RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 27 de junho de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Empresa FoodieFlow

Operador(es): Edgar Menezes e SIlva e Luan Pereira Santos e Jobson Ribeiro Ferreira de Sousa

Encarregado: Guilherme Marchesi Endrigo

E-mail do Encarregado: (endrigo.guilherme@hotmail.com)
Telefone: (11) 91087-2222

2 - NECESSIDADE DE ELABORAR O RELATÓRIO

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) tem como objetivo aprofundar e descrever os processos de tratamento de dados pessoais que geram alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos na Lei Geral de Proteção de Dados (LGPD), bem como às liberdades civis e aos direitos fundamentais. Além disso, o relatório aborda medidas, salvaguardas e mecanismos de mitigação de risco.

Assim, o relatório visa cumprir os requisitos estabelecidos no artigo 5º, inciso II, artigo 10, parágrafo 3º, artigo 14, e artigo 42 da Lei 13.709/2018 - LGPD. Este documento é referente à empresa FoodieFlow, controladora no projeto, que possui um sistema de gerenciamento de pedidos de restaurante. O relatório busca assegurar a conformidade desse sistema com as diretrizes da referida legislação.

3 - DESCRIÇÃO DO TRATAMENTO

Relativamente à natureza, escopo, contexto e finalidade do tratamento, a CONTROLADORA informa que, diante de sua atividade principal de **serviços de alimentação**, que inclui a preparação e a venda de refeições e bebidas para consumo no local ou para entrega e retirada, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

a) coleta e trata dados pessoais e sensíveis relativos à documentação fiscal e regulatória, bem como os dados pessoais nome e email do TITULAR, para identificação do mesmo no contexto da empresa.

b) coleta e trata dados pessoais e sensíveis relativos à documentação fiscal (CPF), endereço e nome do TITULAR, quando for identificado como cliente, e quando este efetuar um pedido de compra através do nosso sistema, para fins de efetuar a entrega das refeições e efetuar a cobrança correta.

c) trata dados pessoais do TITULAR, seja este identificado como cliente ou associado, no contexto do interesse legítimo do controlador em razão de sua responsabilidade na comunicação de dados necessários para cumprir obrigações fiscais às autoridades competentes.

d) trata dados que podem causar danos patrimoniais ao TITULAR, quando este identificado como associado, referente a sigilo fiscal, bancário e tributário, para efetuar pagamentos relativos a serviços prestados pela CONTROLADORA ao TITULAR.

e) trata dados que podem causar danos patrimoniais ao TITULAR, quando este identificado como cliente, referente a sigilo fiscal, bancário e tributário, para receber pagamentos relativos aos serviços de alimentação prestados pela CONTROLADORA ao TITULAR.

Todos dados são coletados e tratados no contexto da prestação de serviços e venda de alimentos, com a finalidade do cumprimento de obrigações fiscais e tributárias, além de obrigações acessórias exigidas pela legislação brasileira.

4 - PARTES INTERESSADAS CONSULTADAS

1. Entidades legais consultadas
    1. FoodieFlow, representado por XPTO, especialista em tributação no contexto da LGPD; XYZ, especialista em avaliação de segurança de dados pessoais no contexto da LGPD;
    2. Secretaria Estadual de Segurança de Dados.
2. Encarregado dos dados, como citado na seção 1.
3. Especialistas de segurança da CONTROLADORA, notadamente:Ederson Ribeiro Paz.
4. Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por Jobson Ribeiro Ferreira de Souza, responsável pelo treinamento e acompanhamento do time em questões de segurança de dados e qualidade da operação.

Todas as partes interessadas participaram, em diferentes momentos, do processo de criação do presente documento. O time de operação de negócio participou na

identificação dos dados operados, no apoio à definição do contexto de operação dos dados, e foi treinado para operar os dados de acordo com a política de dados definida.

Os especialistas de segurança preparam os relatórios técnicos que serviram de base à criação da política de dados e a este relatório. O Encarregado dos dados, junto aos representantes jurídicos do CONTROLADOR, elaboraram este documento, que foi posteriormente validado com as entidades competentes.

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.

Tendo em vista que o legítimo interesse do CONTROLADOR é uma das fundamentações em razão de sua responsabilidade solidária ao TITULAR em caso de irregularidade fiscal e tributária:

- o tratamento dos dados sensíveis é indispensável ao cumprimento das exigências da legislação tributária, fiscal e trabalhista brasileira;
- não há outra base legal possível de se utilizar para alcançar o mesmo propósito;
- o processo atual de fato auxilia no propósito almejado.

Todos os dados coletados com essa finalidade são eliminados após o período exigido pela legislação, que é de 5 (cinco) anos. Enquanto perdurar esse prazo, o encarregado manterá todos os dados criptografados com chaves assimétricas, armazenados em fornecedor de nuvem, com segurança de nuvem e de implementação, e duplo fator de autenticação, inclusive para fins de recuperação de arquivos de segurança e recibos de transmissão e evidência de cumprimento de obrigação acessória e principal.

Caso haja solicitação do fim de vínculo todos os dados coletados com essa finalidade são eliminados imediatamente após solicitação de exclusão do TITULAR. As informações de privacidade aos titulares seguem as diretrizes da obrigatoriedade de se manterem arquivadas todas as evidências fiscais, tributárias e trabalhistas de todas as informações enviadas aos sistemas oficiais da autoridade tributária brasileira.

A entidade CONTROLADORA poderá, a pedido do TITULAR, transferir a ele a guarda de tais informações, ressalvadas àquelas que o próprio CONTROLADOR, por dever de ofício, deve possuir pelo período constante da legislação.

É importante constar que não há, por legislação, a retroatividade do processamento dos dados, em caso de transferência de guarda de informações. Para fins legais, o direito ao esquecimento será garantido para os dados usados em processos transacionais.

6 - IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Com objetivo de garantir a transparência no tratamento dos dados identificamos os riscos , classificados de acordo com sua probabilidade (P) e seu impacto (I). O nível de risco se dá pela multiplicação dos dois fatores. Sendo as mesmas classificadas conforme as gradações representadas pela tabela abaixo:

Classificação	Valor Representativo
Baixo	5
Médio	10
Alto	15

Sendo portanto capaz de ser representado pela matriz de probabilidade x Impacto afim de apoio abaixo:

	IMPACTO (I)		
PROBABILIDADE (P)	5	10	15
5	25	50	75
10	50	100	150
15	75	150	225

Finalmente dessa forma foram identificados como risco e categorizados conforme explicado:

Nº do Risco	Especificação do Risco	P	I	Nível de Risco
R01	Acesso não autorizado.	15	15	225
R02	Uso indevido de informações pessoais.	15	15	225
R03	Desfiguração de dados por falha de software	5	10	50

R04	Indisponibilidade do sistema	5	5	25
R05	Remoção não autorizada.	5	10	50
R06	Informação insuficiente sobre a finalidade do tratamento	5	5	25
R07	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	15	10	150
R08	Falha/erro de processamento	15	5	75
R09	Reidentificação de dados pseudoanonimizados.	15	15	225

7 - MEDIDAS PARA TRATAR OS RISCOS

Com o objetivo de mitigação dos riscos identificados foram criadas algumas estratégias de combate a vulnerabilidade à riscos conforme abaixo:

Efeito sobre o Risco	Medida contenção do Risco	Efeito sobre o Risco	Medida aprovada
R01	Criação de política de uso; Estabelecimento de Acessos por necessidade/ Função; Processos de auditoria;	Reduzir	SIM
R02	Criação de política de uso; Estabelecimento de Acessos por necessidade/ Função; Processos de auditoria; Acordo de confidencialidade;	Reduzir	SIM
R03	Efetuar testes completos e documentados antes de iniciar o uso;	Reduzir	SIM

R04	Controle de failover para falhas que causem indisponibilidade; Monitoramento de todos os componentes da solução	Reduzir	SIM
R05	Controle de Acessos; Reforço do time de segurança da informação; Auditoria; Processo de prevenção a perda de dados;	Reduzir	SIM
R06	Criação de uma política de consentimento Clara, sempre sinalizando o TITULAR conforme mudanças;	Reduzir	SIM
R07	Anonimização quando possível do uso do dado; Política de controle de acessos; Política para reter e eliminação de dados quando solicitados;	Reduzir	SIM
R08	Processo de Validação de Dados na inserção; Testes unitários, qualidade, integração e performance a fim de garantir funcionamento adequado do sistema;	Reduzir	SIM
R09	Revisão constante quanto à análise de riscos sistêmicos; Verificação de Logs de alerta quanto ao risco;	Reduzir	SIM

8 - APROVAÇÃO

Assinaturas:

Representante do CONTROLADOR

Encarregado dos dados