

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

São Paulo, 17 de Março de 2024

1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador: Lanchonete da Rua

Operador(es): Ednei Santos, Janduy Araujo, Lucas Nishimoto, Renan Silva, Tiago Brito

Encarregado: Renan Silva

E-mail do Encarregado: renan.silva@landarua.com

Telefone: (11) 91111-2222

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

Relativamente à natureza, escopo, contexto e finalidade do tratamento, a CONTROLADORA informa que, diante de sua atividade principal de venda de alimentos, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

- a) coleta e trata dados pessoais e sensíveis relativos à autenticação do usuário (CPF, Nome, Email), quando efetuar cadastro através do totem do restaurante, para fins de criar o registro do usuário.
- b) coleta e trata dados pessoais e sensíveis relativos à autenticação do usuário (CPF, Nome, Email) quando for identificado como cliente e quando efetuar compras através do totem do restaurante, para fins de efetuar a identificação.
- c) trata dados pessoais e sensíveis relativos à autenticação do usuário (CPF, Nome, Email), quando for identificado como cliente e quando efetuar compras através do totem do restaurante, para fins de efetuar sugestões de cardápio.
- d) trata dados pessoais e sensíveis relativos à autenticação do usuário (CPF, Nome, Email), quando for identificado como cliente e quando efetuar compras através do totem do restaurante, para fins de efetuar sugestões de cupons de descontos.

- e) trata dados pessoais e sensíveis relativos à autenticação do usuário (CPF, Nome, Email) e escolhas, quando for identificado como cliente e quando efetuar compras através do totem do restaurante, para fins de análise de preferências.
- f) trata dados pessoais e sensíveis relativos identificação do usuário (CPF, nome e email) para fins de campanhas promocionais.

Todos dados são coletados e tratados no contexto da prestação de serviços e venda de produtos, com a finalidade do cumprimento de obrigações fiscais e tributárias, além de obrigações acessórias exigidas pela legislação brasileira. A título exemplificativo, porém não exaustivo, segue link das principais que envolvem dados do TITULAR - http://www.escretoresassociados.com.br/obrigacoes_lgpd.htm

4 - PARTES INTERESSADAS CONSULTADAS

1. Entidades legais consultadas
 1. Lanchonete da Rua, representado por Lispector, C., especialista em tributação no contexto da LGPD; Meireles, C., 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: Joyce J.; Cervantes, M.; Mendes Campos, P.
4. Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por Sagan, C., 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 prepararam 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 dois fornecedores de nuvem diferentes, 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.

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

Identificamos os seguintes riscos, classificados de acordo com sua probabilidade (P) e seu impacto (I). O nível de risco se dá pela multiplicação dos dois fatores. As gradações são 5 (baixo), 10 (médio) e 15 (alto).

N do Risco	Especificação do Risco	P	I	Nível de Risco
R01	Acesso não autorizado	5	5	25
R02	Operação incorreta dos dados	5	10	50
R03	Desfiguração de dados por	5	5	25

N do Risco	Especificação do Risco	P	I	Nível de Risco
R04	falha de software Indisponibilidade e do sistema de operação dos dados	5	5	25

7 - MEDIDAS PARA TRATAR OS RISCOS

Risco	Medida	Efeito sobre o risco	Medida aprovada
R01	1. Analise de Código Fonte nas esteiras de desenvolvimentos	reduzir	sim
R02	1 . Analise de dependências utilizadas pelos sistemas	reduzir	sim
R03	1. Execução de teste de vulnerabilidade (pentest) nos sistemas e infraestruturas	mitigar	sim
R04	1. Campanhas de workshops e conscientização de segurança para os times	reduzir	sim
R05	1. Implementação do WAF e IAST para fazer segurança de borda	reduzir	sim

8 - APROVAÇÃO

Assinaturas:

Representante do CONTROLADOR

Encarregado dos dados ou seu representante

X

Lanchonete da Rua
Controlador

X

Renan Silva
Encarregado