

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 03 de Agosto de 2024

FIAP – 3SOAT

Histórico de Revisões

Data	Versão	Descrição	Autor
03/08/2024	1.0	Conclusão da primeira versão do relatório	Grupo 5 – 3SOAT

FIAP – 3SOAT

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARGADO

Controlador

Grupo 5 – 3SOAT

Operador

Bruno Pulice Faccio
Leonilson Sousa de Alencar Filho
William de Magalhaes Pereira

Encarregado

FIAP – 3SOAT

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

A elaboração do RIPD é necessária devido ao tratamento de dados pessoais reais de clientes, produtos e entregadores, os quais foram gerados internamente para simulação, mas seriam sensíveis e reais em um cenário prático. Apesar de não armazenarmos dados de pagamento, o tratamento de dados pessoais como nome, CPF, endereço e informações de contato justifica a necessidade do RIPD para garantir a conformidade com a Lei Geral de Proteção de Dados (LGPD).

3 – DESCRIÇÃO DO TRATAMENTO

A descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais envolve a especificação da **natureza, escopo, contexto e finalidade** do tratamento.

3.1 – NATUREZA DO TRATAMENTO

- **Coleta:** Em um cenário real, os dados pessoais seriam coletados diretamente dos usuários através de formulários de cadastro na plataforma, como nome, CPF, endereço, telefone e email.
- **Retenção/Armazenamento:** Dados pessoais seriam armazenados em banco de dados seguro, com acesso restrito e controlado, utilizando medidas de segurança robustas.
- **Tratamento/Processamento:** Os dados coletados seriam utilizados para personalizar a experiência do usuário, processar pedidos, e realizar análises para melhorar os serviços

FIAP – 3SOAT

oferecidos. Dados de pagamento não são armazenados, sendo simulados ou tratados por terceiros em sistemas segregados.

- Compartilhamento: Em um cenário real, dados pessoais poderiam ser compartilhados com parceiros de entrega e prestadores de serviços terceirizados que operam em nome do controlador.
- Eliminação: Dados pessoais seriam eliminados após o término do contrato ou mediante solicitação do titular, seguindo as diretrizes da LGPD.
- Fonte de Dados: Os dados são coletados diretamente dos titulares (clientes e entregadores) através da interação com a aplicação.

3.2 – ESCOPO DO TRATAMENTO

- Tipos de dados pessoais tratados: Nome, CPF, endereço, telefone, email, histórico de pedidos.
- Volume de dados: Grande volume devido ao número de clientes e entregadores em uma aplicação real.
- Período de retenção: Dados seriam retidos pelo período necessário para o cumprimento das finalidades do tratamento e conforme a legislação aplicável.
- Número de titulares de dados afetados: Todos os clientes e entregadores cadastrados na plataforma.
- Abrangência geográfica: Tratamento de dados em nível nacional, com possibilidade de expansão para outras regiões.

3.3 – CONTEXTO DO TRATAMENTO

- Relação com os indivíduos: Relacionamento baseado em contrato de prestação de serviço, onde os titulares concordam com o tratamento de seus dados para a execução dos serviços.
- Controle dos dados pessoais: Os indivíduos teriam controle sobre seus dados pessoais, podendo solicitar correções, exclusões ou acesso conforme previsto na LGPD.
- Grupos vulneráveis: O tratamento não envolve dados de crianças ou adolescentes.
- Expectativas dos titulares: Os dados são tratados de acordo com as expectativas definidas nos termos de uso e política de privacidade da aplicação.

3.4 – FINALIDADE DO TRATAMENTO

- Objetivo principal: Execução de serviços de entrega de produtos, personalização da experiência do usuário, e análises para melhorias contínuas do serviço.
- Finalidades secundárias: Análise de comportamento de compra e histórico de pedidos para recomendações personalizadas.
- Benefícios esperados: Melhorias na eficiência das entregas, personalização da experiência do usuário e cumprimento das obrigações contratuais e legais.

FIAP – 3SOAT

4 – PARTES INTERESSADAS CONSULTADAS

- Operador: Grupo 5 – 3SOAT
- Encarregado: Professores 3SOAT / FIAP
- Especialistas: Consultores jurídicos e especialistas em segurança da informação da instituição acadêmica.

5 – NECESSIDADE E PROPORCIONALIDADE

- Fundamentação legal: O tratamento de dados pessoais é necessário para a execução de contratos com os titulares (clientes e entregadores), bem como para o cumprimento de obrigações legais.
- Qualidade dos dados: A instituição adotará medidas para garantir a exatidão, clareza, relevância e atualização dos dados pessoais tratados.
- Medidas de segurança: Implementação de controles de acesso, criptografia, e auditorias regulares para assegurar a integridade e segurança dos dados.

FIAP – 3SOAT

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	10	15	150
R02	Modificação não autorizada.	10	15	150
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	10	10	100
R07	Informação insuficiente sobre a finalidade do tratamento.	10	15	150
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	15	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

Legenda: P – Probabilidade; I – Impacto.

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

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

³ Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

FIAP – 3SOAT

7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida(s)	Efeito sobre o Risco ¹	Risco Residual ²			Medida(s) ³ Aprovada(s)
			P	I	Nível (P x I)	
R01	Controle de acesso lógico, Desenvolvimento seguro, Segurança em redes	Reduzir	50	Sim	R01	Controle de acesso lógico, Desenvolvimento seguro, Segurança em redes
R04	Controle de acesso lógico, Controles criptográficos, Proteção física e do ambiente	Reduzir	25	Sim	R04	Controle de acesso lógico, Controles criptográficos, Proteção física e do ambiente
R06	Limitação da coleta	Reduzir	50	Sim	R06	Limitação da coleta

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

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

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

³ Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.