12. Data Privacy and Security Plan
Zofia Pietrucha, Julia Bisewska, Michał Skoczko

Plan ochrony prywatności i bezpieczeństwa danych

1. Potencjalne zagrożenia bezpieczeństwa

- **Nieautoryzowany dostęp do danych użytkowników**
  Istnieje ryzyko, że osoby nieuprawnione uzyskają dostęp do wrażliwych danych, jeśli mechanizmy uwierzytelniania lub kontroli dostępu będą niewystarczające.
  Proponowane działania:
  - Wprowadzenie uwierzytelniania wieloskładnikowego (MFA).
  - Ograniczenie dostępu do danych poprzez zastosowanie kontroli opartej na rolach (RBAC).
  - Regularne przeglądy logów dostępu w celu identyfikacji podejrzanych działań.
- **Wyciek danych**
  Możliwe są wycieki danych spowodowane lukami w zabezpieczeniach systemu, np. niezałatanymi błędami w oprogramowaniu, atakami SQL injection czy phishingiem.
  Proponowane działania:
  - Regularna aktualizacja oprogramowania i usuwanie znanych podatności.
  - Zabezpieczenie bazy danych poprzez używanie zapytań parametryzowanych.
  - Szkolenie personelu w zakresie rozpoznawania prób phishingowych.
- **Ataki typu man-in-the-middle (MITM)**
  Dane przesyłane między klientem a serwerem mogą być przechwytywane przez osoby trzecie.
  Proponowane działania:
  - Wymuszenie stosowania HTTPS oraz szyfrowania TLS.
  - Użycie protokołu HSTS w celu eliminacji ryzyka przejścia na niezabezpieczone połączenie.
  - Wdrożenie mechanizmów uwierzytelniania tokenowego dla API.

2. Zgodność z przepisami ochrony danych

Plan zakłada pełną zgodność z przepisami RODO poprzez wdrożenie następujących działań:

- **Minimalizacja zbieranych danych** – ograniczenie zbierania informacji do tych niezbędnych do działania systemu.
- **Realizacja praw użytkowników** – udostępnienie narzędzi umożliwiających dostęp, poprawianie lub usuwanie danych osobowych.
- **Regularne audyty** – okresowe przeglądy procedur przetwarzania danych pod kątem zgodności z RODO.

Dodatkowo, zostaną podpisane umowy powierzenia przetwarzania danych (DPA) z zewnętrznymi dostawcami oraz wyznaczony inspektor ochrony danych (IOD).

3. Certyfikaty i audyty

Aby zapewnić zgodność z międzynarodowymi standardami bezpieczeństwa, planuje się uzyskanie następujących certyfikatów:

- ISO/IEC 27001 – standard zarządzania bezpieczeństwem informacji.
- SOC 2 – zgodność w zakresie ochrony danych klientów.

Zewnętrzne audyty będą przeprowadzane raz w roku, a wewnętrzne przeglądy co kwartał.

4. Testy bezpieczeństwa

W celu identyfikacji potencjalnych podatności zostaną przeprowadzone:

- Testy penetracyjne – symulacje ataków w celu oceny bezpieczeństwa systemu.
- Automatyczne skanowanie podatności za pomocą narzędzi takich jak OWASP ZAP.
- Przeglądy kodu – regularne analizy pod kątem zgodności z najlepszymi praktykami bezpieczeństwa.

5. Narzędzia i procedury poprawiające bezpieczeństwo

- **Szyfrowanie** – wszystkie dane wrażliwe będą szyfrowane algorytmem AES-256 (dla danych w spoczynku) oraz TLS 1.3 (dla danych w transmisji).
- **Zabezpieczenia sieciowe** – zastosowanie zapór sieciowych, systemów IDS/IPS oraz segmentacji sieci.
- **Monitoring i alerty** – wdrożenie narzędzi do monitorowania w czasie rzeczywistym oraz systemów alertów.
- **Kopie zapasowe** – regularne tworzenie zaszyfrowanych kopii zapasowych oraz testy procedur odzyskiwania danych.

ZADANIE 7

Roadmap projektu: Serwis internetowy do tworzenia złożonych badań ankietowych

Faza 1: Wstępne planowanie i analiza (1 miesiąc)

- **Kluczowe działania**:
    - Analiza potrzeb użytkowników i badanie rynku.
    - Zdefiniowanie zakresu funkcjonalności etapu pierwszego.
    - Skład zespołu: analityk biznesowy, kierownik projektu, programiści front-end i back-end.

Faza 2: Tworzenie MVP (3 miesiące)

- **Kamień milowy**: Publiczne udostępnienie serwisu umożliwiającego tworzenie prostych ankiet.
- **Opis**: Użytkownicy mogą tworzyć podstawowe ankiety z różnymi typami pytań.

- **Zależności**: Ukończenie fazy wstępnej i przygotowanie środowiska technicznego.

Faza 3: Rozbudowa funkcjonalności (6 miesięcy)

- **Kamień milowy**: Dodanie prostej logiki i bardziej zaawansowanych typów pytań.
- **Opis**: Możliwość ustawiania pomijania pytań, rozwidleń oraz bardziej zaawansowane opcje ankiet.
- **Zależności**: Stabilna wersja MVP.

Faza 4: Personalizacja wyników (3 miesiące)

- **Kamień milowy**: Możliwość dodania podziękowań i automatycznego generowania wyników.
- **Opis**: Ankiety oferują dynamiczne podsumowania wyników po ich zakończeniu.
- **Zależności**: Rozbudowana baza pytań i logiki.

Faza 5: Zaawansowana logika ankiet (6 miesięcy)

- **Kamień milowy**: Umożliwienie tworzenia ankiet z bieżącym obliczaniem wyników, rozwidleniami i dynamicznymi podmiankami pytań; wprowadzenie modelu freemium.
- **Opis**: Użytkownicy mogą budować skomplikowane scenariusze badań.
- **Zależności**: Wdrożenie prostszych form logiki ankiet w poprzednich fazach.

Faza 6: Przetwarzanie danych w serwisie (4 miesiące)

- **Kamień milowy**: Możliwość przetwarzania danych bezpośrednio w serwisie, eliminując konieczność eksportu.
- **Opis**: Wprowadzenie podstawowych funkcji obliczeniowych i filtrowania.
- **Zależności**: Usprawnienie backendu i zarządzania danymi.

Faza 7: Analiza statystyczna (6 miesięcy)

- **Kamień milowy**: Umożliwienie zaawansowanej analizy statystycznej w serwisie.
- **Opis**: Dodanie narzędzi do wizualizacji danych i podstawowych testów statystycznych.
- **Zależności**: Funkcje przetwarzania danych w fazie poprzedniej.

Faza 8: Operacje strategiczne na konkurencji (1 tydzień)

- **Kamień milowy**: Przeprowadzenie "testów odpornościowych" na serwisach konkurencji.
- **Opis**: Symulacje obciążeniowe w celu zrozumienia słabych punktów konkurencji.
- **Zależności**: Zespół ekspertów od cyberbezpieczeństwa i testów penetracyjnych.

Faza 9: Fizyczne wyłączenie konkurencji (1 noc)

- **Kamień milowy**: Zastosowanie "ekstremalnych środków wykluczenia rynkowego".
- **Opis**: Zespół operacyjny podejmuje działania mające na celu eliminację infrastruktury konkurencji w ramach legalnych możliwości.
- **Zależności**: Anonimowość operacji, brak świadków.

Faza 10: Osiągnięcie zysków (3 dni)

- **Kamień milowy**: Uzyskanie dominującej pozycji na rynku i maksymalizacja zysków.
- **Opis**: Implementacja funkcji premium dla użytkowników oraz wzrost przychodów z subskrypcji.
- **Zależności**: Brak konkurencji.