**RELATÓRIO DE IMPACTO**

**À PROTEÇÃO DE DADOS PESSOAIS**

<Local>, <dia> de <mês> de <ano>

**Histórico de Revisões**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versão** | **Descrição** | **Autor** |
| DD/MM/AAAA | 1 | Conclusão da primeira versão do Relatório | XXXXXXXXX |
| DD/MM/AAAA | 2 | Revisão do Relatório após Orientações de Adequação do Encarregado pela Proteção de Dados Pessoais | XXXXXXXXX |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| **ATENÇÃO!**<Os trechos marcados em azul neste modelo são editáveis, notas explicativas ou exemplos, devendo ser substituídos ou excluídos, conforme necessário>.<**Versão 1 – Concluído em DD/MM/AAAA**> |

**RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS**

|  |
| --- |
| **OBJETIVO** |
| O Relatório de Impacto à Proteção de Dados Pessoais visa a descrever as operações de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares de dados pessoais, bem como descrever os controles, implementados ou que serão implementados, que objetivam o tratamento de riscos à segurança da informação, à privacidade e à proteção de dados pessoais.**Referência:** Art. 5º, inc. XVII, da Lei Federal nº 13.709/2018 (LGPD). |

|  |
| --- |
| **1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO** |

|  |
| --- |
| **Controlador** |
| <Nome da pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais (art. 5º, inc. VI, da LGPD)>. |

|  |
| --- |
| **Operador** |
| <Nome da pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador (art. 5º, inc. VII, da LGPD)>. |

|  |  |
| --- | --- |
| **Encarregado** |  |
| <Nome da 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 (art. 5º, inc. VIII, da LGPD).><Quanto aos órgãos da Administração Pública do Município de São Paulo, o Encarregado pela Proteção de Dados Pessoais é o Controlador Geral do Município.> |  |
| **Canal de Comunicação com o Encarregado** |  |
| <O Canal de Comunicação com o Encarregado pela Proteção de Dados Pessoais, no âmbito dos órgãos da Administração Pública do Município de São Paulo, é realizado: (i) sob a forma eletrônica, pelo Portal SP 156 e pelo *e-mail* privacidade@prefeitura.sp.gov.br; e, (ii) sob a forma de correspondência, no Viaduto do Chá, nº 15, 10º andar, Centro, São Paulo/SP, CEP nº 01002-900.> |  |

|  |
| --- |
| **2 – NECESSIDADE DE ELABORAR O RELATÓRIO** |

<Os casos específicos previstos pela LGPD em que o Relatório deverá ou poderá ser solicitado são:

1. para tratamento de dados pessoais realizados para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais;
2. quando houver infração à LGPD em decorrência do tratamento de dados pessoais pelo Poder Público (arts. 31 e 32, LGPD); e
3. a qualquer momento, sob determinação da Autoridade Nacional de Proteção de Dados – ANPD (art. 38, LGPD).>

<Conforme o art. 2°, inc. XIII, do Decreto Municipal nº 59.767/2020, o Plano de Adequação dos órgãos e entidades da Administração Pública Municipal ao sistema normativo relativo à privacidade e à proteção de dados pessoais deve conter, entre outras ações, a relativa à elaboração e à atualização de Relatório de Impacto à Proteção de Dados Pessoais (RIPD). Conforme o art. 4°, parágrafo único, do mesmo Decreto Municipal, devem os órgãos da Administração Pública Municipal observar as diretrizes editadas pelo Controlador Geral do Município, na qualidade de Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município, com relação ao Plano de Adequação – o que inclui o presente *layout* de Relatório.>

<Para tanto, o órgão ou a entidade deverá avaliar se os seus processos existentes ou a serem implementados geram impactos à proteção de dados pessoais, a fim de estruturar ou atualizar o RIPD.>

<Como dispõe o art. 6º, inc. XII, do Decreto Municipal nº 59.767/2020, o Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município poderá requisitar, aos órgãos da Administração Pública Municipal, informações para a compilação de único Relatório de Impacto à Proteção de Dados Pessoais (RIPD), quando solicitado pela ANPD, nos termos do art. 32 da LGPD.>

<Além de casos específicos previstos pela LGPD, no início desta Capítulo II, relativos à elaboração do RIPD, e da atualização anual, como prevista pelo art. 3º da Instrução Normativa CGM nº 01/2022, é indicada a atualização do Relatório sempre que existir a possibilidade de ocorrer impacto à proteção de dados pessoais resultante de:

1. utilização de nova tecnologia ou de outra nova iniciativa com as quais estão sendo ou serão tratados os dados pessoais;
2. qualquer operação de tratamento de dados pessoais que vise à formação de perfil comportamental de pessoa natural (art. 12, § 2º, LGPD);
3. tratamento de dados pessoais com a utilização de tomadas de decisão automatizadas, incluídas as decisões destinadas a definir à formação de perfil comportamental de pessoa natural (art. 20, LGPD);
4. tratamento de dados pessoais de crianças e adolescentes (art. 14, LGPD);
5. tratamento de dados pessoais que possam resultar em algum tipo de dano material ou imaterial aos titulares de dados pessoais, na eventualidade de um incidente de segurança (art. 42, LGPD);
6. tratamento de dados pessoais realizados para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º, LGPD);
7. tratamento de dados pessoais realizado para atender aos interesses legítimos do controlador (art. 10, § 3º, LGPD);
8. alterações em atos normativos que possam gerar impactos aos direitos à privacidade e à proteção de dados pessoais dos titulares; e
9. alterações estruturais da Administração Pública Municipal que possam gerar impactos aos direitos à privacidade e à proteção de dados pessoais dos titulares.>

<Em síntese, nesta etapa deve(m) ser explicitado(s) qual(is) dos itens elencados acima expressa(m) a necessidade de o Relatório ser realizado ou atualizado pelo órgão ou entidade.>

|  |
| --- |
| **3 – DESCRIÇÃO DO TRATAMENTO** |

<A descrição das operações de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza**, do **escopo**,do **contexto** e da **finalidade** do tratamento.>

<A LGPD (art. 5º, inc. X) considera 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”*.>

<O objetivo principal da descrição é o de fornecer um cenário institucional relativo aos processos que envolvam o tratamento dos dados pessoais.>

**3.1 – NATUREZA DO TRATAMENTO**

<A **natureza** representa como o órgão ou a entidade pretende tratar ou trata dados pessoais.>

<Importante descrever, por exemplo:

1. como se realiza o fluxo do tratamento de dados pessoais – ou seja, da coleta à eventual eliminação;
2. qual é a fonte de obtenção de dados pessoais – ou seja, se os dados pessoais foram obtidos a partir do próprio titular de dados pessoais ou se foram obtidos por terceiros, como por outros órgãos ou entidades do Poder Público;
3. com quais órgãos, entidades ou terceiros os dados pessoais são compartilhados, assim como quais são esses dados pessoais compartilhados;
4. quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador e quais são as fases do ciclo de vida do tratamento em que atuam;
5. se adotou, recentemente, algum tipo de nova tecnologia ou de nova iniciativa com as quais estão sendo ou serão tratados os dados pessoais; e
6. controles já implementados e a implementar com o objetivo de salvaguarda a privacidade e a proteção de dados pessoais.>

<Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um fluxograma que demonstre os fluxos dos processos do órgão ou da entidade.>

**3.2 – ESCOPO DO TRATAMENTO**

<O **escopo** representa a abrangência do tratamento de dados pessoais.>

<Nesse sentido, considere destacar:

1. as categorias de dados pessoais tratados, inclusive das categorias de dados pessoais sensíveis;
2. o volume de dados pessoais tratados;
3. a frequência com a qual os dados pessoais são tratados;
4. o período de retenção dos dados pessoais tratados;
5. o número de titulares de dados pessoais envolvidos no tratamento; e
6. a abrangência da área geográfica do tratamento.>

<O levantamento das informações elencadas acima auxilia a determinar se o tratamento de dados pessoais é realizado em alta escala.>

**3.3 – CONTEXTO DO TRATAMENTO**

<Neste subitem, convém destacar um cenário mais amplo, incluindo contextos internos e externos que possam afetar as expectativas dos titulares de dados pessoais ou o impacto sobre o tratamento de dados pessoais.>

<O levantamento das informações destacadas abaixo proporciona a obtenção de parâmetros que objetivamente permitam demonstrar o equilíbrio entre o interesse e a necessidade do controlador em tratar os dados pessoais e os direitos dos titulares dos dados pessoais:

1. natureza do relacionamento do órgão ou da entidade com os titulares de dados pessoais;
2. método de controle que os indivíduos exercem sobre os seus dados pessoais;
3. destaque se o tratamento envolve crianças, adolescentes, idosos, pessoas com deficiência ou outro grupo vulnerável;
4. destacar se o tipo de tratamento de dados pessoais realizado é condizente com as razoáveis expectativas de privacidade dos titulares de dados pessoais; e
5. destacar se há avanços relevantes do órgão ou da entidade em segurança da informação que contribuam para a salvaguarda da privacidade e da proteção de dados pessoais.>

**3.4 – FINALIDADE DO TRATAMENTO**

<A **finalidade** é a razão ou motivo pelo qual se deseja tratar os dados pessoais. É imprescindível estabelecer claramente a finalidade, pois é a finalidade que justifica o tratamento e fundamenta as informações prestadas aos titulares.>

<Neste subitem, é importante detalhar o que se pretende alcançar com o tratamento de dados pessoais, em harmonia com as hipóteses elencadas abaixo, que, materialmente, se referem àquelas presentes nos arts. 7º e 11 da LGPD:

1. consentimento do titular de dados pessoais;
2. cumprimento de obrigação legal ou regulatória pelo controlador;
3. execução de políticas públicas pelo controlador;
4. espécie de estudo realizado por órgão de pesquisa;
5. execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular de dados pessoais, a pedido do próprio titular;
6. exercício regular de direitos em processo judicial, administrativo ou arbitral;
7. proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiros;
8. tutela da saúde;
9. atender aos interesses legítimos do controlador ou de terceiros;
10. proteção do crédito; e
11. garantia da prevenção à fraude e à segurança do titular.>

<Cumpre destacar que os exemplos de finalidades apresentados neste documento não são exaustivos. Desse modo, deve-se informar e detalhar qualquer outra finalidade específica do controlador para o tratamento de dados pessoais, mesmo que essa finalidade não conste nos citados exemplos, mas que tenha relação às hipóteses de tratamento de dados pessoais previstas pelos arts. 7º e 11, da LGPD.

Ao detalhar a finalidade do tratamento dos dados pessoais, é importante:

1. Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais e a sua importância;
2. Informar os benefícios esperados para o órgão ou para a entidade ou mesmo para a sociedade como um todo.>

<Neste momento, deve-se atentar para o caso de a **finalidade** ser para atender ao legítimo interesse do controlador. Nesse caso, somente poderá ser fundamentado o tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, conforme previsto pelo art. 10 da LGPD.

Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:

I - apoio e promoção de atividades do controlador; e

II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

§ 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os

dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento

de dados baseado em seu legítimo interesse.

§ 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.>

<Cumpre ressaltar que devem ser equilibrados os interesses do controlador de dados pessoais com os de terceiros com os quais se tem relacionamento.>

|  |
| --- |
| **4 – PARTES INTERESSADAS CONSULTADAS** |

<Partes interessadas relevantes, internas e externas, consultadas a fim de se obter opiniões legais ou técnicas sobre os dados pessoais que são objeto do tratamento.>

<Neste subitem, é importante identificar:

1. quais partes foram consultadas – como, por exemplo, o operador (art. 5º, inc. VII, LGPD), o Encarregado pela Proteção de Dados Pessoais competente (art. 5º, inc. VIII, LGPD), consultores jurídicos e especialistas em segurança da informação, privacidade e proteção de dados pessoais; e
2. o que cada parte consultada indicou como necessário à salvaguarda dos direitos à privacidade e à proteção e dados pessoais.>

<Caso não seja conveniente registrar o que foi consultado, é importante apresentar o motivo de não se ter realizado esse registro – como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes comprometeria segredo comercial ou industrial ou mesmo reduziria a segurança da informação.>

|  |
| --- |
| **5 – NECESSIDADE E PROPORCIONALIDADE** |

<Descrever como o órgão ou a entidade avalia a necessidade e a proporcionalidade do tratamento de dados pessoais. É necessário demonstrar que as operações realizadas limitam o tratamento ao mínimo necessário para a realização de suas finalidades (art. 6º, inc. III, LGPD).>

<Nesse sentido, destacar:

1. a fundamentação legal para o tratamento dos dados pessoais;
2. caso o fundamento legal seja embasado no legítimo interesse do controlador (art. 10, LGPD), demonstrar que:

a. esse tratamento de dados pessoais é indispensável;

b. não há outra hipótese de tratamento possível de ser utilizada para alcançar a mesma finalidade; e

c. esse tratamento de dados pessoais de fato auxilia na finalidade almejada.

1. Quais medidas são adotadas a fim de assegurar que o operador (art. 5º, inc. VII, LGPD) realize o tratamento de dados pessoais em conformidade ao sistema normativo protetivo à privacidade e aos dados pessoais e respeite os critérios estabelecidos pela organização que exerça o papel de controlador (art. 5º, inc. VI, LGPD);
2. Como estão implementadas as medidas que asseguram a efetivação do exercício dos direitos dos titulares de dados pessoais (arts. 9º e 17 a 22, LGPD); e
3. Quais são as salvaguardas para as transferências internacionais de dados pessoais.>

|  |
| --- |
| **6 – GESTÃO DE RISCOS** |

<O art. 5º, inc. XVII, da LGPD, preconiza que o Relatório de Impacto à Proteção de Dados Pessoais deve descrever as *“medidas, salvaguardas e mecanismos de mitigação de risco”* implementados no âmbito da organização.>

<Para a realização da Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais de seu órgão ou de sua entidade, recomenda-se a consulta à metodologia, orientada pela Controladoria Geral do Município de São Paulo (CGM/SP), presente no “*Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública Municipal*”.>

|  |
| --- |
| **7 – APROVAÇÃO** |

<Este item visa a formalizar a aprovação do Relatório por meio da obtenção das assinaturas do(s) Responsável(is) por sua elaboração, do Encarregado pela Proteção de Dados Pessoais competente e dos demais agentes públicos envolvidos. O(s) Responsável(is) pela elaboração do Relatório pode(m) ser um(os) membro(s) da equipe de trabalho designada à estruturação do Plano de Adequação do órgão ou da entidade ao sistema normativo protetivo à privacidade e aos dados pessoais, desde que com conhecimentos necessários para a elaboração deste documento.>

<O Relatório deve ser revisto e atualizado anualmente ou sempre que quaisquer alterações no órgão ou na entidade possam impactar o tratamento de dados pessoais realizado.>

<No âmbito dos órgãos da Administração Pública Municipal, o Encarregado pela Proteção de Dados Pessoais apenas aprovará o Relatório após prévia análise de todo o Plano de Adequação do órgão por parte da Coordenadoria de Promoção da Integridade (COPI), nos termos da Instrução Normativa CGM nº 01/ 2022>

|  |
| --- |
| **RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<Nome do Responsável>**RF/CPF:** xxxxx<Local>, <dia> de <mês> de <ano> |

|  |
| --- |
| **REPRESENTANTE** **DA COORDENADORIA DE PROMOÇÃO DA INTEGRIDADE** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<Nome do Representante>**RF/CPF:** xxxxx<Local>, <dia> de <mês> de <ano> |

|  |
| --- |
| **ENCARREGADO** **PELA PROTEÇÃO** **DE DADOS PESSOAIS** |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_<Nome do Encarregado>**RF/CPF:** xxxxx<Local>, <dia> de <mês> de <ano> |

<Para saber mais, consulte a Instrução Normativa CGM nº 01/2022 e a Controladoria Geral do Município de São Paulo (CGM/SP), via *e-mail* (privacidade@prefeitura.sp.gov.br) ou via Processo SEI.>