RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

Campo Grande MS, 19 de março de 2024

Histórico de Revisões

Data	Versão	Descrição	Autor
19/03/2024	1.0	Conclusão e revisão da primeira versão do relatório.	Téury Simões Bazzo

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 alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na LGPD e 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
Téury Simões Bazzo

Operador
Matheus Panta

Encarregado	
Gustavo Noberto	
E-mail Encarregado	**Telefone Encarregado**
teste.gov.br	(99)9999-9999

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

Atendimento ao artigo 5o, inciso II, artigo 10, parágrafo 3o., artigo 14, artigo 42 todos da Lei 13.907/2018 - Lei Geral de Proteção de Dados.

3 – DESCRIÇÃO DO TRATAMENTO

Referente a natureza dos dados do cliente, os dados são coletados para fim de realizar uma venda de um produto de uma lanchonete(lanches, bebidas), os dados são obtidos por uma API REST são retidos em uma base de dados estruturada e são tratados para fim de realizar um pedidos.

Referente à natureza dos dados fornecidos pela Food Ltda, são inseridos através de uma API REST ou diretamente no banco de dados, as informações de Categoria de lance, bebida, preço, e ingredientes dos lanches fornecidos.

Referente ao escopo, são coletados obrigatoriamente os dados do pedido que o cliente deseja(Tipo

de produto, Quantidade do produto, Observação sobre o produto), a identificação do cliente é opcional podendo o cliente conceder o dado ou não, caso o cliente queira se identificar ele pode fazer o mesmo via CPF, nome ou email.

Os dados dos clientes, são armazenados e são usados exclusivamente para identificação de quem é o pedido.

O cliente que desejar excluir seus dados da base de dados, o Food Ltda disponibiliza essa opção através de uma API ou entrando em contato com nossa equipe.

Referente a finalidade, todos os dados tem como finalidade fornecer um serviço de qualidade para o consumidor, obtendo o mínimo necessário para executar a operação.

4 – PARTES INTERESSADAS CONSULTADAS

Todas as partes mencionadas abaixo participaram, em diferentes momentos do processo de criação deste documento.

- Food Ltda
- Secretaria Estadual de Segurança dos dados
- Segurança Digital LTDA, controlador responsável Téury Simões Bazzo

5 – NECESSIDADE E PROPORCIONALIDADE

Fundamentação legal: artigo 5o, inciso II, artigo 10, parágrafo 3o., artigo 14, artigo 42 todos da Lei 13.907/2018 - Lei Geral de Proteção de Dados.

A necessidade dos dados fornecedor pela Food LTDA é indispensável para o funcionamento do processo, porém os dados referente ou cliente não é necessário sendo um opção do usuário conceder ou não, e caso queira existe uma política para remoção desses dados caso o cliente deseje.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

As definições e conceitos de riscos adotados neste documento são utilizados como forma de ilustrar a identificação e avaliação de riscos realizada no RIPD. Desse modo, é importante destacar que o gerenciamento de riscos relacionado ao tratamento dos dados pessoais deve ser realizado em harmonia com a Política de Gestão de Riscos do órgão preconizada pela **Instrução Normativa Conjunta MP/CGU nº 1, de 10 de maio de 2016**

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R01	Acesso não autorizado	5	15	75
R02	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	10	15	150

Id	Risco referente ao tratamento de dados pessoais	P[1]	I[2]	Nível de Risco (P x I) [3]
R03	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	10	50

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).

7 – MEDIDAS PARA TRATAR OS RISCOS

Risco	Controle/Medida	Efeito sobre o Risco[1]	Risco Residual[2]			Controle/ Medida[3] Aprovado (a)
			P	I	Nível (P x I)	
R01	GESTÃO DO CONTROLE DE ACESSO: Processo de concessão e revogação de acesso; SEGURANÇA DE APLICAÇÕES: Desenvolvimento Seguro	REDUZIR	5	15	75	SIM
R02	GESTÃO DO CONTROLE DE ACESSO: Processo de concessão e revogação de acesso. APLICAÇÃO DE CRIPTOGRAFIA: Processo de deixar ilegível dados do cliente	REDUZIR	5	15	75	SIM
R03	AMBIENTES DE TESTE: Disponibilização de ambientes de teste com dados fictícios.	REDUZIR	10	5	50	SIM

	CONTROLE INTERNO: Todos os scripts devem passar por análise no ambiente de teste;					

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 do(s) controle(s) descrito(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 controles para tratar o risco.

[3] Controle/medida aprovado(a) pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8 – APROVAÇÃO

O RIPD deve ser revisto e atualizado anualmente ou sempre que existir qualquer tipo de mudança que afete o tratamento dos dados pessoais realizados pela instituição. Detalhes sobre a necessidade de revisão do RIPD podem ser observados no **item 2.5.2.9 do Guia de Boas Práticas LGDP, disponível em**: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf

RESPONSÁVEL PELA ELABORAÇÃO DO RELATÓRIO DE IMPACTO	ENCARREGADO
Téury Simões Bazzo _____ Campo Grande MS, 19 de março de 2024	Gustavo Noberto _____ Campo Grande MS, 19 de março de 2024

AUTORIDADE REPRESENTANTE DO CONTROLADOR	AUTORIDADE REPRESENTANTE DO OPERADOR
Gestor Teste _____ Segurança Digital LTDA Campo Grande MS, 19 de março de 2024	Matheus Panda _____ Campo Grande MS, 19 de março de 2024