**RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS**

São Paulo, 16 de junho de 2024

**1 - IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO**

**Controlador:** Lanchonete Tech Lanches

**Operador(es):** Grupo G12 4Soat, Sistema TechLanches(Denis Barbosa de Amorim, Gabriel Lima Gomes, Mateus Aragão Oliveira, Nicolas de Oliveira Soares e Vitor de Oliveira Lupinetti)

**Encarregado:** Escritório de Advocacia FIAP

**E-mail do Encarregado:** (advocacia@fiap.com)

**Telefone:** (11) 3385-8010

**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 operar uma lanchonete, bem como dos fundamentos legais da necessidade de elaborar o relatório, esclarece que:

* Coleta e trata dados pessoais (nome, CPF, e-mail, telefone e endereço) do TITULAR para inativação de usuário. Esses dados são utilizados para identificar o cliente que realizou a inativação.
* Coleta e trata dados pessoais (nome, CPF e e-mail) do TITULAR para cadastro de usuário. Esse dados são utilizados exclusivamente para que o cliente possa se identificar e realizar pedidos de forma eficiente e personalizada.
* Coleta e trata dados pessoais (CPF) do TITULAR para identificação no totem de autoatendimento. Esse dados são utilizados exclusivamente para que o cliente possa se identificar e realizar pedidos de forma eficiente e personalizada.
* Coleta e trata dados pessoais de pagamento do TITULAR para processamento de transações, bem como para fins fiscais e tributários. Esses dados são utilizados para garantir que o cliente possa realizar pagamentos de forma segura e eficiente, além de atender às obrigações legais e regulamentares.

A coleta e o tratamento dos dados são necessários para o bom funcionamento do sistema de autoatendimento da lanchonete, proporcionando uma experiência mais rápida e conveniente para o cliente. Além disso, esses dados permitem a identificação correta do cliente para a realização de pedidos e pagamentos.

**4 - PARTES INTERESSADAS CONSULTADAS**

Entidades legais consultadas

* Secretaria Estadual de Segurança de Dados.
* Encarregado dos dados, como citado na seção 1.
* Especialistas de segurança da CONTROLADORA, notadamente: Denis Barbosa de Amorim; Gabriel Lima Gomes; Mateus Aragão Oliveira; Nicolas de Oliveira Soares e Vitor de Oliveira Lupinetti
* Time de operação de negócio (e, por conseguinte, dos dados) da CONTROLADORA, representados por Erick Muller; Jorge Doria e Douglas Martins, 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, elaborou 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 em garantir a correta identificação e pagamento por parte do TITULAR:

* O tratamento dos dados pessoais (nome, CPF e e-mail) é indispensável para a opção de identificação do cliente no totem de autoatendimento e para a realização de pagamentos de forma segura e eficiente.
* Não há outra base legal possível de se utilizar para alcançar o mesmo propósito, considerando a necessidade de permitir a opção de identificação correta do cliente para fins de pedidos e pagamentos.
* O processo atual de fato auxilia no propósito almejado, que é fornecer um serviço eficiente e personalizado ao cliente.

Os clientes têm o direito de inativar os seus dados pessoais armazenados pela lanchonete, conforme previsto na legislação aplicável. Para exercer esses direitos, o cliente pode entrar em contato com o encarregado de dados da lanchonete ou realizar a operação diretamente no sistema.

Para fins legais, o direito ao esquecimento será garantido para os dados usados em processos transacionais.

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 | 10 | 15 | 150 |
| R02 | Vazamento de dados devido a falhas na API | 5 | 15 | 75 |
| R03 | Operação incorreta dos dados | 5 | 10 | 50 |
| R04 | Desfiguração de dados por falha de software | 5 | 10 | 50 |
| R05 | Indisponibilidade do sistema de operação dos dados | 5 | 15 | 75 |

**7 - MEDIDAS PARA TRATAR OS RISCOS**

|  |  |  |  |
| --- | --- | --- | --- |
| Risco | Medida | Efeito sobre o risco | Medida aprovada |
| R01 | 1. controle do acesso lógico  2. monitoramento ativo de ações suspeitas no ambiente de operação | reduzir | sim |
| R02 | 1. Autenticação e tratamento nos dados de retorno. | reduzir | sim |
| R03 | 1. treinamento  2. redução de dados para operação | reduzir | sim |
| R04 | 1. efetuar testes completos e documentados antes de iniciar o uso | mitigar | sim |
| R05 | 1. controle de failover para falhas que causem indisponibilidade  2. monitoramento de todos os componentes da solução | reduzir | sim |

**8 - APROVAÇÃO**

**Assinaturas:**

Lanchonete Tech Lanches

Escritório de Advocacia FIAP