SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Governo

DELIBERAÇÃO NORMATIVA CGGDIESP-1, DE 30 DE DEZEMBRO DE 2021[1]

Institui a **POLÍTICA DE GOVERNANÇA DE DADOS E INFORMAÇÕES – PGDI,** no âmbito da Administração Pública Estadual, e dá providências correlatas.

O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, no uso das atribuições que lhe foram conferidas pelo Decreto nº 64.790/2020,

DELIBERA:

Artigo 1º – A **POLÍTICA DE GOVERNANÇA DE DADOS E INFORMAÇÕES – PGDI,** a que se refere o inciso III do artigo 3º do Decreto nº 65.347, de 9 de dezembro de 2020, fica instituída nos termos desta deliberação, visando estabelecer parâmetros para as boas práticas em segurança da informação, para a privacidade e proteção de dados pessoais e para a gestão de dados e informações, no âmbito da Administração Pública estadual.

§ 1º – Para os fins desta PGDI, são adotadas as definições constantes do Glossário que integra este documento como Anexo I.

§ 2º – Normas, procedimentos e padrões específicos serão desenvolvidos e divulgados pela Administração Pública estadual, conforme o Anexo II – Providências e Documentos Complementares.

CAPÍTULO I
DAS DISPOSIÇÕES INICIAIS

Artigo 2º – Para proporcionar um nível adequado de segurança das informações, armazenadas tanto em suporte físico quanto digital, a PGDI estabelece diretrizes de

[1] Publicada no Diário Oficial do Estado em 31 de dezembro de 2021. Disponível no link: http://diariooficial.imprensaoficial.com.br/nav_v6/index.asp?c=31384&e=20211231&p=1

orientação à governança de dados e informações e à estruturação de processos e procedimentos para utilização confiável e segura das informações e dados.

Parágrafo único – As diretrizes a que alude o "caput" deste artigo são estabelecidas em conformidade, no que couber, com os instrumentos de planejamento do Sistema Estadual de Tecnologia da Informação e Comunicação – SETIC, reformulado pelo Decreto nº 64.601, de 22 de novembro de 2019.

Artigo 3º – Esta PGDI se aplica aos órgãos e entidades da Administração Pública estadual, devendo ser observada pelos agentes públicos no exercício de suas atribuições.

Parágrafo Único – Os órgãos e entidades a que se refere o "caput" deste artigo:

1. devem elaborar as normas e procedimentos específicos indicados no Anexo II – Providências e Documentos Complementares, não se limitando às expressamente mencionadas;
2. devem promover as devidas adequações em seus respectivos programas, processos, procedimentos e ferramentas para a governança de dados e informações, de modo a observar a PGDI instituída por esta deliberação, adaptando eventuais especificidades;
3. podem, motivadamente, propor modificações à PGDI à análise do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

Artigo 4º – Sem prejuízo da publicação em Diário Oficial, esta PGDI e respectivos anexos devem ser disponibilizados nos sítios eletrônicos da Central de Dados do Estado de São Paulo – CDESP e dos órgãos e entidades da Administração Pública estadual.

Parágrafo único – Na hipótese a que alude o item 3 do parágrafo único do artigo 3º, as modificações setoriais à PGDI também devem ser disponibilizadas no sítio eletrônico do respectivo órgão ou entidade.

CAPÍTULO II
DOS PRINCÍPIOS

Artigo 5º – A PGDI observa os princípios que regem a atividade administrativa, bem como o seguinte:

I – proporcionalidade: adoção de medidas necessárias, adequadas e possíveis para atendimento do interesse público;

II – confidencialidade: garantia de que a informação não pública não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizada ou credenciada;

III – disponibilidade: garantia de que a informação esteja acessível e utilizável sob demanda por pessoa física ou sistema, órgão ou entidade da Administração Pública estadual devidamente autorizados;

IV – integridade: garantia de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

V – autenticidade: garantia de que a informação é livre de adulteração;

VI – finalidade: garantia de tratamento da informação para propósitos legítimos, específicos, explícitos e informados ao titular;

VII – adequação: compatibilidade do tratamento da informação com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

VIII – necessidade: limitação do tratamento ao mínimo necessário para o alcance da respectiva finalidade, abrangendo apenas os dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento;

IX – livre acesso: garantia, aos titulares dos dados, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;

X – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade do respectivo tratamento;

XI – transparência: fornecimento, aos titulares, de informações claras, precisas e

facilmente acessíveis sobre a realização de operações de tratamento e os respectivos agentes, respeitados os segredos comercial e industrial;

XII – segurança: utilização de medidas 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 difusão;

XIII – prevenção: garantia de adoção de medidas para prevenir a ocorrência de danos em virtude ou durante a realização de operações de tratamento de dados pessoais;

XIV – não discriminação: impossibilidade de realização de operações de tratamento com fins discriminatórios, ilícitos ou abusivos;

XV – responsabilização e prestação de contas: demonstração, pelo agente de tratamento, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

CAPÍTULO III
DOS OBJETIVOS

Artigo 6º – A PGDI tem os seguintes objetivos:

I – estabelecer as diretrizes estratégicas, responsabilidades e competências na implementação de medidas de segurança da informação;

II – preservar e proteger de vulnerabilidades e ameaças as informações contidas em qualquer suporte ou formato, em todo o respectivo ciclo de vida;

III – prevenir e reduzir impactos gerados por incidentes de segurança da informação, de modo a preservar a disponibilidade, confidencialidade, integridade e autenticidade da informação;

IV – cumprir as leis e regulamentos atinentes à segurança da informação e privacidade;

V – promover a conscientização e a capacitação em segurança da informação, dos agentes públicos;

VI – planejar, gerir, supervisionar e controlar informações, incentivando o ciclo de melhoria contínua de processos internos e a observância de boas práticas de governança de dados e informações, evitando incidentes de segurança e reduzindo custos;

VII – propiciar que a Administração Pública estadual gerencie dados como ativos, com a adoção de práticas aderentes e sustentáveis de governança de dados e informações, devidamente incorporadas nas atividades-fim;

VIII – utilizar e fomentar o uso da governança de dados e informações para aperfeiçoar as políticas públicas do Estado;

IX – auxiliar e aperfeiçoar os processos de tomada de decisão pelos gestores estaduais.

CAPÍTULO IV
DIRETRIZES GERAIS

Título I
Governança de Dados e Informações

Seção I
Política de Governança de Dados e Informações

Artigo 7º – Os órgãos e entidades da Administração Pública estadual devem observar, no âmbito de suas atribuições, as diretrizes específicas para a Governança de Dados e Informações, conforme Anexo II, exercendo autoridade e controle, mediante planejamento, monitoramento e execução, sobre a gestão de ativos de dados, com o objetivo de garantir que estes sejam gerenciados de forma adequada, de acordo com esta PGDI e as melhores práticas, em prol da tomada de decisão responsável e qualificada.

Parágrafo único – As diretrizes específicas sobre governança de dados e informações constarão em documentos adicionais, conforme o Anexo II – Providências e Documentos Complementares, e devem dispor, no mínimo, sobre:

1. Segurança de Dados e Informações;
2. Integração e Interoperabilidade de dados;
3. Gerenciamento de Documentos e Conteúdo;

4. Arquitetura de Dados;
5. Modelagem e Design de Dados;
6. Armazenamento e Operações de Dados;
7. Dados de Referência e Dados Mestre;
8. *Data Warehousing* e *Business Intelligence*;
9. Metadados;
10. Qualidade dos Dados;
11. *Big Data* e *Data Science*; e
12. Inteligência Artificial.

Artigo 8º – A PGDI tem como pilares:

I - Gestão de Riscos, compreendendo análise, identificação, gerenciamento e mitigação de riscos de uso indevido de dados e aos direitos e liberdades individuais, no que se refere à privacidade e proteção de dados pessoais;

II - Segurança de Dados, com vistas à proteção da informação, mediante adoção de controles que assegurem a sua confidencialidade, integridade, disponibilidade e autenticidade;

III – Privacidade, abrangendo a proteção de dados pessoais e de dados pessoais sensíveis, por meio de exercício de controles apropriados, monitorados via aplicação de avaliações sistemáticas da governança de dados e informações, propiciando ciclos de melhoria contínua.

Seção II
Segurança de Dados e Informações

Artigo 9º – As atividades de planejamento, desenvolvimento e execução de políticas públicas devem observar a segurança de dados, com observância de normas e procedimentos de autenticação, autorização, acesso e auditoria adequados de dados e informações, de modo a:

I – prevenir acessos não autorizados a dados e informações da Administração Pública estadual;

II – assegurar a conformidade com regulamentos e leis de privacidade, proteção e confidencialidade vigentes no país; e

III – respeitar direitos e garantias das partes interessadas, no que tange à privacidade e à confidencialidade.

Parágrafo Único – As diretrizes específicas sobre segurança de dados da Administração Pública estadual constarão em documentos adicionais, conforme o Anexo II – Providências e Documentos Complementares, e devem dispor, no mínimo, sobre segurança:

I – das instalações;

II – dos dispositivos;

III – de credenciais; e

IV – da comunicação eletrônica.

Seção III
Integração e Interoperabilidade

Artigo 10 – Sempre que possível, os dados devem ser mantidos em formato interoperável e estruturados com vistas ao uso compartilhado, para a execução de políticas públicas, a prestação de serviços públicos, a descentralização da atividade pública e a disseminação e o acesso das informações pelo público em geral, com observância da legislação aplicável.

§1º – As atividades de integração e interoperabilidade devem ser planejadas, desenvolvidas, testadas e implementadas conforme as diretrizes estabelecidas pelo Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo e do Conselho Estadual de Tecnologia da Informação e Comunicação – COETIC.

§2º – Os sistemas integrados e as bases de dados utilizadas pela Administração Pública devem ser objeto de melhoria contínua.

§3º – A estrutura dos dados deve ser arquitetada de modo a torná-los acessíveis a partir

de mecanismos de busca, leitura, consulta e recuperação de dados.

§4º – Os órgãos e entidades responsáveis pela custódia de documentos físicos, nos casos em que não seja possível convertê-los em digitais ou em que exista obrigação legal de armazenamento em meio físico, devem adotar as medidas cabíveis para a preservação da integridade e da inviolabilidade dos dados.

§5º – As diretrizes de integração e interoperabilidade do Estado de São Paulo constarão em documentos adicionais, conforme o Anexo II – Providências e Documentos Complementares, e devem dispor, no mínimo, sobre:

I – interconexão;

II – segurança;

III – meios de acesso;

IV – organização e intercâmbio de informações;

V – áreas de integração para a Administração Pública.

Seção IV
Gestão de Documentos e Informações

Artigo 11 – Os órgãos e entidades devem criar, usar, recuperar e descartar documentos e informações com observância:

I – da legislação de proteção de dados aplicável;

II – das políticas, normas e procedimentos estabelecidos pelo Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo;

III – das demais regras de conformidade editadas pelo órgão ou entidade integrante da Administração Pública, no âmbito de suas atribuições.

Parágrafo Único – A gestão de documentos e informações deve garantir:

1. a respectiva recuperação e uso em formatos não estruturados;
2. recursos de integração entre dados não estruturados e estruturados.

Título II
Segurança da Informação

Seção I
Ativos da Informação

Artigo 12 – As informações geradas, acessadas, manuseadas, armazenadas ou descartadas no exercício das atividades realizadas pela Administração Pública estadual, bem como os demais ativos da informação, devem ser utilizados unicamente para finalidades públicas na persecução do interesse público.

Seção II
Sigilo

Artigo 13 – É vedada a revelação de informações sob a responsabilidade do Estado de São Paulo, excetuando-se aquelas de caráter público, nos termos do Decreto nº 58.052/2012.

Parágrafo Único – Os órgãos e entidades estaduais devem:

1. observar as disposições do Decreto nº 48.897/2004, no que se refere aos documentos de arquivo e sua gestão, aos Planos de Classificação e à Tabela de Temporalidade de Documentos;
2. definir ou atualizar as respectivas normas para a avaliação, guarda e eliminação de documentos de arquivo e providências correlatas;
3. estabelecer ou atualizar os respectivos Planos de Classificação de Documentos e de Tabelas de Temporalidade;
4. providenciar, visando à uniformização de critérios, a integração dos controles de classificação e indexação de dados não estruturados implementados pelo Plano de Classificação e pela Tabela de Temporalidade de Documentos aos controles de classificação e indexação de dados estruturados, nos termos do Decreto nº 58.052/2012.

Seção III
Classificação da Informação

Artigo 14 – As informações sob a responsabilidade do Estado de São Paulo devem ser classificadas e protegidas com controles específicos em todo o seu ciclo de vida.

Parágrafo Único – A classificação a que se refere o "caput" deste artigo deve observar o disposto no Decreto nº 48.897/2004 quanto ao arquivamento, criando uma associação entre dado ou informação e a respectiva classificação e origem.

Artigo 15 – Os órgãos e entidades da Administração Pública estadual devem classificar os dados sob sua responsabilidade, de modo a identificar, no mínimo, a finalidade do tratamento, o tempo necessário de armazenamento da informação e a categoria, na seguinte conformidade:

I - dados públicos;

II - dados sigilosos;

III - dados confidenciais;

IV - dados críticos;

V - dados pessoais;

VI - dados pessoais sensíveis;

VII - dados pessoais de criança e adolescente.

Seção IV
Análise dos Processos e Ativos de Informação

Artigo 16 – Os órgãos e entidades, em intervalos regulares, devem analisar os respectivos processos e ativos de informação, visando assegurar que estejam devidamente inventariados e classificados, com identificação e ciência dos respectivos gestores, controladores e operadores, assim como que sejam mapeadas as vulnerabilidades e ameaças de segurança.

Seção V
Uso dos Ativos de Informação

Artigo 17 - Os ativos de informação sob responsabilidade do Estado de São Paulo devem ser utilizados para o exercício da função pública pelos órgãos e entidades, em conformidade com a legislação aplicável e as diretrizes desta PGDI.

Artigo 18 - A gestão dos ativos de tecnologia da informação da Administração Pública estadual deve atender, além das recomendações de fabricantes e desenvolvedores, as regras estabelecidas pelo processo de gestão de mudanças a que alude o artigo 33 desta PGDI.

Artigo 19 - Os órgãos e entidades da Administração Pública estadual devem realizar e manter devidamente atualizado inventário de hardwares e softwares de sua propriedade.

Artigo 20 - Para armazenar ou transmitir informações sob a responsabilidade do Estado de São Paulo, é vedado o uso de repositórios digitais ou dispositivos removíveis não autorizados ou que não tenham sido homologados para uso pelo órgão ou entidade estadual.

Artigo 21 – O uso de mídias sociais e de aplicativos de comunicação instantânea para o desempenho de atribuições do agente público, bem como para a troca de informações organizacionais é permitido, desde que necessário ao desenvolvimento das atividades do órgão ou entidade e com observância das regras estabelecidas pelo Secretário Extraordinário de Comunicação do Estado de São Paulo.

Artigo 22 – É vedado aos agentes públicos e colaboradores realizar qualquer atividade relacionada à captura de áudio, vídeo ou imagens dentro das dependências das repartições públicas do Estado de São Paulo, sem a prévia e formal autorização do

respectivo órgão ou entidade que integrem.

Seção VI
Treinamento e Conscientização

Artigo 23 – Os órgãos e entidades devem realizar treinamentos periódicos e promover a conscientização e a disseminação da cultura da governança de dados e informações, proteção de dados e segurança da informação aos respectivos agentes públicos.

Parágrafo único - Os planos de treinamento e conscientização devem estimular a educação continuada, atualização periódica e realização de campanhas internas de comunicação a fim de promover a sensibilização para temas relacionados à segurança da informação, à governança de dados e informações e à proteção de dados e informações.

Artigo 24 – A capacitação e constante aperfeiçoamento de agentes públicos ocorrerá preferencialmente por meio do Centro de Excelência em Transformação Digital, ambiente digital mantido e operacionalizado pelo COETIC, de que trata o Decreto nº 64.601, de 22 de novembro de 2019, em articulação com a Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação, da Secretaria de Governo.

Título III
Digital

Seção I
Controle de Acesso

Artigo 25 – Os órgãos e entidades devem estabelecer regras de autenticação para acesso lógico, inclusive com a adoção de mecanismos de segurança que garantam acesso exclusivo por meio de credenciais, nível hierárquico e função compatíveis com o grau de classificação de cada dado ou informação.

§1º – As regras a que se refere o “caput” deste artigo devem estipular mecanismos para

a revisão periódica das autorizações de acesso a dados e informações, no mínimo em razão de contratações, exonerações ou alterações de cargos e funções.

§2º – O acesso aos dados e informações que integram a Central de Dados do Estado de São Paulo – CDESP observará as disposições do Decreto nº 64.790, de 13 de fevereiro de 2020.

Artigo 26 – Os agentes públicos devem acessar os dados estritamente necessários ao desempenho de atividades no âmbito do órgão ou entidade que integrem.

Artigo 27 – Todo acesso a dados e informações terá registro histórico passível de auditoria, contendo, no mínimo:

I – identificação do agente responsável;

II – data e horário;

III – dispositivo de origem;

IV – objeto do acesso;

V – operação realizada.

Parágrafo único – Os princípios do privilégio de acesso e da segregação de funções devem ser observados na estruturação dos processos de trabalho e do acesso aos sistemas, de forma a reduzir o risco de acesso e de modificação de dados não autorizados, não intencionais ou indevidos.

Seção II
Ambientes Físicos e Lógicos

Artigo 28 - Os ativos e ferramentas que suportam informações e processos devem ser confiáveis, íntegros, seguros e disponíveis para o desempenho de atividades no âmbito da Administração Pública estadual.

Parágrafo único – Para garantir a segurança a que se refere o “caput” deste artigo, os sistemas de proteção serão mantidos operacionais e atualizados.

Artigo 29 – Os órgãos e entidades devem estabelecer perímetros de segurança para proteção dos respectivos ativos, bem como implementar controles para identificação e registro de acessos aos seus ambientes físicos.

Seção III
Armazenamento Seguro

Artigo 30 – Os órgãos e entidades devem armazenar dados em meio eletrônico com observância da segurança física e lógica de acesso, bem como da segurança no armazenamento de dados, a partir de mecanismos de criptografia e controle de acesso.
Parágrafo único – Os dados e informações em formato eletrônico devem ser encaminhados para a Central de Dados do Estado de São Paulo – CDESP, no prazo e formato indicados em requisição do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, nos termos do Decreto nº 64.790 de 13 de fevereiro de 2020.

Seção IV
Desenvolvimento de Software

Artigo 31 – O desenvolvimento interno ou externo e as aquisições de softwares devem garantir o cumprimento dos requisitos de segurança da informação, proteção de dados e controle de acesso previstos nesta PGDI e nas demais normas do órgão ou entidade responsável pelo desenvolvimento ou aquisição.

Seção V
Backup

Artigo 32 - Os órgãos e entidades devem manter processo de salvaguarda das informações e dos dados necessários para completa recuperação dos seus sistemas (*Backup*), a fim de atender a requisitos operacionais e legais, além de garantir a continuidade do negócio em caso de falhas ou incidentes, bem como a recuperação o

mais rápido possível.

Seção VI
Gestão de Mudanças

Artigo 33 – Os órgãos e entidades devem estabelecer procedimentos próprios para acompanhamento do andamento e dos resultados de mudanças principalmente em seus respectivos sistemas e infraestrutura tecnológica, e preservar os controles relacionados à disponibilidade, integridade, confidencialidade e autenticidade das informações.

Parágrafo único – Os processos de gestão de mudanças devem ser registrados em um repositório centralizado na Central de Dados do Estado de São Paulo – CDESP, para fins de consulta, padronização e melhorias, nos termos do Decreto nº 64.790/2020.

Seção VII
Resposta a Incidentes de Segurança da Informação

Artigo 34 – Os órgãos e entidades devem manter equipe multidisciplinar de gerenciamento de crises e incidentes de segurança e elaborar Plano de Resposta de Incidentes de Segurança, com observância ao procedimento específico de gestão de incidentes, o qual será oportunamente elaborado e publicado pelo Estado de São Paulo, conforme Anexo II – Providências e Documentos Complementares.

Artigo 35 – Os órgãos e entidades devem orientar os respectivos agentes públicos a reportar de imediato às áreas responsáveis possíveis incidentes de segurança da informação, conforme Anexo II – Providências e Documentos Complementares.

§1º - Na hipótese de incidentes de segurança envolvendo dados pessoais:

1. as áreas responsáveis devem comunicar os seus respectivos Encarregados pelo Tratamento de Dados Pessoais;
2. os Encarregados, sem prejuízo das demais atribuições, devem reportar, tão logo quanto possível, todos os casos de incidentes, suspeitos ou comprovados, ao

Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

§2º - Os desvios, as vulnerabilidades e as falhas de segurança identificados não devem ser explorados ou utilizados indevidamente.

§3º Os incidentes de segurança informados ou detectados devem ser registrados e as evidências, caso encontradas, devem ser protegidas de forma adequada, visando a subsidiar a resposta, a análise forense computacional e as solicitações de informação.

Título IV
Gestão de Risco

Seção I
Gerenciamento de Risco

Artigo 36 - Os órgãos e entidades devem estabelecer procedimento de identificação e avaliação dos riscos relacionados à segurança da informação e adotar as melhores práticas para o seu gerenciamento, estabelecendo medidas mínimas aptas a mitigar a ocorrência dos riscos identificados.

Seção II
Continuidade de negócios

Artigo 37 – Os órgãos e entidades devem estabelecer procedimentos de Gestão de Continuidade do Negócio, em conformidade com os requisitos de segurança da informação previstos nesta PGDI e em seus documentos adicionais, bem como disciplinar a atuação da equipe de gerenciamento de crises e incidentes de segurança, responsável por executar tempestivamente planos de contingência e de recuperação de desastres.

Seção III
Monitoramento

Artigo 38 – Os órgãos e entidades devem estabelecer mecanismos de monitoramento

dos seus respectivos ambientes físicos e lógicos, visando a manutenção da eficácia dos controles implantados, a proteção do patrimônio e da reputação e a identificação de eventos ou alertas de incidentes referentes à segurança da informação.

CAPÍTULO V
DISPOSIÇÕES FINAIS

Artigo 39 – Os agentes públicos estaduais, no desempenho de suas atividades, devem zelar pela segurança, disponibilidade, integridade, autenticidade e confidencialidade de dados e informações sob seus cuidados.

Artigo 40 – Os órgãos e entidades devem estabelecer e manter um programa de revisão e atualização das respectivas políticas de segurança da informação, normas, procedimentos e processos correlatos, visando à garantia de atualidade dos requisitos de segurança técnicos e legais implementados e em conformidade com o disposto no Anexo II – Providências e Documentos Complementares.

Artigo 41 – Eventuais omissões desta PGDI devem ser sanadas pelo Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

Artigo 42 – O descumprimento das disposições desta PGDI será objeto de apuração nas formas e instâncias competentes e poderá implicar, isolada ou cumulativamente, responsabilidade civil, penal e administrativa, assegurada a observância, em qualquer caso, do devido processo legal.

Artigo 43 – Os órgãos e entidades são responsáveis por implementar as diretrizes constantes desta PGDI, bem como por documentar evidências de conformidade e indicadores de qualidade de governança de dados e informações e de segurança da informação, a fim de promover ciclos de melhoria contínua.

§1º – O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo poderá estipular parâmetros de uniformização para implementação de medidas físicas, técnicas e organizacionais relativas à segurança da informação, previstas nesta PGDI.

§2º – A qualquer tempo, o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo poderá modificar as indicações contidas no Anexo II – Providências e Documentos Complementares.

Artigo 44 – Esta deliberação entra em vigor na data de sua publicação.

ANEXO I
Glossário

Administração Pública estadual: órgãos e entidades integrantes da Administração Pública Direta e Indireta do Estado de São Paulo.

Armazenamento e Operações de Dados: fornecem suporte durante todo o ciclo de vida dos dados para maximizar seu valor, desde o planejamento e design até o descarte dos dados.

Arquitetura de Dados: define a estrutura para gerenciar ativos de dados, alinhando-se à estratégia organizacional para estabelecer requisitos e designs de dados estratégicos para atender a esses requisitos.

Atividade-fim: aquela diretamente relacionada ao objetivo do órgão ou entidade, ou seja, ao respetivo campo funcional e finalidade de interesse público que motivou sua constituição.

Ativos de Informação: são ativos de tecnologia da informação, dados, documentos ou qualquer outro elemento que possua valor e esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível.

Ativos de Tecnologia da Informação: quaisquer meios de armazenamento, transmissão e tratamento das informações, como softwares, hardwares e ambientes físicos.

Backup ou Cópia de Segurança: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo a guarda, proteção, recuperação e fidelidade ao original. Também pode se referir à mídia em que a cópia é armazenada.

Banco de Dados Pessoais: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.

Banco de Dados: coleção de dados interrelacionados, representando informações sobre um domínio específico.

Big Data: Refere-se a uma gigantesca quantidade de dados extremamente amplos, gerados a uma velocidade vertiginosa, de diferentes origens e formatos (estruturados ou não), que não podem ser processados por bancos de dados ou aplicações de processamento tradicionais e necessitam de ferramentas especialmente preparadas para lidar com estes grandes volumes, de maneira que toda e qualquer informação, nos diversos meios e formatos, possa ser encontrada, analisada e aproveitada em tempo hábil.

Central de Dados do Estado de São Paulo – CDESP: instituída pelo Decreto nº 64.790/2020, constitui repositório eletrônico de dados e informações, estruturados ou não, gerados ou coletados pela Administração Pública Estadual.

Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo: órgão

colegiado de caráter consultivo, normativo e deliberativo, responsável pela gestão da CDESP e por auxiliar o controlador no desempenho das atividades indicadas no artigo 3º do Decreto nº 65.347/2020.

Conselho Estadual de Tecnologia da Informação e Comunicação – COETIC: órgão colegiado de caráter consultivo, normativo e deliberativo, regido pelos Decretos nº 64.601/2019 e nº 64.731/2020, responsável, entre outros, por analisar e aprovar políticas públicas referentes à Tecnologia, Informação e Comunicação, no âmbito do Estado de São Paulo.

Confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, sistema, órgão público ou entidade não autorizados ou credenciados.

Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, genéticos ou biométricos, quando vinculado a uma pessoa natural.

Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dados de Referência e Dados Mestre: incluem reconciliação e manutenção contínuas de dados compartilhados essenciais para permitir o uso consistente e homogêneo destes dados.

Dados: parte elementar da estrutura do conhecimento incapaz de, por si só, gerar conclusões inteligíveis ao destinatário, mas computáveis.

***Data Science* ou Ciência de Dados:** É uma área interdisciplinar voltada para o estudo e a análise de grandes volumes de dados, estruturados e não-estruturados, para a identificação de padrões ou tendências, extração de conhecimento, geração de conclusões ou recomendações para a tomada de decisão e conquista de resultados de negócios importantes que, em volumes menores, dificilmente seriam alcançados.

Data Warehousing* e *Business Intelligence: incluem os processos de planejamento, implementação e controle para gerenciar os dados de suporte à decisão.

Disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão público ou entidade devidamente autorizados.

Dispositivos Removíveis: dispositivos de armazenamento de informações que podem ser removidos do equipamento principal, possibilitando a portabilidade de dados, como CD, DVD, HD externo, pen drive e equipamentos similares.

Gerenciamento de Documentos e Conteúdo: inclui atividades de planejamento, implementação e controle usadas para gerenciar o ciclo de vida dos dados e informações encontrados em uma variedade de mídias não estruturadas, especialmente os documentos.

Gestão de Mudanças nos aspectos relativos à Segurança da Informação: aplicação de um processo estruturado e de um conjunto de ferramentas de gerenciamento de mudanças, de modo a aumentar a probabilidade de sucesso e fazer com que as mudanças transcorram com mínimos impactos no âmbito dos órgãos públicos e entidades da Administração Pública estadual, visando viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

Gestão de Riscos: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificar, avaliar, e gerenciar potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos.

Gestão de Segurança da Informação: ações e métodos que visam à integração das atividades de gestão de riscos, à gestão de continuidade do negócio, ao tratamento de incidentes, ao tratamento da informação, à conformidade, ao credenciamento, à segurança cibernética, à segurança física, à segurança lógica, à segurança orgânica e à segurança organizacional dos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicação.

Incidente de Segurança com Dados Pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do Titular de Dados Pessoais.

Incidente de Segurança da Informação: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de informação levando à perda individual ou conjunta da confidencialidade, integridade e disponibilidade.

Informação: é o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

Integração e Interoperabilidade de dados: incluem processos relacionados à movimentação e consolidação de dados dentro e entre armazenamentos de dados, aplicativos e organizações.

Integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

Inteligência Artificial (IA): É um ramo da Ciência da Computação e um campo de estudo acadêmico que busca simular ou atingir resultados similares aos da inteligência humana em uma máquina ou computador. Os sistemas de IA são regidos por algoritmos estruturados e sofisticados que adotam técnicas estatísticas clássicas e modernas para separação de conjuntos de elementos, predição de valores em tendências verificáveis ou até o aprendizado de padrões, por meio do *machine learning* ou *deep learning*, simulando comportamento “inteligente” na percepção de ambientes complexos, tomada de atitudes e geração de respostas que maximizem suas chances de sucesso.

Inventário de Processos de Tratamento de Dados: é o registro das operações de tratamento de dados pessoais.

Metadados: incluem atividades de planejamento, implementação e controle para permitir o acesso e uso de padrões, definições, modelos, fluxos de dados e outras informações críticas para compreensão dos dados.

Modelagem e Design de Dados: é o processo de descobrir, analisar, representar e comunicar os requisitos de dados de uma forma precisa e padronizada.

Qualidade de Dados: inclui o planejamento e implementação de técnicas de gerenciamento de qualidade para medir, avaliar e melhorar a adequação dos dados para uso consistente dos dados.

Repositórios Digitais (*Cyberlockers*): plataformas de armazenamento na Internet, a exemplo de *Google Drive, OneDrive, Dropbox, iCloud, Box, SugarSync, Slideshare e Scribd*.

Segurança de Dados e Informações: garante que a privacidade e a confidencialidade dos dados sejam mantidas, que os dados não sejam violados e que os dados sejam acessados de forma adequada.

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Governo

POLÍTICA DE GOVERNANÇA DE DADOS E INFORMAÇÕES – PGDI

ANEXO II

PROVIDÊNCIAS E DOCUMENTOS COMPLEMENTARES

1 – Introdução

Este ANEXO II apresenta de forma integrada as medidas a serem planejadas e desenvolvidas pela Administração Pública estadual para atender à PGDI, podendo ser complementadas por ações de capacitação, treinamento e comunicação interna. Esta relação de providências e documentos complementares também embasará o monitoramento da implementação das diretrizes da PGDI. O conteúdo deste ANEXO II poderá ser revisado e atualizado sempre que necessário.

2 – Organização dos temas

A relação das medidas complementares a serem providenciadas foi organizada da seguinte forma:

1. Cada item decorrente das diretrizes da PGDI está descrito e indica a providência a ser tomada.
2. As diferentes providências podem ser agrupadas em ações ou documentos comuns.
3. Os responsáveis indicados poderão, quando necessário e em atenção às boas práticas de governança, solicitar a participação de outros órgãos ou entidades, conforme o tema tratado e as respectivas competências.
4. A tabela a seguir apresenta:
    a. a descrição do item para desenvolvimento conforme os dispositivos da PGDI;
    b. os responsáveis por realizar, isolada ou conjuntamente, o desenvolvimento da providência;
    c. a providência esperada e o formato de cada documento;
    d. os temas dos itens, os quais, na PGDI são:
        i. Governança de dados e informações
        ii. Integração e interoperabilidade
        iii. Gestão de documentos e informações
        iv. Ativos da Informação
        v. Sigilo
        vi. Classificação da informação
        vii. Análise dos processos e ativos de dados e informações
        viii. Uso dos ativos de informação
        ix. Controle de acesso
        x. Ambientes físicos e lógicos
        xi. Armazenamento seguro de dados e informações
        xii. Desenvolvimento de softwares
        xiii. Backup

xiv. Gestão de mudanças
xv. Resposta a incidentes de segurança da informação
xvi. Gerenciamento de riscos
xvii. Continuidade de negócios
xviii. Monitoramento, revisão e atualização

SÃO PAULO
GOVERNO DO ESTADO
| Secretaria de Governo

3 – Tabela de Providências Complementares e Responsáveis

Descrição	Responsáveis	Providências
Governança de Dados e Informações		
Diretrizes específicas sobre: Segurança de Dados e Informações; Integração e Interoperabilidade de Dados; Arquitetura de Dados; Modelagem e Design de Dados; Armazenamento e Operações de Dados; Dados de Referência e Dados Mestre; *Data Warehousing* e *Business Intelligence*; Metadados; Qualidade dos Dados; *Big Data e Data Science*; e Inteligência Artificial.	Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP)	Regras adicionais
	Órgãos e entidades	Manual técnico procedimental
Integração e Interoperabilidade		
Procedimentos para ciclo de melhoria contínua para integração de sistemas e gestão de dados e informações	CGGDIESP	Procedimento padronizado
	Órgãos e entidades	Manual técnico procedimental
Gestão de Documentos e Informações		
Gestão de documentos e informações não-estruturados	Arquivo Público	Regras adicionais
Ativos da Informação		

Descrição	Responsáveis	Providências
Os dados, informações e demais ativos da informação devem ser utilizados unicamente para as finalidades públicas	CGGDIESP	Modelo padrão do formulário e dos conceitos (Orientação técnica de como fazer o inventário de dados)
	Órgãos e entidades	Manual técnico procedimental
Sigilo		
Normas para a avaliação, guarda e eliminação de documentos de arquivo e providências correlatas	Arquivo Público	Regras adicionais
Planos de Classificação de Documentos	Arquivo Público	Modelo padrão
	Órgãos e entidades	Aplicação conforme modelo
Tabelas de Temporalidade	Arquivo Público	Modelo padrão
	Órgãos e entidades	Aplicação conforme modelo
Integração dos controles de classificação e indexação	Arquivo Público	Especificação técnica com implementação da integração em sistema
Classificação da informação		
Parâmetros para os órgãos e entidades classificarem os dados sob sua responsabilidade contendo, no mínimo a finalidade do tratamento, a categoria (dados públicos, dados sigilosos, dados confidenciais, dados críticos, dados pessoais, dados pessoais sensíveis ou	CGGDIESP/ Arquivo Público	Modelo padrão Especificação técnica com implementação da integração em sistema

Descrição	Responsáveis	Providências
dados pessoais de criança e adolescente) e o tempo necessário de armazenamento da informação.	Órgãos e entidades	Aplicação conforme modelo
Análise dos processos e Ativos de Dados e Informação		
Procedimento de análise periódica dos processos e ativos de dados e informações; Controle do inventário dos processos e ativos de dados e informações; e Identificação dos gestores dos processos e ativos de dados e informações	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental
Uso dos Ativos de Informação		
Processo de gestão de mudança	Conselho Estadual de Tecnologia da Informação e Comunicação (COETIC)	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental
Repositório centralizado dos processos de gestão de mudança	CGGDIESP	Especificação técnica com implementação em sistema
Inventário de hardware e software	COETIC	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental

Descrição	Responsáveis	Providências
Regra complementar de autorização para o uso de repositórios digitais não autorizados ou que não tenham sido homologados	CGGDIESP/ COETIC	Regras adicionais
	Órgãos e entidades	Manual técnico procedimental
Regra complementar de autorização para o uso de dispositivos removíveis não autorizados ou que não tenham sido homologados	Órgãos e entidades	Regras adicionais e manual técnico procedimental
Regras para uso das mídias sociais e aplicativos de comunicação instantânea pela Administração Pública estadual para troca de informações corporativas	Secretário Extraordinário de Comunicação	Regras adicionais
	Órgãos e entidades	Regras adicionais e manual técnico procedimental
Proibição de captura de áudio, vídeo ou imagens dentro das dependências das repartições públicas do Estado de São Paulo, sem a prévia e formal autorização do órgão ou entidade	Órgãos e entidades	Regras adicionais e modelo padrão
Controle de Acesso		
Regras de autenticação para o acesso lógico conforme as diretrizes	CGGDIESP	Regras adicionais
	Órgãos e entidades	Especificação técnica com implementação da integração em sistema

Descrição	Responsáveis	Providências
Procedimentos ou mecanismos para a revisão periódica da cessão e de revogação de acessos aos dados e informações em razão de contratações, exonerações e alteração de cargos e funções	CGGDIESP/RH Central	Orientação técnica
	Órgãos e entidades	Aplicação conforme orientação
Registro histórico dos acessos a dados e informações para auditoria	Órgãos e entidades	Especificação técnica com registro
Ambientes físicos e lógicos		
Sistemas de proteção, ativos e atualizados	CGGDIESP	Orientação técnica
	Órgãos e entidades	Especificação técnica com implementação em sistema
Regras ou critérios ao estabelecimento de perímetros de segurança para proteção de seus ativos	Órgãos e entidades	Regras adicionais e aplicação
Controles para identificação e registro de acessos aos seus ambientes físicos	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental Especificação técnica com implementação em sistema
Armazenamento seguro de dados e informações		

Descrição	Responsáveis	Providências
Procedimentos para segurança física de armazenamento de dados e informações	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental
Procedimentos para segurança lógica no armazenamento de dados e informações	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental
Desenvolvimento de softwares		
Requisitos de segurança da informação, proteção de dados e controles de acesso (em casos de desenvolvimento interno ou externo de sistema ou aquisições ou dispositivos móveis)	CGGDIESP/COETIC	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental
Backup		
Modelo para procedimentos de *backup*	CGGDIESP	Orientação técnica
	Órgãos e entidades	Especificação técnica com implementação em sistema

Descrição	Responsáveis	Providências
Gestão de mudanças		
Modelo para procedimentos para acompanhamento do andamento e dos resultados de mudanças	CGGDIESP	Orientação técnica
	Órgãos e entidades	Especificação técnica com implementação em sistema
Resposta a Incidentes de Segurança da Informação		
Plano de Resposta de Incidentes de Segurança, promovendo: • Comunicação de desvios e falhas de segurança; • Mobilização da equipe de combate; • Registro dos incidentes e das evidências; • Procedimentos para proteção das evidências de forma adequada; • Análise forense computacional e; • Ações de resposta ao incidente, com combate, controle e recuperação.	CGGDIESP	Modelo, Orientação técnica e Fluxo procedimental
	Órgãos e entidades	Plano de Resposta de Incidentes de Segurança conforme Modelo, Orientação técnica e Fluxo procedimental
Gerenciamento de Riscos		
Melhores práticas de gerenciamento de riscos, promovendo: • Identificação de vulnerabilidades e potenciais de exploração; • Estimativa de impacto; • Determinação de alternativas de mitigação e contingência; • Decisão quanto aos riscos identificados; e	CGGDIESP	Orientação técnica sobre melhores práticas

Descrição	Responsáveis	Providências
• Priorização das Ações.		
Procedimento de identificação e avaliação dos riscos	Órgãos e entidades	Manual técnico procedimental com documentação das práticas adotadas
Continuidade de negócios		
Planos de contingência e de recuperação de desastres, promovendo: • Identificação de Sistemas e equipamentos críticos; • Estimativa de impacto; • Determinação de alternativas de redundância, mitigação e contingência; • Decisão quanto aos investimentos necessários e; • Planejamento e execução de testes de contingência e de recuperação.	CGGDIESP	Orientação técnica sobre melhores práticas
Procedimentos de Gestão de Continuidade do Negócio	Órgãos e entidades	Manual técnico procedimental contendo Plano de contingência e de recuperação de desastres que observe a Orientação técnica
Monitoramento, Revisão e Atualização		
Procedimentos para monitoramento dos ambientes físicos e lógicos, promovendo: • Identificação dos Controles implantados; • Determinação de limites de tolerância para não-conformidade dos Controles;	CGGDIESP	Orientação técnica

Descrição	Responsáveis	Providências
• Monitoramento de Alertas; • Desenvolvimento e publicação de relatórios operacionais de conformidade; • Ações de Correção: ▪ Ajustes nos limites de Alertas; ▪ Ajustes (adição/eliminação) de Controles; ▪ Ajustes na configuração de Sistemas; e • Submissão de recomendações para revisão e atualização de políticas, normas, processos e procedimentos operacionais.	Órgãos e entidades	Manual técnico procedimental
Programa de revisão e atualização de políticas, normas, processos e procedimentos	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Governo

DELIBERAÇÃO NORMATIVA CGGDIESP-2, DE 30 DE DEZEMBRO DE 2021[1]

Institui a **POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS – PPDP** no âmbito da Administração Pública Estadual e dá providências correlatas.

O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, no uso das atribuições que lhe foram conferidas pelo Decreto nº 64.790, de 13 de fevereiro de 2020,

DELIBERA:

Artigo 1º - A **POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS (PPDP),** a que se refere o inciso III do artigo 3º do Decreto nº 65.347, de 13 de fevereiro de 2020, fica instituída nos termos desta deliberação, em conformidade com a Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), e alinhada às diretrizes da Política de Governança de Dados e Informações do Estado de São Paulo – PGDI.

§ 1º – Para os fins desta PPDP, são adotadas as definições constantes do Glossário que integra este documento como Anexo I.

§ 2º – A Política de Privacidade e Tratamento de Dados Pessoais integra esta PPDP como Anexo II.

§ 3º – Normas, procedimentos e padrões específicos serão desenvolvidos e divulgados pela Administração Pública estadual, conforme o Anexo III – Providências e Documentos Complementares**.**

[1] Publicada no Diário Oficial do Estado em 31 de dezembro de 2021. Disponível no link: http://diariooficial.imprensaoficial.com.br/nav_v6/index.asp?c=31384&e=20211231&p=1

CAPÍTULO I
ÂMBITO DE INCIDÊNCIA

Artigo 2º - A política instituída por esta deliberação:

I - observa as disposições da LGPD e do Decreto nº 65.347, de 13 de fevereiro de 2020;

II - não se aplica às operações de tratamento de dados pessoais para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;

III – é de observância obrigatória por:

a) órgãos da Administração Pública direta, autarquias e fundações, sem prejuízo da aplicação subsidiária e complementar de normas e regras específicas;
b) empresas públicas e sociedades de economia mista controladas pelo Estado, quando estiverem operacionalizando políticas públicas e no âmbito da execução delas;
c) pessoas jurídicas de direito privado em casos de execução descentralizada de atividade pública, quando houver previsão legal, contratual ou em convênio e instrumentos congêneres.

CAPÍTULO II
OBJETIVOS

Artigo 3º - A PPDP tem por objetivos:

I – divulgar as diretrizes estabelecidas pelo Estado de São Paulo para operações de tratamento de dados pessoais;

II – estabelecer responsabilidades e limites de atuação aos agentes públicos;

III – declarar o compromisso do Estado de proteção do direito à privacidade no desempenho das atividades estatais.

Parágrafo único – As disposições desta PPDP aplicam-se a toda operação de tratamento de dados pessoais realizada pela Administração Pública estadual, sem limitações, devendo ser respeitadas por agentes públicos, bem como por aqueles que:

1. realizem operações de tratamento de dados pessoais em nome do Estado;
2. compartilhem dados pessoais com o Estado ou com terceiros em nome do Estado;
3. utilizem a infraestrutura fornecida pelo Estado para tratamento de dados pessoais.

CAPÍTULO III
TRATAMENTO DE DADOS PESSOAIS

Seção I
Princípios da Proteção dos Dados Pessoais

Artigo 4º - Além daqueles relacionados no artigo 5º da PGDI, a PPDP observa os princípios gerais de proteção de dados pessoais e os direitos do titular previstos na LGPD.

Seção II
Finalidades e Bases legais para Tratamento de Dados Pessoais

Artigo 5º - O tratamento de dados pessoais pela Administração Pública observa as disposições previstas no Capítulo IV da LGPD, com vistas ao atendimento de finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

§1º - A cada finalidade corresponde um fundamento legal, considerando o princípio da legalidade, que autoriza o tratamento de dados pessoais, inclusive de crianças e adolescentes, segundo as hipóteses:

1. execução de Políticas Públicas, previstas em leis e regulamentos ou respaldados em contratos, convênios ou instrumentos congêneres (artigo 7º, III da LGPD);
2. tratamento compartilhado de dados necessários à execução, pela Administração Pública, de políticas públicas previstas em leis ou regulamentos (artigo 11, II, b da LGPD);
3. competências legais ou atribuições legais do serviço público (artigo 23 da LGPD).

§2º - A definição da finalidade e a atribuição dos fundamentos legais a que se referem os artigos 7º e 11 da LGPD considera:

1. o serviço a ser prestado ao particular;
2. a competência estadual na matéria;
3. os dados pessoais cuja coleta é necessária à luz da finalidade do tratamento.

§3º - Os fundamentos legais adotados para o tratamento de dados pessoais pela Administração Pública estadual são atribuídos de acordo com as finalidades do tratamento à luz do caso concreto.

§4º - O consentimento do titular de dados pessoais será exigido para desempenho de atividades excepcionais, em conformidade com o serviço público prestado e as diretrizes emanadas pelos órgãos e entidades com atribuição na matéria, mediante prévia consulta ao Comitê Gestor de Governança de Dados e Informações, conforme Anexo III – Providências e Documentos Complementares.

§5º - O tratamento de dados pessoais de crianças e adolescentes sempre deve ocorrer em seu melhor interesse.

§6º - As informações sobre o tratamento de dados de crianças e adolescentes devem ser fornecidas de maneira simples, clara e acessível, consideradas as características do titular, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança e adolescente.

§7º - As hipóteses de tratamento de dados pessoais pela Administração Pública, assim como a respectiva previsão legal, a finalidade, os procedimentos e as práticas utilizadas

devem ser prévia e expressamente divulgadas em veículos de fácil acesso, preferencialmente nos sítios eletrônicos dos órgãos e entidades, observadas as disposições do Anexo II – Política de Privacidade e Tratamento de Dados Pessoais.

Seção III
Agentes de Tratamento

Artigo 6º - São agentes de tratamento, em conformidade com os conceitos estabelecidos pela LGPD, as orientações e regulamentação emanadas da Autoridade Nacional de Proteção de Dados (ANPD) e o disposto no Decreto nº 65.347/2020:

I - Estado de São Paulo, que exerce o papel de controlador de dados pessoais, por intermédio dos Secretários de Estado, do Procurador Geral do Estado e do Chefe do Poder Executivo;	No âmbito da Administração Pública Direta, as decisões referentes ao tratamento de dados pessoais cabem ao Estado de São Paulo, cujas atribuições de controlador, por força da desconcentração administrativa, são desempenhadas pelos órgãos públicos que o integram, respeitadas suas respectivas competências e campos funcionais.
II - Entidades da Administração Pública Indireta	As entidades, com personalidade jurídica própria, que compõem a Administração Pública Indireta assumem a posição de **controlador** – quando detêm poder de decisão sobre as finalidades e elementos essenciais de tratamento de dados pessoais – **ou de operador** – quando

	realizam o tratamento de dados pessoais de acordo com os interesses de outro agente de tratamento.
Pessoas naturais que ocupam cargo ou emprego ou exercem função na Administração Pública Direta ou Indireta	Não são considerados agentes de tratamento, pois atuam de forma subordinada em nome da pessoa jurídica à qual estão vinculados.
Terceiros	Terceiros que não integram a estrutura da Administração Pública Direta e Indireta do Estado de São Paulo, mas que com ela mantenham vínculo contratual ou de parceria, cujo instrumento jurídico específico estipule a realização de operação de tratamento de dados pessoais, na forma do artigo 26 da LGPD. Os terceiros podem atuar na condição de **controlador** – quando detiverem poder de decisão sobre as finalidades e elementos essenciais de tratamento de dados pessoais – **ou operador** – quando realizarem o tratamento de dados pessoais de acordo com os interesses do Estado de São Paulo ou das entidades da Administração Pública Indireta.

Seção IV
Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo

Artigo 7º - O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo atua como auxiliar do controlador, nos termos do artigo 3º do Decreto nº 65.347, de 9 de dezembro de 2020, cabendo-lhe examinar e aprovar as propostas de adaptação à PPDP, formuladas por órgãos e entidades estaduais.

Seção V
Encarregado de Dados Pessoais

Artigo 8º – A identidade e as informações de contato dos Encarregados pelo Tratamento de Dados Pessoais são divulgadas no sítio eletrônico da Central de Dados do Estado de São Paulo – CDESP.

Parágrafo único – Sem prejuízo do disposto no "caput" deste artigo, cabe às autarquias, fundações, empresas públicas e sociedades de economia mista designar e fazer publicar em sítio eletrônico próprio a identidade e as informações de contato do respectivo encarregado pelo tratamento de dados pessoais naquele âmbito.

Artigo 9º - Aos Encarregados pelo Tratamento de Dados Pessoais da Administração Direta e da Indireta, cabe exercer as atividades relacionadas no § 2º do artigo 43 da LGPD e outras que vierem a ser definidas pela ANPD, especialmente:

I – centralizar o recebimento das comunicações da ANPD direcionadas aos respectivos controladores e coordenar a adoção das providências necessárias ao atendimento;

II – orientar, com o apoio das Comissões de Avaliação de Documentos e Acesso (CADAs), os agentes públicos e os contratados da Administração Pública estadual a respeito das práticas a serem adotadas para a proteção de dados pessoais;

III – adotar as medidas necessárias à elaboração e publicação dos Relatórios de Impacto à Proteção de Dados (RIPD), na forma solicitada pela ANPD;

IV – receber e encaminhar ao órgão ou entidade responsável pela adoção de providências correlatas, as sugestões pertinentes e a relação das medidas voltadas à cessação de eventual violação à LGPD; e

V – executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

§1º - Ao Encarregado pelo Tratamento de Dados Pessoais da Administração Direta, nos termos do Decreto nº 65.347, de 9 de dezembro de 2020, cabe também:

1. subsidiar o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo com dados e informações que viabilizem a coordenação das ações de proteção de dados pessoais no âmbito da Administração Pública estadual; e

2. atuar em constante interlocução com os Serviços de Informação ao Cidadão (SICs), contando com o apoio técnico da Coordenadoria de Tecnologia da Informação e Comunicação – COORTIC, da Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação – SSCTI, da Secretaria de Governo e de quaisquer outras unidades administrativas que se fizerem necessárias.

§2º – Mediante requisição do Encarregado, os órgãos e as entidades da Administração Pública estadual devem encaminhar, no prazo assinalado na requisição, as informações necessárias ao atendimento de solicitações da ANPD.

Seção VI
Direitos dos Titulares de Dados Pessoais

Artigo 10 – Ao titular de dados pessoais são garantidos os direitos previstos na Lei federal nº 12.527, de 18 de novembro de 2011, na LGPD, no Decreto nº 58.052, de 16 de maio de 2012, e no Decreto nº 65.347, de 9 de dezembro de 2020, e, em especial, o

direito de obter, a qualquer momento e mediante requisição, em relação aos seus dados pessoais:

I – confirmação da existência de tratamento;

II – acesso aos dados;

III – correção de dados incompletos, inexatos ou desatualizados;

IV – anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na legislação de proteção de dados;

V – portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da ANPD;

VI – eliminação dos dados pessoais tratados com o consentimento do Titular de Dados Pessoais, exceto nas hipóteses em que a conservação dos dados for legalmente autorizada;

VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;

VIII - informação sobre a possibilidade, quando existente, de não fornecer consentimento e sobre as consequências da negativa, quando cabível;

IX – revogação do consentimento, quando cabível;

X – oposição a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto na LGPD;

XI – solicitação de revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Parágrafo único – Nas hipóteses em que o tratamento já tenha sido autorizado pelo Titular de Dados Pessoais mediante consentimento expresso, eventuais mudanças da

finalidade que não sejam compatíveis com os termos em que foi dado o consentimento original devem ser informadas previamente ao Titular de Dados Pessoais, que poderá revogar o consentimento original, caso discorde da alteração.

Artigo 11 - Os requerimentos do Titular de Dados Pessoais devem ser dirigidos ao Encarregado pelo Tratamento de Dados Pessoais ou ao Serviço de Informação ao Cidadão (SIC) do órgão ou entidade interessados.

Parágrafo único – Os requerimentos a que alude o "caput" deste artigo devem observar os prazos e procedimentos previstos na Lei federal nº 12.527, de 18 de novembro de 2011.

Seção VII
Tratamento de Dados Pessoais (Ciclo de Vida dos Dados Pessoais)

Artigo 12 - Ao realizar operação de tratamento de dados pessoais, a Administração Pública estadual se limitará a utilizar os dados pessoais estritamente necessários ao alcance da finalidade a que se destina a operação correspondente, observando-se o princípio da necessidade, previsto no artigo 6º, III, da LGPD.

Artigo 13 - A Administração Pública estadual deverá prestar, ao titular de dados pessoais, informações claras, precisas e facilmente acessíveis a respeito das operações de tratamento realizadas e os agentes de tratamento responsáveis, visando atender ao princípio da transparência, previsto no artigo 6º, VI, da LGPD.

Parágrafo único – As informações a que se refere o "caput" deste artigo incluem as finalidades, as hipóteses de tratamento e as informações de contato do Encarregado.

Seção VIII
Coleta de Dados Pessoais

Artigo 14 - A coleta de dado pessoal poderá se dar por meio de sistemas de informação ligados a *sites* e aplicativos, pelo recebimento de arquivos, bem como em meio físico, mediante preenchimento de formulários, listas ou registro de interação presencial.

Artigo 15 - O titular deve ser informado a respeito da finalidade do tratamento no momento da coleta dos dados pessoais e, nos casos de impossibilidade imediata, tão logo seja possível.

§1º - A observância do princípio da transparência poderá se dar mediante acesso facilitado à Política de Privacidade e Tratamento de Dados Pessoais específica do órgão ou entidade, que deverá ser elaborada nos moldes constantes do Anexo II desta deliberação.

§2º - A transparência também deve ser observada nos casos de coleta de dados pessoais por meio de *cookies* em *sites* mantidos pela Administração Pública estadual, mediante a disponibilização de "Aviso de *Cookies*".

Seção IX
Uso de Dados Pessoais

Artigo 16 - O tratamento dos dados pessoais é realizado nos limites das finalidades informadas por ocasião da respectiva coleta, com fundamento na LGPD.

§1º - O tratamento, pela Administração Pública estadual, de dados de acesso público ou tornados manifestamente públicos pelo titular deve respeitar os direitos do titular e os princípios da proteção de dados pessoais.

§2º – A possibilidade excepcional de tratamento do dado pessoal para finalidade diversa daquela informada no momento da coleta deverá observar as disposições da LGPD, bem como preservar os direitos do titular.

Seção X
Transferência, Uso compartilhado e Compartilhamento de Dados Pessoais

Artigo 17 - O uso compartilhado de dados pessoais pela Administração Pública estadual atende a finalidades específicas de execução de políticas públicas e atribuição legal, e respeita os princípios de proteção de dados pessoais previstos na LGPD.

§1º - Os dados pessoais devem ser mantidos em formato interoperável e estruturado para o uso compartilhado, com vistas à execução de políticas públicas, à prestação de serviços públicos e à descentralização da atividade pública.

§2º - Sem prejuízo dos dados pessoais armazenados em meios físicos, as operações de tratamento devem se dar preferencialmente por meio da Central de Dados do Estado de São Paulo (CDESP).

§3º - O compartilhamento de dados pessoais no âmbito da Administração Pública estadual dar-se-á mediante acesso de agentes públicos designados e habilitados, por meio da CDESP, preferencialmente.

Artigo 18 - A transferência de dados pessoais a terceiros ocorrerá exclusivamente nas hipóteses e na forma prevista na LGPD.

Artigo 19 - Os dados pessoais somente são compartilhados com entidades privadas mediante existência de formal autorização, a qual somente será emitida nos casos de:

I. execução descentralizada de atividade pública, exclusivamente para esse fim específico e determinado;
II. dados acessíveis publicamente;

III. previsão legal;

IV. transferência respaldada em contratos, convênios ou instrumentos congêneres comunicados previamente à ANPD, nos termos do artigo 26, § 2º da LGPD;

V. prevenção de fraudes e irregularidades;

VI. proteção à segurança e à integridade do Titular de Dados Pessoais; ou

VII. com o consentimento do Titular de Dados Pessoais.

Parágrafo único - O compartilhamento de dados e informações que integram a CDESP ocorrerá exclusivamente por meio de seu portal, mediante autorização do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, nos termos dos artigos 2º, 3º e 5º, VI, do Decreto nº 64.790/2020.

Artigo 20 - O terceiro que receber os dados pessoais, sob as penas da lei, deverá realizar as operações de tratamento com estrita observância da LGPD, desta deliberação e das orientações constantes de instrumento específico que discipline o compartilhamento.

Seção XI
Armazenamento de Dados Pessoais

Artigo 21 - Os dados pessoais são armazenados por período limitado, em conformidade com a finalidade específica do tratamento.

Parágrafo único – Os dados pessoais podem ser armazenados após atingida a finalidade do tratamento nos casos de cumprimento de obrigação legal ou regulatória.

Artigo 22 - Os meios físicos e digitais de armazenamento dos dados pessoais devem preservar a sua segurança e qualidade, bem como sua autenticidade e atualidade, em conformidade com a finalidade do tratamento.

Seção XII
Eliminação dos Dados Pessoais

Artigo 23 - Após cumprida a finalidade do tratamento e findo o prazo de armazenamento autorizado em norma legal ou regulatória, os dados serão eliminados de modo seguro, independentemente se armazenados em meios físicos ou digitais.

§1º - A solicitação do titular de eliminação ou oposição poderá ser indeferida, motivadamente, quando houver fundamento legal para o tratamento do dado, independentemente de consentimento.

§2º - O processo de eliminação de documentos deverá ser feito em conformidade com a avaliação conduzida pelas Comissões de Avaliação de Documentos e Acesso (CADA), de acordo com tabelas de temporalidade de documentos do Arquivo Público do Estado, nos termos do Decreto nº 48.897/2004.

§3º - A eliminação de documentos que não constem da Tabela de Temporalidade de Documentos das atividades-meio, ou das Tabelas de Temporalidade de Documentos das atividades-fim dos órgãos da Administração Pública Estadual, será realizada mediante autorização do Arquivo Público do Estado.

Seção XIII
Normas Internas, Procedimentos e Documentação das Operações de Tratamento

Artigo 24 - As medidas técnicas e administrativas adotadas pela Administração Pública estadual abrangem atividades de treinamento e capacitação.

Artigo 25 - As normas internas e os procedimentos voltados ao desenho de estratégias e regras operacionais de tratamento de dados devem ser elaborados com base nesta PPDP e na PGDI.

§1º - Cada órgão e entidade estadual poderá adaptar normas internas e procedimentos às respectivas especificidades desde que compatíveis com as diretrizes desta PPDP e da PGDI.

§2º - As propostas de adaptação elaboradas nos termos do §1º deste artigo devem ser submetidas à análise do Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

§ 3º - Os processos de tratamento sob responsabilidade da Administração Pública estadual devem ser documentados, nos termos do artigo 1º das Disposições Transitórias do Decreto nº 65.347/2020.

§ 4º - A documentação de que trata o § 2º deste artigo deve integrar o Inventário de Processos de Tratamento de Dados Pessoais a ser mantido pelo órgão ou entidade estadual, discriminando, no mínimo, o fundamento legal para o tratamento, a finalidade, a existência de compartilhamento e o respectivo instrumento, bem como o local de custódia ou armazenamento.

§5º - Cabe às Secretarias de Estado e à Procuradoria Geral do Estado providenciar o registro no Inventário de Processos de Tratamento de Dados Pessoais dos bancos de dados e informações pessoais, estruturados ou não, em suporte físico ou eletrônico, sob sua responsabilidade, com posterior encaminhamento ao Encarregado de Dados Pessoais da Administração Direta e ao Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

§ 6º - Na Administração Pública Indireta, cada entidade deve elaborar o respectivo Inventário de Processos de Tratamento de Dados Pessoais, comunicando ao respectivo Encarregado de Dados Pessoais e ao Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo.

Seção XIV
Relatório de Impacto à Proteção de Dados

Artigo 26 - Para as operações de tratamento que envolvam risco à garantia dos princípios gerais de proteção de dados pessoais ou às liberdades civis e direitos fundamentais dos Titulares de Dados Pessoais, o Encarregado de Dados Pessoais deverá elaborar Relatório de Impacto à Proteção de Dados (RIPD).

§1º - No âmbito da Administração Direta, o Encarregado de Dados Pessoais conta com o apoio dos Chefes de Gabinete das Secretarias de Estado e da Procuradoria Geral do Estado, podendo solicitar a essas autoridades a elaboração do RIDP, para posterior validação.

§2º - O RIPD deve ser elaborado em conformidade com a regulamentação emanada da ANPD, contendo, no mínimo, a descrição dos 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 risco adotados.

§3º - Mesmo nos casos de inaplicabilidade da LGPD por força do disposto no artigo 4º, III e § 1º, o RIPD deve ser elaborado e apresentado à ANPD, caso haja solicitação.

Seção XV
Transferência Internacional de Dados

Artigo 27 - A transferência internacional de dados pessoais independe de volumetria, frequência ou meio, sendo realizada em conformidade com o disposto nos artigos 33 a 36 da LGPD.

Seção XVI
Segurança da Informação

Artigo 28 – Os agentes públicos devem observar as diretrizes sobre segurança da informação previstas na PGDI.

Seção XVII
Incidentes de Segurança com Dados Pessoais

Artigo 29 - Todo incidente de segurança com dados pessoais, confirmado ou sob suspeita, deve ser imediatamente comunicado pelos órgãos e entidades da Administração Pública estadual ao respectivo Encarregado pelo Tratamento de Dados Pessoais, que deverá comunicar ao Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo, conforme Anexo III – Providências e Documentos Complementares.

§1º - O Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo procederá à análise e classificação do incidente e, caso constatado risco ou dano relevante aos Titulares de Dados Pessoais, o colegiado determinará que se proceda à notificação dos indivíduos afetados, agentes públicos e autoridades interessadas.

§2º - Caberá aos Encarregados comunicar ao Titular de Dados Pessoais e à ANPD a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos Titulares de Dados Pessoais.

§3º - Os Chefes de Gabinete das Secretarias de Estado e da Procuradoria Geral do Estado, em interlocução com o Encarregado de Dados Pessoais da Administração Pública Direta do Estado de São Paulo, devem instituir, no respectivo âmbito de atuação, grupo multidisciplinar responsável por atuar na contenção e resposta de incidentes de segurança com dados pessoais.

CAPÍTULO IV
DISPOSIÇÕES FINAIS

Artigo 30 - As violações às disposições desta PPDP estão sujeitas à apuração e sanção, de acordo com a legislação aplicável.

Artigo 31 – A partir desta PPDP serão desenvolvidos Manuais Técnicos e Operacionais a respeito da aplicação das diretrizes, bem como de ações de capacitação direcionadas aos agentes públicos, conforme Anexo III – Providências e Documentos Complementares.

§1º – A qualquer tempo, o Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo poderá modificar as indicações contidas no Anexo III - Providências e Documentos Complementares.

§2º - Eventuais alterações nesta PPDP ou em seus documentos complementares serão imediatamente divulgadas.

Artigo 32 - Esta deliberação entra em vigor na data de sua publicação.

ANEXO I
Glossário

Administração Pública estadual: Administração Pública estadual compreende todos os órgãos públicos e entidades integrantes da Administração Direta e Indireta do Estado de São Paulo. Para os fins deste documento poderá ser simplesmente designada como Administração.

Central de Dados do Estado de São Paulo – CDESP: instituída pelo Decreto nº 64.790/2020, constitui repositório eletrônico de dados e informações, estruturados ou não, gerados ou coletados pela Administração Pública estadual.

Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo: órgão colegiado de caráter consultivo, normativo e deliberativo, responsável pela gestão da CDESP e por auxiliar o controlador no desempenho das atividades indicadas no artigo 3º do Decreto nº 65.347/2020.

Consentimento: manifestação livre, informada e inequívoca pela qual o Titular de Dados Pessoais concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

Controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.

***Cookies*:** arquivos de informação armazenados no computador ou dispositivos móveis do usuário, através do navegador de internet (browser), permitindo que, durante um período, um website "se lembre" das ações e preferências registradas em nome do usuário. Por meio de *cookies*, ao regressar a um website que o usuário já visitou, suas preferências de navegação serão automaticamente aplicadas (tais como idioma, fonte, forma de visualização etc.). Os *cookies* podem ser persistentes (que expiram quando o usuário fecha o navegador) ou de sessão (que permanecem no computador do usuário mesmo após fechar a sessão ou até a sua exclusão).

Dado: parte elementar da estrutura do conhecimento, incapaz de, por si só, gerar conclusões inteligíveis ao destinatário, mas computáveis.

Dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.

Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável.

Dado Pessoal Sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou

político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Encarregado de Dados Pessoais: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os Titulares de Dados Pessoais e a Autoridade Nacional de Proteção de Dados (ANPD).

Incidente de Segurança com Dados Pessoais: qualquer evento adverso confirmado, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do Titular de Dados Pessoais.

Informação: conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

Inventário de Processos de Tratamento de Dados: é o registro das operações de tratamento de dados pessoais.

Operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador.

Relatório de Impacto à Proteção dos Dados Pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Titular de Dados Pessoais: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento de Dados Pessoais: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

ANEXO II

Política de Privacidade e Tratamento de Dados Pessoais

O Estado de São Paulo adota a Política de Privacidade e Tratamento de Dados Pessoais, cabendo aos demais órgãos e entidades da Administração Pública estadual considerar este modelo para a elaboração de suas respectivas Políticas de Privacidade, as quais devem ser publicadas em seus sítios eletrônicos.

POLÍTICA DE PRIVACIDADE E TRATAMENTO DE DADOS PESSOAIS

1. INTRODUÇÃO

A presente Política demonstra o compromisso do **ESTADO DE SÃO PAULO** com a observância das disposições legais e regulamentares aplicáveis nas operações de tratamento de dados pessoais de particulares ("Titular"), realizadas em conformidade com os princípios da Administração Pública, na persecução do interesse público e com o objetivo de executar as competências e atribuições legais do serviço público, observados a Lei federal nº 13.709/2018 ("Lei Geral de Proteção de Dados Pessoais" ou "LGPD") e o Decreto nº 65.347/2020.

Esta Política poderá sofrer atualizações a qualquer tempo, as quais serão divulgadas e consultadas no *site* [*link* para o respectivo sítio eletrônico].

2. SUMÁRIO

Como e por que tratamos Dados?

O **ESTADO DE SÃO PAULO** trata Dados Pessoais de particulares para diversas finalidades, de acordo com o serviço público prestado ou atribuição legal desempenhada, com estrita observância da legislação aplicável. O tratamento de Dados Pessoais ocorrerá sempre que necessário para execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos e convênios da Administração Pública ou, ainda, quando necessário à execução de competências ou atribuições legais do serviço público.

Segurança dos Dados

O **ESTADO DE SÃO PAULO** emprega os melhores esforços para preservar a privacidade e a segurança de ambientes físicos ou eletrônicos, adotando medidas técnicas e organizacionais, físicas (como acesso restrito a pessoas autorizadas) e administrativas (como, por exemplo, normas de segurança, treinamentos e conscientização de servidores e agentes públicos), que objetivam mitigar riscos de ocorrência de incidentes de segurança.

Armazenamento dos Dados

Os Dados Pessoais são armazenados pelo período necessário para o cumprimento das finalidades que justificaram a sua coleta. O período de armazenamento será variável de acordo com a finalidade para a qual as operações de tratamento são realizadas e o prazo de armazenamento autorizado em norma legal ou regulatória.

Quando compartilhamos Dados?

O **ESTADO DE SÃO PAULO** poderá compartilhar Dados Pessoais caso seja necessário para o atendimento dos preceitos da Administração Pública, de finalidade pública ou na persecução do interesse público, sempre observado o princípio da legalidade, nas seguintes hipóteses:

- Quando necessário à execução descentralizada de atividade pública, exclusivamente para esse fim específico e determinado, poderá haver compartilhamento com entidade privada;
- Nos casos em que os Dados Pessoais sejam acessíveis publicamente, observada legislação específica;
- Quando respaldado em contratos, convênios ou instrumentos firmados pela Administração Pública com entes privados;
- Para prevenção de fraudes e irregularidades;
- Para proteção à segurança e à integridade do Titular de Dados Pessoais.

O **ESTADO DE SÃO PAULO** garante que os terceiros autorizados a receber Dados Pessoais observam as diretrizes desta Política e demais normativos internos, a Lei Geral de Proteção de Dados Pessoais e as orientações da Administração Pública estadual.

Quais são seus Direitos?

A Lei Geral de Proteção de Dados Pessoais prevê ao Titular determinados direitos relativos aos respectivos Dados Pessoais, sem prejuízo de outros, previstos em demais leis:

- **Confirmação**: o direito de confirmar a existência do tratamento dos seus dados pessoais pelo **ESTADO DE SÃO PAULO**.
- **Acesso**: o direito de ser informado e ter acesso aos seus dados pessoais sob tratamento do **ESTADO DE SÃO PAULO**.
- **Correção:** o direito de solicitar a atualização ou alteração de Dados Pessoais desatualizados, incompletos ou incorretos.
- **Eliminação:** o direito de ter seus Dados Pessoais eliminados nas hipóteses em que o tratamento se deu com o consentimento do Titular.
- **Anonimização ou bloqueio:** o direito de solicitar que os Dados Pessoais excessivos ao tratamento sejam submetidos à anonimização ou que este tratamento excessivo seja suspenso pela Administração Pública.
- **Revogação**: o direito de revogar o consentimento para as finalidades de tratamento de Dados Pessoais a ele atreladas, quando aplicável.
- **Informação** sobre não fornecer consentimento e as consequências da negativa, quando aplicável.
- **Oposição**: o direito do Titular se opor ao tratamento de Dados Pessoais que esteja desalinhado às determinações da Lei Geral de Proteção de Dados Pessoais.
- **Portabilidade**: solicitar a portabilidade dos seus dados pessoais, de acordo com a regulamentação da Autoridade Nacional de Proteção de Dados.
- **Informação sobre entidades públicas e privadas** com as quais o **ESTADO DE SÃO PAULO** realizou uso compartilhado de Dados Pessoais.
- **Revisão** de decisões tomadas unicamente com base em tratamento automatizado de Dados Pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.

Uso de *Cookies*

Com o intuito de melhorar a navegabilidade em suas plataformas digitais, o **ESTADO DE SÃO PAULO** faz uso de *Cookies*, que consistem em arquivos digitais em formato de texto coletados e armazenados durante a navegação. Os *Cookies* são utilizados para aprimorar a experiência do usuário, tanto em termos de performance, como em termos de usabilidade da plataforma digital, uma vez que os conteúdos disponibilizados serão otimizados, ajustados de acordo com as preferências sistêmicas e, em casos específicos, utilizados para compilar estatísticas anônimas.

A utilização de *Cookies* é recorrente em plataformas digitais e o seu uso não prejudica os dispositivos em que são armazenados, sendo possível gerenciá-los diretamente nas opções do navegador de internet utilizado pelo Titular.

Canais de atendimento

O Titular poderá encaminhar dúvidas, solicitações e reclamações ao Encarregado pelo Tratamento de Dados Pessoais:

Nome do Encarregado
- **E-mail:**
- **Telefone:**

Estamos disponíveis para atendimento de segunda-feira a sexta-feira, das 9h às 17h.

Glossário

Autoridade Nacional de Proteção de Dados (ANPD): órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.

Anonimização: Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Dados Pessoais: Dados relacionados a pessoa natural identificada ou identificável.

Decisões unicamente automatizadas: Trata-se de decisões que afetam um indivíduo e que foram programadas para funcionar automaticamente, sem a necessidade de uma operação humana, com base em tratamento automatizado de Dados Pessoais.

Encarregado de Dados Pessoais: Pessoa indicada pelo **ESTADO DE SÃO PAULO** para atuar como canal de comunicação entre o

controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Tratamento: Toda operação realizada com Dados Pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Governo

POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS – PPDP

ANEXO III

PROVIDÊNCIAS E DOCUMENTOS COMPLEMENTARES

1 – Introdução

Este ANEXO III apresenta de forma integrada as medidas a serem planejadas e desenvolvidas pela Administração Pública estadual para atender à PPDP, podendo ser complementadas por ações de capacitação, treinamento e comunicação interna. Esta relação de providências e documentos complementares também embasará o monitoramento da implementação das diretrizes da PPDP. O conteúdo deste ANEXO III poderá ser revisado e atualizado sempre que necessário.

2 – Organização dos temas

A relação das medidas complementares a serem providenciadas foi organizada da seguinte forma:

1. Cada item decorrente das diretrizes da PPDP está descrito e indica a providência a ser tomada.
2. As diferentes providências podem ser agrupadas em ações ou documentos comuns.
3. Os responsáveis indicados poderão, quando necessário e em atenção às boas práticas de governança, solicitar a participação de outros órgãos ou entidades, conforme o tema tratado e as respectivas competências.
4. A tabela a seguir apresenta:
    a. a descrição do item para desenvolvimento conforme os dispositivos da PPDP;
    b. os responsáveis por realizar, isolada ou conjuntamente, o desenvolvimento da providência;
    c. a providência esperada e o formato de cada documento;
    d. os temas dos itens, os quais, na PPDP são:
        i. Finalidades e Bases legais para Tratamento de Dados Pessoais
        ii. Encarregado de Dados Pessoais
        iii. Direitos dos Titulares de Dados Pessoais
        iv. Coleta de dados pessoais
        v. Uso de dados pessoais
        vi. Transferência, uso compartilhado e compartilhamento de dados pessoais
        vii. Armazenamento e eliminação de dados pessoais
        viii. Normas internas, procedimentos e documentação das operações de tratamento
        ix. Incidentes de Segurança com Dados Pessoais

SÃO PAULO
GOVERNO DO ESTADO
Secretaria de Governo

3 – Tabela de Providências Complementares e Responsáveis

Descrição	Responsáveis	Providências
Finalidades e Bases legais para Tratamento de Dados Pessoais		
Documento com a relação das finalidades e atribuição das bases legais, contendo informações sobre: serviços prestados ao cidadão; competência na matéria para o tratamento; e quais dados pessoais serão coletados	Comitê Gestor de Governança de Dados e Informações do Estado de São Paulo (CGGDIESP)	Modelo padrão
	Órgãos e entidades	Elaboração do documento
Procedimento de verificação da necessidade de obtenção de consentimento do Titular de Dados Pessoais	CGGDIESP	Manual técnico procedimental
Termo de consentimento para os casos aplicáveis com prévia consulta ao Comitê Gestor	CGGDIESP	Modelo padrão de Termo de consentimento
	Órgãos e entidades	Adequação do Modelo à sua realidade
Encarregado de Dados Pessoais		
Interlocução entre o Encarregado de Dados Pessoais da Administração Direta com os órgãos	Encarregado de Dados Pessoais da Administração Direta	Fluxo de interlocução

Descrição	Responsáveis	Providências
Interlocução entre o Encarregado de Dados Pessoais da Administração Direta com as entidades da Administração Indireta e seus respectivos encarregados	Encarregado de Dados Pessoais da Administração Direta	Fluxo de interlocução
Comunicação com a ANPD e com outros órgãos externos à Administração Pública estadual para adotar providências relativas à proteção de dados pessoais	CGGDIESP + Encarregados	Fluxo de comunicação
Elaboração e publicação de Relatórios de Impacto à Proteção de Dados (RIPD)	CGGDIESP	Modelo padrão do RIPD
	Encarregados	Fluxo de elaboração e publicação do RIPD
		Elaboração e publicação dos RIPD
Direitos dos Titulares de Dados Pessoais		
Requerimentos, reclamações, comunicações e sugestões dos Titulares de Dados Pessoais e outros, com sistemática formal de recebimento	Encarregados	Fluxo para atendimento ao cidadão
Coleta de dados pessoais		
Procedimentos para as entradas de informação do dado pessoal, definindo limites para a coleta de dados estritamente necessários para o desempenho de suas funções oficiais, considerando as finalidades de tratamento	Órgãos e entidades	Manual técnico procedimental
Uso de dados pessoais		

Descrição	Responsáveis	Providências
Atualizar ou adequar os serviços digitais ou físicos da Administração Pública estadual (sistemas, sites, aplicativos, portais, formulários) para identificarem dados pessoais visando adequação aos limites da coleta de dados	Órgãos e entidades	Planos de ação para a atualização ou adequação dos serviços digitais e físicos
Procedimento para informar o titular de dados pessoais sobre a finalidade do tratamento de seus dados	Órgãos e entidades	Manual técnico procedimental
Política de Privacidade e Tratamento de Dados Pessoais específica ao serviço público ou ao correspondente órgão público ou entidade da Administração Pública Estadual	CGGDIESP	Orientação técnica
	Órgãos e entidades	Elaboração e publicização da Política de Privacidade e Tratamento de Dados Pessoais
Transferência, uso compartilhado e compartilhamento de dados pessoais		
Procedimentos para o uso compartilhado de dados pessoais pela Administração Pública estadual, incluindo compartilhamento internacional	CGGDIESP	Orientação técnica
	Órgãos e entidades	Manual técnico procedimental
Armazenamento e eliminação de dados pessoais		
Período de armazenamento dos dados considerando a finalidade específica do tratamento	Arquivo Público	Modelo padrão

Descrição	Responsáveis	Providências
Regras para a eliminação dos dados após o prazo de armazenamento determinado	Arquivo Público	Orientação técnica
Normas internas, procedimentos e documentação das operações de tratamento		
Adequação das normas internas e documentação dos procedimentos operacionais voltados ao tratamento de dados para conformidade com a PPDP	Órgãos e entidades	Manual técnico procedimental
Inventário periódico de Processos de Tratamento de Dados e envio da documentação para o Encarregado de Dados e CGGDIESP.	Órgãos	Manual técnico procedimental
		Inventário de Processos de Tratamento de Dados
Inventário periódico de Processos de Tratamento de Dados e envio da documentação para o respectivo Encarregado de Dados.	Entidades	Manual técnico procedimental
		Inventário de Processos de Tratamento de Dados
Incidentes de segurança com dados pessoais		
Procedimentos para identificação e comunicação de incidentes ao Encarregado de Dados Pessoais	CGGDIESP	Fluxo operacional
	Órgãos e entidades	Manual técnico procedimental