da privacidade, mesmo que simplificada. Essa estrutura permite o acompanhamento contínuo das ações de adequação, a articulação entre as áreas envolvidas e o apoio ao encarregado pelo tratamento de dados pessoais.

### Definição de comissão interna, grupo de trabalho ou ponto focal

Cada órgão ou entidade deve avaliar, conforme seu porte e complexidade, a conveniência administrativa da criação de uma comissão interna, de um grupo de trabalho multidisciplinar ou a definição de uma área específica que atue como ponto focal para proteção de dados pessoais e atue de forma coordenada com o encarregado. Esse grupo ou área será responsável por coordenar internamente os esforços de adequação à LGPD, em articulação com o encarregado e com o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP), quando necessário.

A comissão interna ou grupo de trabalho pode contar com representantes das áreas jurídica, tecnologia da informação, ouvidoria, gestão documental, segurança da informação e áreas finalísticas que realizem tratamento de dados pessoais.

### Atribuições e periodicidade de reuniões

As atribuições da comissão interna, do grupo de trabalho ou ponto focal podem incluir:

Participar em conjunto com o encarregado na condução das ações de conformidade.

Coordenar a elaboração e atualização do inventário de dados pessoais.

Mapear riscos e propor medidas de mitigação.

Articular ações de capacitação e sensibilização sobre proteção de dados.

Avaliar situações que envolvam incidentes de segurança com dados pessoais.

Acompanhar a execução do plano de ação de adequação à LGPD.

É uma boa prática que a comissão interna ou o grupo de trabalho se reúna com regularidade, por exemplo, uma vez por mês ou a cada trimestre, para acompanhar o anda-mento das ações, trocar informações, revisar materiais e alinhar próximos passos. Sempre que possível, é interessante manter registros simples dessas reuniões, como resumos ou apontamentos, para facilitar o acompanhamento das decisões e garantir mais transparência no processo.

## Transparência e Divulgação de Informações sobre Privacidade e Proteção de Dados

Um dos elementos primordiais para assegurar a transparência e a conformidade com a LGPD no âmbito da Administração Pública é a adequação das informações disponibilizadas na página oficial do órgão ou entidade. Essa etapa está diretamente fundamentada no princípio da transparência (art. 6º, VI, da LGPD) e no direito de acesso facilita-do aos titulares às informações sobre o tratamento de seus dados (art. 9º da LGPD).

Além disso, no setor público, o art. 23, inciso I, da Lei Geral de Proteção de Dados estabelece que a Administração Pública deve disponibilizar informações claras e atualizadas sobre o tratamento de dados pessoais, bem como as medidas de segurança adotadas. Já o art. 41, §1º, estabelece a necessidade de indicar o encarregado pelo trata-mento de dados pessoais e de divulgar seus dados de contato, viabilizando a comunicação com os titulares e com a ANPD.

Assim, a página oficial deve conter, de forma destacada e em linguagem clara, informações que permitam aos titulares dos dados compreenderem como seus dados são tratados e quais são seus direitos. Isso inclui:

- A publicação da Política de Privacidade e Proteção de Dados Pessoais, com os procedimentos e práticas para a execução dessas atividades, contendo as finalidades e bases legais aplicadas;
- A identificação do encarregado e seus dados de contato;
- Informações claras sobre os direitos dos titulares e a forma de exercê-los;
- Detalhes sobre as medidas de segurança e mecanismos de prevenção adotados pela instituição para proteger os dados pessoais.

Essa etapa reforça o compromisso do órgão ou entidade com a transparência, a segurança e a proteção dos dados pessoais, assegurando o alinhamento às diretrizes da LGPD e fortalecendo a confiança dos cidadãos no uso de seus dados.

## Comunicação com a ANPD

Cabe ao encarregado representar institucionalmente o órgão ou entidade junto à ANPD, prestando informações, recebendo notificações e atuando de forma cooperativa com a autoridade nacional, conforme estabelece o art. 41 da LGPD e a Resolução CD/ANPD nº 18/2024.

Para os órgãos da Administração Direta, essa interlocução é centralizada pela Ouvido-ria Geral do Estado, que responde às comunicações da ANPD e coordena o atendimento às demandas nos órgãos estaduais, uma vez que o titular da OGE exerce a atribuição de Encarregado de Proteção de Dados Pessoais da Administração Direta.

As entidades da Administração Indireta devem realizar o cadastro de seus encarrega-dos diretamente no sistema da ANPD, conforme procedimentos definidos pela autoridade.

## Inventário de Dados Pessoais

O inventário de dados pessoais é mais uma etapa essencial para a conformidade com LGPD, a qual estabelece, em seu art. 37, a necessidade de manter registros das operações de tratamento de dados pessoais.

Contudo, sua elaboração não precisa abranger, de imediato, todos os processos existentes na organização. Em linha com os princípios de boas práticas e de gestão de riscos previstos no art. 50 da LGPD, pode-se adotar uma abordagem gradativa, priorizando a identificação e mapeamento dos processos de trabalho mais relevantes e sensíveis, que envolvam dados pessoais em maior escala ou com maior potencial de impacto. Essa estratégia permite iniciar o processo de adequação de maneira mais objetiva, ajudando a reduzir a complexidade inicial e favorecendo avanços graduais na proteção de dados, a partir das áreas mais críticas.

Nesse sentido, o art. 25, § 4º, da Deliberação Normativa CGGDIESP-2, estabelece que o inventário deve conter, no mínimo, a base legal, a finalidade, o compartilhamento e o local de armazenamento dos dados. Esse mapeamento permite identificar quais dados são tratados, quem é responsável por esse tratamento, com que finalidade são utiliza-dos, onde estão armazenados e por quanto tempo são retidos, promovendo transparência e segurança no processo de adequação à LGPD.

Esse inventário funciona como a base para identificar riscos, corrigir inconformidades, definir políticas de proteção de dados e implementar medidas de segurança apropria-das. Além disso, permite à organização atender de forma adequada às exigências legais, como o atendimento aos direitos dos titulares e a prestação de contas à ANPD.

**Roteiro prático para elaboração**

A seguir, apresenta-se um roteiro prático para construção do inventário de dados pessoais

**Engajamento das áreas internas**

Envolver as áreas que tratam dados pessoais, como jurídico, financeiro, recursos humanos, segurança da informação, comunicação, tecnologia da informação, entre outras.

Definir responsáveis por cada etapa do levantamento e esclarecimento das informações necessárias.

**Identificação do processo de trabalho**

Relacionar os dados pessoais tratados nos processos de trabalho da organização, não se restringindo a ferramentas ou sistemas específicos.

Exemplo: "Atendimento ao titular de dados pessoais" - as informações podem ser coletadas por meio de formulários online, registros de ligações telefônicas ou atendimento presencial. Mesmo que existam diferentes sistemas e canais, o inventário deve mapear

como esses dados são tratados em todas as etapas, desde o recebimento do pedido até a resposta ao titular, considerando o fluxo, as responsabilidades e os riscos envolvidos.

Essa abordagem garante uma visão completa e integrada de como os dados são utilizados e protegidos ao longo do ciclo de vida do processo de trabalho.

### Levantamento do fluxo do tratamento

Descrever o caminho percorrido pelos dados desde a coleta até o descarte, quando couber: forma de coleta (formulário eletrônico, sistema, e-mail, etc.), armazenamento, uso e forma de descarte.

Exemplo: No processo de inscrição em um curso de capacitação, os dados pessoais dos participantes são coletados por meio de um formulário eletrônico disponível no site da instituição. Esses dados são armazenados em um sistema interno de gestão de cursos. Durante o uso, as informações são acessadas pela equipe responsável para organizar as turmas, emitir certificados e enviar comunicações relacionadas ao curso. Após a conclusão das atividades e o prazo definido na Tabela de Temporalidade, os dados serão descartados de forma segura, sendo excluídos do sistema.

### Identificação dos dados tratados

Listar claramente os dados pessoais tratados. Exemplo: nome completo, CPF, e-mail institucional, dados bancários.

### Classificação dos dados tratados

Indicar se os dados são: Hipótese legal para o tratamento

**Pessoais:** que identificam ou podem identificar uma pessoa física.

**Pessoais Sensíveis:** que tratam de origem racial, convicção religiosa, dados de saúde, aspectos da vida sexual, dados biométricos etc.

**Hipótese legal para o tratamento**

Identificar o inciso do art. 7º da LGPD (ou art. 11 para dados pessoais sensíveis) que fundamenta o tratamento. Exemplo: art. 7º, inciso II – cumprimento de obrigação legal ou regulatória.

**Finalidade do tratamento**

Justificar institucionalmente o motivo da coleta e uso dos dados. Exemplo: execução de contrato, atendimento ao titular, política pública.

**Base legal/normativa complementar**

Indicar a norma, decreto, contrato ou outro instrumento jurídico que autoriza ou exige o tratamento. Exemplo: Lei nº 12.527/2011 (Lei de Acesso à Informação), Decreto nº 68.155/2023.

**Forma de coleta dos dados**

Descrever como os dados são obtidos. Exemplo: formulário eletrônico, atendimento presencial, e-mail institucional.

**Sistemas utilizados**

Informar os sistemas em que os dados são armazenados ou processados. Exemplo: SEI, Fala.SP.

**Período de retenção**

Indicar por quanto tempo os dados são armazenados, de acordo com o Plano de Classificação e a Tabela de Temporalidade de Documentos, quando couber (Decreto nº 63.382/2018).

**Forma de descarte**

Descrever o método de eliminação ao final do período de retenção, quando couber. Exemplo: exclusão da base de dados, destruição física segura.

**Medidas de segurança**

Registrar as medidas adotadas para garantir a proteção dos dados pessoais. Exemplo: acesso restrito por perfis, uso de senhas, criptografia.

**Compartilhamento de dados pessoais**

Informar se há compartilhamento de dados pessoais com outras entidades.

O compartilhamento de dados pessoais pelo Poder Público, conforme capítulo IV da LGPD e Guia Orientativo da ANPD sobre Tratamento de dados pessoais pelo Poder Público, é a operação em que órgãos e entidades públicas transferem ou permitem o acesso a bases de dados para outros entes públicos ou privados, sempre com finalidades públicas específicas. Esse uso compartilhado deve ser formalizado, justificado e registrado, com base legal clara, medidas de segurança, respeito aos direitos dos titulares e duração definida, assegurando a transparência e a confiança, bem como deve ser avaliada a eventual incidência de hipótese de compartilhamento com entidade privada que necessite de comunicação à ANPD, nos termos dos artigos 26 e 27 da LGPD.

No caso específico da Administração Direta do Estado de São Paulo, é importante ressaltar que a atuação do Poder Público ocorre de forma desconcentrada, sendo o controlador de dados o próprio Estado. Por isso, quando dados pessoais transitam entre órgãos da Administração Direta, isso não é considerado necessariamente um compartilhamento, mas sim uma continuidade do tratamento. Mesmo nesses casos, continuam valendo as exigências de registro e o respeito aos princípios da LGPD.

**Transferência internacional**

Indicar se há transferência de dados para fora do país e quais dados são transferidos.

Essa prática de transferência internacional de dados pessoais está sujeita a restrições e salvaguardas previstas no Capítulo V da LGPD. Isso significa que a transferência somente pode ocorrer se houver mecanismos adequados de proteção (como cláusulas contratuais específicas, normas corporativas globais, ou se o país de destino

possuir grau de proteção de dados pessoais equivalente ao previsto na legislação brasileira).

Além disso, é necessário garantir a transparência e a segurança dos dados transferi-dos, bem como a possibilidade de exercício dos direitos dos titulares, mesmo fora do país.

**Atualização e governança do inventário**

Consolidar as informações em um documento ou planilha e manter o inventário atua-lizado conforme mudanças nos processos, sistemas, finalidades ou legislações aplicá-veis.

## Avaliação de Riscos e Segurança da Informação

A avaliação de riscos no tratamento de dados pessoais é uma etapa determinante para garantir a conformidade com a LGPD. Essa avaliação permite identificar vulnerabilidades nos processos, sistemas e rotinas institucionais, bem como definir medidas de mitigação adequadas para proteger os dados contra acessos não autorizados, vazamentos, perdas ou outras formas de uso indevido, levando em conta a estrutura da organização, a escala e volume de suas operações, a sensibilidade dos dados tratados, bem como a probabilidade e gravidade de eventuais danos aos titulares.

Portanto, a proteção de dados deve estar alinhada aos princípios da segurança e da prevenção (art. 6º, VII e VIII da LGPD), cabendo ao controlador a adoção de medidas técnicas e administrativas disponíveis e aptas a proteger os dados pessoais, considerando a natureza da informação, as características da operação e os riscos envolvidos.

**Boas práticas**

As seguintes boas práticas contribuem para ampliar a efetividade da proteção dos da-dos pessoais e o fortalecimento de uma cultura que privilegie o adequado tratamento de dados pessoais na organização:

- Mapeamento contínuo dos riscos relacionados ao ciclo de vida dos dados, incluindo coleta, uso, armazenamento, compartilhamento e descarte, especialmente nos processos mais relevantes, considerando as variáveis de impacto e probabilidade relacionadas a esses riscos;
- Classificação da informação de acordo com o grau de sensibilidade dos dados tratados;
- Treinamento e capacitação periódica das equipes sobre privacidade, segurança da informação e boas práticas de tratamento de dados pessoais;
- Revisão de contratos e convênios que envolvam o compartilhamento de dados com terceiros, com cláusulas específicas sobre proteção de dados;
- Monitoramento regular para avaliação da conformidade e identificação de fragilidades nos controles existentes;
- Gestão de incidentes com plano estruturado para resposta e comunicação à ANPD e aos titulares, quando necessário.
- Medidas técnicas e administrativas adequadas.

A seguir, apresentam-se medidas que devem ser consideradas no setor público estadual para prover a segurança da informação e mitigar riscos no tratamento de dados pessoais:

**Medidas técnicas (foco em processos de trabalho):**

- Definição clara de fluxos de tratamento de dados pessoais nos processos de trabalho, com etapas bem delimitadas de coleta, uso, compartilhamento, armazenamento e descarte;
- Restrição de acesso aos dados pessoais apenas às unidades ou servidores que necessitam dessas informações para execução das atividades, conforme princípios de necessidade e minimização;
- Adoção de formulários padronizados para a coleta de dados

pessoais, com campos definidos conforme a finalidade do tratamento;

- Registro sistemático das operações de tratamento realizadas no processo (ex: recebimento, consulta, envio, alteração ou eliminação de dados);
- Utilização de sistemas e ferramentas oficiais para execução dos processos, evitando o uso de meios informais ou não autorizados (como e-mails pessoais, planilhas locais não protegidas etc.);
- Organização e controle do armazenamento de documentos e registros que contenham dados pessoais, físicos ou digitais, com indicação de tempo de guarda e critérios para eliminação conforme tabela de temporalidade.

**Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD)**

Nos casos em que forem identificados riscos relevantes às liberdades civis e garantias fundamentais dos titulares, a elaboração de um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) será necessária. Previsto no art. 38 da LGPD, o RIPD deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

A elaboração do RIPD reforça a transparência e a responsabilidade do controlador, além de ser uma ferramenta de prestação de contas, que poderá ser solicitado pela ANPD em auditorias ou processos de fiscalização.

Portanto, diante da constatação de riscos significativos ao tratamento de dados pessoais, a elaboração de um RIPD deve integrar o ciclo de governança e segurança da informação, assegurando que as decisões institucionais priorizem a conformidade com a LGPD e a confiança dos titulares.

A Autoridade Nacional de Proteção de Dados disponibiliza em sua página um "Perguntas e Respostas" bem completo, que pode auxiliar significativamente a elaboração de um RIPD.

# 5. Direitos dos Titulares e Atendimento

A LGPD dispõe sobre o estímulo à adoção de padrões técnicos que facilitem o controle pelos titulares dos seus dados pessoais, dispondo, especialmente em seu Capítulo III, sobre os direitos dos titulares, tais como acesso, retificação, anonimização, eliminação, portabilidade, revogação de consentimento e informações sobre o compartilhamento. Esses direitos, didaticamente abordados como ARCO (acesso, retificação, cancelamento e oposição), são reconhecidos como indispensáveis para a proteção de dados pessoais, conforme o Guia de Direitos dos Titulares da ANPD e artigos 9º e 18 da Lei nº 13.709/2018. Eles asseguram que os titulares possam supervisionar e decidir como seus dados são tratados, reforçando a autodeterminação informativa.

O reconhecimento desses direitos não se limita à legislação brasileira, estando presente, por exemplo, no General Data Protection Regulation (GDPR), regulamento europeu sobre a proteção de dados pessoais. Nesse sentido, cabe acrescentar que tanto o Trata-do da União Europeia (TUE) quanto a Carta dos Direitos Fundamentais da União Euro-peia (CDFUE) garantem aos cidadãos europeus o direito à proteção dos dados pessoais que lhes dizem respeito. Esse arcabouço europeu foi fundamental para a criação dos direitos ARCO, que representam os pilares do controle do indivíduo sobre seus próprios dados (BLADES; HERRERA-GONZÁLEZ, 2016).

No contexto da Administração Pública Estadual, garantir o atendimento adequado a essas demandas, observando os direitos dos titulares de dados pessoais, é primordial para promover transparência, confiança e respeito aos direitos dos cidadãos.

## Canais de atendimento ao titular

O principal canal para o exercício dos direitos dos titulares no Estado de São Paulo é a Plataforma Integrada de Ouvidoria e Acesso à Informação - FALA.SP, disponível no endereço https://www.falasp.sp.gov.br, especialmente na Administração Direta, estando aderente ao disposto no § 3º do art. 23 da LGPD. Por meio dessa plataforma, qualquer titular de dado pessoal pode registrar manifestações relacionadas a:

Pedidos de acesso à informação para os casos de confirmação de existência ou acesso a dados pessoais;

Solicitações de providências ou reclamações para as demais demandas relacionadas à proteção de dados pessoais;

Cada órgão ou entidade deve acompanhar periodicamente as manifestações recebidas pela Plataforma FALA.SP, garantindo respostas dentro dos prazos legais e com informações claras e completas.

## Fluxo de resposta a requisições

Embora cada instituição possa adaptar seu procedimento conforme sua estrutura, recomenda-se a adoção de um fluxo básico de atendimento aos titulares:

1. Recebimento da solicitação via Plataforma Fala.SP (Ouvidoria e SIC);

Esse procedimento ocorre em conformidade com o art. 23 da LGPD, que autoriza o tratamento de dados pessoais por órgãos e entidades para o atendimento de suas finalidades e no exercício de competências legais, citando expressamente em seu § 3º a observância, conforme a natureza da demanda, dos prazos e procedimentos da Lei nº 12.527/2011 (Lei de Acesso à Informação), bem como o disposto em outras leis específicas, sendo, portanto, também aplicável ao Poder Executivo estadual a Lei federal nº 13.460/2017, que dispõe sobre a participação, proteção e defesa do usuário de serviços públicos, definindo prazos e procedimentos para o tratamento de manifestações de ouvidoria.

2. Análise preliminar da demanda para verificar se está clara e completa;

3. Encaminhamento à área responsável pelo tratamento dos dados, inclusive ao encarregado, quando for o caso;

4. Resposta técnica elaborada com base na LGPD e na realidade do tratamento;

5. Retorno ao titular, por meio da própria plataforma.

## Integração com a LAI e as Ouvidorias

A interface entre a LGPD, a LAI e a Lei nº 13.460/2017 é determinante para assegurar o equilíbrio entre transparência, acesso à informação e proteção de dados pessoais no serviço público. A LAI garante o direito de acesso às informações públicas, promovendo a participação cidadã, enquanto a LGPD assegura o adequado tratamento de dados pessoais durante todo o seu ciclo de vida.

Observa-se, portanto, a existência de enfoques complementares e harmônicos: ambas promovem a transparência na administração pública, ao mesmo tempo em que garantem a proteção dos dados pessoais dos cidadãos, fortalecendo a confiança, a segurança jurídica e a legitimidade democrática na gestão das informações públicas (BIONI et al., 2022).

Já a Lei nº 13.460/2017 reforça o papel das Ouvidorias na proteção dos direitos dos usuários, estabelecendo diretrizes para o recebimento e encaminhamento de manifestações sobre a prestação dos serviços públicos, inclusive no que diz respeito à forma como os dados pessoais são tratados.

Assim, essas legislações dão o fundamento para que os pedidos de acesso a dados pessoais sejam tratados pelo Serviço de Informação ao Cidadão - SIC, observando prazos e procedimentos da LAI, enquanto as manifestações relacionadas a providências sobre o tratamento de dados pessoais devem ser analisadas pelas Ouvidorias, em conformidade com a Lei nº 13.460/2017. Essa integração normativa garante que os titulares tenham seus direitos respeitados e possam exercer controle efetivo sobre o tratamento de suas informações pessoais.

Essa distinção ajuda a organizar o fluxo interno de trabalho e a garantir que cada tipo de demanda seja endereçado corretamente. A atuação coordenada entre os responsáveis pela LAI, pela Ouvidoria e pela proteção de dados é essencial para assegurar respostas adequadas, consistentes e em conformidade com a legislação vigente.

Cabe acrescentar, ainda, que o reporte de incidentes envolvendo dados pessoais possui procedimento específico definido pela Resolução CD/ANPD nº 15/2024, dada a urgência do reporte a ser dado ao encarregado para comunicação imediata à ANPD, quando puder acarretar risco ou dano relevante aos titulares, nos termos do art. 48 da LGPD, como veremos a seguir.

# 6. Gestão de Incidentes de Segurança com Dados Pessoais

A gestão de incidentes de segurança é indispensável para proteger dados pessoais e mitigar riscos como vazamentos e acessos indevidos. A Resolução CD/ANPD nº 15/2024 estabelece diretrizes e procedimentos para a notificação e resposta a esses incidentes, complementando as exigências da LGPD e fortalecendo a confiança dos titulares, definindo que a comunicação de incidente de segurança à ANPD deverá ser realizada pelo controlador, por intermédio do encarregado, no prazo de três dias úteis, podendo ser complementada, justificadamente, no prazo de 20 dias úteis da comunicação inicial. Ou seja, o órgão ou entidade deve adotar providências imediatas com as informações que dispuser, não sendo adequado aguardar o levantamento de todas os itens para só depois providenciar o comunicado à autoridade nacional.

A norma da ANPD dispõe sobre o que pode acarretar risco ou dano relevante aos titulares em um incidente de segurança, que deve ser caracterizado a partir de seu potencial para "afetar significativamente interesses e direitos fundamentais dos titulares", envolvendo, cumulativamente, ao menos um dos seguintes critérios:

I - dados pessoais sensíveis;

II - dados de crianças, de adolescentes ou de idosos;

III - dados financeiros;

IV - dados de autenticação em sistemas;

V - dados protegidos por sigilo legal, judicial ou profissional; ou

VI - dados em larga escala.

Ainda, menciona no § 1º de seu artigo 5º que:

> "O incidente de segurança que possa afetar significativamente interesses e direitos fundamentais será caracterizado, dentre outras situações, naquelas em que a atividade de tratamento puder impedir o exercício de direitos ou a utilização de um serviço, assim como ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou roubo de identidade."

Dentre as informações mais relevantes a serem imediatamente levantadas para comunicação à ANPD, o § 2º do artigo 6º da Resolução CD/ANPD nº 15/2024 destaca as seguintes:

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;

III - as medidas técnicas e de segurança utilizadas para a proteção dos dados pessoais, adotadas antes e após o incidente, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

V - os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador;

VIII - os dados do encarregado ou de quem represente o controlador;

IX - a identificação do controlador e, se for o caso, declaração de que se trata de agente de tratamento de pequeno porte;

X - a identificação do operador, quando aplicável;

XI - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e

XII - o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente.

Dada a relevância de uma gestão eficaz de incidentes, observamos a necessidade de que seja seguido um conjunto de etapas bem definidas:

**Detecção:** identificação da ocorrência ou suspeita de incidente, por meio de canais internos, monitoramento de sistemas ou relato de terceiros.

**Contenção:** adoção imediata de medidas para evitar o agravamento da situação, como bloqueio de acessos, interrupção de processos ou isolamento de sistemas afetados.

**Notificação:** avaliação da gravidade do incidente e, se necessário, comunicação às instâncias competentes, como:

- Titulares de dados afetados;
- Encarregado de dados;
- Autoridade Nacional de Proteção de Dados, sempre por meio do encarregado de dados.

**Mitigação:** execução de ações corretivas para reduzir danos, restaurar sistemas e implementar melhorias para prevenir recorrências

A resposta adequada e tempestiva pode minimizar os impactos e evitar sanções administrativas.

# 7. Capacitação e Cultura de Proteção de Dados

A proteção de dados pessoais na Administração Pública vai além da adoção de medi-das técnicas e legais. A efetiva implementação da LGPD guarda estreita relação com a cultura organizacional, com o engajamento de todos os servidores e colaboradores no respeito à privacidade e no uso responsável das informações pessoais. Para isso, é preciso investir em capacitação contínua e estratégias de sensibilização.

## Medidas de sensibilização

Promover uma cultura de proteção de dados envolve ações educativas que tornem o tema parte do cotidiano institucional. Boas práticas incluem:

- inserir a pauta de proteção de dados em reuniões internas e comunicados institucionais;
- utilizar campanhas temáticas (ex: "Semana da Privacidade") para divulgar conceitos-chave;
- estimular a participação dos servidores em atividades de formação sobre o tema;
- valorizar e divulgar boas práticas já adotadas por setores ou equipes.

A sensibilização deve alcançar não apenas áreas técnicas e jurídicas, mas todos os envolvidos em atividades que tratam dados pessoais, incluindo atendimento ao público, recursos humanos, tecnologia da informação e demais áreas administrativas e finalísticas.

## Canais divulgação e formatos possíveis

A diversidade de formatos ajuda a alcançar públicos variados e a manter o interesse pelo tema. Entre os recursos que podem ser utilizados, destacam-se:

- vídeos curtos e didáticos sobre conceitos básicos da LGPD;
- cartilhas e folhetos digitais, com linguagem acessível e exemplos práticos;
- cursos em formato e-learning, com trilhas formativas personalizadas;
- palestras, seminários e eventos presenciais ou virtuais, com especialistas inter-nos ou externos;
- capacitações promovidas em parceria com a CGE, PRODESP ou a Escola de Governo do Estado de São Paulo (EGESP).

É determinante manter um repositório institucional com os materiais produzidos e divulgar os conteúdos de forma contínua nos canais internos.

## Indicadores de adequação à LGPD

Acompanhar a adequação da organização à LGPD é importante para fortalecer a cultura de proteção de dados e assegurar o cumprimento das obrigações legais. Para isso, sugere-se o uso de indicadores que permitam medir avanços e identificar áreas que demandam aprimoramento. Alguns exemplos de indicadores de adequação à LGPD incluem:

- percentual de servidores capacitados sobre LGPD;
- grau de conhecimento percebido pelos servidores (via pesquisa interna);
- incorporação de critérios de proteção de dados em processos de trabalho e normativos;
- existência e aplicação de planos de resposta a incidentes de segurança com da-dos pessoais;
- existência e atualização de políticas e normativos internos sobre privacidade.

Esses indicadores auxiliam na identificação de pontos de melhoria e no planejamento de ações futuras, fortalecendo a governança de dados e a conformidade com a LGPD.

# 8. Monitoramento e Melhoria Contínua

A adequação à LGPD não se esgota em ações pontuais. Trata-se de um processo contínuo, que exige monitoramento constante, atualização de práticas e melhoria dos controles internos. A cultura que privilegia a proteção de dados deve ser mantida ativa ao longo do tempo, com atenção a novos riscos, mudanças tecnológicas, normativas e organizacionais.

## Monitoramento interno

Cada órgão ou entidade deve estabelecer mecanismos internos de acompanhamento da conformidade, garantindo que os processos de tratamento de dados pessoais continuem aderentes à legislação e às políticas institucionais. Algumas boas práticas incluem:

**Verificações** periódicas do inventário de dados pessoais.

**Avaliações** internas de riscos e controles relacionados à privacidade.

**Revisão** de contratos, formulários e sistemas que tratam dados pessoais.

**Análise** de ocorrências relacionadas a incidentes ou manifestações de titulares.

A atuação do encarregado, com apoio do comitê, grupo de trabalho ou ponto focal é 9. para promover esse monitoramento contínuo.

## Atualização de políticas e procedimentos

As políticas, normas internas e procedimentos relacionados à proteção de dados devem ser revistos e atualizados sempre que houver mudanças relevantes na estrutura organizacional, nos sistemas de informação, nos

fluxos de tratamento de dados ou na legislação aplicável.

Recomenda-se a revisão periódica, ao menos anual, dos seguintes documentos:

- Inventário de dados pessoais;
- Fluxos de atendimento a titulares;
- Planos de resposta a incidentes;
- Termos de uso e avisos de privacidade publicados nos canais oficiais.

A manutenção desses documentos atualizados reforça o compromisso com a transparência institucional

## Relatórios periódicos

Os órgãos e entidades da Administração Pública Estadual podem elaborar relatórios periódicos de acompanhamento das ações relacionadas à proteção de dados pessoais, como forma de registrar o andamento das atividades, identificar avanços, apontar desafios e orientar decisões futuras. Esses relatórios também servem como base para relatórios gerencias e para o fortalecimento da governança interna em proteção de dados.

Esses relatórios podem incluir:

- Etapas concluídas e pendentes do plano de adequação;
- Quantitativo de manifestações de titulares recebidas e atendidas;
- Medidas de capacitação e sensibilização promovidas;
- Ocorrência e tratamento de incidentes de segurança com dados pessoais.

Essas informações são úteis para o acompanhamento do grau de maturidade dos órgãos e entidades, além de permitir o planejamento de ações integradas de apoio e capacitação.

# 9. Saiba Mais!

A conformidade com a LGPD é um compromisso contínuo e indispensável para a Administração Pública, exigindo atenção permanente aos processos, à cultura de proteção de dados e às demandas dos titulares. Nesse contexto, destaca-se o papel orientativo da Controladoria Geral do Estado de São Paulo (CGE), que, por meio da Ouvidoria Geral do Estado (OGE), atua como ponto de apoio para órgãos e entidades no processo de adequação à LGPD.

A CGE está à disposição para oferecer orientações e esclarecer dúvidas sobre a aplicação da LGPD, em especial no âmbito da Administração Direta. A Coordenadoria de Proteção de Dados da CGE atua para auxiliar as áreas na implementação das diretrizes da lei, a fim de que as práticas estejam alinhadas à legislação vigente e promovendo a melhoria contínua na governança de dados.

Para entrar em contato com a Coordenadoria de Proteção de Dados e contar com o apoio orientativo da CGE, utilize o e-mail: dai.cge@sp.gov.br

Para acesso aos guias e manuais elaborados pela Autoridade Nacional de Proteção de Dados, consulte https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/materiais-educativos.

Para conhecer um pouco mais sobre a Política Estadual de Proteção de Dados Pessoais, além das finalidades, fundamentos e princípios aplicados ao tratamento de dados pessoais realizado pela Controladoria Geral do Estado, consulte https://www.controladoriageral.sp.gov.br/cge/canaisComunicacao/privacidade_e_protecao_de_dados_lgpd.

A atuação integrada e colaborativa dos órgãos e entidades é determinante para fortalecer a governança em privacidade e assegurar a proteção dos direitos dos titulares de dados pessoais no âmbito do Governo do Estado de São Paulo.

São Paulo são todos!

# Links Úteis e Referências

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Atuação do encarregado pelo tratamento de dados pessoais. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_da_atuacao_do_encarregado_anpd.pdf/view. Acesso em: 07 agosto 2025.

_____. Autoridade Nacional de Proteção de Dados (ANPD). Definições dos agentes de tratamento de dados pessoais e do encarregado - versão 10-2021. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-agentes-de-tratamento-e-encarregado-versao-1-0-defeso-eleitoral.pdf. Acesso em: 07 agosto 2025.

_____. Autoridade Nacional de Proteção de Dados (ANPD). Hipóteses legais de trata-mento de dados pessoais – Legítimo interesse. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publica-co-es/guia_orientativo_hipoteses_legais_tratamento_de_dados_pessoais_legitimo_interesse. Acesso em: 07 agosto 2025.

_____. Autoridade Nacional de Proteção de Dados (ANPD). Tratamento de dados pessoais pelo Poder Público. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_orientativo_tratamento_de_dados_pessoais_pelo_poder_publico. Acesso em: 07 agosto 2025.

_____. Autoridade Nacional de Proteção de Dados (ANPD). Resolução CD/ANPD nº 15, de 24 de abril de 2024. Diário Oficial da União: seção 1, Brasília, DF, 25 abr. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024. Acesso em: 28 maio 2025.

_____. Autoridade Nacional de Proteção de Dados (ANPD). Resolução CD/ANPD nº 18, de 16 de julho de 2024. Diário Oficial da União: seção 1, Brasília, DF, 17 jul. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-18-de-16-de-julho-de-2024-572632074. Acesso em: 28 maio 2025.

_____. Comitê Central de Governança de Dados. Guia LGPD: proteção de dados pes-soais. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/guias/guia_lgpd.pdf. Acesso em: 28 maio 2025.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm. Acesso em: 28 maio 2025.

_____. Lei nº 13.460, de 26 de junho de 2017. Dispõe sobre participação, proteção

e defesa dos direitos do usuário dos serviços públicos da administração pública. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13460.htm. Acesso em: 28 maio 2025.

_____. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pes-soais e altera outras leis. Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 28 maio 2025.

BIONI, Bruno Ricardo; DA SILVA, Paula Guedes Fernandes; MARTINS, Pedro Bastos Lobo. Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito do acesso. Cadernos Técnicos da CGU, ano 2022, v.1, p. 9-12, mar/2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504. Acesso em: 06 agosto de 2025.

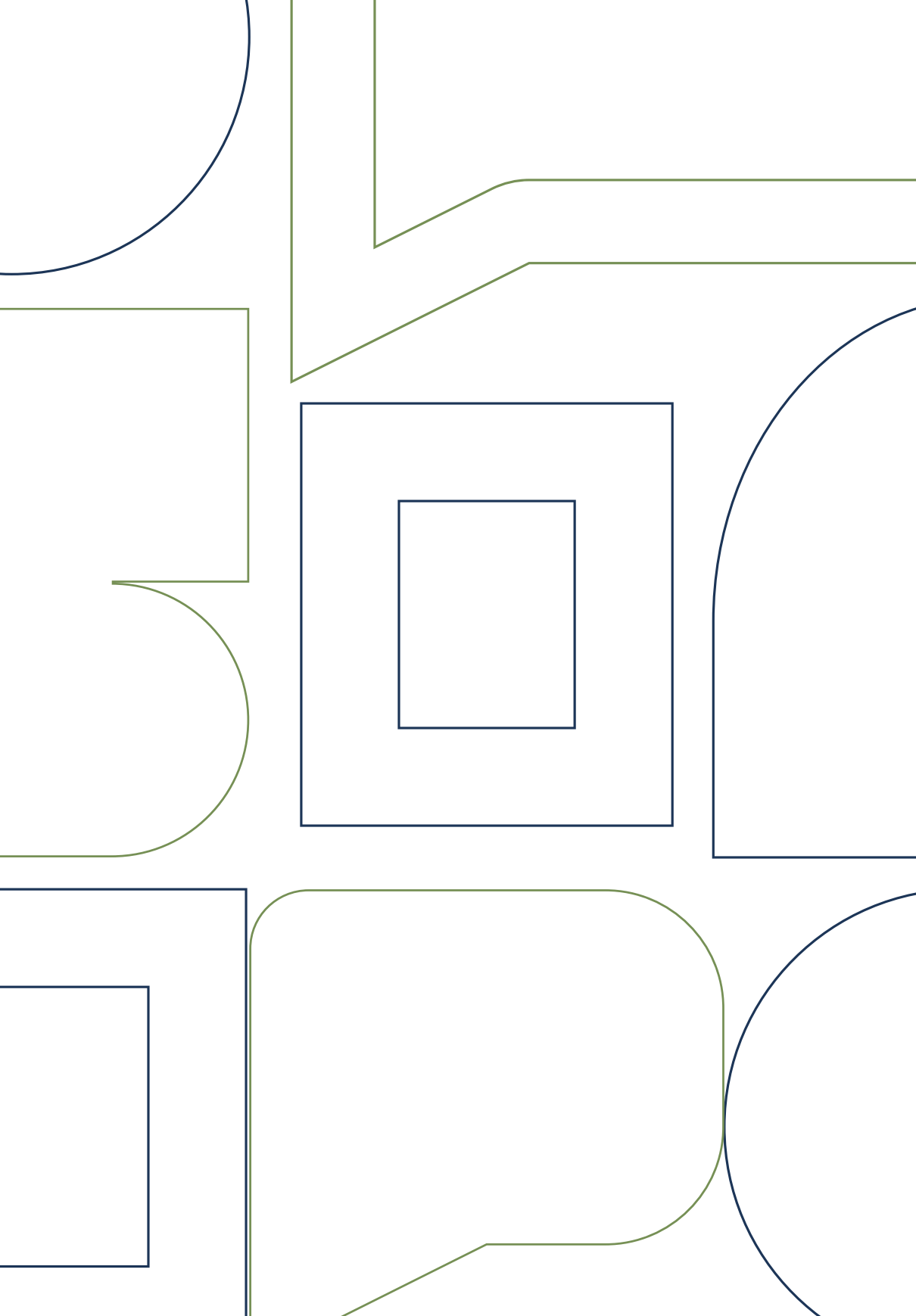
BLADES, Nicholas; HERRERA-GONZÁLEZ, Fernando. An Economic Analysis os Personal Data Protection Obligations in the European Union. Conference Paper, 27th European Regional Conference of the International Telecommunications Society (ITS): "The Evolu-tion of the North-South Telecommunications Divide: The Role for Europe", ano 2016, p. 12-13, set.2016. Disponível em: https://www.econstor.eu/bitstream/10419/148661/1/Blades-Herrera-Gonzalez.pdf . Acesso em: 06 agosto de 2025.

CRISTÓVAM, José Sérgio da Silva; BERGAMINI, José Carlos Loitey; HAHN, Tatiana Meinhart. Governança de dados no setor público brasileiro: uma análise a partir da Lei Geral de Proteção de Dados (LGPD). Interesse Público, ano 23, n. 129, p. 75-101, set./out. 2021. Disponível em: https://bd.tjmg.jus.br/bitstreams/6f402190-80fa-459b-b4ef-89f06d583117/download. Acesso em: 28 maio 2025.

Rede Nacional de Ouvidorias. Guia de boas práticas da LGPD – 2. ed. Disponível em: https://www.gov.br/ouvidorias/pt-br/central-de-conteudos/produtos_da_renouv/guiadeboaspraticasdalgpd2ed.pdf. Acesso em: 28 maio 2025.

SÃO PAULO. Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo. Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021. Aprova as diretrizes para o Inventário de Dados Pessoais. Disponível em: https://cggdiesp.sp.gov.br/cdesp/cggdiesp/normativos. Acesso em: 28 maio 2025.

_____. Decreto nº 65.347, de 9 de dezembro de 2020. Dispõe sobre a Política de Privacidade e Proteção de Dados Pessoais da Administração Pública estadual. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2020/decreto-65347-09.12.2020.html. Acesso em: 28 maio 2025.



SÃO PAULO
GOVERNO DO ESTADO
SÃO PAULO SÃO TODOS