### **Plan Prywatności i Bezpieczeństwa Danych**

Plan prywatności i bezpieczeństwa danych ma na celu zidentyfikowanie potencjalnych zagrożeń związanych z ochroną danych użytkowników w aplikacji do planowania aktywności fizycznych. Dokument zawiera szczegółowy opis strategii, narzędzi oraz procesów mających na celu ochronę danych osobowych użytkowników, zapewnienie zgodności z regulacjami prawnymi (np. RODO), a także realizację testów związanych z bezpieczeństwem (np. testów penetracyjnych). Oprócz tego opisuje wdrożenie nowoczesnych narzędzi takich jak szyfrowanie, ochrona transmisji danych, a także mechanizmy monitorowania podejrzanych aktywności.

**Lista potencjalnych zagrożeń bezpieczeństwa**

**1.Nieautoryzowany dostęp do danych użytkowników**

**Opis zagrożenia:**  
Nieautoryzowany dostęp do danych oznacza możliwość, że osoby trzecie (np. cyberprzestępcy lub nieuprawnieni pracownicy) uzyskają dostęp do wrażliwych danych użytkowników. Dane te mogą obejmować:

* Lokalizację GPS (historia tras, aktywności użytkowników w czasie rzeczywistym),
* Dane osobowe zawarte w profilu użytkownika (np. imię, nazwisko, e-mail),
* Historię aktywności fizycznej użytkowników (np. zrealizowane treningi, osiągnięcia).

**Skutki takiego zagrożenia mogą obejmować:**

* Wycieki danych użytkowników, które mogą prowadzić do ich wykorzystania w celach niezgodnych z prawem (np. śledzenie użytkownika).
* Utrata zaufania użytkowników do aplikacji, co może wpłynąć na jej reputację i powodzenie na rynku.
* Możliwość wykorzystania danych do kradzieży tożsamości, oszustw finansowych lub innych działań przestępczych.
* Naruszenie regulacji prawnych, co może skutkować wysokimi karami finansowymi.

**2.Przechwycenie danych podczas przesyłania**

**Opis zagrożenia:**  
Przechwycenie danych podczas przesyłania występuje, gdy dane przesyłane między urządzeniem użytkownika a serwerami aplikacji zostaną przechwycone przez osoby trzecie. Dzieje się tak szczególnie w niezabezpieczonych sieciach Wi-Fi lub w przypadku braku odpowiedniego szyfrowania transmisji danych.

* Podsłuchania przesyłanych danych,
* Modyfikacji danych w trakcie przesyłu (tzw. ataki typu Man-in-the-Middle).

**Skutki takiego zagrożenia mogą obejmować:**

* Kradzież danych logowania użytkowników, co może umożliwić przejęcie kont użytkowników przez atakujących.
* Uzyskanie przez osoby trzecie informacji o lokalizacji użytkownika, co może prowadzić do naruszenia ich bezpieczeństwa fizycznego.
* Dostęp do danych wrażliwych, takich jak historia tras czy dane zdrowotne, które mogą zostać wykorzystane w celach przestępczych lub komercyjnych.
* Osłabienie zaufania do aplikacji, co może prowadzić do spadku liczby użytkowników.

**3.Naruszenie zgodności z RODO**

**Opis zagrożenia:**

Brak przestrzegania przepisów RODO może wynikać z braku świadomości w zakresie przepisów prawnych lub braku odpowiednich mechanizmów wspierających prawa użytkowników (np. prawo do usunięcia danych, prawo do przeniesienia danych). Aplikacja, która nie spełnia wymagań Rozporządzenia o Ochronie Danych Osobowych (RODO), naraża się na:

* Wysokie kary finansowe nakładane przez organy regulacyjne za nieprzestrzeganie przepisów ochrony danych.
* Utrata zaufania użytkowników, którzy mogą obawiać się, że ich dane nie są właściwie chronione.
* Trudności w skalowaniu aplikacji na rynki europejskie, gdzie RODO jest szczególnie restrykcyjne.
* Możliwość wystąpienia skarg użytkowników, które mogą skutkować dodatkowymi kontrolami lub pozwami sądowymi.

**Przykłady problemów z RODO:**

* Brak uzyskania świadomej zgody użytkownika na przetwarzanie jego danych,
* Uniemożliwienie użytkownikowi wglądu lub usunięcia swoich danych,
* Niejasna polityka prywatności.

**Strategie ograniczania ryzyka**

**1.Nieautoryzowany dostęp do danych użytkowników**

**Działania zapobiegawcze:**

1. **Szyfrowanie danych w spoczynku:**
   1. Wszystkie dane przechowywane na serwerach aplikacji będą szyfrowane za pomocą algorytmu AES-256, co uniemożliwi ich odczytanie przez osoby trzecie w przypadku uzyskania dostępu do bazy danych.
   2. Klucze szyfrowania będą przechowywane w bezpiecznych modułach HSM (ang. Hardware Security Module), aby zapobiec ich wyciekowi.
2. **Autoryzacja wielopoziomowa (2FA):**
   1. Wprowadzenie dwuskładnikowego uwierzytelniania (np. kod SMS, aplikacja uwierzytelniająca) dla użytkowników logujących się do aplikacji.
   2. Administratorzy i pracownicy wewnętrzni będą korzystać z jeszcze bardziej zaawansowanych metod uwierzytelniania (np. sprzętowe klucze bezpieczeństwa).
3. **Regularne testy penetracyjne:**
   1. Testy te będą regularnie przeprowadzane przez zewnętrzne zespoły ekspertów w celu identyfikacji potencjalnych luk w systemie.
   2. Raporty z testów zostaną wykorzystane do natychmiastowej poprawy zabezpieczeń.

**2.Przechwycenie danych podczas przesyłania**

**Działania zapobiegawcze:**

1. **Szyfrowanie transmisji:**
   1. Cała komunikacja między urządzeniem użytkownika a serwerem będzie chroniona za pomocą protokołów HTTPS i TLS (Transport Layer Security).
   2. Certyfikaty SSL będą regularnie aktualizowane i odnawiane.
2. **Bezpieczne sesje:**
   1. Tokeny sesji będą stosowane do autoryzacji użytkowników i automatycznie wygasały po określonym czasie nieaktywności.
   2. Tokeny będą przypisywane do konkretnych urządzeń i kryptograficznie podpisywane, aby zapobiec ich podrobieniu.
3. **Monitorowanie anomalii:**
   1. Mechanizmy analizy behawioralnej będą monitorować nietypową aktywność użytkowników i ostrzegać o potencjalnych zagrożeniach.
   2. Przykład: Próba logowania z nietypowej lokalizacji lub adresu IP spowoduje czasowe zablokowanie konta.
4. **Edukacja użytkowników:**
   1. Informowanie użytkowników o zagrożeniach związanych z używaniem niezabezpieczonych sieci Wi-Fi oraz zalecanie korzystania z sieci VPN podczas korzystania z aplikacji.

**3.Naruszenie zgodności z RODO**

**Działania zapobiegawcze:**

1. **Polityka prywatności:**
   1. Użytkownicy będą mieli dostęp do jasnej i zrozumiałej polityki prywatności, która wyjaśni:
      1. Jakie dane są zbierane,
      2. W jakim celu są przetwarzane,
      3. Jak użytkownik może zarządzać swoimi danymi.
2. **System zarządzania zgodami:**
   1. Aplikacja będzie wymagała wyraźnej zgody użytkownika na przetwarzanie jego danych podczas rejestracji.
   2. Użytkownik będzie mógł w każdej chwili zmienić swoje ustawienia prywatności i wycofać zgodę na przetwarzanie danych.
3. **Audyt zgodności:**
   1. Regularne audyty przeprowadzane przez zewnętrzne firmy specjalizujące się w ochronie danych.
   2. Raporty z audytów będą publicznie dostępne, aby budować zaufanie użytkowników.
4. **Funkcja usuwania danych:**
   1. Umożliwienie użytkownikowi usunięcia konta i wszystkich powiązanych danych w aplikacji w dowolnym momencie