Cartilha de Conformidade com Privacidade por Design para o Projeto

Objetivos: Guiar a implementação desses princípios no projeto;

1. Fornecer um recurso prático e utilizável para revisar e monitorar a conformidade com a privacidade ao longo do ciclo de vida do projeto
2. Informar seus usuários sobre como o projeto lida com os princípios fundamentais de privacidade.

Entregável: Cartilha de Conformidade com a Privacidade por Design, formato PDF

Sumário

1. Introdução

Somos o Grupo 2 - Pega Gato, composto por alunos do terceiro ano do Inteli, e estamos desenvolvendo um projeto para a Aegea com o objetivo de melhorar a detecção de fraudes no consumo de água. Neste documento, fornecemos uma diretriz prática e abrangente para garantir que os princípios de Privacidade por Design (PbD) sejam incorporados em todas as fases do nosso projeto desse módulo.

Atualmente, a Aegea utiliza estratégias como verificação de padrões de consumo e fiscalização por agentes de campo. No entanto, existe uma necessidade crescente de melhorar a assertividade dessas práticas. O objetivo é desenvolver uma aplicação que utilize Machine Learning para aprimorar a detecção de fraudes e a eficácia das ações corretivas nesses casos. Sendo assim, a privacidade por design é uma abordagem importante a ser utilizada no projeto, a qual visa integrar a proteção de dados e a privacidade desde a criação e desenvolvimento do projeto, assegurando que os dados pessoais dos usuários sejam protegidos de forma satisfatória.

Nossa missão é assegurar que a privacidade dos dados seja um princípio fundamental do projeto, seguindo práticas e padrões que garantam a conformidade e a proteção dos dados em todas as etapas.

1.1 Objetivos

O objetivo do projeto é determinar a probabilidade de um comportamento de consumo ser fraudulento, considerando dados históricos e, se necessário, a influência de variáveis exógenas como índices macroeconômicos, climáticos e geográficos. A abordagem deve ser holística, garantindo que o modelo preditivo identifique fraudes e forneça informações úteis para a tomada de decisões.

2. Princípios Fundamentais de PbD

O Privacy by Design é composto por diferentes princípios, os quais norteiam a tomada de decisão, principalmente no que diz respeito à proteção da privacidade das informações, tanto dos usuários, quanto das fontes de dados. O seu principal objetivo é garantir a incorporação de princípios de privacidade desde o início do processo de desenvolvimento dos sistemas, produtos ou serviços criados. É possível, nas descrições a seguir, conferir os principais princípios adotados pelo movimento de privacidade por design:

1. **Proativo, não reativo; preventivo, não remediativo:** este princípio busca antecipar e evitar os eventos adversos relacionados à privacidade antes que eles ocorram.

2. **Privacidade como padrão:** a privacidade deve ser automaticamente protegida em qualquer sistema ou prática empresarial, sem que o usuário precise realizar qualquer ação.

3. **Privacidade incorporada no design**: a privacidade deve ser incorporada no design e arquitetura dos sistemas e práticas empresariais, tornando-se parte essencial da funcionalidade principal.

4. **Funcionalidade completa – soma positiva, não soma zero:** a privacidade por design busca acomodar todos os interesses legítimos de maneira "ganha-ganha", evitando escolhas de soma zero, como privacidade versus segurança.

5. **Segurança de ponta a ponta – proteção ao longo do ciclo de vida:** este princípio sugere que a privacidade deve ser continuamente protegida em todo todo o ciclo de vida dos dados, desde a criação até a exclusão dos mesmos.

6. **Visibilidade e transparência:** privacidade por design assegura que os processos e operações são visíveis e transparentes para todos os stakeholders, garantindo responsabilidade e confiança.

7. **Respeito pela privacidade do usuário**: os interesses do indivíduo devem ser colocados em primeiro lugar, oferecendo configurações de privacidade robustas, notificações adequadas e opções amigáveis ao usuário, centrando as operações em torno da gestão de dados pessoais do indivíduo.

3.Aplicação prática no projeto

O **primeiro princípio** que está sendo aplicado no projeto é ''Proativo e não Reativo; Preventivo, e não Remediativo ''. Em todo final de Sprint deve ser feito uma entrega que já leva em conta a privacidade do usuário. Formas de mitigar a perda de privacidade não deve ser considerado uma *feature* ou algo a ser aplicado apenas no final do projeto. Também não deve-se esperar que o parceiro atente o grupo para correções de privacidade, essa deve ser uma atenção que parte ativamente dos desenvolvedores. Todos esses pontos de atenção levam ao desenvolvimento de um MVP que já assegura a privacidade dos usuários.

O **segundo princípio** é "Privacidade como configuração padrão". Aplicando ao projeto, sem que haja um pedido prévio ou exigência, deve-se assegurar a privacidade dos usuários desde a base de dados.

O **terceiro princípio** é privacidade reforçada pelo design, em que, desde a construção o projeto não permitirá que usuários visualizem dados além dos seus.

Em direção ao **quarto princípio**, funcionalmente completo, nenhuma funcionalidade do projeto será afetada ou restringida devido à política de dados.

Aplicando o **quinto princípio** "Segurança ponta a ponta – Proteção do ciclo de vida", deve ficar claro ao usuário que ele não deve carregar dados sensíveis do usuário, isso ainda no início da aplicação. Da mesma forma, no final do modelo, não deve-se permitir que o modelo inferir conclusões que expõe por "lógica" dados sensíveis do usuário.

Visibilidade e transparência, **sexto princípio**. É possível auditar os próprios dados, bem como adicionar e atualizar novos dados.

Por fim, o **sétimo princípio** será, para nós, um ponto importante a ser considerado. Apesar de termos um usuário alvo para a utilização desse projeto, ele está sendo desenvolvido com base em dados de clientes que podem ser, ou não, comprometedores. Esses dados contam com muitas informações sensíveis, como a localização da moradia do cliente, seu comportamento de consumo de água e seus registros de fraudes. Com isso, no processo de construção do modelo de redes neurais, é fundamental que levemos em consideração, também, os interesses, necessidades e desafios enfrentados pelos clientes da Aegea.

4.Checklist de Conformidade

1. Checklist de Conformidade
    - ☐ Os riscos quanto à segurança dos dados foram avaliados?
    - ☐ O usuário está ciente da coleta de dados?
    - ☐ O planejamento foi concluído antecipadamente?
    - ☐ A proteção de dados foi integrada ao sistema?
    - ☐ Quando solicitados, são coletados apenas os dados necessários?
    - ☐ Foram utilizadas abordagens funcionais de proteção de dados?
    - ☐ As interfaces e operações são projetadas de forma a permitir decisões informadas e centradas no usuário?
    - ☐ Arquitetura segura implementada

5. Referências

https://www.ufrgs.br/cpd/wp-content/uploads/2022/05/UFRGS-Cartilha_Privacy_by_Design.pdf

https://privacy.ucsc.edu/resources/privacy-by-design--foundational-principles.pdf