

Deliberação Normativa CGGDIESP-2, de 30-12-2021

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 Dec. 64.790-2020, 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.

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:

<p>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;</p>	<p>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.</p>
<p>II - Entidades da Administração Pública Indireta</p>	<p>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.</p>

<p>Pessoas naturais que ocupam cargo ou emprego ou exercem função na Administração Pública Direta ou Indireta</p>	<p>Não são considerados agentes de tratamento, pois atuam de forma subordinada em nome da pessoa jurídica à qual estão vinculados.</p>
<p>Terceiros</p>	<p>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.</p>

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 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 Pessoais
- ✓ Segurança dos Dados
- ✓ Armazenamento dos Dados
- ✓ Quando compartilhamos Dados
- ✓ Direitos dos Titulares Uso de Cookies
- ✓ Canais de atendimento
- ✓ Glossário

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.

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

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
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

Descrição	Responsáveis	Providências
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		
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

Descrição	Responsáveis	Providências
	Órgãos e entidades	Elaboração e publicação 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
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		

Descrição	Responsáveis	Providências
Procedimentos para identificação e comunicação de incidentes ao Encarregado de Dados Pessoais	CGGDIESP	Fluxo operacional
	Órgãos e entidades	Manual técnico procedimental