Procedura Naruszenia Ochrony Danych Osobowych - Dailyflex Personeelsdiensten B.V.

Ostatnia aktualizacja*: 01-01-2025*

1. Cel

Celem niniejszej procedury jest **szybkie wykrywanie**, **badanie**, **rejestrowanie**, **obsługa** oraz – w razie potrzeby – **zgłaszanie** (podejrzenia) naruszeń ochrony danych osobowych odpowiednim organom i interesariuszom, zgodnie z **Ogólnym Rozporządzeniem o Ochronie Danych (RODO)**.
Procedura ta chroni prywatność osób, których dane dotyczą, oraz zapewnia zgodność z obowiązkami prawnymi firmy **Dailyflex Personeelsdiensten B.V.**

2. Czym jest naruszenie ochrony danych?

Naruszenie ochrony danych osobowych to incydent bezpieczeństwa, w wyniku którego dane osobowe zostają utracone lub przypadkowo udostępnione osobom nieupoważnionym. Przykłady:

- Utrata pendrive'a lub laptopa zawierającego dane osobowe
- Dostęp do danych osobowych przez osobę nieupoważnioną
- Wysłanie danych osobowych do niewłaściwego odbiorcy
- Ataki hakerskie, phishingowe lub ransomware
- Wyciek danych (data exfiltration)
- Luka w oprogramowaniu

3. Zgłaszanie naruszenia

Każdy pracownik lub podmiot przetwarzający, który zauważy (możliwe) naruszenie, musi **niezwłocznie** zgłosić ten fakt do:

Osoba pierwszego kontaktu
Henriëtte van Santen
Inspektor Ochrony Danych (IOD)
T 174 - 28 72 73
M 06 - 83 02 15 26
E henriette@dailyflex.nl

Osoba drugiego kontaktu
Ronald Saarloos
Dyrektor Generalny
T 0174 - 28 72 73
M 06 - 83 02 15 26
E ronald@dailyflex.nl

Zgłoszenie powinno zawierać, jeśli to możliwe:

- Datę i godzinę wykrycia
- Krótki opis incydentu
- Zaangażowane systemy lub dane
- Imię i nazwisko zgłaszającego
- Dane kontaktowe zgłaszającego

4. Ocena zgłoszenia

IOD lub wyznaczona osoba odpowiedzialna podejmuje następujące kroki:

- **Weryfikacja**: Czy rzeczywiście doszło do naruszenia?
- **Analiza ryzyka**, zgodnie z wytycznymi holenderskiego Urzędu Ochrony Danych (AP):
    - Rodzaj wyciekłych danych (np. dane szczególne, finansowe)
    - Liczba osób, których dane dotyczą
    - Możliwe konsekwencje dla osób fizycznych
    - Stopień zabezpieczenia (np. szyfrowanie)
- **Dokumentacja**: Rejestracja incydentu w wewnętrznym rejestrze naruszeń (nawet jeśli zgłoszenie do AP nie jest wymagane)

5. Zgłoszenie do holenderskiego Urzędu Ochrony Danych (AP)

Jeśli istnieje ryzyko naruszenia praw i wolności osób fizycznych, należy dokonać zgłoszenia **w ciągu 72 godzin** za pośrednictwem: autoriteitpersoonsgegevens.nl > Melden datalek

Zgłoszenie powinno zawierać m.in.:

- Opis incydentu
- Rodzaj i zakres wyciekłych danych
- Liczbę osób, których dane dotyczą
- Podjęte lub planowane środki zaradcze
- Osobę kontaktową dla AP
- Ocenę konsekwencji

Nieprzekazanie zgłoszenia lub jego opóźnienie może skutkować karami finansowymi.

6. Informowanie osób, których dane dotyczą

Osoby, których dane dotyczą, powinny zostać **bezpośrednio poinformowane**, jeżeli istnieje wysokie ryzyko dla ich praw i wolności. Przykłady:

- Wycieki numerów BSN (odpowiednik PESEL) lub danych medycznych
- Duża liczba osób (10 lub więcej)
- Dane łatwe do nadużycia
- Inne istotne kryteria według Dailyflex

Sposoby komunikacji:

- E-mail
- List
- Telefonicznie

Treść powiadomienia:

- Zrozumiały opis naruszenia
- Możliwe konsekwencje
- Dane kontaktowe w Dailyflex
- Podjęte środki
- Zalecenia dla osoby (np. zmiana hasła)

7. Wewnętrzna rejestracja

Wszystkie naruszenia są rejestrowane, również te, które nie wymagają zgłoszenia do AP. Rejestr zawiera:

- Datę i godzinę incydentu oraz wykrycia
- Opis incydentu
- Zaangażowane systemy / pracownicy
- Rodzaj danych
- Liczba osób, których dane dotyczą
- Ocena ryzyka
- Podjęte działania
- Status zgłoszenia (do AP i/lub osób fizycznych)
- Ewaluacja (wyciągnięte wnioski)

Okres przechowywania: 2 lata

8. Zapobieganie i szkolenia

Szkolenia i zwiększanie świadomości (coroczne):

- RODO i zasady ochrony prywatności
- Rozpoznawanie naruszeń
- Procedura zgłaszania
- Praktyczne znaczenie ochrony danych

Środki techniczne i organizacyjne:

- Kontrola dostępu (role, uprawnienia)
- Silne hasła, uwierzytelnianie wieloskładnikowe (MFA), polityka haseł
- Szyfrowanie danych (w spoczynku i podczas przesyłania)
- Aktualne zapory ogniowe i programy antywirusowe
- Regularne kopie zapasowe i procedury odzyskiwania
- Testy penetracyjne (min. raz w roku)
- Zarządzanie aktualizacjami oprogramowania

Ewaluacja roczna:

- Skuteczność środków
- Analiza naruszeń
- Testowanie procedur
- Dostosowanie do zmian w prawie i technologii

9. Umowy powierzenia przetwarzania danych

Jeśli Dailyflex występuje jako podmiot przetwarzający, umowy powierzenia przetwarzania danych są okresowo weryfikowane pod kątem zgodności z niniejszą procedurą. Wszelkie odstępstwa są dokumentowane w sposób jednoznaczny.