APROVA Instrução Normativa CGGDIESP-9/PPDP referente ao Anexo III, 3 – Tabela de Providências Complementares e Responsáveis – Finalidades e Bases legais para Tratamento de Dados Pessoais: **Orientação Técnica e Modelo - Elaboração de Política de Privacidade e Tratamento de Dados Pessoais**, da Deliberação Normativa CGGDIESP-2, de 30/12/2021.

ORIENTAÇÃO TÉCNICA

Elaboração de Política de Privacidade e Tratamento de Dados Pessoais

1. Objetivos

Esta orientação técnica tem os seguintes objetivos:

- Recomendar procedimento para elaboração de Política de Privacidade e Tratamento de Dados Pessoais, providência requerida pela Política de Proteção de Dados Pessoais (PPDP), no âmbito da Administração Pública estadual, instituída pela Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021.
- Subsidiar a elaboração de Política de Privacidade e Tratamento de Dados Pessoais para publicização, conforme disposto na PPDP, em seu Anexo II.
- Orientar a utilização e o preenchimento do modelo de Política de Privacidade e Tratamento de Dados Pessoais definido pela PPDP, em seu Anexo II, que acompanha esta orientação técnica.

2. Sumário

3. Abrangência

Órgãos e entidades da Administração Pública estadual.

4. Principais documentos relacionados e referenciais bibliográficos

- Política de Governança de Dados e Informações (PGDI).
- Política de Proteção de Dados Pessoais (PPDP), considerando, em seu Anexo III, a décima segunda providência, "Política de Privacidade e Tratamento de Dados Pessoais específica ao serviço público ou ao correspondente órgão público ou entidade da Administração Pública Estadual".
- Guia Orientativo do CGGDIESP que define modelo padrão e instrui sobre o "Preenchimento do documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados", conforme primeira providência requerida pela PPDP, em seu Anexo III.
- Manual Técnico Procedimental do CGGDIESP que instrui sobre o "procedimento de verificação da necessidade de obtenção de consentimento do Titular de Dados Pessoais", conforme segunda providência requerida pela PPDP, em seu Anexo III.
- Manual Técnico Procedimental a ser elaborado pelos órgãos e entidades que instrui sobre os "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", conforme nona providência requerida pela PPDP, em seu Anexo III.
- Planos de Ação a serem elaborados pelos órgãos e entidades para a "atualização ou adequação dos 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", conforme décima providência requerida pela PPDP, em seu Anexo III.
- Orientação Técnica do CGGDIESP que instrui sobre "Procedimentos para o uso compartilhado de dados pessoais pela Administração Pública estadual, incluindo compartilhamento internacional", conforme décima terceira providência requerida pela PPDP, em seu Anexo III.
- Decreto Estadual nº 65.347, de 9 de dezembro de 2020, que dispõe sobre a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), no âmbito do Estado de São Paulo.
- Lei Federal nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD)
- Lei Estadual nº 17.262, de 9 de abril de 2020, que institui o Plano Plurianual – PPA para o quadriênio 2020-2023.

- ANPD. Guia orientativo – Tratamento de dados pessoais pelo Poder Público. [Brasília]: ANPD, jan. 2022.

5. Glossário

Termos e siglas	Definição
ANPD	Autoridade Nacional de Proteção de Dados. Órgão da Administração Pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo o território nacional.
CGGDIESP	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 Estadual nº 65.347/2020.
Controlador de dados pessoais	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 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, genéticos ou biométricos, quando vinculado a uma pessoa natural.
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).
LGPD	Lei Geral de Proteção de Dados – Lei nº 13.709/2018. Promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo, essa Lei rege o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.
PGDI	Política de Governança de Dados e Informações. Instituída pela Deliberação Normativa CGGDIESP-1, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, que estabelece 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, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
Política	Documento que estabelece as diretrizes a serem aplicadas em uma organização tendo em vista os objetivos definidos para ela.
PPDP	Política de Proteção de Dados Pessoais. Instituída pela Deliberação Normativa CGGDIESP-2, de 30 de dezembro de 2021, publicada no DOE de 31 de dezembro de 2021, e corresponde à compilação de normas e regras de boas práticas de governança e proteção para tratamento de Dados Pessoais, de observância obrigatória pelos Órgãos e Entidades da Administração Pública estadual.
SSCTI	Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação da Secretaria de Governo do Estado de São Paulo.
Titular de dados pessoais	Pessoa natural a quem se referem os dados pessoais objeto que são 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.

Termos e siglas	Definição
Uso compartilhado de dados	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.

6. Contexto

A promulgação da LGPD, no Brasil, levantou uma série de exigências quanto ao tratamento de dados pessoais. Entre essas exigências está a adoção de uma Política de Privacidade e Tratamento de Dados Pessoais, documento cujo objetivo é explicar ao usuário, de forma clara, concisa e de fácil acesso, quais são os dados pessoais tratados e como eles são coletados e armazenados, entre outras informações.

Os órgãos e as entidades da Administração Pública estadual devem elaborar e publicizar sua Política de Privacidade e Tratamento de Dados Pessoais, conforme disposto na PPDP, em seu Anexo II, de forma a atender à LGPD, em especial a seu artigo 23, inciso I, que trata da obrigação das instituições do Poder Público em relação à divulgação dos tratamentos de dados pessoais que realizam.

Disponibilizar ao público (usuário/cidadão), em seu *site*, as diretrizes adotadas na Política de Privacidade e Tratamento de Dados Pessoais, a fim de garantir a ele fácil acesso a informações claras e precisas sobre os tratamentos de dados realizados e respectivos agentes de tratamento, conforme determinado no Decreto Estadual nº 65.347/2020, colabora também para que os órgãos e as entidades atendam ao princípio da transparência preconizado pela LGPD, em seu artigo 6º, inciso VI, bem como às diretrizes da PPDP, em seu artigo 13.

7. Relação de temas abordados

- Política de Privacidade e Tratamento de Dados Pessoais.
- Justificativa e finalidade do tratamento de dados pessoais.
- Uso de *cookies*.
- Canais de atendimento aos titulares de dados pessoais.
- Uso compartilhado de dados pessoais por órgãos e entidades da Administração Pública estadual.

8. Descrição das orientações técnicas (diretrizes, regras e/ou procedimentos)

A LGPD, em seus artigos 7º e 11, permite à Administração Pública tratar e compartilhar os dados pessoais necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, bem como a dispensa de obter consentimento do titular para realizar tratamento compartilhado de dados pessoais sensíveis que sejam necessários à execução de políticas públicas previstas em leis ou regulamentos. Contudo, em seu artigo 23, a Lei determina que esse tratamento pode ocorrer desde que

sejam informadas as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas utilizadas para a execução dessas atividades, em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

Para subsidiar o cumprimento dessa exigência por todos os órgãos e entidades da Administração Pública estadual, estabeleceu-se o "Modelo para Elaboração da Política de Privacidade e Tratamento de Dados Pessoais" que acompanha esta orientação técnica. Trata-se de arquivo eletrônico de texto com conteúdo e estrutura definidos pela PPDP, em seu Anexo II, e específicos para o Poder Público no exercício de suas atividades e prerrogativas com vistas a facilitar o entendimento do usuário/cidadão.

A estrutura da Política de Privacidade e Tratamento de Dados Pessoais a ser elaborada pelo órgão ou entidade é, portanto, preestabelecida conforme descrito a seguir. Orienta-se **utilizar o texto** do modelo fornecido, **preenchendo-se as partes indicadas entre colchetes** de acordo com a atuação do órgão ou entidade.

Finalizada a elaboração do documento, deve-se proceder à sua publicização disponibilizando-o na primeira página do *site* do órgão ou entidade.

8.1. Estrutura da Política de Privacidade e Tratamento de Dados Pessoais

A Política de Privacidade e Tratamento de Dados Pessoais preestabelecida no âmbito da Administração Pública estadual tem a seguinte estrutura:

- "**Introdução**": informa ao usuário/cidadão o objetivo da Política de Privacidade e Tratamento de Dados Pessoais, bem como a legislação que justifica sua implantação;
- "**Sumário**": apresenta os temas abordados no documento;
- "**Como e por que tratamos dados?**": apresenta as finalidades dos tratamentos de dados pessoais realizados, suas bases normativas e os dados pessoais tratados, agrupados em blocos de serviços, programas e ações (ver item 8.2 desta orientação técnica);
- "**Segurança dos dados**": representa um compromisso com o usuário/cidadão em relação à segurança e à proteção dos dados pessoais tratados na medida em que declara serem empregados os melhores esforços para preservar a privacidade dele mediante adoção de medidas técnicas, organizacionais, administrativas e físicas com objetivo de mitigar todo e qualquer risco;
- "**Armazenamento dos dados**": informa sobre o armazenamento dos dados pessoais durante o prazo necessário para o cumprimento das finalidades;
- "**Quando compartilhamos dados**": informa as situações em que os dados pessoais são compartilhados sem necessidade de consentimento do titular (ver item 8.5 desta orientação técnica);
- "**Quais são seus direitos?**": informa os direitos do usuário/cidadão em relação a seus dados pessoais e o tratamento deles;

- "**Uso de *cookies***": explicita que o órgão ou entidade utiliza *cookies* em suas plataformas digitais (ver item 8.3 desta orientação técnica);
- "**Canais de atendimento**": informa canais diretos de comunicação com o encarregado de dados pessoais (ver item 8.4 desta orientação técnica);
- "**Glossário**": esclarece o significado de termos pertinentes à Política de Privacidade e Tratamento de Dados Pessoais.

8.2. Orientações para preenchimento do item "Como e por que tratamos dados?"

Esse item tem como objetivo descrever a finalidade e a base normativa dos tratamentos de dados pessoais executados no órgão ou entidade. Tendo em vista que a finalidade é o que determina os critérios e as formas de tratamento, recomenda-se que as informações sejam agrupadas em bloco de serviços finalísticos, programas ou ações, de acordo com a finalidade do tratamento, utilizando-se para isso a tabela presente no modelo que acompanha esta orientação técnica. Para preenchê-la, orienta-se tomar como base o "Documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados – RoPA", procedente da primeira providência da PPDP.

O entendimento de alguns conceitos é essencial para a elaboração do item "Como e por que tratamos dados?", a saber:

- De acordo com o PPA 2020-2023 **programas** são os meios pelos quais o Governo do Estado de São Paulo viabiliza as mudanças de médio e longo prazos para a sociedade. Por meio dos programas, os objetivos estratégicos são executados. Os programas finalísticos, foco da Política de Privacidade e Tratamento de Dados Pessoais, têm por objetivo viabilizar o acesso da população aos bens e serviços públicos e à mudança nas condições de vida dos seus beneficiários diretos. Esses bens e serviços consistem nos produtos entregues por cada programa (conforme Lei Estadual nº 17.262/2020). Os programas são compostos por **ações**, e é por meio delas que são gerados os produtos.
- **Serviço público finalístico** diz respeito à atividade-fim prestada pela Administração Pública estadual, diretamente (incluindo as funções públicas) ou em regime de autorização, concessão ou permissão, e voltada aos cidadãos ou aos usuários do serviço público.
- **Base normativa** é aquilo que dá legitimidade à execução do serviço finalístico, ou seja, Lei, Decreto, Portaria, Resolução, Norma ou respaldo em contratos, convênios e instrumentos congêneres estabelecidos para execução de políticas públicas ou de competências, atribuições legais e finalidades públicas do órgão ou entidade. Não se trata da base legal para o tratamento de dados pessoais pela Administração Pública, mas da norma ou instrumento que legitima ou estabelece o serviço finalístico.

É necessário relacionar todos os dados pessoais tratados pelo órgão ou entidade na execução de cada serviço finalístico informado. Observa-se que devem ser tratados apenas os dados pessoais

mínimos necessários para que o serviço finalístico possa ser executado e concluído com sucesso. Caso seja observada, no "Documento com a relação dos serviços finalísticos prestados ao cidadão, contendo informações sobre as respectivas finalidades, atribuição das bases legais e quais dados pessoais são tratados – RoPA", procedente da primeira providência da PPDP, a presença de dados que não sejam estritamente necessários, o órgão ou entidade deverá proceder a revisão e ajuste de processos de trabalho internos, manuais, ferramentas e sistemas, a fim de que sejam tratados apenas os dados pessoais essenciais à execução de seus serviços finalísticos. Deverá também elaborar planos de ação e mudanças nos sistemas e ferramentas utilizados, de modo a suprimir a obrigatoriedade de campos que se referem a dados não necessários para o tratamento específico, bem como promover treinamento das equipes para que esses planos e alterações sejam de fato implementados. Com essas ações, o órgão ou entidade executará a nona e a décima providências da PPDP, atendendo ao princípio da necessidade (limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados) constante na LGPD, em seu artigo 6º, inciso III, na PGDI, em seu artigo 5º, inciso VIII, e na PPDP, em seu artigo 12.

8.3. Orientações sobre o item "Uso de *cookies*"

Esse item tem como objetivo destacar a utilização de *cookies* para captura de dados e informações do usuário/cidadão destinada à otimização da navegação em plataformas digitais. Sempre que esse tipo de instrumento técnico for adotado no *site* ou outra plataforma digital do órgão ou entidade, orienta-se manter o texto do modelo definido pela PPDP e que acompanha esta orientação técnica. Caso esse tipo de instrumento técnico não seja adotado em nenhuma das plataformas digitais utilizadas pelo órgão ou entidade para execução de seus serviços finalísticos, o item "Uso de *cookies*" pode ser suprimido de sua Política de Privacidade e Tratamento de Dados Pessoais.

Destaca-se que, sempre que o *site* ou outra plataforma digital do órgão ou entidade realiza ou subsidia qualquer tratamento de dado pessoal, ela deve oferecer ao usuário/cidadão as opções de aceitar, não aceitar ou personalizar o uso de *cookies*.

8.4. Orientações para preenchimento do item "Canais de atendimento"

Esse item tem como objetivo informar sobre a possibilidade do usuário/cidadão titular dos dados pessoais enviar dúvidas, solicitações e reclamações sobre os tratamentos de dados realizados pelo órgão ou entidade, identificando-se o nome do encarregado de dados pessoais, as formas de contato e o horário de atendimento.

Destaca-se que nas entidades da Administração Pública Indireta o encarregado de dados pessoais deve ser determinado de acordo com o Decreto Estadual nº 65.347/2020, em seu artigo 8º, ao passo que nos órgãos da Administração Pública Direta o encarregado de dados pessoais é o Ouvidor Geral da Administração Direta.

8.5. Esclarecimento sobre o uso compartilhado de dados pessoais

A ANPD, em seu *Guia orientativo* (2022), esclarece que, no âmbito do Poder Público,

> o compartilhamento de dados pessoais é a operação de tratamento pela qual órgãos e entidades públicos conferem permissão de acesso ou transferem uma base de dados pessoais a outro ente público ou a entidades privadas visando ao atendimento de uma finalidade pública.

A LGPD, no seu art. 26 traz: "O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei".

As hipóteses descritas no modelo de Política de Privacidade e Tratamento de Dados Pessoais definido pela PPDP são aquelas admitidas e amparam o órgão ou entidade no uso compartilhado de dados pessoais com entes públicos e privados para finalidade pública ou na persecução do interesse público, no que tange a execução de políticas públicas ou atribuições legais pelos órgãos e entidade para finalidades específicas. Importante destacar que deve-se atribuir uma base legal previstas no artigo 7º e 11 que autoriza o tratamento compartilhado de dados pessoais e dados sensíveis., No entanto, qualquer compartilhamento diverso ou no caso do serviço público prestado não ser compulsório, deverá ser avaliada a necessidade do consentimento do titular dos dados pessoais. Orienta-se, caso necessário, consultar o Manual Técnico Procedimental de Verificação da Necessidade de Obtenção de Consentimento do Titular de Dados Pessoais, que corresponde à segunda providência da PPDP.

Destaca-se que as diretrizes para o compartilhamento de dados por órgãos e entidades da Administração Pública estadual estão estabelecidas na PPDP, em sua Seção X – Transferência, Uso Compartilhado e Compartilhamento de Dados Pessoais, e que os procedimentos acerca dessa questão estão orientados na décima terceira providência da PPDP.

8.6. Modelo fornecido

Acompanha esta orientação técnica o "Modelo para Elaboração da Política de Privacidade e Tratamento de Dados Pessoais", conforme definido pela PPDP, em seu Anexo II, em formato de arquivo eletrônico de texto (Word). Tal disponibilização é feita no Portal do COETIC (http://www.coetic.sp.gov.br/) na página de Governança de Dados e Informações