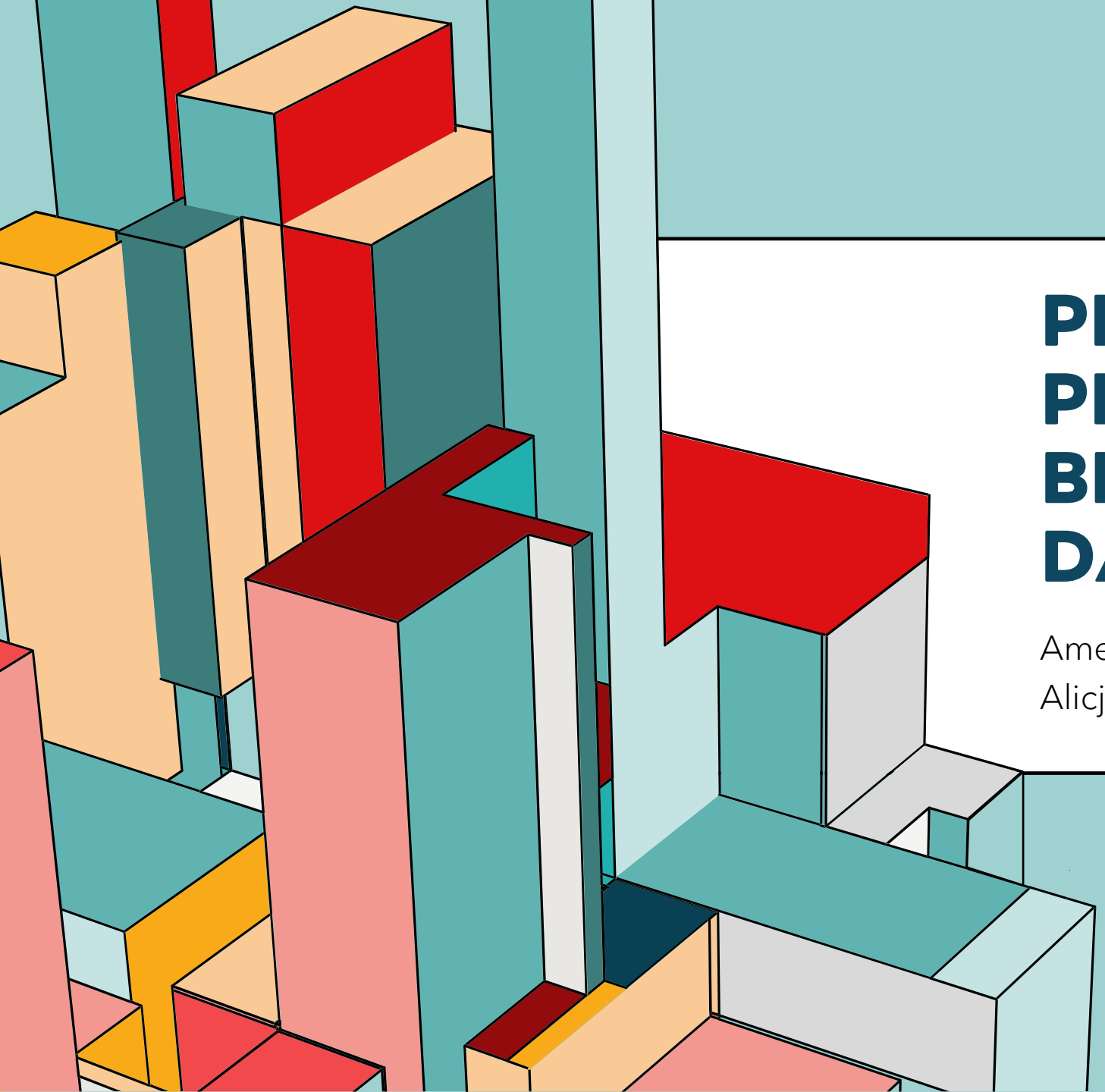


PLAN OCHRONY PRYWATNOŚCI I BEZPIECZEŃSTWA DANYCH

Amelia Hajkowska
Alicja Szulc

POTENCJALNE ZAGROŻENIA BEZPIECZEŃSTWA

Nieautoryzowany dostęp do danych użytkowników

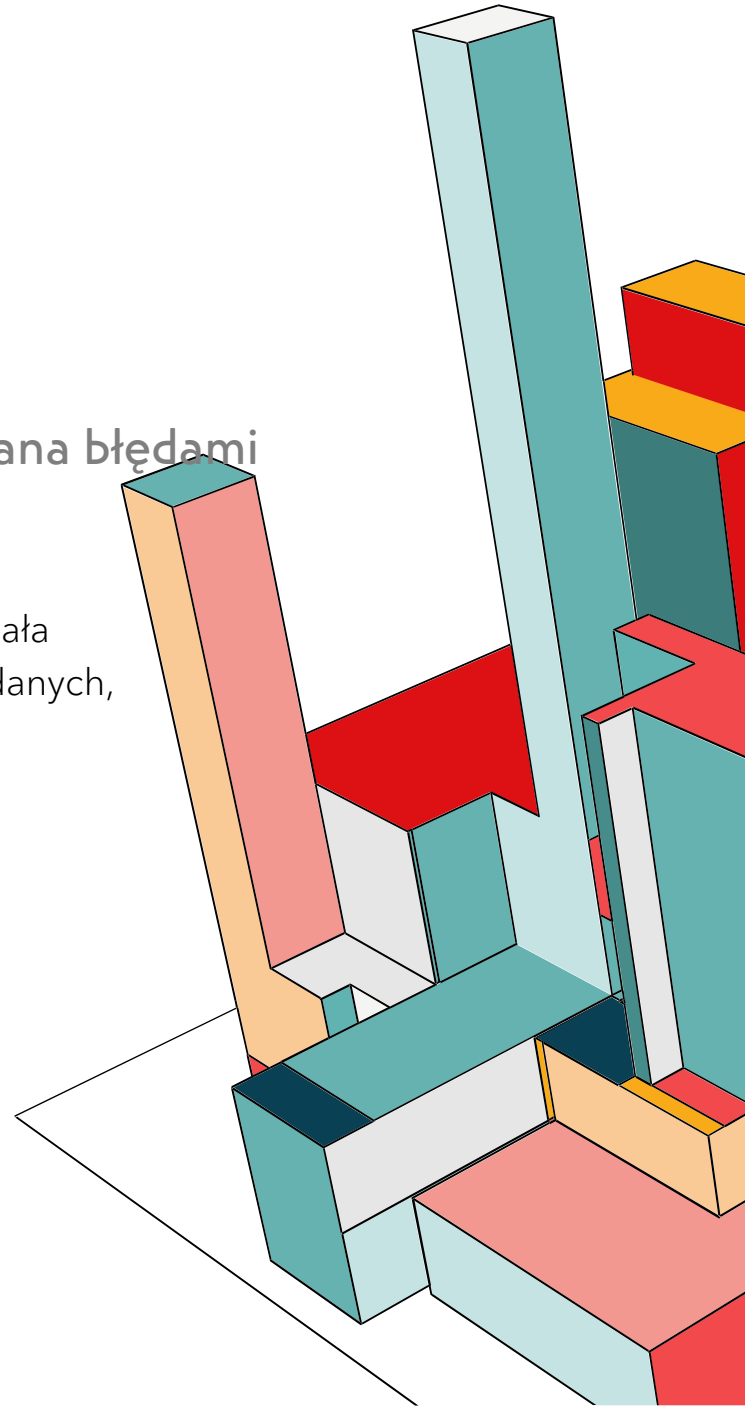
Utrata prywatnych danych użytkowników, projektów, zdjęć, które mogą być wykorzystane nielegalnie.

Ataki typu "Man-in-the-Middle" (MitM)

Komunikacja pomiędzy aplikacją a serwerem może zostać przechwycona, szczególnie podczas przesyłania wrażliwych danych (np. loginów, haseł, danych projektów).

Utrata danych spowodowana błędami synchronizacji w chmurze

Jeśli synchronizacja danych nie działa poprawnie, może dojść do utraty danych, nadpisania ich lub ich usunięcia.



STRATEGIE ŁAGODZENIA RYZYKA

Szyfrowanie danych

Wykorzystanie protokołów TLS (Transport Layer Security) do zabezpieczenia komunikacji między aplikacją a serwerem (szyfrowanie danych w trakcie transmisji).

Szyfrowanie wrażliwych danych lokalnie na urządzeniu (np. dane osobowe, zdjęcia projektów) z wykorzystaniem AES (Advanced Encryption Standard).

Autoryzacja i uwierzytelnianie

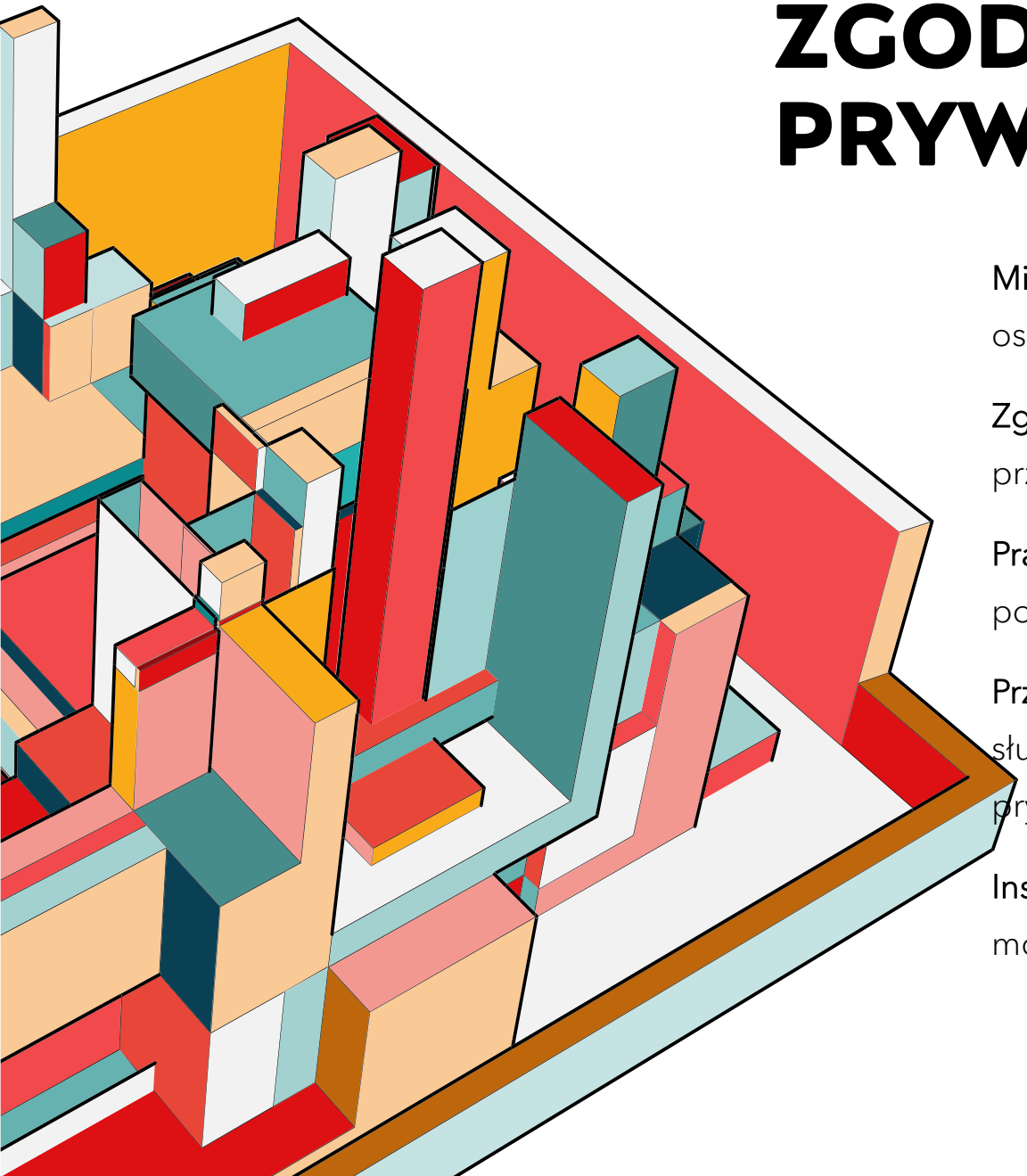
Wprowadzenie dwuetapowego uwierzytelniania (2FA) dla użytkowników, aby dodatkowo chronić dostęp do aplikacji.

Zastosowanie OAuth 2.0 lub OpenID Connect do autoryzacji użytkowników, aby uniknąć przechowywania haseł na serwerach.

Regularne aktualizacje i audyty kodu

Wdrażanie regularnych audytów bezpieczeństwa, w tym testów penetracyjnych i code review.

Regularne aktualizowanie zależności i bibliotek, aby zminimalizować ryzyko związane z wykorzystaniem przestarzałych, podatnych na ataki wersji.



ZGODNOŚĆ Z PRAWEM I PRYWATNOŚCIĄ DANYCH

Minimalizacja danych: Aplikacja będzie zbierać tylko niezbędne dane osobowe, np. e-mail, jeśli wymagana jest rejestracja.

Zgoda użytkownika: Przed zbieraniem danych użytkownik wyrazi zgodę na ich przetwarzanie, a także będzie mógł wycofać ją w dowolnym momencie.

Prawa użytkowników: Użytkownicy będą mieli prawo do dostępu, poprawiania, usunięcia oraz przenoszenia swoich danych.

Przejrzystość: Aplikacja jasno określi, jakie dane są gromadzone, do czego służą oraz jak długo będą przechowywane, zapewniając pełną politykę prywatności.

Inspektor Ochrony Danych (DPO): W przypadku dużej skali działania aplikacji może być potrzebny DPO do monitorowania zgodności z RODO.

WYMAGANE CERTYFIKACJE I AUDYTY

Certyfikacje

ISO 27001: Certyfikacja związana z zarządzaniem bezpieczeństwem informacji jest jedną z kluczowych, szczególnie dla aplikacji, które przechowują prywatne dane użytkowników i wrażliwe informacje projektowe. Spełnienie standardu ISO 27001 jest rekomendowane dla organizacji przetwarzających znaczną ilość danych.

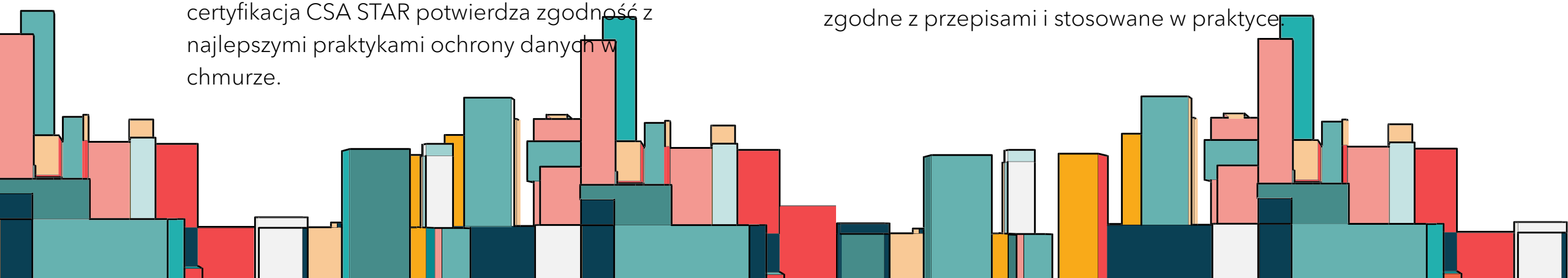
Certyfikacja CSA STAR (Cloud Security Alliance): Dla aplikacji, które przechowują dane w chmurze, certyfikacja CSA STAR potwierdza zgodność z najlepszymi praktykami ochrony danych w chmurze.

Audyty bezpieczeństwa

Testy penetracyjne: Regularnie przeprowadzane przez zewnętrznych specjalistów, aby wykryć i naprawić potencjalne luki w zabezpieczeniach.

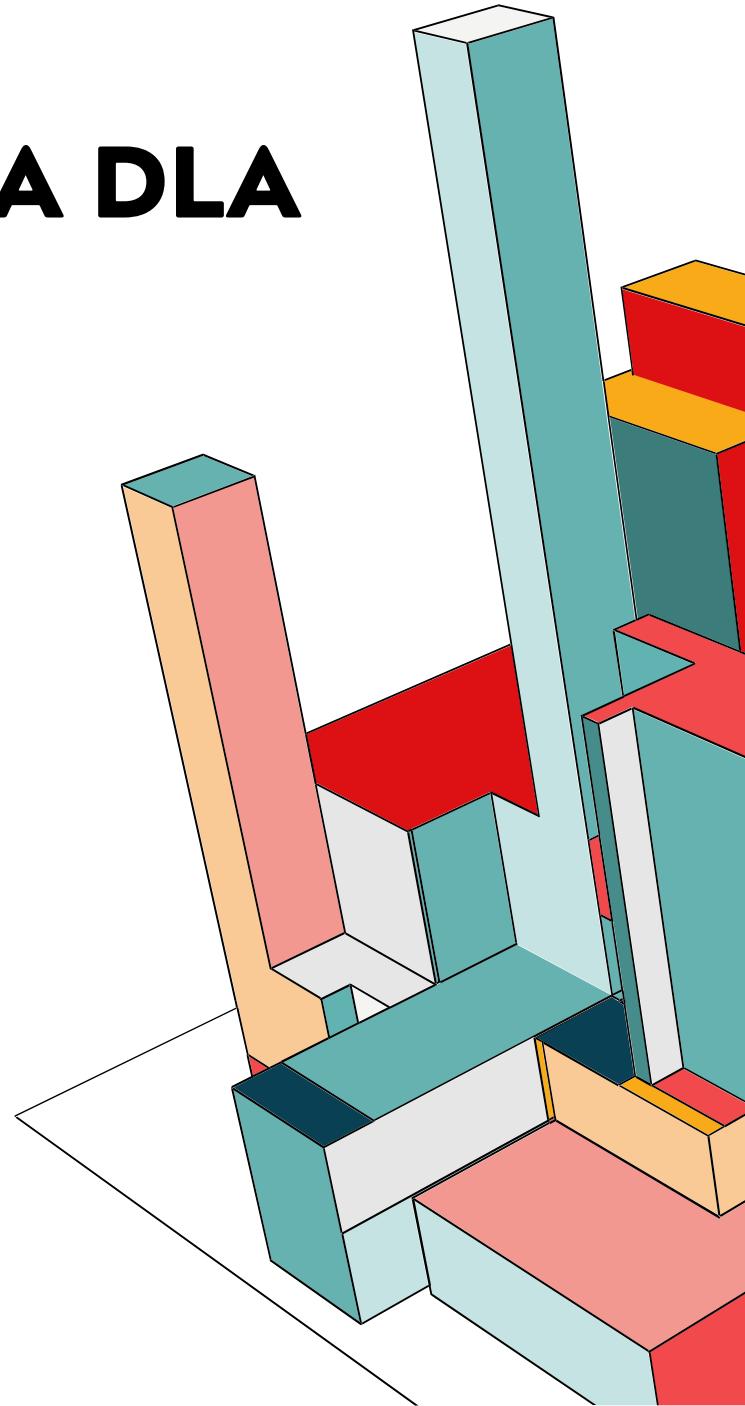
Audyty zgodności RODO: Zewnętrzne audyty zapewniają zgodność przetwarzania danych z przepisami RODO i standardami ochrony danych.

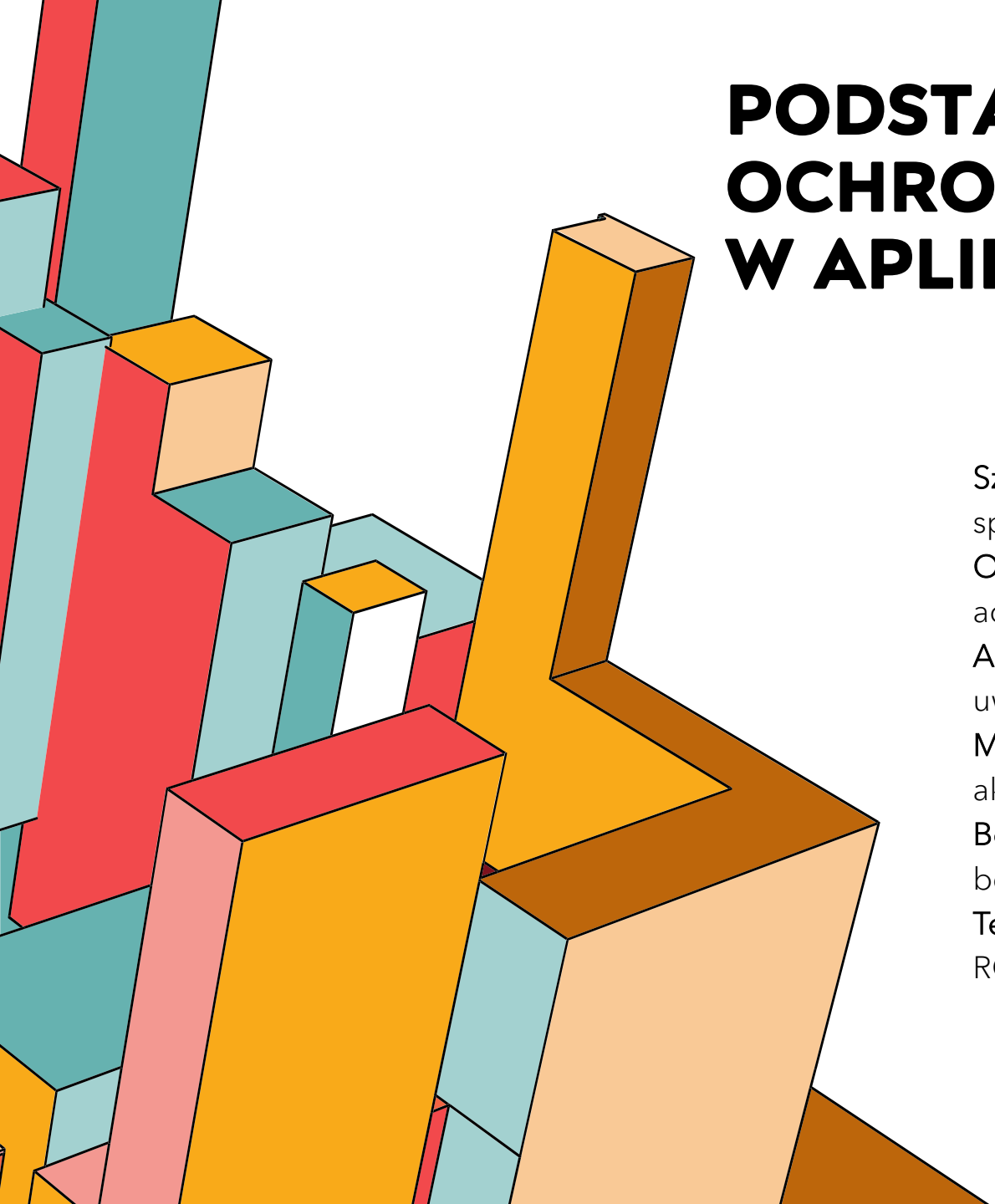
Audyt wewnętrzny: Przeprowadzany co najmniej raz w roku, by upewnić się, że wszystkie procedury bezpieczeństwa i ochrony danych są zgodne z przepisami i stosowane w praktyce.



PLAN TESTÓW BEZPIECZEŃSTWA DLA APLIKACJI

Testy penetracyjne: Regularne testy (co kwartał i po aktualizacjach) obejmujące kluczowe moduły aplikacji, jak logowanie i komunikacja z serwerem. Testy symulują różne rodzaje ataków, aby wykryć potencjalne luki.
Analiza kodu: Użycie automatycznych narzędzi oraz przegląd ręczny w celu wykrycia podatności na poziomie kodu, jak SQL injection czy XSS.
Testy infrastruktury: Skanowanie serwerów i sprawdzanie zabezpieczeń sieciowych, by zapewnić ochronę przed atakami DDoS i innymi zagrożeniami sieciowymi.
Testy mobilne: Weryfikacja uprawnień aplikacji oraz zabezpieczeń przechowywania danych na urządzeniu użytkownika.
Raporty i działania naprawcze: Po testach generowane są raporty i wdrażane poprawki w celu utrzymania zgodności z przepisami i bezpieczeństwa aplikacji.





PODSTAWOWE NARZĘDZIA I METODY OCHRONY BEZPIECZEŃSTWA DANYCH W APLIKACJI

Szyfrowanie: Zabezpieczenie danych podczas transmisji (TLS/HTTPS) oraz w spoczynku (AES). Hasła haszowane (bcrypt/SHA-256).
Ochrona sieci: Firewalle, systemy IDS/IPS oraz VPN ograniczający dostęp administracyjny.
Autoryzacja i uwierzytelnianie: OAuth 2.0, OpenID, i dwuskładnikowe uwierzytelnianie (2FA).
Monitorowanie: Narzędzia SIEM, centralne logowanie oraz analiza aktywności.
Bezpieczne API i przechowywanie: Ograniczenia liczby zapytań, tokenizacja, bezpieczne klucze.
Testy bezpieczeństwa: Regularne testy penetracyjne i audyty zgodności z RODO oraz innymi regulacjami.

DZIĘKUJEMY ZA UWAGĘ