Linde Material Handling

Środki techniczne i organizacyjne zgodne z RODO

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

1. Kontrola dostępu do obszarów przetwarzania (dostęp fizyczny)
    - Utrzymywanie 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 dostępu fizycznego do niezbędnego minimum (zasada najmniejszych uprawnień)
    - Zapewnienie fizycznej ochrony terenu, budynków i pomieszczeń poprzez ogrodzenia, zabezpieczone drzwi i zabezpieczone okna
    - Zarządzanie kluczami oraz kartami dostępu
    - Ograniczenie dostępu do serwerowni do ściśle ograniczonej grupy upoważnionych osób, w tym stosowanie środków wykrywania włamań
    - Zarządzanie ruchem osób odwiedzających w lokalizacjach objętych zakresem
2. Kontrola dostępu do systemów przetwarzania danych (uwierzytelnianie)
    - Zapewnienie silnego uwierzytelniania użytkowników (MFA) dla personelu operacyjnego pracującego z aplikacją
    - Uwierzytelnianie użytkowników technicznych za pomocą bezpiecznych protokołów uwierzytelniania
    - Zapewnienie uwierzytelniania sieciowego pomiędzy systemami lub ich komponentami za pomocą certyfikatów maszynowych (interfejsy)
    - Umożliwienie innym aplikacjom uwierzytelniania z wykorzystaniem użytkowników technicznych i bezpiecznych protokołów
    - Zapewnienie stosowania zasad „czystego ekranu", „czystego biurka" oraz „czystej przestrzeni roboczej" w lokalizacjach i przez osoby objęte usługami przetwarzania danych
    - Zapewnienie strefy DMZ oraz bramy aplikacyjnej dla dostępu z sieci zewnętrznych (np. Internetu)
    - Wdrożenie ochrony przed złośliwym oprogramowaniem (w tym EDR na stacjach roboczych i serwerach)
3. Kontrola dostępu do poszczególnych obszarów systemów przetwarzania danych (autoryzacja)
    - Dokumentowanie koncepcji ról i uprawnień
    - Ograniczenie dostępu do niezbędnego minimum (zasada najmniejszych uprawnień)
    - Stosowanie spersonalizowanych kont użytkowników dla personelu operacyjnego pracującego z aplikacją
    - Zapobieganie dostępowi do aplikacji przy użyciu kont domyślnych lub testowych
    - Stosowanie procesu regularnej weryfikacji oraz cofania uprawnień
    - Tworzenie odrębnych kont administratorów do zarządzania systemami
    - Zapewnienie bezpiecznego usuwania lub niszczenia informacji (zarówno danych, jak i dokumentów fizycznych), gdy nie są już potrzebne
    - Zapewnienie, aby aplikacje posiadały funkcjonalności wielodostępowe (multi-tenant) lub stosowanie dedykowanych systemów do przetwarzania danych w różnych celach
4. Rozdzielenie przetwarzania dla różnych celów
    - Stosowanie odrębnych środowisk: deweloperskiego, testowego/zapewnienia jakości oraz produkcyjnego
5. Pseudonimizacja
    - Zapewnienie usuwania (anonimizacji) danych osobowych ze zbiorów danych przed ich wykorzystaniem do celów innych niż te, dla których zostały pierwotnie zebrane
6. Szyfrowanie
    - Stosowanie aktualnych technologii szyfrowania w celu zabezpieczenia danych przechowywanych

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

1. Kontrola wprowadzania danych
    - Rejestrowanie logowań użytkowników oraz nieudanych prób logowania
    - Rejestrowanie działań związanych z zarządzaniem użytkownikami
    - Określenie terminów przechowywania i usuwania danych dzienników (logów)
    - Zapewnienie walidacji danych wejściowych
2. Kontrola transmisji danych
    - Uzgadnianie zasad dotyczących interfejsów
    - Stosowanie aktualnych zabezpieczeń warstwy transportowej (uwierzytelnianie i szyfrowanie) przy przesyłaniu danych
    - Oddzielenie bezpośredniego dostępu zewnętrznego 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 stacjach roboczych i serwerach)
    - Regularne pozyskiwanie informacji o podatnościach oprogramowania
    - Usuwanie podatności zgodnie z określonymi czasami reakcji, w zależności od ich krytyczności
    - Regularna identyfikacja i usuwanie słabych punktów
    - Wdrażanie kopii zapasowych zgodnie z koncepcją backupu
    - Zapewnienie regularnego testowania odtwarzania kopii zapasowyc
    - Regularne skanowanie bezpieczeństwa w celu wykrywania podatności i słabości w trakcie rozwoju (statyczna i dynamiczna analiza bezpieczeństwa)
    - Przeprowadzanie regularnych analiz bezpieczeństwa dla głównych wydań lub istotnych zmian funkcjonalnych (testy penetracyjne)
    - Usuwanie zidentyfikowanych podatności i słabości zgodnie z ich krytycznością
    - Utrzymywanie systemu zapasowego typu „cold stand-by"
    - Zapewnienie odpowiednich fizycznych środków ciągłości działania dla centrów danych oraz innej istotnej infrastruktury IT (w tym redundancji zasilania, połączeń sieciowych, ochrony przed wodą oraz systemów gaszenia pożaru)
    - Funkcjonowanie centralnej organizacji zarządzania podatnościami dla wszystkich systemów objętych zakresem

IV. Proces regularnego testowania, oceny i ewaluacji skuteczności środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych (art. 32 ust. 1 lit. d RODO)

1. Zarządzanie ochroną danych
    - Potwierdzanie poziomu potrzeby ochrony (klasyfikacja bezpieczeństwa informacji dla zaangażowanych aktywów informacyjnych)
    - Regularna weryfikacja zgodności z wymaganiami usługowymi
    - Uwzględnianie wymagań bezpieczeństwa na etapie rozwoju aplikacji (security by design)
    - Uwzględnianie wymagań ochrony danych na etapie rozwoju usługi lub aplikacji (privacy by design)
    - Zapewnienie zgodności z wymaganiami i zasadami przy korzystaniu z oprogramowania open source
    - Planowanie i dokumentowanie cyklu życia oprogramowania aplikacji
    - Podnoszenie świadomości administratorów aplikacji w zakresie bezpieczeństwa IT
    - Funkcjonowanie systemu zarządzania bezpieczeństwem informacji (ISMS) z dedykowanymi rolami odpowiedzialnymi za wdrażanie odpowiednich środków bezpieczeństwa, regularną ocenę ich skuteczności oraz ich dostosowywanie w razie potrzeby
    - Funkcjonowanie systemu zarządzania ochroną danych (DPMS) z dedykowanymi rolami odpowiedzialnymi za dokumentowanie czynności przetwarzania danych, wdrażanie odpowiednich

środków ochrony danych, regularną ocenę ich skuteczności oraz ich dostosowywanie w razie potrzeby

2. Zarządzanie reagowaniem na incydenty
    - Definiowanie zdarzeń bezpieczeństwa informacji w odniesieniu do działań użytkowników
    - Stosowanie zsynchronizowanych znaczników czasu przy rejestrowaniu działań użytkowników
    - Regularna analiza danych logów w celu sprawdzenia, czy wystąpiły zdarzenia lub incydenty bezpieczeństwa informacji
    - Funkcjonowanie organizacji reagowania na incydenty 24/7, zapewniającej terminową analizę i reakcję na zdarzenia bezpieczeństwa
    - Utrzymywanie planów reagowania na incydenty bezpieczeństwa informacji dla istotnych incydentów
3. Ochrona danych w fazie domyślnej (art. 25 ust. 2 RODO)
    - Zapewnienie, że przy zbieraniu i wykorzystywaniu danych osobowych obowiązkowe są wyłącznie dane niezbędne do realizacji określonego celu
4. Kontrola zadań (Job Control)
    - Zapewnienie starannego doboru podwykonawców, zawierania z nimi umów powierzenia przetwarzania danych oraz przekazywania im obowiązujących środków technicznych i organizacyjnych
    - Zapewnienie, że wszystkie dane osobowe przetwarzane w roli podmiotu przetwarzającego są usuwane po zakończeniu umowy o świadczenie usług, o ile przepisy prawa nie wymagają ich dłuższego przechowywania
    - Zapewnienie regularnych szkoleń z zakresu bezpieczeństwa informacji, w tym zasad dopuszczalnego użytkowania informacji, dla wszystkich pracowników mających dostęp do danych aplikacji
    - Zapewnienie, że wszyscy pracownicy mający dostęp do danych osobowych zostali zobowiązani do zachowania poufności