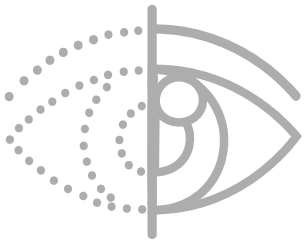
CARTILHA

Elaboração de Relatório de Impacto à Proteção de Dados (RIPD)

LGPD NA FCAV

Fundação Vanzolini



O Relatório de Impacto à Proteção de Dados (RIPD) é um **documento que descreve os processos de tratamento** de dados pessoais que podem gerar alto risco às liberdades civis e aos direitos fundamentais dos titulares. A Lei Geral de Proteção de Dados Pessoais (LGPD) determina que o controlador elabore RIPD incluindo **medidas, salvaguardas e mecanismos de mitigação de risco**. Por meio dele, a instituição demonstra como gerencia os riscos associados ao tratamento de dados pessoais e como se prepara para enfrentá-los. O RIPD também pode ser solicitado pela Autoridade Nacional de Proteção de Dados (ANPD), caso seja necessário ela verificar a conformidade da instituição com a legislação.

Tendo em vista que o RIPD atende aos princípios de **transparência**, **segurança**, **prevenção** e **prestação de contas**, a FCAV possui, em seu Programa de Governança em Privacidade e Proteção de Dados, um procedimento especialmente dedicado às diretrizes de sua elaboração, no qual estão definidas as informações que esse documento deve conter e os responsáveis por elaborá-lo e guardá-lo.

Por que é importante

Mais do que uma obrigação legal, o RIPD configura boa prática para **mitigação dos riscos** envolvidos no tratamento de dados pessoais. Ele contribui para **melhorar a governança de dados**, pois sua elaboração possibilita identificar lacunas nos processos internos e, consequentemente, tomar providências para **fortalecer a segurança da informação**. Caso haja investigação sobre incidentes, ele ajuda a diminuir possíveis sanções administrativas, visto que prova a **adoção de medidas para evitar desvios** no tratamento de dados. Assim, o RIPD é uma maneira de reduzir riscos legais e operacionais.

O RIPD também é um **instrumento de transparência**, pois mostra, à ANPD e aos titulares, como a FCAV trata os dados pessoais, demonstrando sua responsabilidade e conformidade com a legislação vigente. Portanto, o RIPD é uma ferramenta de gestão de riscos e de **garantia do direito fundamental à privacidade e da proteção de dados** pessoais, bem como de **salvaguarda** da Fundação e de sua reputação.

Como acontece

Para entender como o RIPD é elaborado, é importante conhecer alguns conceitos:

1. **Controlador:** É quem decide como e por que os dados pessoais são tratados. Muitas vezes, a FCAV exerce esse papel ao desempenhar suas atividades.
2. **Dado pessoal:** É qualquer informação que permita identificar uma pessoa física, por exemplo, nome, número de CPF e endereço de *e-mail*.
3. **Dado pessoal sensível:** É qualquer dado de uma pessoa física sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, saúde ou vida sexual, além de dado genético ou biométrico.
4. **Encarregado pelo Tratamento de Dados Pessoais:** É a pessoa indicada pela FCAV para fazer a interface entre ela e os titulares dos dados ou a Autoridade Nacional de Proteção de Dados (ANPD).
5. **Risco:** É a combinação da probabilidade de um evento indesejado ocorrer e o impacto que ele pode causar. O risco deve ser continuamente monitorado para que sejam implementadas medidas preventivas.
6. **Transparência:** É a garantia, aos titulares de dados pessoais, de informações claras, precisas e facilmente acessíveis sobre o tratamento de seus dados e respectivos agentes, observados os segredos comercial e industrial.
7. **Tratamento de dados pessoais:** É toda operação realizada com dados pessoais, por exemplo, coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão e extração.

A elaboração do RIPD deve ter como objetivos:

- ☑ garantir que o **tratamento de dados** pessoais esteja alinhado à necessidade e seja **proporcional aos objetivos** pretendidos (e comunicados);
- ☑ avaliar se o **conjunto de dados tratados** é o **mínimo necessário** para a execução da atividade (caso haja meios que envolvam menor volume de dados pessoais, a FCAV deverá proceder aos ajustes cabíveis);
- ☑ verificar detalhadamente as **medidas técnicas e organizacionais de proteção** dos dados pessoais tratados.

Como controlador, a FCAV pode ser solicitada a fornecer RIPD para a ANPD. Contudo, na Fundação, em atenção aos princípios de responsabilização e prestação de contas, a elaboração desse documento segue um fluxo estruturado, independentemente da existência de requisição da ANPD.

Quando se identifica que um **tratamento de dados** pessoais pode implicar **alto risco** às liberdades civis, aos direitos fundamentais dos titulares ou a qualquer princípio de proteção de dados previsto na LGPD – o que pode ser feito por meio do documento chamado Registro das Atividades de Tratamento de Dados Pessoais (*Record of Processing Activities* – RoPA) –, inicia-se a **elaboração do RIPD para o processo ou o projeto** que envolve o tratamento em questão.

Para determinar que o tratamento de dados pessoais apresenta alto risco, são considerados sobretudo os seguintes critérios:

- ☑ tratamento de dados pessoais **sensíveis**;
- ☑ uso de **novas tecnologias**;
- ☑ uso de técnicas de **perfilamento** (criação de perfis – *profiling*) ou de **decisões automatizadas** para emitir juízos sobre os titulares ou para auxiliar na tomada de decisões quanto à oferta de serviço, oportunidade ou benefício;
- ☑ tratamento de dados pessoais de crianças, adolescentes ou outros **grupos vulneráveis**;
- ☑ tratamento de dados pessoais em **larga escala**, ou seja, de muitos titulares.

Outros critérios podem ser estabelecidos pelo Encarregado pelo Tratamento de Dados Pessoais.

O **gestor** de cada área corporativa ou de negócios é responsável por **identificar os processos** da sua área que envolvem tratamento de dados pessoais de **alto risco**. Quando detecta essa situação, ele comunica imediatamente o Encarregado pelo Tratamento de Dados Pessoais, por meio de um formulário específico, no qual **detalha o tratamento** a ser realizado considerando sua natureza, seu escopo, seu contexto e sua finalidade, entre outros parâmetros.

A necessidade de RIPD também pode ser identificada pelo Encarregado quando de sua análise do RoPA. Nesses casos, o Encarregado solicita a elaboração do RIPD ao gestor da área corporativa ou de negócios responsável pelo processo em questão.

Ao receber o formulário específico do RIPD preenchido pelo gestor, o **Encarregado detecta e analisa riscos**, examina os **impactos** e a probabilidade de danos aos titulares e identifica as medidas necessárias para mitigar ou eliminar os riscos aos titulares, ou seja, **define ações técnicas e/ou administrativas** que devem ser implementadas para **reduzir** os riscos.

A **Área de Tecnologia da Informação** auxilia os gestores das áreas no registro das **medidas de segurança da informação** já adotadas e na implementação de novas medidas que sejam necessárias.

Em todos os casos, o **RIPD é armazenado**, em segurança, pelo Encarregado pelo Tratamento de Dados Pessoais e **atualizado** pelo gestor da área responsável, periodicamente ou sempre que houver alteração no fluxo de dados ou no processo correspondente ao tratamento em questão.

O que isso tem a ver comigo

Como o RIPD é uma forma de **demonstrar a gestão de riscos** à privacidade, a conformidade legal e a transparência no tratamento de dados pessoais, ele deve ser elaborado e atualizado em todos os casos especificados pela FCAV. Isso só é possível se todos os colaboradores se **mantiverem alertas aos tratamentos** realizados e **informarem a seu gestor as situações em que possa haver risco** à privacidade ou a qualquer outro princípio de proteção de dados pessoais.

Cada colaborador que lida com dados pessoais deve seguir as diretrizes da Fundação, informar seu gestor sobre toda mudança em processo de trabalho que envolva dados pessoais e contribuir na implementação de medidas que garantam a segurança da informação.

O que acontece se não for respeitado

Se, em qualquer processo da FCAV, houver falha que possa levar à violação das liberdades civis ou dos direitos fundamentais dos titulares de dados pessoais ou ao desrespeito a qualquer princípio de proteção de dados previsto na LGPD, os titulares ficarão expostos, e a Fundação poderá enfrentar sérias consequências, como penalidades legais, multas e danos à sua reputação.

Por isso é imprescindível que todos os colaboradores desempenhem suas atividades em consonância com as diretrizes, as orientações e as normas estabelecidas pela Fundação, a fim de mitigar riscos à segurança e à proteção de dados pessoais. Se o colaborador transgredir as regras da FCAV no contexto do Programa de Governança em Privacidade e Proteção de Dados, podem ser aplicadas medidas disciplinares previstas em políticas internas e contratos. A terceiros/fornecedores, podem ser aplicadas sanções contratuais.

Este documento foi elaborado para fins informativos e não substitui a íntegra do documento normativo "Procedimento para elaboração de Relatório de Impacto à Proteção de Dados (RIPD)", que estabelece diretrizes específicas para gestores e colaboradores diretamente envolvidos.