ENTREGÁVEL 05 – PÓSTECH
FIAP

Aluno: Guilherme Munhoz Novais

RM: RM352819

SÃO PAULO – dezembro 2024

Sumário

SÃO PAULO – dezembro 2024

Relatório de Impacto à Proteção de Dados (RIPD)

1. Descrição do Sistema

- **Nome do Projeto:** FiapFastFood.
- **Arquitetura:** Microserviços utilizando o padrão Saga para coordenação de transações distribuídas.
- **Mecanismo de Comunicação:** Apache Kafka para comunicação assíncrona entre microserviços.
- **Dados Pessoais Tratados:** Nome, endereço, telefone e número de CPF.
- **Finalidade do Tratamento:** Identificação e autenticação de clientes para pedidos, comunicação e entrega de produtos.

2. Análise de Necessidade

- **Justificativa para a Coleta de Dados:**
    - **Nome:** Identificação única do cliente.
    - **Endereço:** Necessário para a entrega dos pedidos.
    - **Telefone:** Comunicação direta com o cliente sobre status de pedidos ou outras necessidades.
    - **CPF:** Garantia de autenticidade e prevenção contra fraudes.
- **Minimização de Dados:** Apenas os dados estritamente necessários para realizar os serviços de pedidos e entregas são coletados.

3. Base Legal para o Tratamento dos Dados

- O tratamento de dados pessoais está baseado no **consentimento explícito** do titular, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD), artigo 7º, inciso I. Os dados são utilizados para fins contratuais, relacionados à entrega de produtos e comunicação com os clientes.

4. Uso do Padrão Saga e Kafka

- **Descrição do Padrão Saga:** O Saga coordena a consistência de transações entre microserviços que manipulam pedidos e dados de clientes, garantindo que, mesmo com falhas parciais, as operações sejam compensadas adequadamente.
- **Comunicação via Kafka:** Kafka é utilizado para transmitir eventos entre microserviços de maneira assíncrona, facilitando a orquestração de transações distribuídas.

5. Avaliação de Riscos

- **Riscos Identificados:**
    - Vazamento de dados pessoais (nome, endereço, telefone e CPF) devido a acessos não autorizados em um ambiente distribuído.
    - Exposição de dados em comunicação entre microserviços ou através de tópicos no Kafka.
    - Problemas de segurança relacionados ao uso de eventos com dados pessoais sensíveis transmitidos pelo Kafka.

- **Impacto para o Titular dos Dados:**
    - Exposição de dados pessoais para terceiros pode resultar em fraudes, acesso indevido a informações, ou riscos à privacidade e segurança física.

- **Medidas de Mitigação:**
    - Criptografia dos dados armazenados e durante a transmissão entre microserviços e nos eventos Kafka.
    - Segregação de tópicos Kafka com controles de acesso rigorosos, limitando quem pode publicar e consumir eventos.
    - Tokenização ou mascaramento dos dados sensíveis, como CPF, nos eventos Kafka quando aplicável.

6. Medidas de Segurança

- **Criptografia:**
    - Dados de CPF e endereço são criptografados tanto em repouso quanto em trânsito.
    - Kafka é configurado para usar TLS/SSL para criptografar a comunicação entre produtores e consumidores.

- **Controle de Acesso:**
    - Autenticação e autorização rigorosas para todos os microserviços e tópicos Kafka.
    - Uso de JWTs (JSON Web Tokens) para validação de acessos aos microserviços e Kafka.

- **Monitoramento e Auditoria:**
    - Logs detalhados de todas as transações distribuídas e eventos Kafka são mantidos para auditoria e detecção de possíveis acessos não autorizados ou falhas de segurança.

7. Transferência de Dados

- **Compartilhamento com Terceiros:** Não há compartilhamento de dados com terceiros fora da arquitetura interna dos microserviços. Todos os dados são tratados internamente com garantias de segurança.

- **Transferência Internacional:** Caso haja transferência de dados para servidores fora do país, serão aplicadas medidas adequadas para garantir a conformidade com a LGPD, como o uso de cláusulas contratuais padrão.

8. Plano de Resposta a Incidentes

- **Notificação:** Em caso de violação de dados, a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados serão notificados imediatamente, conforme previsto na LGPD.
- **Medidas de Contenção:** Protocolos serão acionados para isolar incidentes e mitigar o impacto de falhas de segurança. O fluxo Saga também permite a compensação de transações em caso de falha, evitando que dados incorretos ou comprometidos sejam processados.

9. Encarregado pelo Tratamento de Dados (DPO)

- Um **Encarregado de Proteção de Dados** será designado para supervisionar a conformidade com a LGPD, agir como ponto de contato entre os titulares de dados e a empresa, e garantir a comunicação com a ANPD.