Relatório de Impacto à Proteção de Dados (RIPD)

Sistema de Restaurante

Data do Relatório: 20/03/2024

---

1. **Informações Gerais do Sistema:**

- **Nome da Controladora:** FIAP - SOAT1
- **Descrição:** Sistema de agendamento e controle de pedidos de restaurante.

2. **Processo de Coleta, armazenamento e tratamento de dados:**

- **Coleta de Dados:** São coletados dados como e-mail, documento fiscal (CPF), endereço de residência, telefone celular e dados de pagamento, necessários para a identificação e pagamento dos pedidos realizados pelo usuário.

- **Armazenamento de Dados**: Os dados são armazenados em banco de dados, com a devida criptografia quando necessário e regras de acesso, importante ressaltar que os dados de pagamento são coletados, mas não armazenados, diferente dos dados de autenticação.

- **Processamento de Pedidos**: Os dados são utilizados para a identificação do usuário e a devida associação com os pedidos criados pelo mesmo e seu controle.

- **Gestão de Clientes**: Gerenciamento do acesso e pedidos, notificação do *status* dos pedidos e possíveis ofertas para o usuário e identificação do endereço aonde será enviado o pedido.

- **Análise de Dados**: Os dados são analisados para obter *insights* sobre o desempenho operacional, padrões de consumo, eficácia de campanhas de marketing e outras métricas relevantes para a tomada de decisões estratégicas.

- **Segurança de Dados**: São implementadas medidas de segurança para proteger os dados contra acessos não autorizados, perda, roubo ou divulgação inadequada. Isso inclui a implementação de políticas de segurança, treinamento de funcionários e auditorias regulares de segurança.

- **Conformidade com Regulamentações**: A controladora garante o cumprimento das regulamentações de proteção de dados LGPD.

- **Consentimento do Cliente**: A controladora pede o consentimento para o uso dos dados do usuário no momento que usar os serviços fornecidos e garante que em caso de mudanças no uso dos dados o consentimento será pedido novamente ao usuário.

- **Retenção de Dados**: A controladora define políticas para a retenção e exclusão segura de dados, garantindo que os dados sejam mantidos apenas pelo tempo necessário para os fins para os quais foram coletados.

3. **Responsabilidades dos Envolvidos:**
   - **Controlador**: Responsável pelo controle e supervisão dos dados coletados, garantindo conformidade com as políticas de privacidade e regulamentos aplicáveis.

   - **Operador**: Responsável pela operação do sistema, incluindo a coleta e registro adequado dos dados dos clientes.

   - **Encarregado**: Responsável por garantir a segurança e integridade dos dados armazenados, implementando medidas de segurança da informação e monitoramento.

4. **Medidas de Segurança Implementadas:**

   - Todas as rotas do sistema passam por sistemas que validam a autenticação e permissão de acesso.

   - A infraestrutura apresenta controle de acesso e segue as melhores práticas de segurança e manutenção/revisão dos nossos sistemas. As informações dos usuários são acessadas apenas por pessoas autorizadas quando necessário.

   - São implementadas políticas de acesso e controle de permissões para garantir que apenas usuários autorizados tenham acesso aos dados do sistema.

   - O sistema passa regularmente por verificações de segurança abrangentes, incluindo avaliações de vulnerabilidades de infraestrutura e conformidade com as diretrizes da OWASP.

5. Procedimentos de Exclusão de Dados:

Os dados coletados são eliminados após 5 anos conforme exigido por lei. Durante esse período, são mantidos criptografados. As informações de privacidade seguem as diretrizes fiscais, tributárias e trabalhistas, com possibilidade de transferência ao titular sob solicitação. Não há retroatividade no processamento de dados e o direito ao esquecimento é garantido para dados usados em transações. Quando uma exclusão é solicitada, todos os dados associados ao cliente são removidos. O histórico de pedidos relacionados ao cliente será desvinculado de suas informações pessoais e atribuído a um cliente anônimo.

6. Monitoramento e Auditoria:

O sistema é monitorado regularmente quanto a possíveis violações de segurança ou acesso não autorizado aos dados dos clientes, com procedimentos de auditoria para garantir a conformidade.

7. Considerações Finais:

A controladora está em conformidade com os princípios da LGPD, incluindo legalidade, transparência, minimização de dados, exatidão, limitação de finalidade, integridade e confidencialidade.

- As políticas de privacidade e os avisos de consentimento estão claramente disponíveis para os usuários e são facilmente acessíveis.
- Mecanismos de consentimento explícito são implementados sempre que necessário para o processamento de dados pessoais.
- Procedimentos adequados estão em vigor para responder a solicitações de acesso, retificação, exclusão e portabilidade de dados.