RIPD – Relatório de Impacto de Proteção de Dados.

Perguntas e respostas - Texto completo ANPD

1. O que é o Relatório de Impacto à Proteção de Dados Pessoais (RIPD)?

O RIPD é a documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados. Deve conter, ainda, as medidas, salvaguardas e mecanismos de mitigação de risco, nos termos dos artigos 5º, inciso XVII, e 38 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

2. Quem é o responsável pela elaboração do RIPD?

O controlador é o agente de tratamento responsável pela elaboração do RIPD, nos termos dos art. 5º, inciso XVII, e 38, da LGPD.

3. Em qual contexto a ANPD recomenda que seja elaborado o RIPD?

Como regra geral, é recomendado elaborar o RIPD em todo contexto em que as operações de tratamento de dados pessoais possam gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados, conforme art. 5º, inciso XVII, e art. 55-J, inciso XIII, da LGPD, o que deverá ser avaliado pelo agente de tratamento.

A LGPD lista, ainda, situações específicas em que o RIPD poderá ser exigido pela ANPD, como:

- nas operações de tratamento efetuadas para fins exclusivos de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais (art. 4º, § 3º);
- quando o tratamento tiver como fundamento a hipótese de interesse legítimo (art. 10, § 3º);
- para agentes do Poder Público, incluindo determinação quanto à publicação do RIPD (art. 32); e
- para controladores em geral, quanto às suas operações de tratamento, incluindo as que envolvam dados pessoais sensíveis (art. 38).

Portanto, haverá situações em que o controlador elaborará o RIPD para atender à determinação da ANPD ou, em atenção ao princípio da responsabilização e prestação de contas (art. 6º, X), ao verificar que o tratamento a ser realizado pode implicar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados.
Além disso, a LGPD prevê a possibilidade de que os controladores, para cumprimento dos princípios da segurança e da prevenção (art. 6º, VII e VIII), implementem programa de governança em privacidade que, entre outros itens, estabeleça políticas e salvaguardas

adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade (art. 50, § 2º, I, d), procedimento que pode envolver a elaboração de RIPD.

4. Quando elaborar o RIPD?

Recomenda-se elaborar o RIPD antes de o controlador iniciar o tratamento dos dados pessoais para a finalidade desejada, justamente para que ele possa avaliar, de antemão, os possíveis riscos associados a esse tratamento.
Dessa forma, o controlador conseguirá, antes mesmo de usar os dados pessoais para aquela finalidade, identificar a probabilidade de ocorrência de cada fator de risco e o seu impacto sobre as liberdades e direitos fundamentais dos titulares e adotar as medidas, as salvaguardas e os mecanismos de mitigação de risco apropriados à hipótese.

Contudo, caso não seja possível elaborar o RIPD antes do início do tratamento, recomenda-se elaborá-lo assim que se identificar um tratamento que possa gerar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e às liberdades civis e aos direitos fundamentais do titular de dados

De todo modo, o controlador deverá, ainda, elaborar o RIPD caso seja solicitado pela ANPD.

5. Quais critérios e metodologias devem ser utilizados para a gestão de riscos?

A gestão de riscos é um processo sistemático da gestão organizacional que determina a aplicação equilibrada de controles diante do perfil de riscos.

As diretrizes gerais do processo de gestão de risco de privacidade, além de estarem alinhadas à política de segurança do responsável, poderão considerar, entre outros aspectos, objetivos estratégicos, processos, estrutura organizacional, requisitos da LGPD e demais normativos aplicáveis.

A identificação e análise dos fatores de risco devem ser documentadas e justificadas para que possam demonstrar que as decisões tomadas em relação à gestão de riscos foram as medidas mais adequadas com base nas informações disponíveis.

A avaliação de risco dificilmente irá representar a totalidade dos fatores de risco envolvido no tratamento. Cabe ao controlador identificar o maior número possível de fatores, principalmente os mais relevantes, que possam afetar os dados pessoais que serão tratados. Para cada fator identificado deve estimar a probabilidade de materialização do risco e o impacto inerente. Esse impacto dependerá dos danos que possam ser causados aos titulares, em particular no âmbito dos seus direitos e liberdades.

Destaca-se que a existência de múltiplos fatores de risco pode aumentar o nível de risco do tratamento considerado individualmente. Quando existem diferentes fatores de risco, é necessário interpretar como esses fatores podem interagir entre si para aumentar o nível

de risco do tratamento, analisando suas dependências e efeitos combinados ou as interações mútuas.

Nesse cenário, a gestão de risco pode ser feita por diferentes metodologias. Recomenda-se, no entanto, adotar aquelas que são reconhecidas como boas práticas pela comunidade técnica de segurança, privacidade e proteção de dados.
A decisão da metodologia a ser adotada é de responsabilidade do controlador. O processo de avaliação do nível de risco deve levar em conta as possíveis consequências sobre os titulares dos dados pessoais, tais como a perda de confidencialidade, integridade ou disponibilidade de dados, reversão da anonimização ou pseudonimização, uso de dados para fins incompatíveis, violação de liberdades e direitos, ou qualquer forma de tratamento inadequado ou ilícito.

6. Quais são os requisitos mínimos que o RIPD deve conter e que poderão ser exigidos pela ANPD?

Conforme o art. 38 da LGPD, o RIPD deverá conter, pelo menos:

a) a descrição dos tipos de dados pessoais coletados ou tratados de qualquer forma;
b) a metodologia usada para o tratamento e para a garantia da segurança das informações; e
c) a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

É importante que o relatório seja suficientemente detalhado, para que a ANPD e o próprio controlador tenham compreensão ampla de como ocorre o tratamento dos dados pessoais e os possíveis riscos associados a ele.
Assim, recomenda-se ao controlador descrever os tipos de dados pessoais tratados, as operações de tratamento (art. 5º, X, da LGPD), suas finalidades (incluindo interesses legítimos) e hipóteses legais, e avaliar a necessidade e a proporcionalidade das operações de tratamento, os riscos para os direitos e liberdades dos titulares de dados e as medidas a serem adotadas para minimizar esses riscos.

Em qualquer caso a ANPD poderá solicitar informações adicionais, sempre que necessário.

7. O RIPD deve ser público?

Embora a divulgação do RIPD não seja, em regra, obrigatória, permitir o acesso ao público em geral pode ser uma medida que demonstra a preocupação do controlador com a segurança dos dados pessoais que estão sob sua responsabilidade e seu compromisso com a privacidade dos titulares, além de atender aos princípios do livre acesso, da transparência e da responsabilização e prestação de contas, previstos, respectivamente, pelo art. 6º, incisos IV, VI e X, da LGPD.

Para isso, o controlador pode disponibilizar o RIPD em meios de fácil acesso pelo titular, especialmente em seus sítios eletrônicos, com informações sobre suas atividades de tratamento de dados pessoais, de forma clara, adequada e ostensiva. Contudo, nesse caso a versão pública do RIPD pode ser distinta da versão interna, no intuito de resguardar segredos comercial e industrial e outras informações protegidas por lei.
Especificamente em relação a entidades e órgãos públicos, o RIPD deverá ser publicado: (i) por determinação da ANPD, nos termos do art. 32 da LGPD; ou (ii) pelo próprio controlador, quando não identificada hipótese de sigilo aplicável ao caso, em conformidade com a Lei nº 12.527, de 18 de novembro de 2011.

8. O controlador deve elaborar um RIPD único para todas as suas operações de tratamento ou um RIPD para cada operação?

Um RIPD corresponde a cada projeto/processo do controlador que contenha um conjunto de operações de tratamento voltadas para uma mesma finalidade.

Em alguns casos, isso pode se traduzir em relatórios diferentes para cada operação de tratamento, especialmente se o controlador possui operações muito distintas. Ao elaborar relatórios separados para um conjunto de tratamentos que possuam a mesma finalidade, é possível visualizar melhor os tratamentos realizados e identificar com maior precisão os riscos associados a eles.
No entanto, se o controlador realiza múltiplas operações de tratamento similares em termos de natureza, finalidade e riscos é razoável que seja elaborado apenas um RIPD que inclua todas essas operações de tratamento.

É importante também observar que, em cenários em que há compartilhamento de dados pessoais entre diferentes controladores, cada controlador poderá ser responsável por um RIPD, ainda que utilizem uma plataforma compartilhada, uma vez que as finalidades do tratamento poderão ser distintas.

9. O que considerar como "alto risco" para fins de elaboração do RIPD?

Enquanto não for editado regulamento específico sobre o RIPD, os controladores podem, no que couber, adotar como parâmetro o conceito de tratamento de alto risco definido no art. 4º do Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte, aprovado pela Resolução nº 2/2022.

De acordo com esse dispositivo, o tratamento será de alto risco se verificada, no caso concreto, a presença de, ao menos, um critério geral (“larga escala” ou “afetar significativamente interesses e direitos fundamentais dos titulares”) e de um critério específico (“uso de tecnologias emergentes ou inovadoras”, “vigilância ou controle de zonas acessíveis ao público”, “decisões tomadas unicamente com base em tratamento automatizado de dados pessoais” ou “utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos”).

Considerando esses critérios, recomenda-se elaborar o RIPD, por exemplo, se o tratamento de dados pessoais abranger número significativo de titulares (“larga escala”, critério geral) e dados pessoas sensíveis (critério específico). Outro exemplo que pode ser mencionado é a decisão tomada unicamente com base em tratamento automatizado de dados pessoais (critério específico), da qual possa resultar a negativa para o exercício de um direito ou para a utilização de um serviço (“afetar significativamente interesses e direitos”, critério geral).

Ressalte-se que, para fins de elaboração do RIPD, esses critérios não devem ser considerados exaustivos, de modo que o controlador poderá verificar a existência de alto risco em situações diferentes das indicadas. Assim, em conformidade com o princípio da responsabilização e prestação de contas, cabe ao controlador avaliar as circunstâncias relevantes do caso concreto, a fim de identificar os riscos envolvidos e as medidas de prevenção e segurança apropriadas, considerando os possíveis impactos às liberdades e direitos fundamentais dos titulares e a probabilidade de sua ocorrência.

10. O RIPD deve ser encaminhado para a ANPD?

A LGPD não determina, como regra geral, o encaminhamento do relatório à ANPD. Não obstante, no exercício efetivo das suas atribuições fiscalizatórias e nas hipóteses previstas na LGPD, a Autoridade poderá requerer ao controlador o encaminhamento do RIPD, além de cópia de documentos, físicos ou digitais, e de dados e informações relevantes para a avaliação das atividades de tratamento de dados pessoais.

Assim, o controlador tem o dever de encaminhar o RIPD apenas quando requisitado pela ANPD, sujeitando-se a medidas de fiscalização em caso de descumprimento.

11. O controlador pode consultar a ANPD em caso de dúvida sobre as salvaguardas e as medidas a serem adotadas para mitigar os riscos identificados?

A ANPD não responde individualmente consultas jurídicas em tese ou que demandem a emissão de pronunciamento específico sobre uma condição hipotética ou concreta. Nesse sentido, não cabe manifestação da ANPD sobre as salvaguardas e medidas adequadas a serem adotadas para mitigar os riscos identificados em um determinado caso.

Não obstante, o controlador pode encaminhar suas dúvidas e questionamentos para a ANPD, por meio do endereço eletrônico ouvidoria@anpd.gov.br. As demandas recebidas são avaliadas e consolidadas, podendo ser consideradas no processo de elaboração de regulamentos ou para fins de futuras orientações sobre o tema.

12. O encarregado deve ser consultado no processo de elaboração do RIPD?

Considerando as atribuições legais definidas nos artigos 5º, inciso VIII, e 41 da LGPD, é desejável que o encarregado seja consultado na elaboração e na análise das conclusões do RIPD. O controlador também poderá consultar outros membros de sua organização, eventuais operadores ou o público externo, incluindo, entre outros, especialistas e titulares de dados pessoais.

13. É necessário registrar, no RIPD, opiniões divergentes identificadas durante o processo de elaboração?

Ainda que não exista exigência específica da necessidade de registro de diferentes opiniões identificadas no processo de elaboração do RIPD, esse registro, incluindo as justificativas para a opção adotada, pode ser considerado uma boa prática em termos de transparência, responsabilização e prestação de contas.

Enquanto a matéria não estiver regulamentada, controladores de dados têm flexibilidade para determinar as melhores estruturas e formatos de seu RIPD, da forma que mais se ajuste às práticas de trabalho existentes na organização, observadas as disposições pertinentes da LGPD.

14. O que fazer após elaborar o RIPD?

Após elaborar o RIPD, o controlador verificará a viabilidade de prosseguir ou não com os processos de tratamento de dados pessoais que ensejaram a elaboração do relatório ou a necessidade de modificação na forma do tratamento.

O agente de tratamento observará as recomendações provenientes do RIPD, especialmente no que se refere à implementação de medidas, salvaguardas e mecanismos de mitigação de riscos adotados.

Por fim, recomenda-se ao controlador a revisão contínua do RIPD, em especial, quando houver fatos novos que possam ensejar mudanças nos riscos identificados, tais como alteração nas operações de tratamento, identificação de novos fatores de risco, agravamento dos fatores de risco anteriormente identificados, ou em caso de novas regulamentações ou orientações emitidas pela ANPD.

15. Quais dados e informações incluir no RIPD?

É recomendável que o RIPD reúna os seguintes dados e informações:

a) Identificação dos agentes de tratamento e do encarregado;
b) Outras partes interessadas/envolvidas. Informar se foram consultadas na elaboração do RIPD e pareceres emitidos;
c) Justificativa da necessidade de elaboração do relatório (por exemplo: alto risco, solicitação da ANPD, gestão de riscos e prevenção, outros);
d) Projeto/Processo que justifica a elaboração do RIPD;
e) Sistemas de informação relacionados ao projeto/processo que justifica a elaboração do RIPD;
f) Tratamento de dados;
    I. Descrição do tratamento (desde a coleta até a eliminação);
    II. Dados pessoais (informar todos os tipos de dados pessoais tratados, de forma completa);
    III. Dados pessoais sensíveis (informar todos os tipos de dados pessoais sensíveis tratados, de forma completa);
    IV. Categorias de titulares (por exemplo, clientes, funcionários do controlador, filhos de funcionários do controlador, funcionários de clientes, autores de ações judiciais, beneficiários de apólices, terceiros prestadores de serviços);
    V. Dados de crianças e adolescentes ou de outra categoria de vulneráveis, como idosos, se houver;
    VI. Volume de dados pessoais tratados e número de titulares envolvidos no tratamento;
    VII. Fonte de coleta;
    VIII. Finalidade do tratamento (Justifique a finalidade de tratamento para cada dado);
    IX. Informar quais são os compartilhamentos internos e externos (inclusive transferência internacional, se houver);
    X. Política de armazenamento (descrever os prazos de retenção e métodos de descarte);
g) Análise de hipótese legal. Justifique a escolha da hipótese legal para cada finalidade de tratamento;
h) Análise de princípios da LGPD;
i) Riscos identificados ao titular;
j) Resultado apurado com base na metodologia utilizada pelo agente de tratamento:

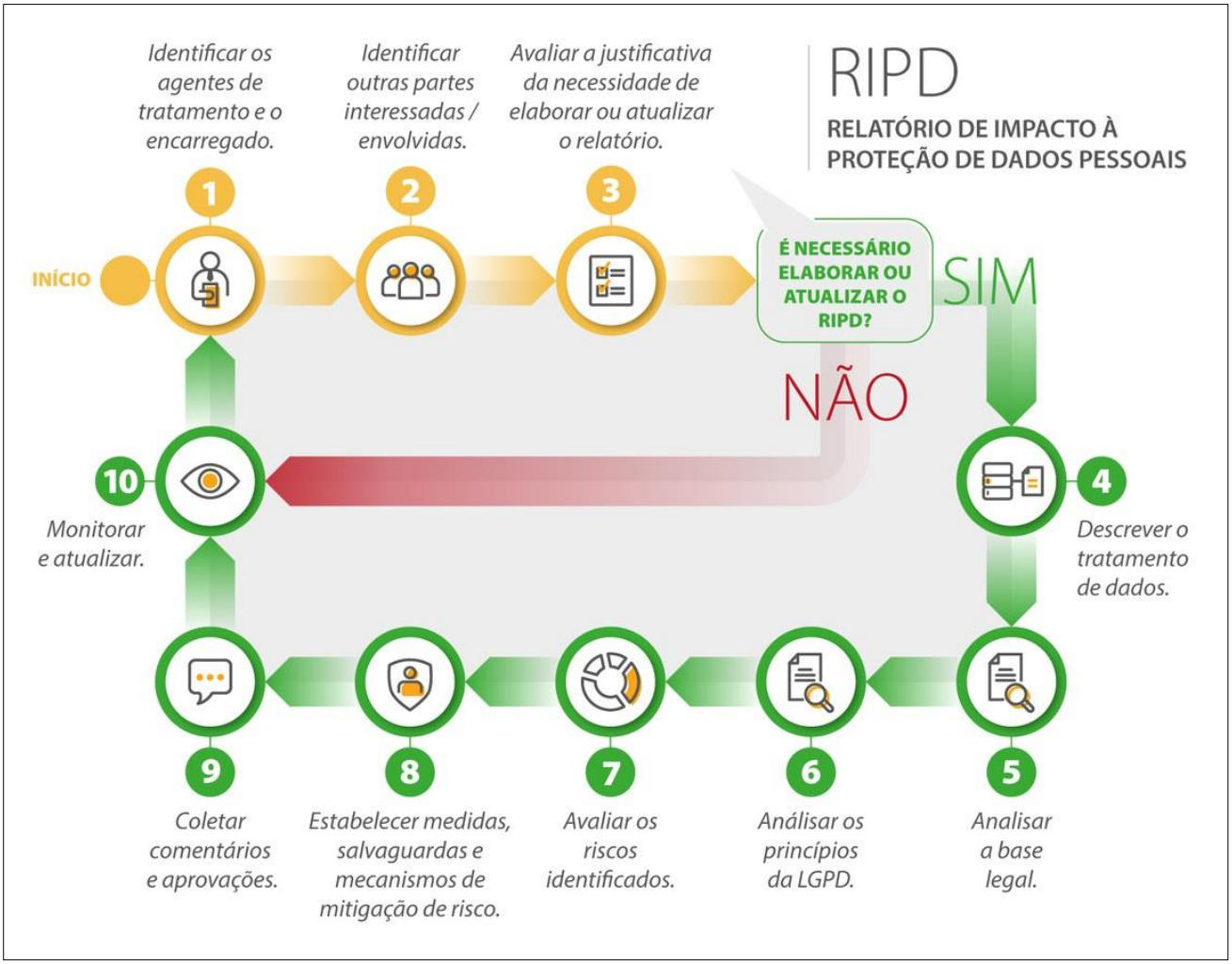
Descrição do risco e do impacto para os titulares	Probabilidade	Impacto	Risco total

k) Medidas, salvaguardas e mecanismos de mitigação de risco:

Risco	Tratamento do risco*	Risco após o tratamento	Risco residual

* Descrever as medidas adotadas para mitigação do risco.

l) Comentários e aprovações.



Transcrição na integra de publicação de 06/04/2023 as 16h49 em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd/relatorio-de-impacto-a-protecao-de-dados-pessoais