GOVERNANÇA EM PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Fundamentos normativos

Emenda Constitucional nº 115/2022:

"Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais."

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Fundamentos normativos

Lei Federal nº 13.709/2018:

"Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Fundamentos normativos

Decreto Municipal nº 59.767/2020:

"Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta."

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Decreto Municipal nº 59.767/2020:

Conforme o art. 2º, inc. XIII, do Decreto Municipal nº 59.767/2020, o Plano de Adequação à Privacidade e à Proteção de Dados Pessoais é o "*conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais.*"

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Decreto Municipal nº 59.767/2020:

O Plano de Adequação à Privacidade e à Proteção de Dados Pessoais, como conceituado pelo art. 2º, inc. XIII, do Decreto Municipal nº 59.767/2020, remete-se ao art. 50, *caput*, da Lei Geral de Proteção de Dados Pessoais (LGPD), a tratar de todo o conjunto de regras de boas práticas e de Governança em Privacidade e Proteção de Dados Pessoais adotado.

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Decreto Municipal nº 59.767/2020:

O art. 4º, incs. I, II, e III, do Decreto Municipal nº 59.767/2020, dispõe, especificamente, de três práticas relativas à Governança em Privacidade e Proteção de Dados Pessoais, como elencadas anteriormente:

(i) Registro das Operações de Tratamento de Dados Pessoais; e
(ii) Mapeamento do Fluxo de Dados Pessoais;
(iii) Plano de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, incluindo:
  (iii.i) Relatório de Impacto à Proteção de Dados Pessoais.

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Instrução Normativa CGM/SP nº 01/2022:

“Estabelece disposições referentes ao tratamento de dados pessoais no âmbito da Prefeitura do Município de São Paulo.”

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Instrução Normativa CGM/SP nº 01/2022:

Possui como objetivo a padronização, no Poder Executivo do Município de São Paulo, da realização das práticas de: (i) Registros das Operações de Tratamento de Dados Pessoais; e de (ii) Planos de Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais, com a realização de Relatórios de Impacto à Proteção de Dados Pessoais.

Além disso, visa a subsidiar a elaboração das práticas de: (i) conscientização da população e capacitação dos agentes públicos sobre a LGPD; e de (ii) Mapeamento do Fluxo de Dados Pessoais, que será viabilizado após a estruturação de um Cadastro Base de Pessoas e de um "*Login Único*" no âmbito da Prefeitura do Município, nos termos do Decreto Municipal nº 60.663/2021.

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Registro das Operações de Tratamento de Dados Pessoais:

Orientações Gerais	Versão 13/01/2023
O Encarregado pela Proteção de Dados Pessoais da Prefeitura do Município de São Paulo, no uso de suas atribuições legais, conforme dispõe a Instrução Normativa nº 01, de 21 de julho de 2022, da Controladoria Geral do Município de São Paulo (CGM/SP), disponibiliza, para toda a Administração Pública do Município de São Paulo, *layout* de "*Mapeamento de Dados Pessoais*" (*"Registro das Operações de Tratamento de Dados Pessoais"*), a ser preenchido a partir do mapeamento de cada processo realizado pelos órgãos ou entidades, com a finalidade de subsidiá-los em seus planos de adequação ao sistema normativo de proteção de dados pessoais. Este mapeamento visa a identificar as operações de tratamento de dados pessoais realizadas no âmbito da Administração Pública Municipal e deve ser atualizado regularmente, com base nas alterações dos fluxos dos processos de cada órgão ou entidade e nos termos das normas aplicáveis sobre proteção de dados pessoais. A guia "*Lista de Processos*", presente neste Anexo I da Instrução Normativa, contém tabela a ser preenchida com os processos do órgão ou entidade. Processo, neste caso, diz respeito a um conjunto de atividades ou tarefas orientadas por um objetivo e não se confundem, portanto, com Processos SEI. O mapeamento de cada processo deverá estar descrito como uma cópia da guia "*Mapeamento - Processo X*", com a substituição de "*X*" pelo Número de Identificação do Processo, especificado na guia *"Lista de Processos"*. A guia "*Listas Úteis*" contém exemplos para o preenchimento das guias. As guias *"Base 1"* e *"Base 2"* alimentam as demais com informações pré-definidas.	
Os órgãos e entidades poderão se utilizar, para o preenchimento deste Anexo I, "*Mapeamento de Dados Pessoais*", e do Anexo II, "*Relatório de Impacto à Proteção de Dados Pessoais*", bem como em todo o seu processo de adequação, das normas ABNT NBR ISO nº 31000:2018, ABNT ISO/TR nº 31004:2015, ABNT NBR/IEC nº 31010:2021, ABNT NBR ISO/IEC nº 27001:2013, ABNT NBR ISO/IEC nº 27002:2022, ABNT NBR ISO/IEC nº 27701:2020, ABNT NBR ISO/IEC nº 29100:2020, ABNT NBR ISO/IEC nº 29134:2020, e ABNT NBR ISO/IEC nº 29151/2020.	

Deseja saber mais sobre tratamento de dados pessoais?
Instrução Normativa CGM/SP nº 01, de 21 de julho de 2022
Decreto Municipal nº 59.767, de 15 de setembro de 2020
Lei Federal nº 13.709, de 14 de agosto de 2018
ABNT NBR ISO/IEC nº 27001:2013
ABNT NBR ISO/IEC nº 27002:2013
ABNT NBR ISO/IEC nº 27701:2019
ABNT NBR ISO/IEC nº 29100:2020
ABNT NBR ISO/IEC nº 29134:2020
ABNT NBR ISO/IEC nº 29151:2020
ABNT NBR ISO/IEC nº 31000:2018
ABNT NBR ISO/IEC nº 31004:2015
ABNT NBR ISO/IEC nº 31010:2021

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Registro das Operações de Tratamento de Dados Pessoais:

Lista dos processos que tratam ou não tratam dados pessoais									
Controlador	Nome:	Município de São Paulo	*E-mail:*		Endereço:	Viaduto do Chá, nº 15, Centro, São Paulo/SP, CEP 01020-900			
			Telefone:	(11) 3113-8000					
Encarregado	Nome:		*E-mail:*		Endereço:				
			Telefone:						

Número de Identificação do Processo	Código do Órgão	Sigla do Órgão e Nome	Código da Função	Denominação da Função	Processo	Finalidade do tratamento de dados pessoais	Trata dados pessoais sensíveis?	Data de criação do Mapeamento	Data de atualização do Mapeamento
1									
2									
3									
4									
5									
6									
7									
8									
9									
10									

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Relatório de Impacto à Proteção de Dados Pessoais:

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

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**>

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

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.>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

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

(i) 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;

(ii) quando houver infração à LGPD em decorrência do tratamento de dados pessoais pelo Poder Público (arts. 31 e 32, LGPD); e

(iii) a qualquer momento, sob determinação da Autoridade Nacional de Proteção de Dados – ANPD (art. 38, LGPD).>

<Conforme o art. 2º, 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. 4º, 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:

(i) utilização de nova tecnologia ou de outra nova iniciativa com as quais estão sendo ou serão tratados os dados pessoais;

(ii) qualquer operação de tratamento de dados pessoais que vise à formação de perfil comportamental de pessoa natural (art. 12, § 2º, LGPD);

(iii) 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);

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

(v) 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);

(vi) 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);

(vii) tratamento de dados pessoais realizado para atender aos interesses legítimos do controlador (art. 10, § 3º, LGPD);

(viii) alterações em atos normativos que possam gerar impactos aos direitos à privacidade e à proteção de dados pessoais dos titulares; e

(ix) 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.>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/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:

(i) como se realiza o fluxo do tratamento de dados pessoais – ou seja, da coleta à eventual eliminação;

(ii) 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;

(iii) com quais órgãos, entidades ou terceiros os dados pessoais são compartilhados, assim como quais são esses dados pessoais compartilhados;

(iv) 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;

(x) se adotou, recentemente, algum tipo de nova tecnologia ou de nova iniciativa com as quais estão sendo ou serão tratados os dados pessoais; e

(v) 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.>

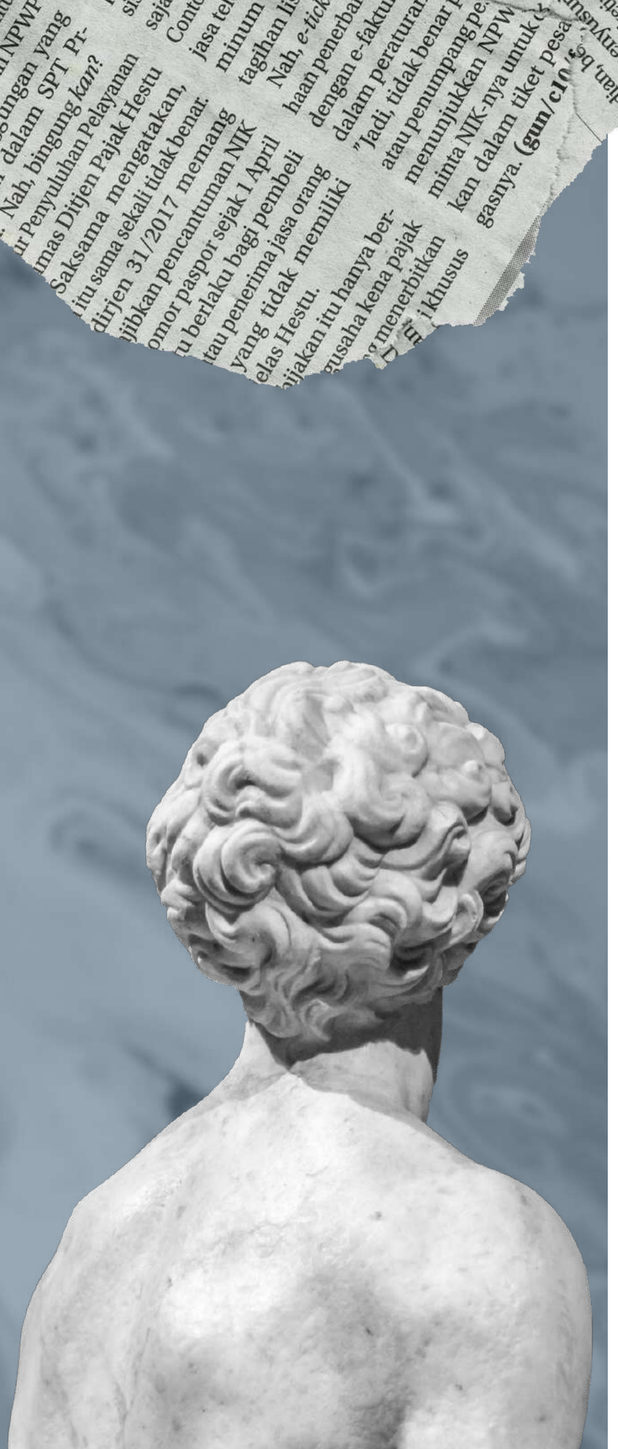
<Nesse sentido, considere destacar:

(i) as categorias de dados pessoais tratados, inclusive das categorias de dados pessoais sensíveis;

(ii) o volume de dados pessoais tratados;

(iii) a frequência com a qual os dados pessoais são tratados;

(iv) o período de retenção dos dados pessoais tratados;



(v) o número de titulares de dados pessoais envolvidos no tratamento; e

(vi) 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:

(i) natureza do relacionamento do órgão ou da entidade com os titulares de dados pessoais;

(ii) método de controle que os indivíduos exercem sobre os seus dados pessoais;

(iii) destaque se o tratamento envolve crianças, adolescentes, idosos, pessoas com deficiência ou outro grupo vulnerável;

(iv) destacar se o tipo de tratamento de dados pessoais realizado é condizente com as razoáveis expectativas de privacidade dos titulares de dados pessoais; e

(v) 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. 7° e 11 da LGPD:

(i) consentimento do titular de dados pessoais;

(ii) cumprimento de obrigação legal ou regulatória pelo controlador;

(iii) execução de políticas públicas pelo controlador;

(iv) espécie de estudo realizado por órgão de pesquisa;

(v) execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular de dados pessoais, a pedido do próprio titular;

(vi) exercício regular de direitos em processo judicial, administrativo ou arbitral;

(vii) proteção da vida ou da incolumidade física do titular de dados pessoais ou de terceiros;

(viii) tutela da saúde;

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

(ix) atender aos interesses legítimos do controlador ou de terceiros;

(x) proteção do crédito; e

(xi) 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. 7° e 11, da LGPD.

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

(i) Indicar qual(is) o(s) resultado(s) pretendido(s) para os titulares dos dados pessoais e a sua importância;

(ii) 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.
> § 1° Quando o tratamento for baseado no legítimo interesse do controlador, somente os
> dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
> § 2° O controlador deverá adotar medidas para garantir a transparência do tratamento
> de dados baseado em seu legítimo interesse.
> § 3° 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.>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

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:

(i) quais partes foram consultadas – como, por exemplo, o operador (art. 5°, inc. VII, LGPD), o Encarregado pela Proteção de Dados Pessoais competente (art. 5°, inc. VIII, LGPD), consultores jurídicos e especialistas em segurança da informação, privacidade e proteção de dados pessoais; e

(ii) 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.>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

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. 6°, inc. III, LGPD).>

<Nesse sentido, destacar:

(i) a fundamentação legal para o tratamento dos dados pessoais;

(ii) 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.

(iii) Quais medidas são adotadas a fim de assegurar que o operador (art. 5°, 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. 5°, inc. VI, LGPD);

(iv) Como estão implementadas as medidas que asseguram a efetivação do exercício dos direitos dos titulares de dados pessoais (arts. 9° e 17 a 22, LGPD); e

(v) Quais são as salvaguardas para as transferências internacionais de dados pessoais.>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

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*".>

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

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>

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

<ESPAÇO DESTINADO À IDENTIFICAÇÃO DO ÓRGÃO/ENTIDADE>

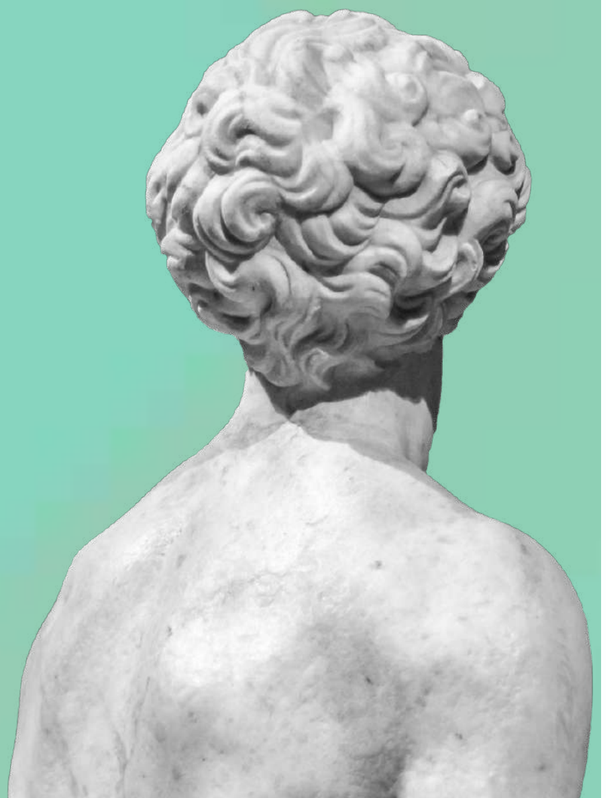
ENCARREGADO PELA PROTEÇÃO DE DADOS PESSOAIS

_____

<Nome do Encarregado>
RF/CPF: xxxxx
<Local>, <dia> de <mês> de <ano>

<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.>

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO



Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Conscientização e capacitação dos agentes públicos sobre o tema:

(i) Guia Orientativo sobre a Privacidade e a Proteção de Dados Pessoais para a Administração Pública do Município de São Paulo:

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

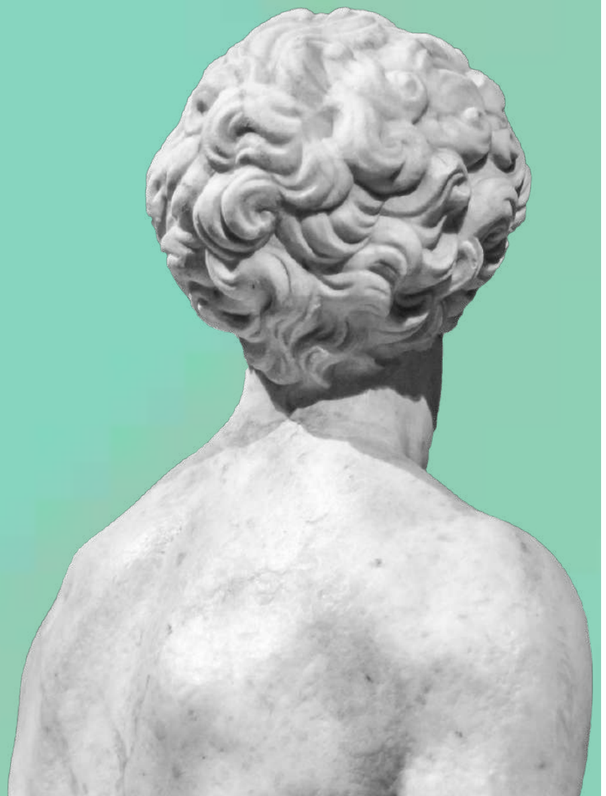
Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Conscientização e capacitação dos agentes públicos sobre o tema:

(ii) Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo:



CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO

Mapeamento de Processos

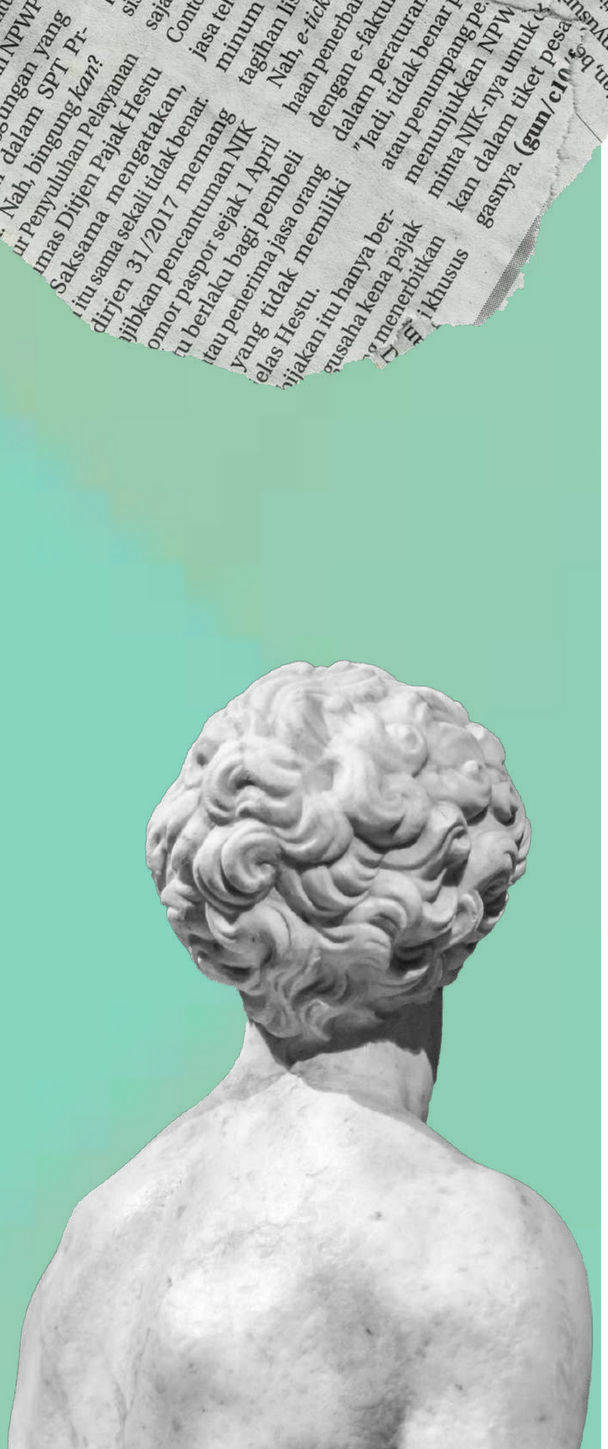
<“ *Nome do órgão/entidade” / “ Nome da divisão” > / <Versão nº [....]: DD/MM/AAAA>*
<“ ***Nome do Processo”*** >
<“ *Objetivo do Processo”* >

Etapa [...]:

i. **Objetivo: <**“ *indicação do objetivo específico desta etapa do processo”* >
ii. **Recursos humanos utilizados nesta etapa: <**“ *divisões do órgão ou entidade e agentes públicos envolvidos nesta etapa do processo”* >;
iii. **Recursos físicos e tecnológicos utilizados nesta etapa: <**“ *infraestrutura física e tecnológica nesta etapa do processo”* >;
iv. **Comunicação e compartilhamento das informações: <**“ *modo de comunicação entre os recursos humanos utilizados e o modo de compartilhamento das informações entre esta etapa com a(s) anterior(es) e a(s) seguinte(s) etapa(s)>*
v. **Recursos informacionais desta etapa:**
   a. **Rol de documentos gerados ou compartilhados:** <“ *documento é o substrato/suporte em que uma informação gerada ou compartilhada é representada a partir de diferentes expressões da percepção humana, como a escrita, a imagem, o áudio e o vídeo”* >
   b. **Rol de informações geradas ou compartilhadas:** “ *Informação é o conhecimento documentado. Neste caso, diz respeito ao objeto/assunto das informações que são geradas ou compartilhadas”* >.

Taxonomia de Dados Pessoais

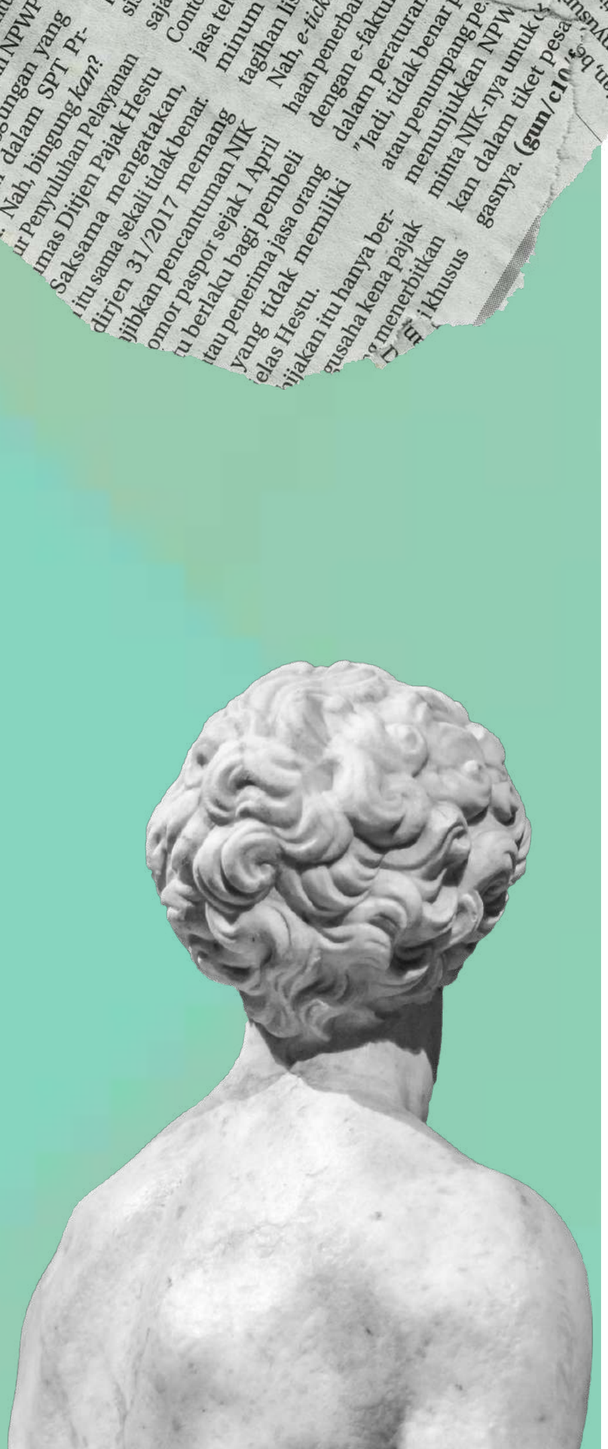
- Dados
  - Dados Pessoais
    - Categorias ordinárias de dados pessoais
      - Identificação pessoal
        - Detalhes de identificação pessoal
        - Dados de identificação eletrônica
        - Dados de identificação pessoal atribuídos por instituições governamentais
        - Dados de localização eletrônica
      - Corpo
        - Detalhes biográficos
        - Detalhes militares
        - Detalhes física
        - Detalhes imigratórios
      - Mente
        - Descrição psicológica
      - Imagem
        - Vídeo e imagem
          - Voz
          - Vídeo e imagem enquanto relacionadas à segurança pública
    - Categorias especiais de dados pessoais
      - Dados pessoais de crianças e adolescentes
        - Dados pessoais de crianças
        - Dados pessoais de adolescentes
      - Dados pessoais sensíveis
        - Origem racial ou étnica
        - Convicção religiosa
        - Filiação a organização de caráter religioso
        - Opinião política
        - Filiação a organização de caráter político
        - Filiação a sindicato
        - Genéticos
        - Biométricos



- Categorias ordinárias de dados pessoais
  - Hábitos
    - Detalhes sobre hábitos pessoais
    - Detalhes sobre estilo de vida
    - Detalhes sobre distinções
    - Detalhes sobre bens e direitos enquanto relacionados aos hábitos pessoais
    - Detalhes sobre viagens e acolhimentos
    - Detalhes sobre denúncias, incidentes ou acidentes
    - Detalhes sobre núcleos sociais
    - Detalhes sobre uso de mídias
  - Lazer
    - Detalhes sobre os interesses de lazer
  - Consumo
    - Detalhes sobre bens e serviços enquanto relacionados aos hábitos de consumo
  - Finanças
    - Detalhes de identificação financeira
    - Detalhes sobre recusos financeiros
    - Detalhes sobre dívidas e despesas
    - Detalhes sobre situação financeira
    - Detalhes sobre empréstimos, hipotecas e linhas de crédito
    - Detalhes sobre assistência financeira
    - Detalhes de apólice de seguro
    - Detalhes de plano de pensão
    - Detalhes sobre transações financeiras
    - Detalhes sobre compensações financeiras
    - Detalhes sobre atividades profissionais
    - Detalhes sobre acordos e ajustes comerciais
    - Detalhes sobre autorizações enquanto relacionadas ao tratamento de dados financeiros

- Residência
  - Detalhes residênciais
- Família
  - Detalhes sobre relacionamentos atuais
  - Detalhes sobre relacionamentos anteriores
  - Detalhes sobre núcleo familiar
- Educação
  - Dados acadêmicos
  - Detalhes financeiros-acadêmicos
  - Detalhes sobre qualificações e experiências acadêmico-profissionais
- Trabalho
  - Detalhes sobre ocupações atuais
  - Detalhes sobre processos de seleção
  - Detalhes sobre rescisões
  - Detalhes sobre ocupações anteriores
  - Detalhes sobre avaliações de desempenho
  - Detalhes sobre disciplina e absenteísmo
- Filiações
  - Detalhes sobre associações às quais é filiado o titular de dados pessoais
- Conflitos
  - Detalhes sobre processos judiciais em curso
  - Detalhes sobre decisões judiciais
  - Detalhes sobre processos administrativos em curso
  - Detalhes sobre decisões administrativas

Questionário sobre a Privacidade e a Proteção de Dados Pessoais



<"Nome do órgão/entidade"
"Nome da divisão">
<"Versão nº [....]: DD/MM/AAAA">

<"*Nome do Processo*">

<"Objetivo do Processo">

1. Há operador(es) que atua(m) neste processo? Se sim, identifique-o(s).
   Resposta:

2. Em qual(is) fase(s) do ciclo de vida do tratamento de dados pessoais o(s) operador(es) atua(m)?
   <Ciclos de vida representam diferentes ações de tratamento de dados pessoais, como elencadas anteriormente, que se iniciam pela coleta e finalizam-se pela eliminação.>
   Resposta:

3. Como os dados pessoais são tratados, tendo em vista o ciclo do tratamento de dados pessoais?
   <Descrever como os dados pessoais são coletados, produzidos, recepcionados, reproduzidos, extraídos, analisados, guardados, compartilhados, usados e eliminados.>
   <Neste quesito, procure refletir sobre o tratamento de dados pessoais conforme as etapas existentes no processo, descritas em "Contextualização de Processos", porque todo processo também possui um ciclo de vida.>
   <Exemplo de descrição do fluxo de tratamento de dados pessoais:
   1. Os dados pessoais são coletados mediante preenchimento de formulário eletrônico; 2. Os dados pessoais são transferidos, armazenados ou arquivados na nuvem ou em servidores dedicados; 3. A empresa "X" fornece uma quantidade "Y" para armazenamento em nuvem e se compromete a manter o armazenamento em território nacional; 4. Os dados pessoais podem ser eliminados: (i) a pedido do titular, caso não sejam necessários à consecução de interesse público; (ii) após a utilização por desnecessidade de armazenamento; ou (iii) por temporalidade.>
   Resposta:

4. Qual é a abrangência da área geográfica do tratamento de dados pessoais?
   <Informar se a abrangência dos dados pessoais tratados é nacional, estadual, distrital, municipal ou regional.>
   Resposta:

5. Qual é a fonte dos dados pessoais?
   <Informar se os dados pessoais tratados se originam dos próprios titulares de dados pessoais, de seus responsáveis legais, ou de outros sujeitos, como, e.g., a partir da Receita Federal, quando de consulta de CPF.>
   Resposta:

6. Entre as hipóteses de tratamento elencadas pelo art. 7º[3] e 11[4], da LGPD, qual(is) é (são) a(s) que fundamenta(m) o tratamento de dados pessoais realizado neste processo?
   <Copie, nesta resposta, o caput do(s) art.(s) 7º e/ou 11, da LGPD, mais o(s) inciso(s) que fundamenta(m) o tratamento de dados pessoais.>
   <O art. 7º diz respeito ao tratamento de dados pessoais, exceto aqueles que se enquadram na categoria de dados pessoais sensíveis.>
   <O art. 11 diz respeito ao tratamento de dados pessoais sensíveis, considerados aqueles contenham dados 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.>
   <Excepcionalmente, é possível fundamentar-se em mais de uma hipótese de tratamento, uma vez que um processo poderá ter diferentes tipos de tratamento de dados pessoais.>
   <No âmbito da Controladoria Geral do Município de São Paulo, destacam-se as hipóteses de tratamento elencadas no art. 7º, incs. I e II, da LGPD.>
   Resposta:

7. Qual(is) é (são) a(s) finalidade(s) do tratamento de dados pessoais deste processo? Qual(is) a(s) previsão(ões) legal(is) que respalda(m) essa(s) finalidade(s)?
   Resposta:

8. Quais são os resultados pretendidos, ao titular de dados pessoais, com o tratamento realizado neste processo?

---

[3] "Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;
IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;
VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou
X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."

[4] "Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
a) cumprimento de obrigação legal ou regulatória pelo controlador;
b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
e) proteção da vida ou da incolumidade física do titular ou de terceiro;
f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais."

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Questionário sobre a Privacidade e a Proteção de Dados Pessoais

Resposta:

9. Quais os benefícios esperados ao órgão, à Prefeitura do Município e/ou a sociedade, como um todo, com relação a esse tratamento?
   Resposta:

10. Informe as categorias ordinárias de dados pessoais tratadas neste processo, de acordo com os enunciados a seguir e os descrevendo com base: (i) no tempo de retenção dos dados pessoais; e (ii) na fonte de retenção dos dados pessoais.
    <Em caso de inexistência de tratamento de determinada categoria de dados pessoais, responda "Não há".>
    < O tempo de retenção de dados pessoais se relaciona à Política Municipal de Gestão Documental, assim como ao Sistema de Arquivo do Município de São Paulo.>
    <A fonte de retenção de dados pessoais é o substrato no qual os dados pessoais são representados. São exemplos que poderão ser utilizados, isolada ou cumulativamente, a depender do caso concreto: nuvem (especificar servidor), documento eletrônico DOCX e similares, documento eletrônico PDF e similares, planilha eletrônica EXCEL e similares, mídia eletrônica MP3 e similares, mídia eletrônica MP4 e similares, mídia eletrônica JPEG e similares, disco óptico (CD, DVD e Blu-Ray), pen-drive, cartão de memória, HD externo, SSD, fita magnética, disquete, disco fonográfico (vinil, compacto-simples e goma-laca), cilindro fonográfico, material biológico e papel.>
    <Deve ser especificado o tempo e a fonte de retenção para cada subcategoria de dados pessoais elencada, na eventualidade de serem armazenadas, temporal ou materialmente, de forma distinta. Ou seja, havendo duas subcategorias de dados pessoais em "Detalhes de identificação pessoal", como "nome" e "endereço residencial", devem ser descritos os distintos tempos e fontes de retenção dessas duas subcategorias.>

    Identificação pessoal: <***há*** *ou* ***não há.***>

    a. Detalhes de identificação pessoal: *<Descrever se são tratados dados como nome, endereço residencial, histórico de endereços anteriores, número de telefone fixo residencial, número de celular pessoal, e-mail pessoal, etc.>*
       Tempo de retenção:
       Fonte de retenção:
       i. Dados de identificação pessoal atribuídos por instituições governamentais: *<Descrever se são tratados dados de identificação como CPF, RG, número de passaporte, número de carteira de motorista, número de registro em conselho profissional, etc.>*
          Tempo de retenção:
          Fonte de retenção:
    b. Dados de identificação eletrônica: *<Descrever se são tratados dados como endereços IP, cookies, etc.>*
       Tempo de retenção:
       Fonte de retenção:
    c. Dados de localização eletrônica: *<Informar se são tratados dados de comunicação de torres de celulares (e.g., GSM), dados de GPS, etc.>*
       Tempo de retenção:
       Fonte de retenção:

    Corpo: <***há*** *ou* ***não há.***>

    a. Detalhes biográficos: *<Descrever se são tratados dados pessoais como idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade.>*
       Tempo de retenção:
       Fonte de retenção:
    b. Detalhes militares: *<Descrever se são tratados dados como situação militar, patente militar e distinções militares.>*
       Tempo de retenção:
       Fonte de retenção:
    c. Descrição física: *<Dados de descrição física são informações físicas de uma pessoa com possibilidade de serem visivelmente identificadas. Descrever se são tratados dados como altura, peso, cor do cabelo, cor dos olhos, características distintivas, etc.>*
       Tempo de retenção:
       Fonte de retenção:
    d. Detalhes imigratórios: *<Descrever se são tratados dados como detalhes sobre visto, autorização de trabalho, limitações de residência ou movimentação, condições especiais relacionadas à autorização de residência, etc.>*
       Tempo de retenção:
       Fonte de retenção:

    Mente: <***há*** *ou* ***não há.***>

    a. Descrição psicológica: *<Descrever se são tratados dados sobre personalidade ou caráter.>*
       Tempo de retenção:
       Fonte de retenção:

    Imagem: <***há*** *ou* ***não há.***>

    a. Vídeo e imagem: *<Descrever se são tratados arquivos de vídeos, fotos digitais, fitas de vídeo, etc.>*
       Tempo de retenção:
       Fonte de retenção:
       a. Vídeo e imagem enquanto relacionados à segurança pública: *<Descrever se são tratadas imagens e/ou vídeos de câmeras de segurança/vigilância (e.g., CFTV), etc.>*
          Tempo de retenção:
          Fonte de retenção:
    b. Voz: *<Descrever se são tratadas fitas e arquivos digitais de voz, bem como outros registros de gravações de voz.>*
       Tempo de retenção:
       Fonte de retenção:

    Hábitos: <***há*** *ou* ***não há.***>

    a. Detalhes sobre hábitos pessoais: *<Descrever se são tratados dados como uso de tabaco, uso de álcool, hábitos alimentares e dieta alimentar.>*
       Tempo de retenção:
       Fonte de retenção:
    b. Detalhes sobre estilo de vida: *<Descrever se são tratados dados como informações sobre o uso de bens ou serviços e comportamentos característicos dos titulares dos dados.>*
       Tempo de retenção:
       Fonte de retenção:

Questionário sobre a Privacidade e a Proteção de Dados Pessoais

c. Detalhes sobre distinções: <*Descrever se são tratados dados como distinções civis, administrativas ou militares.*>
   Tempo de retenção:
   Fonte de retenção:
d. Detalhes sobre bens e direitos enquanto relacionados aos hábitos pessoais: <*Descrever se são tratados dados sobre bens e outros direitos enquanto relacionados aos hábitos pessoais do titular.*>
   Tempo de retenção:
   Fonte de retenção:
e. Detalhes sobre viagens e deslocamentos: <*Descrever se são tratados dados sobre antigas residências e deslocamentos, visto de viagem, autorizações de trabalho, etc.*>
   Tempo de retenção:
   Fonte de retenção:
f. Detalhes sobre denúncias, incidentes ou acidentes: <*Descrever se são tratados dados como informações sobre um acidente, incidente ou denúncia na qual o titular dos dados está envolvido, a natureza dos danos ou ferimentos, pessoas envolvidas, testemunhas, etc.*>
   Tempo de retenção:
   Fonte de retenção:
g. Detalhes sobre núcleos sociais: <*Descrever se são tratados dados como amigos, parceiros de negócios, relacionamentos com pessoas que não sejam familiares próximos, etc.*>
   Tempo de retenção:
   Fonte de retenção:
h. Detalhes sobre uso de mídias: <*Descrever se são tratados dados que definem o comportamento de uso de mídias e meios de comunicação.*>
   Tempo de retenção:
   Fonte de retenção:

Lazer: <***há** ou **não há**.*>

a. Detalhes sobre interesses de lazer: <*Descrever se são tratados dados sobre hobbies, esportes, dentre outros interesses.*>
   Tempo de retenção:
   Fonte de retenção:

Consumo: <***há** ou **não há**.*>

a. Detalhes sobre bens e serviços enquanto relacionados aos hábitos de consumo: <*Descrever se são tratados dados sobre bens e serviços consumidos pelo titular de dados.*>
   Tempo de retenção:
   Fonte de retenção:

Finanças: <***há** ou **não há**.*>

a. Dados de identificação financeira: <*Descrever se são tratados dados como números de identificação, números de contas bancárias, números de cartões de crédito ou débito, códigos secretos, etc.*>
   Tempo de retenção:
   Fonte de retenção:
b. Detalhes sobre recursos financeiros: <*Descrever se são tratados dados como renda, posses, investimentos, renda total, renda profissional, poupança, datas de início e término dos investimentos, receita de investimento, dívidas sobre ativos, etc.*>
   Tempo de retenção:
   Fonte de retenção:
c. Detalhes sobre dívidas e despesas: <*Descrever se são tratados dados como total de despesas, aluguéis, empréstimos, hipotecas e outras formas de crédito.*>
   Tempo de retenção:
   Fonte de retenção:
d. Detalhes sobre a situação financeira: <*Descrever se são tratados dados de solvência, ou seja, avaliação do rendimento e avaliação de capacidade de pagamento.*>
   Tempo de retenção:
   Fonte de retenção:
e. Detalhes sobre empréstimos, hipotecas e linhas de crédito: <*Descrever se são tratados dados como natureza do empréstimo, valor emprestado, saldo remanescente, data de início, período do empréstimo, taxa de juros, visão geral do pagamento e detalhes sobre as garantias.*>
   Tempo de retenção:
   Fonte de retenção:
f. Detalhes sobre assistência financeira: <*Descrever se são tratados dados como de benefícios, assistência, bonificações, subsídios, etc.*>
   Tempo de retenção:
   Fonte de retenção:
g. Detalhes de apólice de seguro: <*Descrever se são tratados dados como natureza da apólice de seguro, detalhes sobre os riscos cobertos, valores segurados, período segurado, data de rescisão, pagamentos feitos, recebidos ou perdidos, situação do contrato, etc.*>
   Tempo de retenção:
   Fonte de retenção:
h. Detalhes de plano de pensão: <*Descrever se são tratados dados como data efetiva do plano de pensão, natureza do plano, data de término do plano, pagamentos recebidos e efetuados, opções, beneficiários, etc.*>
   Tempo de retenção:
   Fonte de retenção:
i. Detalhes sobre transações financeiras: <*Descrever se são tratados dados como valores pagos e a pagar pelo titular dos dados, linhas de crédito concedidas, avais, forma de pagamento, visão geral do pagamento, depósitos e outras garantias, etc.*>
   Tempo de retenção:
   Fonte de retenção:
j. Detalhes sobre compensações: <*Descrever se são tratados dados como de detalhes sobre compensações reivindicadas, valores pagos ou outros tipos de compensação, etc.*>
   Tempo de retenção:
   Fonte de retenção:
k. Detalhes sobre atividades profissionais: <*Descrever se são tratados dados de atividades profissionais executadas pelo titular de dados, como natureza da atividade, natureza dos bens ou serviços utilizados ou entregues pela pessoa em registro, relações comerciais, etc.*>
   Tempo de retenção:
   Fonte de retenção:
l. Detalhes sobre acordos e ajustes comerciais: <*Descrever se são tratados dados como detalhes sobre acordos ou ajustes comerciais, acordos sobre representação ou acordos legais, etc.*>

Questionário sobre a Privacidade e a Proteção de Dados Pessoais

Tempo de retenção:
Fonte de retenção:

m. Detalhes sobre autorizações enquanto relacionadas ao tratamento de dados financeiros: <*Descrever se são tratados dados financeiros baseados no consentimento de seu titular*>.
Tempo de retenção:
Fonte de retenção:

Residência: <***há*** *ou* ***não há.***>

a. Detalhes residenciais: <*Descrever se são tratados dados sobre natureza da residência, propriedade própria ou alugada, duração da residência nesse endereço, aluguel, custos, classificação da residência, detalhes sobre a avaliação, nomes das pessoas que possuem as chaves.*>
Tempo de retenção:
Fonte de retenção:

Família: <***há*** *ou* ***não há.***>

a. Detalhes sobre relacionamentos atuais: <*Descrever se são tratados dados como nome do cônjuge ou companheiro(a), nome de solteiro(a), do cônjuge ou companheiro (a), data de casamento, data do contrato de coabitação, número de filhos, etc.*>
Tempo de retenção:
Fonte de retenção:
b. Detalhes sobre relacionamentos anteriores: <*Descrever se são tratados dados sobre casamentos ou parcerias anteriores, divórcios, separações, nomes de parceiros anteriores, etc.*>
Tempo de retenção:
Fonte de retenção:
c. Detalhes sobre núcleo familiar: <*Descrever se são tratados dados sobre outros familiares ou membros da família do titular de dados.*>
Tempo de retenção:
Fonte de retenção:

Educação: <***há*** *ou* ***não há.***>

a. Dados acadêmicos: <*Descrever se são tratados dados sobre diplomas, certificados obtidos, resultados de exames, avaliação do progresso dos estudos, histórico escolar, grau de formação, etc.*>
Tempo de retenção:
Fonte de retenção:
b. Dados financeiro-acadêmicos: <*Descrever se são tratados dados sobre taxas de inscrição e custos pagos, financiamento, formas de pagamento, registros de pagamento, etc.*>
Tempo de retenção:
Fonte de retenção:
c. Detalhes sobre qualificações e experiências acadêmico-profissionais: <*Descrever se são tratados dados sobre certificações profissionais, interesses profissionais, interesses acadêmicos, interesses de pesquisa, experiência de ensino, etc.*>
Tempo de retenção:
Fonte de retenção:

Trabalho: <***há*** *ou* ***não há.***>

a. Detalhes sobre ocupações atuais: <*Descrever se são tratados dados sobre empregador, descrição do cargo e função, antiguidade, data de recrutamento, local de trabalho, especialização ou tipo de empresa, modos e condições de trabalho, cargos anteriores e experiência anterior de trabalho no mesmo empregador, etc.*>
Tempo de retenção:
Fonte de retenção:
b. Detalhes sobre processos de seleção: <*Descrever se são tratados dados sobre data de seleção, método de seleção, fonte de seleção, referências, detalhes relacionados à período de estágio, etc.*>
Tempo de retenção:
Fonte de retenção:
c. Detalhes sobre rescisões: <*Descrever se são tratados dados sobre data de rescisão, motivo, período de notificação, condições de rescisão, etc.*>
Tempo de retenção:
Fonte de retenção:
d. Detalhes sobre ocupações anteriores: <*Descrever se são tratados dados sobre ocupações anteriores e empregadores, períodos sem emprego, serviço militar, etc.*>
Tempo de retenção:
Fonte de retenção:
e. Detalhes sobre avaliações de desempenho: <*Descrever se são tratados dados sobre avaliações de desempenho ou qualquer outro tipo de análise de qualificação ou habilidades profissionais.*>
Tempo de retenção:
Fonte de retenção:
f. Detalhes sobre disciplina e absenteísmo: <*Descrever se são tratados dados sobre registros de absentismo, motivos de ausência, medidas disciplinares, etc.*>
Tempo de retenção:
Fonte de retenção:

Filiações: <***há*** *ou* ***não há.***>

a. Detalhes sobre associações as quais é filiado o titular de dados pessoais (exceto profissionais, políticas, sindicatos ou qualquer outra associação que se enquadre em dados pessoais sensíveis): <*Descrever se são tratados dados sobre participação em organizações de caridade ou benevolentes, clubes, parcerias, grupos, etc.*>
Tempo de retenção:
Fonte de retenção:

Conflitos: <***há*** *ou* ***não há.***>

a. Detalhes sobre processos judiciais em curso: <*Descrever se são tratados dados sobre suspeitas de violações, conexões conspiratórias com criminosos conhecidos, inquéritos ou ações judiciais (civis ou criminais) empreendidas por ou contra o titular de dados, etc.*>
Tempo de retenção:
Fonte de retenção:
b. Detalhes sobre decisões judiciais: <*Descrever se são tratados dados sobre decisões cíveis e criminais que envolvam o titular de dados.*>
Tempo de retenção:
Fonte de retenção:

Questionário sobre a Privacidade e a Proteção de Dados Pessoais

c. Detalhes sobre processos administrativos em curso: *<Descrever se são tratados dados sobre processos administrativos em curso que envolvam o titular de dados.>*
   Tempo de retenção:
   Fonte de retenção:
d. Detalhes sobre decisões administrativas: *<Descrever se são tratados dados de decisões administrativas, como em processos administrativos disciplinares, e sanções respectivas, como advertências e multas, além de qualquer outro tipo de sanção administrativa prevista em normas ou regulamentos administrativos.>*
   Tempo de retenção:
   Fonte de retenção:

Outros: *<**Há** ou **não há**. Especifique se há outras categorias de dados pessoais tratadas que não tenham sido contempladas anteriormente.>*

11. Informe as categorias de dados pessoais sensíveis tratadas neste processo, de acordo com os enunciados a seguir e os descrevendo com base: (i) no tempo de retenção dos dados pessoais; e (ii) na fonte de retenção dos dados pessoais.
<Dado pessoal sensível é todo 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.>
<Em caso de inexistência de tratamento de determinada categoria de dados pessoais, responda "Não há".>
< O tempo de retenção de dados pessoais se relaciona à Política Municipal de Gestão Documental, assim como ao Sistema de Arquivo do Município de São Paulo.>
< A fonte de retenção de dados pessoais é o substrato no qual os dados pessoais são representados. São exemplos que poderão ser utilizados, isolada ou cumulativamente, a depender do caso concreto: nuvem (especificar servidor), documento eletrônico DOCX e similares, documento eletrônico PDF e similares, planilha eletrônica EXCEL e similares, disco óptico (CD, DVD e Blu-Ray), pen-drive, cartão de memória, HD externo, SSD, fita magnética, disquete, disco fonográfico (vinil, compacto-simples e goma-laca), cilindro fonográfico, material biológico e papel.>
<Deve ser especificado o tempo e a fonte de retenção para cada subcategoria de dados pessoais elencada, na eventualidade de serem armazenadas, temporal ou materialmente, de forma distinta. Ou seja, havendo duas subcategorias de dados pessoais sensíveis, devem ser descritos os distintos tempos e fontes de retenção dessas duas subcategorias.>

Dados pessoais sensíveis: *<**há** ou **não há**.>*

a. Revelem origem racial ou étnica:
   Tempo de retenção:
   Fonte de retenção:
b. Revelem convicção religiosa:
   Tempo de retenção:
   Fonte de retenção:
c. Revelem filiação a organização de caráter religioso:
   Tempo de retenção:
   Fonte de retenção:
d. Revelem opinião política:
   Tempo de retenção:
   Fonte de retenção:
e. Revelem filiação a organização de caráter político:
   Tempo de retenção:
   Fonte de retenção:
f. Revelem filiação a sindicato:
   Tempo de retenção:
   Fonte de retenção:
g. Revelem filiação a organização de caráter filosófico:
   Tempo de retenção:
   Fonte de retenção:
h. Refiram-se à saúde ou à vida sexual:
   Tempo de retenção:
   Fonte de retenção:
i. Refiram-se a dados genéticos:
   Tempo de retenção:
   Fonte de retenção:
j. Refiram-se a dados biométricos: *<Descrever se são tratados dados de impressões digitais e de voz, digitalizações de íris, reconhecimento facial, reconhecimento de formato de dedo ou mão, assinaturas dinâmicas, etc.>*
   Tempo de retenção:
   Fonte de retenção:

12. Com qual frequência os dados pessoais são tratados?
<Descrever em que frequência os dados são tratados. Isso representa a disponibilidade e horário de funcionamento do sistema automatizado ou processo manual que trata os dados pessoais.>
Resposta:

13. Qual o volume de categorias de dados pessoais tratados?
<Informar o volume total de categorias de dados pessoais e de dados pessoais sensíveis descritos neste mapeamento de dados pessoais relacionados a determinado processo.
Exemplo:
Categorias de dados pessoais tratados:
Idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade.
Categorias de dados pessoais sensíveis tratadas:
Tratamento de dados pessoais de saúde como CID10 e data de último exame médico.
Neste caso, a informação que deve ser preenchida é:
São tratadas 6 categorias de dados pessoais (idade, sexo, data de nascimento, local de nascimento, estado civil e nacionalidade) e 02 categorias de dados pessoais sensíveis (CID10 e data de último exame médico), totalizando 08 categorias tratados pelo processo.>
Resposta:

14. Quais são as categorias de titulares de dados pessoais deste processo? São tratados dados pessoais de crianças, adolescentes e outros grupos vulneráveis?
<Informar quem são os titulares de dados pessoais deste processo. Exemplos: crianças e adolescentes, munícipes, servidores ativos e inativos, pacientes, educandos, etc.>
Resposta:

15. Os dados pessoais tratados neste processo são compartilhados? Se sim, com quem?
<Informe o nome da empresa ou instituição com a qual os dados pessoais são compartilhados. Exemplos: Microsoft, Google, IBGE, Ministério Público, Receita Federal, Controladoria-Geral da União e Ministério da Saúde.>
<Apenas devem ser indicadas instituições que não façam parte da Prefeitura do Município de São Paulo, o que inclui sua administração pública direta e indireta. Exclui-se, dessa forma, a PRODAM,

Questionário sobre a Privacidade e a Proteção de Dados Pessoais

mas inclui-se as empresas com as quais esta compartilha os dados pessoais tratados pela Prefeitura do Município.> Resposta:
16. Em sua análise, há medida(s) de segurança, técnicas e administrativas, atualmente em curso que proteja(m) os dados pessoais tratados neste processo? Se sim, qual(is)? *<Indicar se existem atualmente medidas de segurança, técnicas e administrativas, aptas à proteção dos dados pessoais, isto no âmbito de seu órgão ou entidade, ou, se aplicável, de forma global, na Prefeitura do Município de São Paulo ou em sua entidade. Exemplos: controles de segurança em recursos humanos; controles de acesso físico; controles de acesso lógico; controles de segurança física e do ambiente; controles de segurança nas comunicações; controles de conformidade das licitações, contratos administrativos, convênios e instrumentos congêneres; Política de Segurança da Informação; Política de Senhas; Política de Mesa Limpa; Política de Backup; Política de Privacidade e Proteção de Dados Pessoais; Política de Cookies; e Política de Gestão de Incidentes de Segurança da Informação.>* Resposta:
17. Há transferência internacional dos dados tratados neste processo? Se sim, qual(is) é (são) a(s) categoria(s) de dados pessoais e de dados pessoais sensíveis transferidas? Essa transferência internacional está protegida por alguma garantia? *<Indicar se os dados pessoais tratados neste processo são transferidos, como para armazenamento por provedor de nuvem, para fora do Brasil. Em caso afirmativo, se possível, indicar o país no qual os dados pessoais são tratados.>* *<São exemplos de garantias para a realização de transferência internacional de dados pessoais: acordo de cooperação internacional; certificação regularmente emitida; cláusulas contratuais específicas para determinada transferência; cláusulas-padrão contratuais; código de conduta regularmente emitido; cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional; cumprimento de obrigação legal ou regulatória pelo controlador; execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular; execução de política pública ou atribuição legal do serviço público; exercício regular de direitos em processo judicial, administrativo ou arbitral; fornecimento de consentimento específico pelo titular de dados pessoais; normas corporativas globais; país que fornece um nível adequado de proteção; proteção da vida ou da incolumidade física do titular ou de terceiro; selo regularmente emitido; e transferência autorizada pela Autoridade Nacional de Proteção de Dados (ANPD).>* Resposta:
18. Quais são os contratos de serviços e/ou soluções de tecnologia da informação que possuem relação com o tratamento de dados pessoais deste processo? *<Informe os números e os "links" de acesso dos contratos de serviços e/ou soluções de tecnologia da informação que realizam algum tipo de operação de tratamento com os dados pessoais deste processo.>* Resposta:

Entrevistas à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Pauta de Entrevista		
<"Nome do órgão/entidade"/ "Nome da divisão">		
Número: *<"Número sequencial da Entrevista">*		
Data: *<DD/MM/AAAA>*		

Hora: *<HH:MIN>*		
Local: <"*Se presencial, inserir endereço. Se online, indicar aplicativo utilizado e 'link'"***>**		
Entrevistadores	**Setor**	***Status***
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Entrevistados	**Setor**	***Status***
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
<"Inserir nome do agente público.">	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Medida	**Subtema**	**Objetivo**
<"Medida de segurança presente na norma técnica que é objeto de avaliação para implementação.">	*<"Conjunto temático de medidas de segurança.>"*	*<"Objetivo de uma medida de segurança.">*
<"Medida de segurança presente na norma técnica que é objeto de avaliação para implementação.">	*<"Conjunto temático de medidas de segurança.>"*	*<"Objetivo de uma medida de segurança.">*

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Entrevistas à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Ata de Entrevista		
<"Nome do órgão/entidade"/ "Nome da divisão">		
Número: *<"Número sequencial da Entrevista">*		
Data: *<DD/MM/AAAA>*		
Hora: *<HH;MIN>*		
Local: <*"Se presencial, inserir endereço. Se online, indicar aplicativo utilizado e 'link'">*		
Entrevistadores	**Setor**	***Status***
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Entrevistados	**Setor**	***Status***
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
"Inserir nome do agente público."	*<"Inserir setor ao qual faz parte o agente público.">*	*<"Presente/Ausência justificada/Ausência não justificada.">*
Quesitos e Respostas		

<"Controles relacionados devem sempre ser citados pelo(s) Entrevistador(es) no início de cada série de Quesitos. Os controles podem ser encontrados no Anexo VI do Guia, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'.">

<"Exemplo">

<"Controles relacionados a esta série de Quesitos são: (i) [....]; e (ii) [...], disponíveis no Anexo VI do 'Guia Orientativo sobre a Instrução Normativa CGM/SP nº 01/2022 para a Administração Pública do Município de São Paulo', 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'">

<"Existem Políticas, no setor, relativas à Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais?>
<"Respondeu [Nome], [Cargo/Função], que [...]">

<Já houve algum incidente de segurança da informação?>
<"Respondeu [Nome], [Cargo/Função], que [...]">

Informações adicionais
<"Comentários adicionais a critério do(s) Entrevistador(es) ou mesmo por solicitação do(s) Entrevistado(s).">

Próximos passos

Responsável	**Ação**	**Data**
<"Inserir nome do agente público.">	*<"Inserir ação a ser realizada pelo agente público">*	*<DD/MM/AAAA>*
<"Inserir nome do agente público.">	*<"Inserir ação a ser realizada pelo agente público">*	*<DD/MM/AAAA>*

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Questionário de Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Risco	Risco Inerente		Controles propostos	Efeito sobre o risco	Risco residual	
	(P)	(I)			(P)	(I)
R"*x*" – <"*Descrição do risco, com o subsídio da Tabela 'Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'*> Processos: "*xx*"; "*xy*"; e "xz".	<"*Muito alta, alta, média, baixa ou muito baixa*">	<"*Muito alto, alto, médio, baixo ou muito baixo*">	<"*Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'*">	<"*Reduzir, evitar, Compartilhar, aceitar ou potencializar*">	<"*Muito alta, alta, média, baixa ou muito baixa*">	<"*Muito alto, alto, médio, baixo ou muito baixo*">
			<"*Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais.'*">	<"*Reduzir, evitar, Compartilhar, aceitar ou potencializar*">		
R"*x*" – <"*Descrição do risco, com o subsídio da Tabela 'Exemplos de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'*> Processos: "*xx*"; "*xy*"; e "xz".	<"*Muito alta, alta, média, baixa ou muito baixa*">	<"*Muito alto, alto, médio, baixo ou muito baixo*">	<"*Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'*">	<"*Reduzir, evitar, Compartilhar, aceitar ou potencializar*">	<"*Muito alta, alta, média, baixa ou muito baixa*">	<"*Muito alto, alto, médio, baixo ou muito baixo*">
			<"*Descrição conforme diretrizes de implementação presentes no Anexo externo a este documento, 'Gestão de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais'*">	<"*Reduzir, evitar, Compartilhar, aceitar ou potencializar*">		

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Taxonomia de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Identificação	Risco	Escopo
1	Acesso não autorizado	Acesso indevido (permissão indevida) a um ambiente físico ou lógico.
2	Modificação não autorizada	Usuário sem permissão de alteração para um determinado registro realiza modificação não autorizada.
3	Perda	Perdas provocadas tanto por ações intencionais de usuários oriundas de uma exclusão indevida ou devida e não comunicada, quanto por ações não intencionais, como falhas em sistemas e sobrescrita de dados.
4	Roubo	Dados roubados nas dependências internas do controlador/operador, como falhas nos controles de segurança dos sistemas, a exemplo da ausência ou fraca criptografia e falha de sistema que permita escalação de privilégio.
5	Remoção não autorizada	Usuário sem permissão para retirar ou copiar dados pessoais para outro local.
6	Coleta excessiva	Coleta de dados pessoais em quantidade superior ao necessário à finalidade da atividade a qual terá o tratamento de dados pessoais.
7	Informação insuficiente sobre a finalidade do tratamento	O tratamento de dados pessoais deve atender a uma finalidade específica a ser informada de forma transparente ao titular de dados pessoais.

Taxonomia de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

8	Tratamento sem consentimento do titular de dados pessoais na hipótese em que o tratamento não esteja previsto em normas aplicáveis	Controlador de dados pessoais não obtém o consentimento do titular de dados pessoais para realizar um tratamento de dados sem norma que lhe diga respeito.
9	Falha em considerar os direitos do titular de dados pessoais	Falha na garantia de atendimento dos direitos do titular, conforme descritos, sobretudo, entre os arts. 9º e 17 a 23 da LGPD.
10	Compartilhar dados pessoais com terceiros sem o consentimento do titular na hipótese em que o consentimento esteja previsto em normas aplicáveis	Organização compartilha os dados pessoais sem hipótese de tratamento de dados que lhe autoriza.
11	Retenção prolongada de dados pessoais sem necessidade	O término da prestação de um serviço ou do prazo da retenção dos dados pessoais para fins legais deve culminar com a exclusão e/ou descarte seguro dos dados pessoais.
12	Associação indevida, direta ou indireta, de dados pessoais ao titular	A realização de todo tratamento de dados pessoais deve estar em conformidade com as normas aplicáveis. Qualquer tratamento que não atenda esse requisito pode produzir dados pessoais e informações pessoais com associações indevidas.
13	Erro de processamento	Dados de entrada que não são corretamente validados e operações de tratamento automatizadas de sistema que alteram de maneira indevida a composição do dado armazenado, a exemplo de execução de *scripts* de banco de dados que atualiza dado pessoal com dado equivocado e ausência de validação dos dados de entrada.
14	Reidentificação de dados pseudonimizados	Dados pessoais podem ser reidentificados por cruzamento de dados pessoais.
15	Exposição a vulnerabilidades diversas	Existência de vulnerabilidade que, uma vez explorada, pode gerar outras vulnerabilidades ou mesmo outros riscos

Questionário de Percepção de Riscos à Segurança da Informação, à Privacidade e à Proteção de Dados Pessoais

Descrição de Controle(s)	Parâmetro
Inexistente(s)	1
Fraco(s)	0,8
Mediano(s)	0,6
Satisfatório(s)	0,4
Forte(s)	0,2

Probabilidade	Descrição	Frequência	Parâmetro
Muito baixa	**Improvável:** evento nunca ocorreu e, em situações excepcionais, o evento poderá até ocorrer, mas nada nas circunstâncias indica essa possibilidade	<= 20%	1
Baixa	**Rara:** evento nunca ocorreu, mas de forma inesperada ou casual, o evento poderá até ocorrer, mas as circunstâncias pouco indicam essa possibilidade	> 20% e <=40%	2
Média	**Possível**: evento já ocorreu no passado e, de alguma forma, o evento poderá ocorrer, pois as circunstâncias indicam moderadamente essa possibilidade	>40% e <=60%	5
Alta	**Provável:** evento já ocorreu no passado e, de forma até esperada, o evento poderá ocorrer, pois as circunstâncias indicam fortemente essa possibilidade	> 60% e <= 80%	8
Muito alta	**Praticamente certa**: de forma inequívoca, o evento está ocorrendo ou já ocorreu e as circunstâncias indicam claramente que poderá ser recorrente em um curto espaço de tempo	>80%	10

Impacto	Impacto de Conformidade	Parâmetro
Muito baixo	Descumprimento de políticas e processos internos de maneira reversível	1
Baixo	Descumprimento de políticas e processos internos de maneira irreversível	2
Médio	Descumprimento de atos normativos municipais de maneira reversível	5
Alto	Descumprimento de atos normativos municipais de maneira irreversível	8
Muito alto	Descumprimento de atos normativos estaduais e federais	10

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Conscientização e capacitação dos agentes públicos sobre o tema:

(iii) Curso de Capacitação em Privacidade e Proteção de Dados Pessoais:

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

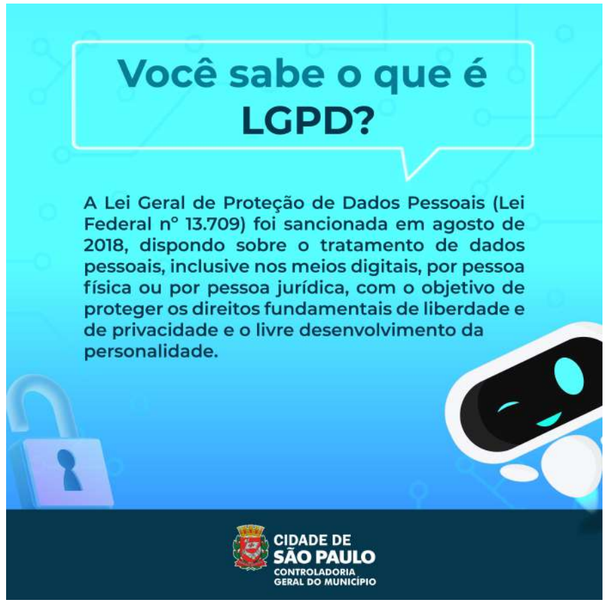
Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Conscientização e capacitação dos agentes públicos sobre o tema:

(iv) Campanha de Conscientização em Privacidade e Proteção de Dados Pessoais:



CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

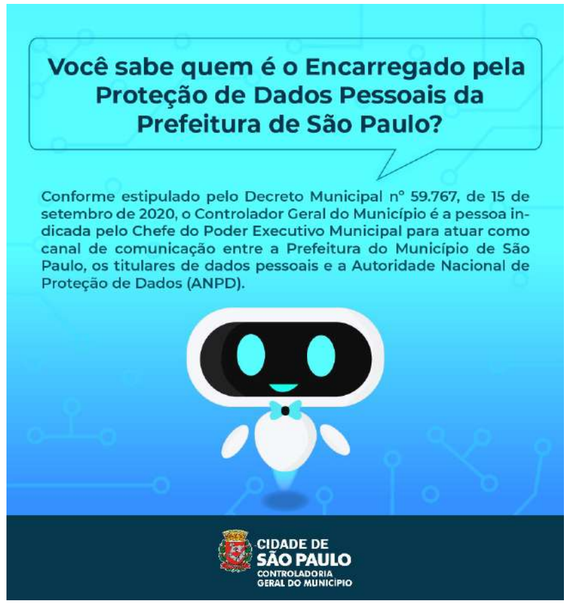
Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Conscientização e capacitação dos agentes públicos sobre o tema:

(iv) Campanha de Conscientização em Privacidade e Proteção de Dados Pessoais:



CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

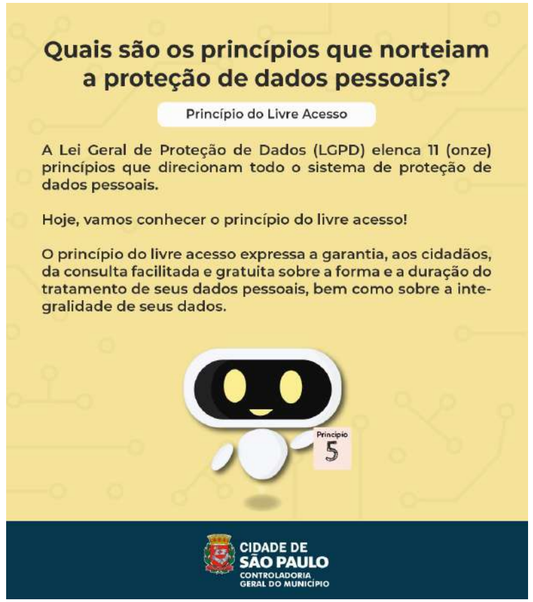
Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Conscientização e capacitação dos agentes públicos sobre o tema:

(iv) Campanha de Conscientização em Privacidade e Proteção de Dados Pessoais:



CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Diálogo das fontes entre a Lei de Acesso à Informação (LAI) e a LGPD:

(i) Diálogo entre as hipóteses de tratamento de dados pessoais:

Nesse sentido, traz o art. 31 da LAI disposições sobre o tratamento de dados pessoais, principalmente relativas à divulgação desses dados a terceiros. Conforme o art. 31, § 1º, incs. I e II, os dados pessoais terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 anos a contar da data de seu tratamento, ao próprio titular de dados pessoais e a agentes públicos legalmente autorizados, podendo ser autorizada a sua divulgação a terceiros diante do consentimento do titular a que os dados se refiram ou por outras hipóteses legais.

Governança

Governança em Privacidade e Proteção de Dados Pessoais na Cidade de São Paulo

Plano de Adequação à Privacidade e à Proteção de Dados Pessoais

Diálogo das fontes entre a Lei de Acesso à Informação (LAI) e a LGPD:

(i) Diálogo entre as hipóteses de tratamento de dados pessoais:

Como se sabe, a LGPD traz tanto a hipótese legal do consentimento do titular quanto outras a justificar o tratamento de dados pessoais (art. 7º) e de dados pessoais sensíveis (art. 11). Nesse sentido, é possível a divulgação de dados pessoais de um titular a terceiros, independentemente do consentimento, se essa divulgação é justificada diante de outras hipóteses legais.

CIDADE DE SÃO PAULO
CONTROLADORIA GERAL DO MUNICÍPIO

OBRIGADO!

CIDADE DE
SÃO PAULO
CONTROLADORIA
GERAL DO MUNICÍPIO

CONTATO:

controladoriageral@prefeitura.sp.gov.br
privacidade@prefeitura.sp.gov.br