Środki techniczne i organizacyjne zgodnie z RODO

I. Poufność (art. 32 ust. 1 lit. a + b RODO)

1. Kontrola dostępu do obszarów przetwarzania *(dostęp fizyczny)*

- Utrzymanie koncepcji bezpieczeństwa fizycznego dla lokalizacji objętych zakresem, w tym stref bezpieczeństwa fizycznego
- Zapewnienie odpowiednich środków kontroli dostępu do budynków i obszarów znajdujących się w różnych strefach bezpieczeństwa fizycznego
- Ograniczenie fizycznego dostępu do wymaganego minimum (zasada minimalnych uprawnień)
- Zapewnienie fizycznej ochrony obwodu, budynków i pomieszczeń za pomocą ogrodzenia, zabezpieczonych drzwi i zabezpieczonych okien.
- Zarządzanie kluczami i kartami dostępu
- Ograniczenie dostępu do serwerowni do ściśle ograniczonej grupy upoważnionych osób, w tym środki do wykrywania ataków
- Zarządzanie gośćmi w lokalizacjach

2. Kontrola dostępu do systemów przetwarzania danych *(uwierzytelnianie)*

- Zapewnienie personelowi obsługującego aplikację silnego uwierzytelniania użytkowników (MFA)
- Uwierzytelnianie użytkowników technicznych za pomocą bezpiecznych protokołów uwierzytelniania
- Zapewnienie uwierzytelniania sieciowego między systemami lub komponentami systemu za pomocą certyfikatu maszynowego (interfejsy)
- Umożliwienie innym aplikacjom uwierzytelniania użytkowników technicznych za pomocą bezpiecznych protokołów uwierzytelniania
- Stosowanie zasad „czystego ekranu", „czystego biurka" i „czystej ściany" w na stanowiskach i przez osoby zajmujące się przetwarzaniem danych.
- zapewnienie DMZ i bramy aplikacji dla dostępu z sieci zewnętrznych (np. Internetu)
- Wdrożenie ochrony przed złośliwym oprogramowaniem (w tym EDR klientów i serwerów).

3. Kontrola dostępu do określonych obszarów systemów przetwarzania danych *(autoryzacja)*

- Dokumentowanie koncepcji określającej role i uprawnienia
- Ograniczenie dostępu do wymaganego minimum (zasada minimalnych uprawnień)
- Zapewnienie spersonalizowanych kont użytkownikom pracującym nad aplikacją
- Zapobieganie dostępowi do aplikacji za pomocą kont domyślnych lub testowych
- Regularne kontrolowanie i unieważnianie uprawnień
- Zapewnienie oddzielnych kont administratorom zarządzającym systemami

- Zapewnienie bezpiecznego usuwania w przypadku niepotrzebnych informacji (w tym danych i fizycznych dokumentów).
- Sprawdzanie, czy aplikacje zapewniają obsługę wielu użytkowników lub wykorzystują dedykowane systemy do przetwarzania danych do różnych celów.

4. Rozdzielenie przetwarzania do różnych celów

- Korzystanie z oddzielnego środowiska programistycznego, testowego/produkcji i kontroli jakości.

5. Pseudonimizacja

- Zapewnienie usuwania danych osobowych (anonimizowanych) znajdujących się w zbiorach danych, zanim zostaną one wykorzystane w celu innym niż ten, w którym zostały pierwotnie uzyskane.

6. Szyfrowanie

- Stosowanie najnowocześniejszego szyfrowania w celu zabezpieczenia danych

II. Integralność (art. 32 ust. 1 lit. b RODO)

1. Kontrola wprowadzanych danych

- Rejestrowanie logowania i nieudanych prób logowania przez użytkowników
- Rejestrowanie działań związanych z zarządzaniem użytkownikami
- Określenie okresu przechowywania i terminu usuwania danych logowania
- Zapewnienie walidacji danych wejściowych

2. Kontrola transmisji

- Koordynowanie umów dotyczących interfejsów
- Korzystanie z najnowocześniejszych zabezpieczeń w warstwie transportowej (uwierzytelnianie i szyfrowanie) do przesyłania danych
- Oddzielenie bezpośredniego zewnętrznego dostępu do aplikacji
- Rejestrowanie przychodzącej i wychodzącej komunikacji danych
- Zapewnienie kodowania danych wyjściowych

III. Dostępność i odporność (art. 32 ust. 1 lit. b RODO)

1. Kontrola dostępności

- Wdrożenie ochrony przed złośliwym oprogramowaniem (w tym EDR na klientach i serwerach)
- Regularne uzyskiwanie/przeglądanie informacji o lukach w oprogramowaniu
- Poprawianie luk w zabezpieczeniach zgodnie z terminem na naprawę wg ich krytyczności
- Regularne identyfikowanie i korygowanie słabych punktów
- Wdrażanie kopii zapasowych zgodnie z koncepcją tworzenia kopii zapasowych
- Regularne przeprowadzanie testów przywracania kopii zapasowych
- Wykonywanie regularnie skanowania w poszukiwaniu luk i słabych punktów podczas tworzenia oprogramowania

  (statyczna i dynamiczna analiza bezpieczeństwa)

- Przeprowadzanie regularnej analizy niebezpieczeństwa pod kątem luk i słabych punktów w przypadku głównych wersji lub istotnych zmian funkcji (testy penetracyjne).
- Wykonywanie napraw zidentyfikowanych luk i słabych punktów wg ich krytyczności
- Zapewnienie rezerwowego systemu zabezpieczeń
- Zapewnienie odpowiednich fizycznych środków gwarantujących ciągłość działania centrów danych i innej krytycznej infrastruktury IT (w tym rezerwowego zasilania, połączenia z siecią, zabezpieczenia przed wodą, środków przeciwpożarowych).
- Obsługa centralnej organizacji zarządzania podatnością na zagrożenia dla wszystkich systemów w zakresie

IV. Regularne testowanie, ocena i ewaluacja skuteczności środków technicznych i organizacyjnych wdrożonych w celu zapewnienia bezpieczeństwa przetwarzania danych (art. 32 ust. 1 lit. d RODO)

1. Zarządzanie ochroną danych

- Potwierdzenie potrzeb w zakresie ochrony (klasyfikacja bezpieczeństwa informacji dla zaangażowanych aktywów informacyjnych)
- Regularne kontrolowanie zgodności z wymaganiami dotyczącymi świadczenia usług
- Uwzględnianie specyfikacji bezpieczeństwa podczas opracowywania aplikacji (bezpieczeństwo na etapie projektowania)
- Uwzględnianie wymogów ochrony danych podczas opracowywania usługi lub aplikacji (uwzględnianie ochrony prywatności w fazie projektowania)
- Zapewnienie zgodności z wymogami i zasadami podczas korzystania z oprogramowania open source
- Planowanie i dokumentowanie cyklu życia oprogramowania aplikacji
- Podnoszenie świadomości administratorów aplikacji w zakresie bezpieczeństwa IT
- Zastosowanie systemu zarządzania bezpieczeństwem informacji (ISMS) określającego dedykowane role w zakresie bezpieczeństwa informacji, i odpowiedzialność za wdrożenie odpowiednich środków bezpieczeństwa informacji, regularną ocenę ich skuteczności, oraz dostosowywanie środków w razie potrzeby.
- Zastosowanie systemu zarządzania ochroną danych (DPMS) określającego dedykowane role w zakresie bezpieczeństwa informacji, i odpowiedzialność za wdrożenie odpowiednich środków bezpieczeństwa informacji, regularną ocenę ich skuteczności, oraz dostosowywanie środków w razie potrzeby.

2. Zarządzanie incydentami

- Definiowanie zdarzeń mających wpływ na bezpieczeństwo informacji w odniesieniu do działań użytkowników
- Używanie zsynchronizowanych znaczników czasu podczas rejestrowania działań użytkownika

- Przeprowadzanie regularnej analizy danych logowania w celu sprawdzenia, czy wystąpiły jakiekolwiek zdarzenia lub incydenty mające wpływ na bezpieczeństwo informacji.
- Prowadzenie systemu całodobowego monitorowania zapewniającego analizowanie i podejmowanie kroków w związku ze zdarzeniami mającymi wpływ na bezpieczeństwo.
- Opracowanie planu reagowania na incydenty mające wpływ na bezpieczeństwo informacji.

3. Domyślna ochrona danych (art. 25 ust. 2 RODO)

- Zapewnienie, aby gromadzone i wykorzystywane były jedynie konieczne w tym celu dane osobowe.

4. Kontrola pracy

- Zapewnienie starannego wyboru podwykonawców, zawieranie z podwykonawcami umów o przetwarzanie danych oraz przekazywanie środków technicznych i organizacyjnych do podprzetwarzania danych.
- Zapewnienie po zakończeniu umowy o świadczenie usług usuwania wszystkich danych osobowych wykorzystywanych przez podmiot przetwarzający, chyba że istnieje obowiązek przechowywania ich przez dłuższy okres czasu.
- Zapewnienie wszystkim pracownikom, którzy mają dostęp do danych aplikacji regularnych szkoleń w zakresie bezpieczeństwa informacji, w tym ich dozwolonego użycia podczas przetwarzania informacji.
- Zapewnienie, aby wszyscy pracownicy mający dostęp do danych osobowych zostali zobowiązani do zachowania poufności.