**Potencjalne Ryzyka Bezpieczeństwa**

**Nieautoryzowany dostęp do danych użytkowników**

* + **Ryzyko:** Złośliwe osoby mogą uzyskać nieautoryzowany dostęp do kont użytkowników, co grozi ujawnieniem danych wrażliwych, takich jak adresy e-mail czy szczegóły płatności.
  + **Strategie minimalizacji ryzyka:**
    - Wdrożenie uwierzytelniania dwuskładnikowego (MFA).
    - Stosowanie haszowania i solenia haseł (np. bcrypt).
    - Regularny przegląd i aktualizacja zasad kontroli dostępu.

**Przejęcie danych podczas transmisji**

* + **Ryzyko:** Dane wrażliwe, takie jak szczegóły płatności czy wiadomości na czacie, mogą zostać przechwycone podczas komunikacji między aplikacją a serwerem.
  + **Strategie minimalizacji ryzyka:**
    - Wykorzystanie protokołu TLS (Transport Layer Security) do szyfrowania transmisji danych.
    - Użycie bezpiecznej komunikacji API z uwierzytelnianiem tokenowym (np. OAuth2).

**Zagrożenia wewnętrzne lub niewłaściwe wykorzystanie danych**

* + **Ryzyko:** Pracownicy lub zewnętrzni kontrahenci mogą celowo lub przypadkowo ujawnić dane użytkowników.
  + **Strategie minimalizacji ryzyka:**
    - Ograniczenie dostępu do danych wrażliwych wyłącznie do osób, które tego potrzebują.
    - Regularne szkolenia z zakresu bezpieczeństwa dla pracowników.
    - Wdrożenie logowania i monitoringu w celu wykrywania nietypowych wzorców dostępu.

**Strategie Ochrony i Zgodności**

**Zgodność z RODO**

* + Zapewnienie jasnych mechanizmów zgody na zbieranie danych.
  + Umożliwienie użytkownikom usuwania swoich danych na żądanie.
  + Prowadzenie szczegółowej dokumentacji dotyczącej przetwarzania danych.

**Anonimizacja i minimalizacja danych**

* + Przechowywanie wyłącznie danych niezbędnych do funkcjonowania aplikacji.
  + Użycie anonimowych identyfikatorów zamiast przechowywania danych osobowych w logach systemowych.

**Testy penetracyjne i audyty**

* + Regularne przeprowadzanie testów penetracyjnych w celu wykrycia luk bezpieczeństwa.
  + Zatrudnianie certyfikowanych audytorów do oceny zgodności z RODO i innymi przepisami.

**Narzędzia i Podejścia do Poprawy Bezpieczeństwa**

**Szyfrowanie:**

* + Stosowanie szyfrowania AES-256 dla wrażliwych danych przechowywanych w systemie.

**Ochrona sieci:**

* + Zastosowanie zapór sieciowych (firewall) w celu zapobiegania nieautoryzowanemu dostępowi do serwerów.
  + Użycie Web Application Firewall (WAF) do monitorowania i filtrowania ruchu HTTP.

**Monitorowanie i reagowanie na incydenty:**

* + Korzystanie z narzędzi SIEM (Security Information and Event Management) do monitorowania i generowania alertów w czasie rzeczywistym.
  + Opracowanie planu reagowania na incydenty, aby skutecznie radzić sobie z wyciekami danych.