RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (RIPD)

ÍNDICE:

1

O que é o RIPD e qual seu objetivo?

RIPD é a sigla para “Relatório de Impacto à Proteção de Dados”, uma das exigências previstas na LGPD[1]. Trata-se de um documento exigido do controlador de dados que é o agente de tratamento responsável por tomar decisões sobre como os dados pessoais serão tratados, incluindo, a definição do tipo de dado, a finalidade do tratamento e a forma como o dado será tratado.

O RIPD deve descrever os processos de tratamento de dados pessoais que possam representar riscos às liberdades civis e aos direitos fundamentais. O referido documento também deve prever medidas, salvaguardas e mecanismos para mitigar esses riscos.[2] Embora a elaboração do RIPD seja recomendada principalmente para operações de tratamento de alto risco aos titulares de dados, é importante considerá-lo para qualquer outro processo que envolva uma grande quantidade de dados pessoais, como criação de perfis, dados pessoais sensíveis e dados de titulares considerados vulneráveis.

O objetivo do RIPD é avaliar os riscos de determinada operação de tratamento de dados pessoais e determinar medidas para mitigar os riscos identificados. O RIPD pode ser solicitado a qualquer momento pela Autoridade Nacional de Proteção de Dados (“ANPD"), portanto é essencial que as organizações possuam o documento para as operações mencionadas anteriormente (i.e., operações de tratamento de dados pessoais de alto risco; que envolvam uma grande quantidade de dados pessoais, dados pessoais sensíveis ou dados de titulares vulneráveis).

A elaboração do RIPD é uma exigência legal e, também, uma boa prática de gestão de riscos para as organizações. Isso porque, além de evitar sanções e multas da ANPD, ajuda a garantir a confiança dos titulares de dados pessoais e de parceiros comerciais relevantes.

[1] LGPD, Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.

[2] LGPD, Art. 5º, inc. XVII. "relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco".

2 Como identificar a necessidade de elaboração de um RIPD?

Conforme previsto na LGPD, as hipóteses em que o RIPD poderá ser solicitado pela ANPD são:

Quando a operação de tratamento for fundamentada na base legal do legítimo interesse[3]

A qualquer momento sob determinação da ANPD[4]

No entanto, no final do ano de 2020, a "Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia" publicou um "Guia e Template de RIPD"[5] ("Guia") que prevê situações em que é indicada a elaboração do RIPD, quais sejam:

- Uso de uma nova 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 operação de tratamento que vise à formação de perfil comportamental
- tratamento de dado pessoal sensível
- tratamento de dados pessoais para tomada de decisões automatizadas que possam ter efeitos legais, incluídas as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito, ou ainda, os aspectos da personalidade de um indivíduo
- tratamento de dados pessoais de crianças e adolescentes
- tratamento de dados que possa resultar em algum tipo de dano patrimonial, moral, individual ou coletivo aos titulares de dados, se houver incidente de segurança da informação
- 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
- tratamento de dados pessoais fundamentado no interesse legítimo do controlador
- alterações nas leis e regulamentos aplicáveis à proteção de dados, ou mesmo em políticas e normas internas, operação do sistema de informações, alteração de fluxos de dados
- reformas administrativas que implicam em nova estrutura organizacional resultante de incorporação, fusão ou cisão de órgãos ou entidades

Em síntese, o ideal é que a organização elabore o RIPD antes do início de qualquer operação de tratamento de dados de risco alto, avaliando desde o seu início o potencial risco de impacto aos titulares de dados pessoais. Além disso, é importante considerá-lo para qualquer outro processo que envolva o tratamento de dados pessoais em grande escala, utilização de soluções inovadoras, criação e definição de perfil, dados pessoais sensíveis e dados de titulares vulneráveis.[6]

[3] LGPD, Art. 10, inc. II, § 3º.
[4] LGPD, Art. 32.
[5] Disponível em: <Guia e Template: Relatório de Impacto à Proteção de Dados Pessoais>. Acesso em 15 mar. 2023.
[6] EUROPEAN COMISSION. Guidelines on Data Protection Impact Assessment (DPIA). Disponível em: <https://ec.europa.eu/newsroom/article29/items/611236/en>. Acesso em: 15 mar. 2023.

3

O Privacy by design no RIPD

O modelo “Privacy by Design” (PbD), foi originalmente publicado em 1995 em um relatório conjunto apresentado por Ann Cavoukian, autora do modelo, e por John Borking da Autoridade Holandesa de Proteção de Dados. Em 2010, o conceito foi reconhecido como essencial para proteção da privacidade e ganhou destaque em diversos modelos orientadores de privacidade e proteção de dados ao redor do mundo.

A ideia do RIPD alinhado ao Privacy by Design é analisar os riscos e prevenir potenciais violações de privacidade desde o início de determinada operação de tratamento dos dados pessoais em um negócio/operação. Dessa forma, ao invés de ser apenas uma medida corretiva, a sua abordagem é preventiva.

Combinar o RIPD com o Privacy by Design permite descrever os processos de determinada operação de tratamento de dados pessoais desde o seu início, de forma completa e com a avaliação dos potenciais riscos e medidas de prevenção relacionadas à respectiva operação de tratamento. Considerando que o RIPD aborda essencialmente o tratamento de dados com alto risco para os titulares, o Privacy by Design é determinante para um uso responsável e seguro dos dados pessoais, auxiliando na elaboração e implementação do documento.

4

Quais são os aspectos que devem ser abordados no RIPD?

De acordo com o artigo 38, parágrafo único da LGPD, um RIPD deverá conter, no mínimo, os seguintes itens:

I.
Descrição dos tipos de dados coletados

II.
Metodologia utilizada para a coleta e garantia da segurança das informações

III.
Análise do controlador em relação às medidas, salvaguardas e mecanismos de mitigação de risco adotados

Embora a LGPD preveja a elaboração do RIPD, o tema ainda será regulado mais detalhadamente pela ANPD, conforme disposto em sua agenda regulatória. No entanto, o governo federal já disponibilizou o Guia, que pode auxiliar os controladores de dados e os seus encarregados de proteção de dados (ou simplesmente "Encarregado") na elaboração de um RIPD.

Ainda, é essencial que as organizações sigam as regras e diretrizes específicas da LGPD ao utilizar a base legal do legítimo interesse para o tratamento de dados pessoais.

Em linhas gerais, o Guia prevê oito etapas para a elaboração do RIPD, quais sejam:

1. IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E ENCARREGADO

Identificação do controlador, operador e Encarregado no RIPD, este último com a inclusão do e-mail e telefone de contato, uma vez que ele é o canal de comunicação entre o controlador, titulares de dados e a ANPD.

2. NECESSIDADE DE ELABORAÇÃO DO RIPD

A organização deve avaliar se é necessário elaborar o RIPD e, se for o caso, se será elaborado um único RIPD para todas as operações de tratamento de dados ou um RIPD para cada projeto.

A adequação acima deve ser avaliada internamente pela própria organização. Se for uma organização que possui vários projetos, serviços e sistemas com tratamento expressivo de dados, deverá optar pela elaboração de RIPDs distintos. Se for uma organização com poucas operações de tratamento de dados, poderá optar pela elaboração de um único RIPD.

A avaliação também deve considerar os casos em que o RIPD deve ou pode ser solicitado pela ANPD e nas hipóteses elencadas no Item 2.

3. DESCRIÇÃO DO TRATAMENTO DE DADOS PESSOAIS

Identificação do controlador, operador e Encarregado no RIPD, este último com a inclusão do e-mail e telefone de contato, uma vez que ele é o canal de comunicação entre o controlador, titulares de dados e a ANPD.

NATUREZA

Como a organização realiza ou pretende realizar o tratamento de dados, descrevendo como os dados pessoais são coletados, armazenados, tratados, usados e eliminados; a fonte de dados; se há compartilhamento e com quais organizações são compartilhados os dados; os operadores envolvidos no tratamento e em qual fase do tratamento, se há utilização de novas tecnologias que podem aumentar o risco de vazamento; e as medidas de segurança adotadas para proteger esses dados.

ESCOPO

A abrangência do tratamento de dados da organização, descrevendo os tipos de dados pessoais tratados, especificando se há dados pessoais sensíveis, o volume de dados coletados e tratados, a quantidade e frequência do tratamento, o período de retenção, o número de titulares afetados e a abrangência geográfica do tratamento.

CONTEXTO

A identificação de quais fatores internos e externos à organização podem impactar o tratamento de dados e as expectativas do titular, descrevendo a natureza da relação do controlador com o titular; nível/método de controle que o titular tem sobre seus dados; se o tratamento é alinhado à expectativa do titular e à finalidade divulgada; a experiência anterior do controlador nesse tipo de tratamento; e os avanços tecnológicos e de segurança da organização que podem contribuir para a proteção dos dados pessoais.

FINALIDADE

A razão para o tratamento desejado, conforme as hipóteses previstas nos artigos 7º e 11 da LGPD, para justificar o tratamento e informar ao titular de dados. É importante indicar os resultados do tratamento pretendidos para o titular e os benefícios esperados para o órgão, entidade ou para a sociedade.

4. AGENTES OU INTERESSADOS ENVOLVIDOS NA OPERAÇÃO

Listar todos os envolvidos consultados sobre os dados pessoais que são ou serão objeto de tratamento, como o operador, Encarregado, gestores, especialistas em segurança da informação, consultores jurídicos, dentre outros. É necessário também listar a opinião de cada parte com relação aos riscos do tratamento de dados.

5. NECESSIDADE E PROPORCIONALIDADE

Demonstrar se os dados coletados estão limitados ao mínimo necessário para atingir a finalidade proposta, sendo pertinentes, proporcionais e não excessivos. É importante garantir, ainda, a qualidade dos dados, sua exatidão, clareza, relevância e atualização, além de descrever as medidas para atendimento aos direitos dos titulares.

6. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Identificar os riscos que geram potencial impacto frente aos titulares de dados pessoais, a partir de uma matriz de risco que seja capaz de elencar todos os tipos de riscos frente ao tratamento de dados pessoais, a fim de que seja possível elencar medidas, salvaguardas e mecanismos de mitigação de risco.

7. MEDIDAS UTILIZADAS PARA COLETA E SEGURANÇA DOS DADOS PESSOAIS E TRATAMENTO DE RISCOS

Conforme a LGPD dispõe, os agentes de tratamento devem adotar medidas 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.[7]

A organização precisa ter em mente processos e soluções de segurança e de privacidade para se manter em conformidade com a LGPD, bem como elencar as medidas aplicáveis para o tratamento de cada potencial risco no tratamento de dados dos titulares.

8. APROVAÇÃO PELOS RESPONSÁVEIS

Etapa em que é necessária a formalização do RIPD através das assinaturas dos responsáveis pela aprovação do documento, sendo estes o representante do controlador, o representante do operador, o Encarregado e o responsável pela elaboração do relatório.

9. REVISÃO

É relevante que a organização esteja atenta aos procedimentos de revisão do RIPD, tendo em vista o dinamismo de operações e negócios de uma organização e, ainda, considerando a importância da avaliação contínua das operações de tratamento de dados pessoais.

[7] LGPD, Art. 46.

5

A importância da elaboração de um RIPD e como podemos ajudá-lo

A elaboração do RIPD é uma oportunidade para a organização avaliar seu nível de conformidade com a LGPD e demonstrar seu compromisso com a privacidade e proteção dos dados pessoais, tanto para os titulares de dados quanto para a ANPD. Dessa forma, a organização também demonstra seu comprometimento com o princípio da responsabilização e prestação de contas, cumprindo as normas de proteção de dados e demonstrando a eficácia de todas as medidas aplicadas .

No Campos Thomaz & Meirelles Advogados, oferecemos assessoria completa para adequação à LGPD e todas as exigências relacionadas à legislação sobre privacidade e proteção de dados pessoais.

Nossos reconhecimentos

Análise Advocacia (2021)

Chambers & Partners Brazil (2021 e 2022)

Leaders League (2021 e 2022)

Transactional Track Record (2021 e 2022)

The Legal 500 (2022)

Conheça nossos Sócios

Alan Campos Thomaz

Sócio

Tecnologia e Negócios Digitais, Privacidade e Proteção de Dados, Fintechs e Propriedade Intelectual

at@camposthomaz.com

+55 11 9 8375.2627 +1 (650) 6436652

Sérgio Meirelles

Sócio

Societário, M&A, Venture Capital e Wealth

sergio@camposthomaz.com

+55 11 9 7551.9865

Filipe Starzynski

Sócio

Contencioso & Law Enforcement, Consultivo Cível, Imobiliário, Trabalhista e Família

filipe@camposthomaz.com

+55 11 9 7151.9639

Juliana Sene Ikeda

Sócia

Propriedade Intelectual, Tecnologia, Contratos e Life Sciences

juliana@camposthomaz.com

+55 11 9 8644.1613

Nos acompanhe em nossas redes

campos thomaz & meirelles advogados

Assine nossa newsletter