RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

FIAP Postech Software Architecture - SOAT 4 - Grupo 23

Histórico de Revisões

Data	Versão	Descrição	Autor
06/07/2024	1.0	Conclusão da primeira versão do relatório	Ana J L Santos

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 ENCARREGADO

Controlador Departamento de Segurança	
Operador SOAT 4 GRUPO 23	
Encarregado Ana J L Santos	
E-mail Encarregado privacidade@webcafeteriaf.com.br	**Telefone Encarregado** +9999 (0) 999 799 9 799

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

O RIPD do WEB CAFETERIA foi elaborado para os seguintes objetivos:

2.1 Para atendimento à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e regulamentações emanadas pela Autoridade Nacional de Proteção de Dados -ANPD.

2.2 Para orientação e direcionamento dos funcionários do WEB CAFETERIA com relação ao tratamento das informações pessoais de clientes, colaboradores e demais interlocutores, que por necessidade de negócios são coletadas em seus processos formais.

2.3 Para definição de políticas internas de garantia da segurança e governança dos dados pessoais coletados;

2.4 Para garantia de proteção e mitigação de riscos eventualmente envolvidos evitando:

i) ameaças ou riscos à privacidade; à segurança; à integridade e/ou à confidencialidade;

ii) destruição acidental ou ilícita; perda; alteração; divulgação ou acesso não autorizado;

iii) quaisquer outras formas ilegais de tratamento; e

iv) incidentes de segurança ou privacidade.

3 – DESCRIÇÃO DO TRATAMENTO

Os sistemas e processos do WEB CAFETERIA foram desenhados para a captação somente dos dados que se fazem pertinentes para a elaboração de contratos comerciais; cadastro de clientes e fornecedores; informações para atendimentos a demandas fiscais e legais; registros de funcionários e para ações de marketing

3.1 – NATUREZA DO TRATAMENTO

3.1.1 Os dados pessoais são coletados mediante preenchimento de formulário eletrônico do WEB CAFETERIA pelo titular dos dados pessoais. Os dados são transferidos e armazenados nos servidores cloud na Amazon Web Services (AWS), administrados pelo WEB CAFETERIA e localizados no Norte da Virginia, nos EUA.

3.1.2 A fonte de dados é o titular dos dados pessoais mediante o preenchimento de formulário eletrônico do WEB CAFETERIA.

3.1.3 É compartilhado com o Mercado Pago o email do usuário para emissão do código PIX para pagamento.

3.1.4 O operador de dados pessoais é a administração da empresa WEB CAFETERIA (SOAP4 GRUPO 23), o qual é responsável pela implementação do sistema que automatiza todas as

operações de tratamento de dados pessoais (Coleta, Retenção, Processamento, Compartilhamento e Eliminação).

3.1.5 As medidas de segurança atualmente adotadas são: Controle de Acesso Lógico, Controles Criptográficos, Controles de Segurança em Redes, Proteção Física e do Ambiente.

3.2 – ESCOPO DO TRATAMENTO

3.2.1 Os dados pessoais tratados pelo WEB CAFETERIA abrangem: - Informações de identificação pessoal: Nome, e-mail, CPF ou CNPJ e data de nascimento;

3.2.2 Os dados coletados de acordo com o item 3.2.1 são para estrito cumprimento de relações comerciais, contratuais e legais, protegidos por cláusulas de sigilo. Todo funcionário do WEB CAFETERIA é treinado e assina termo de ciência com relação às informações;

3.2.3 A quantidade de dados pessoais tratados é de 4 dados pessoais. A frequência de tratamento dos dados pessoais é 24x7 (24 horas por dia nos 7 dias da semana).

3.2.4 Os dados pessoais obtidos serão mantidos armazenados durante a existência da empresa. Esse período de armazenamento poderá ser revisto em alinhamento a qualquer nova disposição legal sobre prazo de retenção.

3.2.5 A abrangência do tratamento de dados pessoais é nacional para manutenção do cadastro único dos clientes.

3.3 – CONTEXTO DO TRATAMENTO

3.3.1 Qualquer coleta de dados pessoais é avisada ao titular através de documentos informativos no site do WEB CAFETERIA no contato via e-mail organizacional e por aditivos de contrato, no caso de funcionários;

3.3.2 A política de sigilo da organização garante ciência por parte de todos os colaboradores do cuidado no trato com as informações pessoais e na proibição de qualquer compartilhamento sem o consentimento pessoal do titular e da organização.

3.3.3 O WEB CAFETERIA utiliza recursos de segurança robustos para evitar qualquer acesso indevido em sua base de dados.

3.3.4 Qualquer atualização, compartilhamento dos dados pessoais ou acessos suspeitos são avisados ao titular. Embora os campos Nome, CPF e e-mail sejam restritos para alteração. O titular pode requisitar informações sobre seus dados pessoais a qualquer momento.

3.4 – FINALIDADE DO TRATAMENTO

A finalidade para a coleta de dados pessoais pelo WEB CAFETERIA atende exclusivamente:

3.4.1 O cumprimento de obrigação legal fiscal, comercial ou regulatória;

3.4.2 Execução de contrato de compra e venda de mercadorias e outros contratos, assim como de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

3.4.3 Atender aos interesses legítimos para o pleno funcionamento da organização.

Para a elaboração do presente documento foram consultados representantes internos da organização; consultores jurídicos e analistas das empresas que prestam serviços de armazenamento de informações através das ferramentas contratadas, bem como necessidade de consumidores, clientes e prestadores.

4 – PARTES INTERESSADAS CONSULTADAS

4.1 Analistas de Segurança da Informação da WEB CAFETERIA: Consultados para identificar oportunidades de melhoria na proteção dos dados pessoais tratados

4.2 Consultor Jurídico: Responsável por emitir parecer sobre a conformidade do tratamento de dados em relação aos aspectos legais da LGPD.

4.3 Coordenadores, Servidores e Diretores da WEB CAFETERIA: Consultados para obter informações técnicas e administrativas sobre o processo de trabalho executado.

4.4 Encarregado do Tratamento de Dados Pessoais: Conduziu o levantamento e apreciou as

informações técnicas, administrativas, legais e de riscos fornecidas pelas demais partes consultadas.

4.5 Com exceção dos clientes, todas as demais partes consultadas participaram do processo de análise de riscos relativos ao tratamento dos dados pessoais

5 – NECESSIDADE E PROPORCIONALIDADE

5.1 – FUNDAMENTAÇÃO LEGAL

5.1.1 A base legal para o tratamento de dados pessoais é o artigo 7º, inciso I da LGPD: “mediante o fornecimento de consentimento pelo titular”; e inciso II da LGPD: “para o cumprimento de obrigação legal ou regulatória pelo controlador”.

5.2 – QUALIDADE E MINIMIZAÇÃO DOS DADOS

5.2.1 A seleção dos dados a serem coletados para a implementação dos processos da WEB CAFETERIA foi baseada na premissa de coletar o mínimo necessário de dados pessoais para a execução de suas atividades, incluindo a elaboração de contratos comerciais e trabalhistas.

5.3 – MEDIDAS PARA ASSEGURAR CONFORMIDADE DO OPERADOR

5.3.1 Em intervalos planejados, a WEB CAFETERIA realiza auditorias internas sobre as medidas de segurança das suas plataformas, conduzidas por profissionais qualificados, para assegurar a conformidade com as diretrizes estabelecidas.

5.3.2 Internamente, o acesso aos sistemas que gerenciam e armazenam os dados pessoais é protegido por uma política de senhas individuais.

5.3.3 Tanto o sistema de segurança quanto a política de confidencialidade garantem o tratamento adequado das informações coletadas, permitindo ações corretivas em caso de violação.

5.4 – MEDIDAS PARA ASSEGURAR DIREITOS DO TITULAR DOS DADOS

5.4.1 Os sistemas da WEB CAFETERIA estão configurados para que os titulares dos dados possam fazer as solicitações previstas no artigo 18º da LGPD. A Política de Privacidade informa sobre os direitos dos titulares e pode ser acessada em webcaferia.com.br/politica-privacidade.

5.4.2 Se um usuário identificar alguma falha ou vulnerabilidade de segurança no sistema, ele pode reportá-la pelo e-mail privacidade@webcafeteria.com.br.

5.4.3 Quando solicitado pelo titular dos dados, a WEB CAFETERIA fornecerá informações de privacidade (confirmação de existência ou acesso aos dados pessoais) via e-mail ou impresso, conforme a solicitação.

5.5 – SALVAGUARDAS PARA AS TRANSFERÊNCIAS INTERNACIONAIS DE DADOS

5.5.1 O armazenamento de dados em servidores internacionais e a subsequente transferência de dados para fora do país estão em conformidade com o artigo 33º da LGPD, que detalha as permissões para transferências internacionais de dados pessoais.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

6.1 Para identificar e avaliar os riscos no tratamento de dados pessoais pela WEB CAFETERIA, utilizou-se a Matriz Impacto x Probabilidade. Esta abordagem ajuda a determinar o nível de risco e a descrever medidas e salvaguardas para mitigá-los.

6.1.1 Para cada risco identificado, determina-se a probabilidade (P) de ocorrência e o impacto (I) caso ocorra, avaliando o potencial de risco para cada evento.

6.2.1 Os níveis de probabilidade e impacto são multiplicados para obter os níveis de risco, que guiarão a aplicação das medidas de segurança necessárias, conforme os parâmetros estabelecidos na tabela a seguir:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Divulgação não autorizada de dados sensíveis	5	15	75
R02	Erro na anonimização de dados pessoais	5	10	50
R03	Falha na atualização de consentimentos	10	15	150
R04	Vazamento de dados de clientes	5	15	75
R05	Uso indevido de dados para marketing direto	10	15	150
R06	Inadequação na gestão de cookies e rastreamento	5	10	50
R07	Acesso indevido por funcionários internos	10	15	150
R08	Retenção excessiva de dados de clientes	15	15	225
R09	Falha na implementação de medidas de segurança física	5	15	75
R10	Incidente de segurança em fornecedor de serviços	10	15	150
R11	Retenção prolongada de dados pessoais sem necessidade.	5	10	50
R12	Roubo.	10	15	150
R13	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	10	15	150
R14	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75

* verde, é entendido como baixo;
* amarelo, representa risco moderado; e
* vermelho, indica risco alto.

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 - Acesso não autorizado	Implantação de uma política de acesso às informações.	Evitar	5	15	75	Sim

R03 - Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento	Incluir cláusulas específicas sobre o tratamento e	Evitar	5	5	25	Sim

do titular dos dados pessoais.	compartilhamento de dados pessoais.					
R04 - Falha na proteção dos direitos de acesso dos titulares de dados	Realizar revisões regulares para garantir o cumprimento dos direitos de acesso dos titulares	Evitar	5	5	25	Sim
R05 - Erro durante o processamento de dados pessoais	Implementar procedimentos de validação para assegurar a integridade do processamento de dados	Reduzir	5	15	75	Sim
R07 - Modificação não autorizada de dados pessoais	Implementar controles robustos de autenticação e autorização para prevenir modificações não autorizadas	Evitar	5	15	75	Sim
R08 - Perda de dados pessoais por falta de backups adequados	Manter backups frequentes e um plano de recuperação de desastres para mitigar perdas de dados	Reduzir	5	15	75	Sim
R09 - Reidentificação indevida de dados pseudonimizados	Implementar técnicas avançadas de pseudonimização e restrições rigorosas de acesso aos dados pseudonimizados	Evitar	5	5	25	Sim
R10 - Exclusão não autorizada de dados pessoais	Manter registros detalhados de operações de exclusão e monitorar atividades suspeitas para detectar exclusões	Evitar	5	10	50	Sim

	não autorizadas					
R12 - Roubo de dados pessoais por acesso não autorizado	Implementar restrições estritas de acesso e criptografia de dados para prevenir roubos de dados .	Evitar	5	15	75	Sim
R13 - Tratamento de dados sem o consentimento explícito do titular	Obter consentimento explícito dos titulares antes de qualquer tratamento de dados e manter políticas de privacidade atualizadas	Evitar	5	5	25	Sim

	privacidade acessível e compreensível					
R14 - Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	Adotar medidas que preservem a privacidade e a confidencialidade desses dados com a pseudonimização correta dos dados pessoais.	Evitar	5	5	25	Sim

Legenda:

[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.

8 – APROVAÇÃO

Rúbrica

Responsável pela elaboração do RIPD

Rúbrica

Encarregado

Rúbrica

Autoridade
Representante do Controlador

Rúbrica

Autoridade
Representante do Operador