<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

<Local>, <dia> de <mês> de <ano>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

Histórico de Revisões

Data	Versão	Descrição	Autor
DD/MM/AAAA	1	Conclusão da primeira versão do Relatório	XXXXXXXXXXXX
DD/MM/AAAA	2	Revisão do Relatório após análise do Encarregado pela Proteção de Dados Pessoais	XXXXXXXXXXXX

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>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPDP

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os 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.

Referências: 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 à Administração Pública Direta 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 da Administração Pública Direta do Município de São Paulo, é realizado por meio da **Ouvidoria Geral do Município de São Paulo (OGM/SP)**, através do **Portal SP 156** e do atendimento presencial no espaço "**Aqui tem Ouvidoria"**, localizado na Rua Dr. Falcão Filho, nº 69, Centro, CEP 01009-000.>

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

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

• 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 (exceções previstas pelo art. 4º, inciso III, LGPD);

• quando houver infração da LGPD em decorrência do tratamento de dados pessoais por órgãos públicos (arts. 31 e 32, LGPD); e

• a qualquer momento sob determinação da ANPD (art. 38, LGPD).>

<Conforme o art. 2º, inc. XIII, do Decreto Municipal nº 59.767/2020, o plano de adequação contém,

dentre outras etapas, a necessidade da elaboração e atualização de Relatório de Impacto à Proteção de Dados. De acordo com o art. 4º, parágrafo único, do mesmo Decreto Municipal, devem as Secretarias e Subprefeituras observar as diretrizes editadas pelo Controlador Geral do Município, com relação ao plano de adequação, o que inclui o presente *layout* de Relatório.>

<Quando for necessária a elaboração do RIPDP, o órgão ou entidade deve avaliar se os programas, sistemas de informação e processos existentes ou a serem implementados geram impactos à proteção de dados pessoais, a fim de estruturar ou atualizar o RIPDP.>

<Como dispõe o art. 6º, inc. XII, do Decreto Municipal nº 59.767/2020, o Encarregado pela Proteção de Dados Pessoais, que é o Controlador Geral do Município, no âmbito da Administração Pública Direta, poderá requisitar, às Secretarias e Subprefeituras, informações para a compilação de único Relatório de Impacto à Proteção de Dados (RIPDP), quando solicitado pela ANPD, nos termos do art. 32 da LGPD.>

<Além dos casos específicos previstos pela LGPD, no início desta seção 2, relativos à elaboração do RIPDP, 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:

• uma tecnologia, serviço ou outra nova iniciativa em que dados pessoais e dados pessoais sensíveis sejam ou devam ser tratados;

• rastreamento da localização dos indivíduos ou qualquer outra ação de tratamento que vise a formação de perfil comportamental de pessoa natural, se identificada (art. 12, § 2º, LGPD);

• tratamento de 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"* (art. 5º, inc. II, LGPD);

• processamento de dados pessoais a fim de serem tomadas decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade (art. 20, LGPD);

• tratamento de dados pessoais de crianças e adolescentes (art. 14, LGPD);

• tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver vazamento (art. 42, LGPD);

• 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);

• tratamento no interesse legítimo do controlador (art. 10, § 3º, LGPD);

• alterações nas leis e regulamentos aplicáveis à privacidade, política e normas internas, operação do sistema de informações, propósitos e meios para tratar dados, fluxos de dados novos ou alterados, *etc.*; e

• reformas administrativas que implicam em nova estrutura organizacional resultante da incorporação, fusão ou cisão de órgãos ou entidades.>

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

3 – DESCRIÇÃO DO TRATAMENTO

<A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e 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 dessa descrição é fornecer um cenário institucional relativo aos processos que envolvam o tratamento dos dados pessoais, fornecendo subsídios para a avaliação e o tratamento de riscos.>

3.1 – NATUREZA DO TRATAMENTO

<A **natureza** representa como o órgão ou entidade pretende tratar ou trata o dado pessoal.>

<Importante descrever, por exemplo:

• como os dados pessoais são coletados, retidos/armazenados, tratados, usados e eliminados;

• fonte de dados (por exemplo: titular de dados, planilha eletrônica, arquivo .xml, formulário em papel, etc.) utilizada para coleta dos dados pessoais;

• com quais órgãos, entidades ou empresas dados pessoais são compartilhados e quais são esses dados;

• quais são os operadores que realizam o tratamento de dados pessoais em nome do controlador (agente de tratamento) e destacar em quais fases (coleta, retenção, processamento, compartilhamento, eliminação) eles atuam;

• se adotou recentemente algum tipo de nova tecnologia ou método de tratamento que envolva dados pessoais. A informação sobre o uso de nova tecnologia ou método de tratamento é importante no sentido de possibilitar a identificação de possíveis riscos resultantes de tal uso; e

• medidas de segurança atualmente adotadas.>

<Na elaboração dessa descrição, é importante considerar a possibilidade de consultar um diagrama ou qualquer outra documentação que demonstre os fluxos de dados do órgão ou entidade.>

3.2 – ESCOPO DO TRATAMENTO

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

<Nesse sentido, considere destacar:

• as informações sobre os tipos dos dados pessoais tratados, ressaltando quais dos dados são considerados dados pessoais sensíveis;

• o volume dos dados pessoais coletados e tratados;

• a extensão e frequência em que os dados são tratados;

• o período de retenção, que é a informação sobre quanto tempo os dados pessoais são mantidos, retidos ou armazenados;

• o número de titulares de dados afetados pelo tratamento; e

• 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

<Nesta seção, convém destacar um cenário mais amplo, incluindo fatores internos e externos que podem afetar as expectativas dos titulares dos dados pessoais ou o impacto sobre o tratamento dos dados.>

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

• natureza do relacionamento do órgão ou entidade com os indivíduos;

• nível ou método de controle que os indivíduos exercem sobre os dados pessoais;

• destacar se o tratamento envolve crianças, adolescentes ou outro grupo vulnerável;

• destacar se o tipo de tratamento realizado sobre os dados é condizente com a expectativa dos titulares dos dados pessoais. Ou seja, se o dado pessoal não é tratado de maneira diversa do que é determinado em normas e regulamentos e se é comunicado pelo órgão ou entidade ao titular de dados;

• destaque de qualquer experiência anterior com esse tipo de tratamento de dados;

• destaque de avanços relevantes do órgão ou entidade em tecnologia ou segurança que contribuam para a proteção dos 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 o que justifica o tratamento e fornece os elementos para informar o titular dos dados.>

<Nesta seção, é importante detalhar o que se pretende alcançar com o tratamento dos dados pessoais, em harmonia com as hipóteses elencadas abaixo, que se referem àquelas presentes nos arts. 7º e 11 da LGPD, no que for aplicável:

• cumprimento de obrigação legal ou regulatória pelo controlador;

• execução de políticas públicas;

• alguma espécie de estudo realizado por órgão de pesquisa;

• execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

• exercício regular de direitos em processo judicial, administrativo ou arbitral;

• proteção da vida ou da incolumidade física do titular ou de terceiro;

• tutela da saúde;

• atender aos interesses legítimos do controlador ou de terceiro;

• proteção do crédito; e

• 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 tratamento dos dados pessoais, mesmo que essa finalidade não conste nos citados exemplos.

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

• Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais, informando o quão importantes são esses resultados;

• Informar os benefícios esperados para o órgão, entidade ou para a sociedade como um todo.>

<Neste momento, deve-se atentar para o caso de a **finalidade** ser para atender o legítimo interesse do controlador (agente de tratamento). Nesse caso, somente poderá ser fundamentado 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 dos indivíduos com os quais se tem relacionamento.>

4 – PARTES INTERESSADAS CONSULTADAS

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

<Nessa seção, é importante identificar:

• quais partes foram consultadas, como, por exemplo: operador (art. 5º, inc. VII, LGPD), Encarregado pela Proteção de Dados Pessoais (art. 5º, inc. VIII, LGPD), gestores, especialistas em segurança da informação, consultores jurídicos, etc.; e

• o que cada parte consultada indicou como importante de ser observado para o tratamento dos dados pessoais em relação aos possíveis riscos referentes às atividades de tratamento em análise. Também deve se observar os riscos de não-conformidade ante a LGPD e demais normas relativas à proteção de dados pessoais, bem como ante aos instrumentos internos de controle (políticas, processos e procedimentos voltados à proteção de dados pessoais e privacidade).>

<Caso não seja conveniente registrar o que foi consultado, então é importante apresentar o motivo de não se ter realizado tal registro, como, por exemplo, apresentar justificativa de que informar o registro das opiniões das partes internas comprometeria segredo comercial ou industrial, fragilizaria a segurança da informação, ou seria desproporcional ou impraticável realizar o registro das opiniões obtidas.>

5 – NECESSIDADE E PROPORCIONALIDADE

<Descrever como o órgão ou entidade avalia a necessidade e a proporcionalidade de dados pessoais. É necessário demonstrar que as operações realizadas sobre os dados pessoais limitam o tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos com relação às finalidades do tratamento de dados pessoais (art. 6º, inc. III, LGPD).>

<Nesse sentido, destacar:

• A fundamentação legal para o tratamento dos dados pessoais;

• Caso o fundamento legal seja embasado no legítimo interesse do controlador (art. 10, LGPD), demonstrar que:

- esse tratamento de dados pessoais é indispensável;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito; e
- esse processamento de fato auxilia no propósito almejado.

• Como será garantida a qualidade (exatidão, clareza, relevância e atualização de dados pessoais) e a minimização de dados pessoais;

• Quais medidas são adotadas a fim de assegurar que o operador (art. 5º, inc. VII, LGPD) realize o

tratamento de dados pessoais conforme a LGPD e respeite os critérios estabelecidos pelo órgão ou entidade que exerça o papel de controlador (art. 5º, inc. VI, LGPD);

• Como estão implementadas as medidas que asseguram o direito do titular de dados pessoais de obter do controlador (agente de tratamento) o previsto pelo art. 18 da LGPD;

• Como o órgão ou entidade pretende fornecer informações de proteção de dados pessoais para os titulares;

• Quais são as salvaguardas para as transferências internacionais de dados pessoais.>

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

<O art. 5º, inc. XVII, da LGPD, preconiza que o Relatório de Impacto à Proteção de Dados Pessoais deve descrever *"medidas, salvaguardas e mecanismos de mitigação de risco"*.>

<Antes de definir essas medidas, salvaguardas e mecanismos, é necessário identificar os riscos que geram impacto potencial sobre o titular de dados pessoais.>

<Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco e o possível impacto na eventualidade da ocorrência do risco, a fim de avaliar o nível potencial de risco para cada evento.>

<Parâmetros escalares podem ser utilizados para representar os níveis de **probabilidade** e **impacto** que, após a multiplicação, resultarão em níveis de risco, que direcionarão a aplicação de medidas de segurança. Os parâmetros escalares adotados neste documento são apresentados na tabela a seguir:>

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

<A figura a seguir apresenta a **Matriz Probabilidade x Impacto**, instrumento de apoio para a definição dos critérios de classificação do nível de risco.>

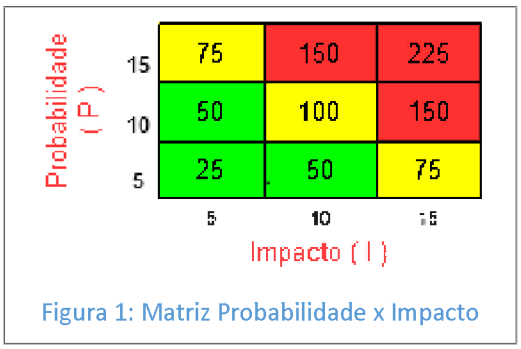

Figura 1: Matriz Probabilidade x Impacto

<O produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

- verde, é entendido como baixo;

- amarelo, representa risco moderado; e
- vermelho, indica risco alto.>

<As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação, a análise e a gestão de riscos realizados no RIPDP.>

	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
	<Risco 1>			
	<Risco 2>			
	<Risco N>			

Legenda: P – Probabilidade; I – Impacto.

[1] **Probabilidade:** chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] **Impacto:** resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] **Nível de Risco:** magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23).

<A título de informação, é destacada a seguir uma lista não exaustiva de **riscos à privacidade e proteção de dados pessoais e à segurança da informação**. A probabilidade, o impacto e o nível dos riscos indicados são apenas exemplificativos, devendo ser avaliados de acordo com o contexto de cada órgão ou entidade. Os doze primeiros riscos foram obtidos da norma ISO/IEC 29134:2017, seção 6.4.4.>

	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
1	Acesso não autorizado.	10	15	150
2	Modificação não autorizada.	10	15	150
3	Perda.	5	15	75
4	Roubo.	5	15	75
5	Remoção não autorizada.	5	15	75
6	Coleção excessiva.	10	10	100
7	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
8	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
9	Falha em considerar os direitos do titular dos dados pessoais (*e.g.*, perda do direito de acesso).	5	15	75

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
13	Falha/erro de processamento (*v.g.*, execução de *script* de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, *etc.*).	5	15	75
14	Reidentificação de dados pseudonimizados.	5	15	75

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

7 – MEDIDAS PARA TRATAR OS RISCOS

<Os agentes de tratamento devem adotar medidas de segurança, 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 qualquer forma de tratamento inadequado ou ilícito (LGPD, art. 46).>

<Importante reforçar que as medidas para tratar os riscos podem ser: de segurança, técnicas ou administrativas.>

<A coluna "*Medida(s)*" pode ser preenchida com uma medida de segurança ou controle específico adotado para tratamento do risco identificado na seção 6 deste Relatório.>

<**O órgão ou entidade nem sempre precisa eliminar todos os riscos.** Nesse sentido, pode-se decidir que alguns **riscos são aceitáveis** – até um risco de nível alto – devido aos benefícios do tratamento de dados pessoais e as **dificuldades de mitigação. No entanto, se houver um risco residual de nível alto, é recomendável consultar a Autoridade Nacional de Proteção de Dados (ANPD) antes de prosseguir com as operações de tratamento dos dados pessoais**.>

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
<Risco 1>	<Medida 1; Medida 2; Medida N>					
<Risco 2>	<Medida 1; Medida 2; Medida N>					
<Risco N>	<Medida 1; Medida 2; Medida N>					

Legenda: P – Probabilidade; I – Impacto.

Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir | Evitar | Compartilhar | Aceitar.

[2] **Risco residual** é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelos agentes de tratamento. Preencher a coluna com: Sim | Não.

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

<A seguir, são apresentados exemplos de medidas para tratar tipos de riscos, previamente identificados, a fim de demonstrar o preenchimento da tabela apresentada>.

Risco	Medida(s)	Efeito sobre o Risco	Risco Residual			Medida(s) Aprovada(s)
			P	I	Nível (P x I)	
Acesso não autorizado	1. Controle de acesso lógico	Reduzir	5	10	50	Sim
	2. Desenvolvimento seguro					
	3. Segurança em redes					
Roubo	1. Controle de acesso lógico	Reduzir	5	5	25	Sim
	2. Controles criptográficos					
	3. Proteção física e do ambiente					
Coleção excessiva	1. Limitação da coleta	Reduzir	5	10	50	Sim

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

8 – APROVAÇÃO

<Esta seção **visa a formalizar a aprovação do RIPDP** por meio da obtenção das assinaturas do responsável pela elaboração do RIPDP, pelo Encarregado e por demais autoridades. O responsável pela elaboração do Relatório pode ser o próprio Chefe de Gabinete, com relação às Secretarias e Subprefeituras, no âmbito da Administração Pública Direta, ou qualquer outra pessoa designada com conhecimento necessário para realizar esta tarefa>.

<**O RIPDP deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento de dados pessoais** realizados pelo órgão ou entidade.>

<No âmbito da Administração Pública Direta, o Encarregado apenas aprovará o RIPDP após prévia análise de todo o plano de adequação por parte da Coordenadoria de Promoção da Integridade (COPI), nos termos da Instrução Normativa>.

<Mais informações, consulte a Instrução Normativa CGM nº 01/ 2022 e a Controladoria Geral do Município, via SEI.>

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>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

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