Opis zastosowanych środków technicznych i organizacyjnych.

Dokumentacja RODO/GDPR

Nakiedy Sp. z o.o.
ul. 3 Maja 15/4
84-200 Wejherowo

Biuro operacyjne

- zamykane pomieszczenia biurowe
- czujnik dymu
- dostęp do komputerów tylko za pomocą „mocnego" hasła
- zastosowano środki ochrony przed szkodliwym oprogramowaniem
- użyto system firewall do ochrony dostępu do sieci komputerowej
- użyto system zdalnego zarządzania urządzeniami mobilnymi w szczególności telefonami komórkowymi
- zainstalowane wygaszacze ekranu
- wykonywana jest aktualizacja aplikacji i systemów operacyjnych
- dostęp do danych osobowych następuje wyłącznie z użyciem szyfrowanych połączeń internetowych zawsze z użyciem wielostopniowej autoryzacji (nazwa użytkownika, hasło, jednorazowy token)
- żadne dane osobowe nie są przechowywane fizycznie w biurze, zarówno w formie elektronicznej jak i papierowej
- osoby mające dostęp do przetwarzanych danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych
- przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego
- osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
- monitory komputerów, na których przetwarzane są dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane
- wdrożono politykę ochrony danych osobowych
- przeprowadzane jest regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych
- ewidencjonowane są incydenty dot. bezpieczeństwa danych osobowych

Centrum danych

Korzystamy z centrum danych prowadzonego przez certyfikowaną firmę Amazon AWS Inc. Sprzęt, infrastruktura oraz organizacja spełnia najwyższe wymagania w zakresie zabezpieczeń oraz bezpieczeństwa danych co potwierdzają poniższe certyfikaty:

- SOC1/SSAE16/ISAE3402 (formerly SAS70)
- SOC2
- SOC3
- FISMA
- FedRAMP
- DODSRG Levels 2 and 4
- PCIDSSLevel1
- EU Model Clauses
- ISO9001 /ISO27001 / ISO 27017 / ISO 27018
- ITAR
- IRAP
- FIPS 140-2
- MLPS Level 3
- MTCS

Pełny zakres oraz procedury zostały opisane na stronie dostawcy:
https://aws.amazon.com/whitepapers/#security

Dodatkowo mając zdalny dostęp do infrastruktury oraz sprzętu wprowadzone zostały następujące środki:

- dostęp do serwerów możliwy jest tylko z jednego adresu IP
- komunikacja z serwerami jest szyfrowana
- dostęp do konfiguracji możliwy jest tylko po podaniu loginu, hasła oraz jednorazowego tokenu
- serwery chroni firewall, system użytkowników i praw systemu linux
- ograniczenie dostępu do poziomu poleceń systemowych w zależności od stanowiska pracy,
- oprogramowanie monitorujące pracę serwera
- codziennie, automatycznie tworzone są kopie zapasowe, w przypadku bazy danych kopie ciągłe (mirroring)
- w przypadku awarii głównego serwera bazy danych automatyczne przełączenie na jego kopie
- logi dostępu do usługi
- pełna separacja środowiska serwera www od serwera bazy danych gdzie przechowywane są dane osobowe
- inne usługi jak wysyłka poczty czy wiadomości sms w pełni odseparowane od danych osobowych
- dostęp do danych posiadają wyłącznie upoważnieni i odpowiednio przeszkoleni pracownicy
- wyznaczony została osoba nadzorująca przestrzeganie zasad ochrony przetwarzanych danych osobowych,
- pracownicy mający dostęp do zbiorów danych zostali zaznajomieni z powszechnie obowiązującymi przepisami dotyczącymi ochrony danych osobowych,
- prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych,