Urząd Ochrony Danych Osobowych

Dotychczasowe doświadczenia w zakresie zgłaszania naruszeń ochrony danych osobowych i zawiadamiania o nich osób, których dane dotyczą

Tomasz Struk

Zespół Współpracy z Administratorami Danych
Urząd Ochrony Danych Osobowych

Warszawa, 14.01.2019 r.

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

PLAN PREZENTACJI

Urząd Ochrony Danych Osobowych

1. Formularz zgłaszania naruszeń.
2. Jakie są najczęściej występujące błędy w zgłoszeniach naruszeń ochrony danych osobowych?
3. Jakie działania należy podejmować w celu ograniczenia występowania najczęstszych typów naruszeń ochrony danych osobowych?

Zgłoszenie naruszenia ochrony danych osobowych **musi co najmniej**:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

(art. 33 ust. 3 RODO)

1. Typ zgłoszenia

Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie)
(np. sygnatura w Twoim wewnętrznym rejestrze naruszeń)
Kliknij tutaj, aby wprowadzić tekst.

(•) Zgłoszenie kompletne/jednorazowe	( ) Zgłoszenie wstępne	( ) Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić datę.

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- ☐ Nazwiska i imiona
- ☐ Imiona rodziców
- ☐ Data urodzenia
- ☐ Numer rachunku bankowego
- ☐ Adres zamieszkania lub pobytu
- ☐ Numer ewidencyjny PESEL
- ☐ Adres e-mail
- ☐ Nazwa użytkownika i/lub hasło
- ☐ Dane dotyczące zarobków i/lub posiadanego majątku
- ☐ Nazwisko rodowe matki
- ☐ Seria i numer dowodu osobistego
- ☐ Numer telefonu
- ☐ Wizerunek
- ☐ Inne, wskaż jakie:

Kliknij tutaj, aby wprowadzić tekst.

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

Kliknij tutaj, aby wprowadzić tekst.

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

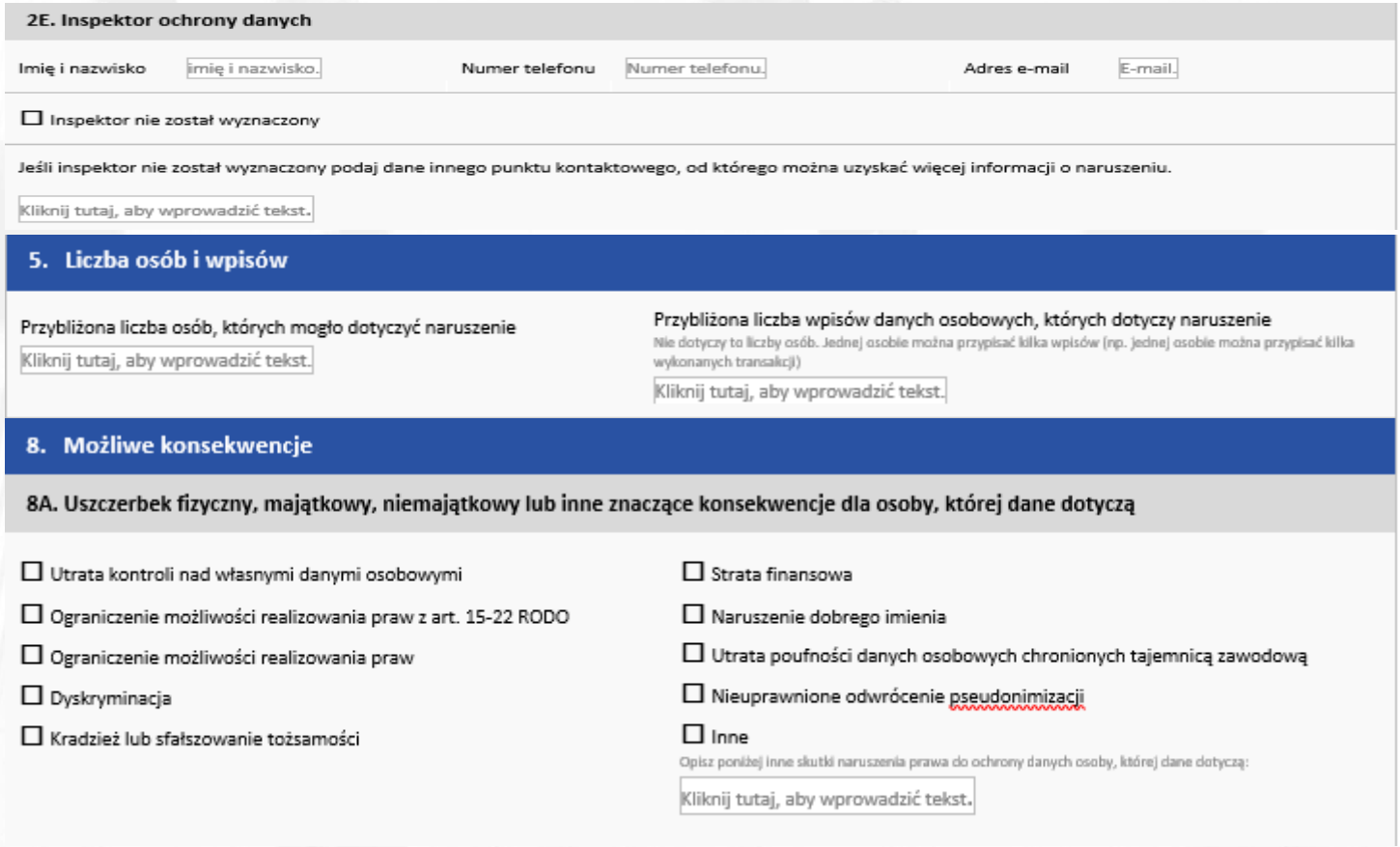
9C. Środki zastosowane lub proponowane w celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Najczęściej występujące błędy w zgłoszeniach naruszeń ochrony danych osobowych

Urząd Ochrony Danych Osobowych

Brak informacji wymaganych w art. 33 ust. 3 RODO



2E. Inspektor ochrony danych

Imię i nazwisko: imię i nazwisko. | Numer telefonu: Numer telefonu. | Adres e-mail: E-mail.

☐ Inspektor nie został wyznaczony

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

5. Liczba osób i wpisów

Przybliżona liczba osób, których mogło dotyczyć naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

Kliknij tutaj, aby wprowadzić tekst.

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- ☐ Utrata kontroli nad własnymi danymi osobowymi
- ☐ Ograniczenie możliwości realizowania praw z art. 15-22 RODO
- ☐ Ograniczenie możliwości realizowania praw
- ☐ Dyskryminacja
- ☐ Kradzież lub sfałszowanie tożsamości
- ☐ Strata finansowa
- ☐ Naruszenie dobrego imienia
- ☐ Utrata poufności danych osobowych chronionych tajemnicą zawodową
- ☐ Nieuprawnione odwrócenie pseudonimizacji
- ☐ Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

Kliknij tutaj, aby wprowadzić tekst.

Lakoniczne i nierzetelne wypełnianie zgłoszeń

Nierzetelne, zdawkowe przekazywanie informacji uniemożliwia ocenę prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych.

Najczęściej występujące błędy w zgłoszeniach naruszeń ochrony danych osobowych

Urząd Ochrony Danych Osobowych

Wypełnianie zgłoszeń w sposób rutynowy.

Najczęstsze błędy:

1. **Podanie niewłaściwej liczby osób, której dane dotyczą;**
2. **Podanie niewłaściwej kategorii danych;**
3. **Wskazanie niewłaściwego poziomu ryzyka;**
4. **Podanie niewłaściwego czasu zaistnienia naruszenia;**

Najczęściej występujące błędy w zgłoszeniach naruszeń ochrony danych osobowych

Urząd Ochrony Danych Osobowych

Brak przeprowadzenia prawidłowej oceny ryzyka naruszenia praw lub wolności osób fizycznych

Więcej informacji na temat oceny ryzyka można znaleźć w poradniku Prezesa UODO dostępnym na stronie internetowej:

https://www.uodo.gov.pl/pl/123/208

Zgłaszanie naruszenia ochrony danych osobowych przez podmiot przetwarzający.

Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.

(art. 33 ust. 2 RODO)

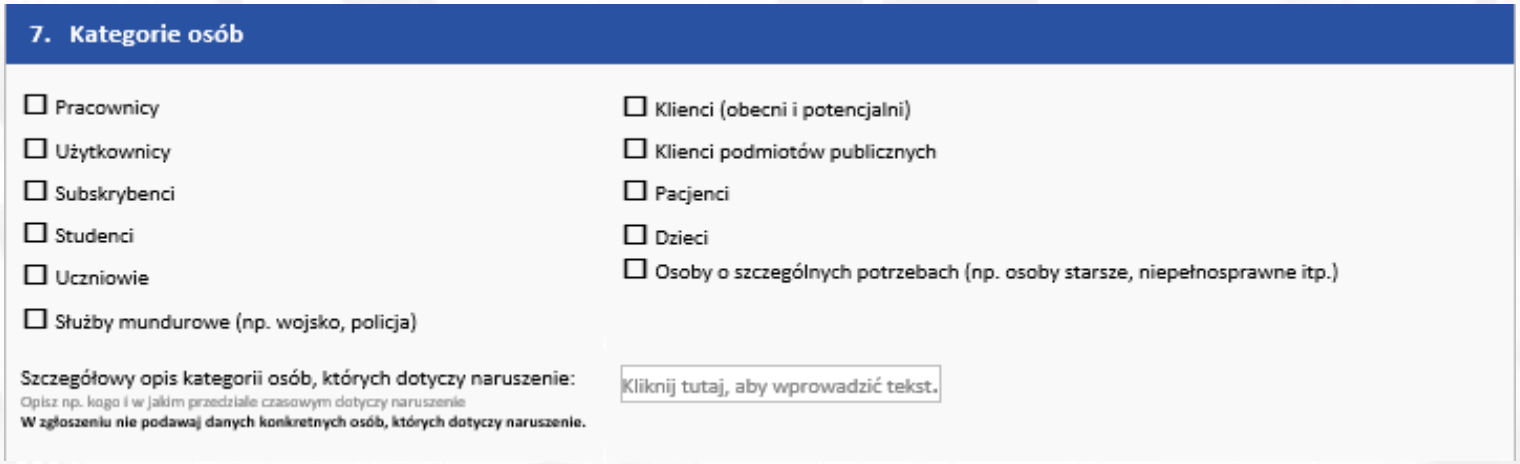
RODO zobowiązuje podmiot przetwarzający do pomagania administratorowi z wywiązania się z obowiązków określonych w art. 33 RODO np. poprzez udzielenie dostępnych mu w danej sprawie informacji.

(art. 28 ust. 3 lit. f RODO)

Najczęściej występujące błędy w zgłoszeniach naruszeń ochrony danych osobowych

Urząd Ochrony Danych Osobowych

Podanie w treści zgłoszenia danych osobowych osób, których dotyczy naruszenie.



7. Kategorie osób

- ☐ Pracownicy
- ☐ Użytkownicy
- ☐ Subskrybenci
- ☐ Studenci
- ☐ Uczniowie
- ☐ Służby mundurowe (np. wojsko, policja)
- ☐ Klienci (obecni i potencjalni)
- ☐ Klienci podmiotów publicznych
- ☐ Pacjenci
- ☐ Dzieci
- ☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie:
Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie
W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

Zgodnie z art. 33 ust. 3 RODO administrator powinien w zgłoszeniu podać tylko kategorie danych osobowych, których dotyczy naruszenie. Niewłaściwą praktyką jest podawanie w zgłoszeniu naruszenia jakichkolwiek konkretnych imion, nazwisk czy adresów zamieszkania osób, których dane dotyczą.

Nieprawidłowe zawiadamianie osób o naruszeniu ochrony danych osobowych

Zgodnie z art. 34 ust. 2 RODO prawidłowe zawiadomienie powinno:

1. jasnym i prostym językiem opisywać charakter naruszenia ochrony danych osobowych;
2. zawierać przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b, c i d RODO, czyli:
   a) imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenia innego punktu kontaktowego, od którego można uzyskać więcej informacji;
   b) opis możliwych konsekwencji naruszenia ochrony danych osobowych;
   c) opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Jakie działania należy podejmować w celu ograniczenia występowania najczęstszych typów naruszeń ochrony danych osobowych?

Urząd Ochrony Danych Osobowych

Naruszenia polegające na udostępnieniu danych osobowych nieuprawnionym osobom w związku z wysyłaniem poczty elektronicznej.

Jakie działania należy podejmować w celu ograniczenia występowania najczęstszych typów naruszeń ochrony danych osobowych?

Urząd Ochrony Danych Osobowych

Naruszenia polegające na zagubieniu lub kradzieży niezabezpieczonych (niezaszyfrowanych) urządzeń informatycznych z danymi osobowymi (smartfony, komputery przenośne).

Jakie działania należy podejmować w celu ograniczenia występowania najczęstszych typów naruszeń ochrony danych osobowych?

Urząd Ochrony Danych Osobowych

Sam fakt utraty danych osobowych w wyniku zagubienia czy kradzieży urządzeń lub nośników nie musi prowadzić do naruszenia praw lub wolności osób, których dane dotyczą, jeżeli administrator zastosował skuteczne, adekwatne środki zabezpieczenia.

W zależności od sytuacji takimi środkami mogą być:

- skuteczne szyfrowanie pamięci urządzeń/plików z danymi osobowymi (zgodne z aktualną wiedzą techniczną);
- dodatkowe (mechanizmy weryfikacji użytkownika np. hasło, PIN).

Jakie działania należy podejmować w celu ograniczenia występowania najczęstszych typów naruszeń ochrony danych osobowych?

Urząd Ochrony Danych Osobowych

Naruszenia polegające na udostępnieniu dokumentacji medycznej osobie nieuprawnionej.

Urząd Ochrony Danych Osobowych

Naruszenia polegające na zablokowaniu dostępności do danych osobowych

W przypadku, gdy komputery są podłączone do sieci internetowej, w celu ich zabezpieczenia konieczne jest:

- aktualizowanie **oprogramowania antywirusowego**;
- aktualizowanie **oprogramowania kontrolującego dostęp do komputera z zewnątrz** (firewall).

Administratorzy powinni zapewnić odpowiednie procedury, aby ich personel zwracał szczególną uwagę podczas użytkowania **nieznanych urządzeń USB** oraz zachował wzmożoną czujność przy **otwieraniu załączników poczty elektronicznej.**

Naruszenia polegające na zagubieniu przez pracowników dokumentów zawierających dane osobowe klientów

W celu eliminowania naruszeń tego typu należy:

- przy wyjazdach do klientów ograniczyć ilość dokumentacji do niezbędnego minimum (nie zabierać danego dnia dokumentacji klientów, z którymi nie jest na ten dzień umówione spotkanie);
- tam gdzie jest to możliwe przewozić dokumentację w formie elektronicznej (na zaszyfrowanych urządzeniach informatycznych).

Urząd Ochrony Danych Osobowych

Naruszenia polegające na wysyłce dokumentów na niewłaściwy adres korespondencyjny

Administrator powinien:

- przeprowadzać regularne szkolenia pracowników z zakresu ochrony danych, w tym bezpieczeństwa danych;
- wprowadzić procedury kontroli poprawności adresu przy wysyłce dokumentów zawierających dane osobowe;
- weryfikować poprawność adresu z klientem przed wysyłką dokumentów;

Urząd Ochrony Danych Osobowych

Niewłaściwa anonimizacja danych osobowych oraz niszczenie archiwalnej dokumentacji

Administrator powinien:

- przeprowadzać regularne szkolenia pracowników z zakresu ochrony danych, w tym bezpieczeństwa danych;
- wprowadzić szczegółowe instrukcje postępowania z dokumentami zawierającymi dane osobowe, w tym sposobów anonimizacji danych;
- wprowadzić wewnętrzne procedury regulujące przechowywanie archiwalnych dokumentów oraz ich późniejsze niszczenie.

Urząd
Ochrony
Danych
Osobowych

Dziękuję za uwagę

Tomasz Struk

t_struk@uodo.gov.pl