Relatório de Impacto à Proteção de Dados Pessoais

1. Introdução

Este relatório avalia o impacto do projeto sobre a proteção de dados pessoais, com foco na conformidade com legislações como a LGPD (Lei Geral de Proteção de Dados - Brasil) e a GDPR (General Data Protection Regulation - UE).

O projeto inclui:

API (Flask) que recebe imagens e processa informações sobre doenças em plantas.

Interface Cliente (Node.js/Express) que fornece acesso ao usuário final.

Docker Compose para orquestração de serviços.

2. Análise de Tratamento de Dados Pessoais

2.1 Coleta de Dados

Os serviços analisados lidam com:

Imagens enviadas via /inferencia_image (serviço servico1.py).

Mensagens de texto enviadas via /inferencia_chat (serviço servico2.py).

Risco Identificado:

Embora o projeto pareça focado em análise de doenças em plantas, caso o usuário envie imagens contendo rostos ou outros dados pessoais, a aplicação poderá armazenar ou processar informações sensíveis sem consentimento explícito.

A rota /inferencia_chat recebe mensagens de usuários, o que pode incluir dados sensíveis ou pessoais, sem nenhuma validação de conteúdo.

2.2 Armazenamento de Dados

As imagens são salvas no diretório /API/images/, garantindo que possam ser acessadas para processamento.

Ponto Importante:

Apesar de as imagens serem armazenadas, não há acesso externo a esses dados. O armazenamento ocorre apenas para que o modelo de machine learning possa realizar as inferências. Nenhuma funcionalidade do sistema expõe ou compartilha essas informações.

Risco Identificado:

Se não forem estabelecidos mecanismos de descarte periódico, os arquivos podem se acumular desnecessariamente.

Caso o sistema tenha vulnerabilidades, há um risco remoto de acesso indevido.

3. Segurança dos Dados

3.1 Falta de Autenticação

As APIs Flask não possuem autenticação. Qualquer usuário pode enviar requisições sem necessidade de credenciais.

O Express.js (server.js) não tem medidas de proteção contra acessos não autorizados.

Risco Identificado:

Ataques maliciosos podem explorar a API aberta e enviar dados inválidos ou maliciosos.

Não há restrições de IP ou autenticação para uso das rotas.

3.2 Falta de Criptografia

Não há medidas de criptografia para proteger imagens armazenadas.

Não há uso de HTTPS indicado no docker-compose.yml.

Risco Identificado:

Se os dados forem interceptados durante a transmissão (MITM Attack), podem ser expostos.

Imagens armazenadas podem ser acessadas indevidamente sem proteção, caso haja vulnerabilidades.

4. Recomendações

Para melhorar a conformidade com a LGPD e GDPR, recomenda-se:

Autenticação e Autorização

Implementar tokens JWT ou OAuth para restringir acesso à API.

Criar níveis de permissão para limitar operações críticas.

Proteção de Dados Sensíveis

Anonimizar imagens antes do armazenamento (exemplo: hash do nome do arquivo).

Não armazenar mensagens do chat ou criar um mecanismo de expiração automática.

Criptografia e Segurança

Usar SSL/TLS para todas as comunicações entre cliente e servidor.

Implementar armazenamento seguro para imagens (exemplo: AWS S3 com criptografia).

Consentimento e Transparência

Criar uma política de privacidade clara explicando como os dados são processados.

Adicionar termos de uso antes que o usuário envie imagens ou mensagens.

Proteção contra Acessos Indevidos

Limitar acessos com Rate Limiting para evitar abusos da API.

Proteger uploads com validação do tipo de arquivo e tamanho máximo permitido.

5. Conclusão

O projeto não expõe dados armazenados para terceiros e não permite acesso externo às imagens ou mensagens. No entanto, há riscos relacionados à segurança e privacidade, especialmente no armazenamento contínuo de arquivos sem criptografia e na ausência de autenticação na API.

Para garantir conformidade com a LGPD e GDPR, recomenda-se implementar autenticação, criptografia e políticas claras de retenção e descarte de dados.