URZĄD OCHRONY DANYCH OSOBOWYCH

RODO W SZKOLNEJ ŁAWCE – VADEMECUM NARUSZEŃ

Andrzej Zielonka - Tomasz Struk
Departament Kontroli i Naruszeń
Urząd Ochrony Danych Osobowych

Warszawa, 09 czerwca 2020 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. Procedura zgłaszania naruszeń do organu nadzorczego.
2. Najczęściej występujące przykłady naruszeń w placówkach oświatowych.
3. Definicje i pojęcia związane z tematem naruszeń.
4. Naruszenie ochrony danych osobowych czy przetwarzanie niezgodne z prawem.

ZGŁASZANIE NARUSZEŃ ORGANOWI NADZORCZEMU

URZĄD OCHRONY DANYCH OSOBOWYCH

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, **chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

(art. 33 ust. 1 RODO)

ZGŁASZANIE NARUSZEŃ ORGANOWI NADZORCZEMU

URZĄD OCHRONY DANYCH OSOBOWYCH

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

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

W JAKI SPOSÓB ZAWIADOMIĆ UODO O NARUSZENIU

URZĄD 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)

FORMA ZGŁOSZENIA NARUSZENIA

Rozporządzenie 2016/679 nie precyzuje w jakiej formie należy zgłosić naruszenie do organu nadzorczego. Wymaga jedynie aby takie zgłoszenie zawierało co najmniej informacje wskazane w art. 33 ust. 3 rozporządzenia 2016/679. Oznacza to, iż administrator może zgłosić naruszenie w dowolnej formie, tj. w formie **tradycyjnej lub elektronicznej** (np. ePUAP, e-mail).

KTO POWINIEN PRZESŁAĆ ZGŁOSZENIE NARUSZENIA DO UODO

Zgodnie z przepisami ogólnego rozporządzenia o ochronie danych osobowych zgłoszenie naruszenia ochrony danych osobowych dokonuje **administrator**.

URZĘDOWY FORMULARZ ZGŁOSZENIA NARUSZENIA

URZĄD OCHRONY DANYCH OSOBOWYCH

1. Typ zgłoszenia

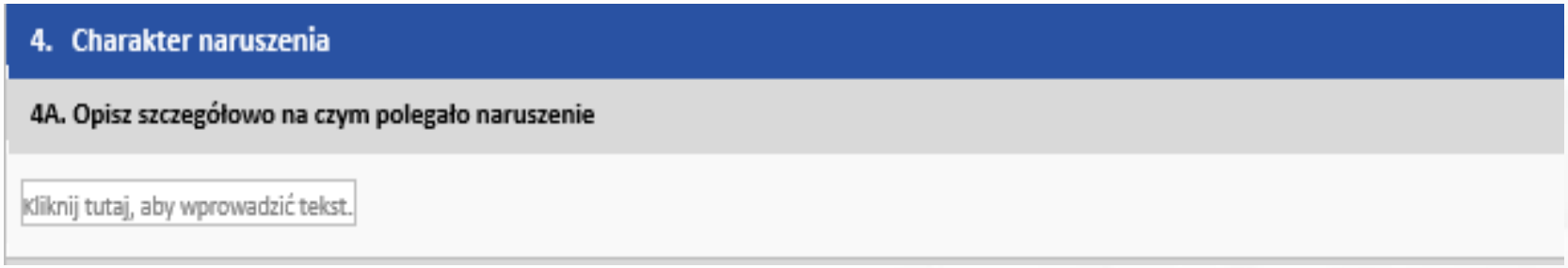
Wskaż czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze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

URZĘDOWY FORMULARZ ZGŁASZANIA NARUSZEŃ

URZĄD OCHRONY DANYCH OSOBOWYCH



URZĘDOWY FORMULARZ ZGŁOSZENIA NARUSZENIA

URZĄD OCHRONY DANYCH OSOBOWYCH

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.

URZĘDOWY FORMULARZ ZGŁASZANIA NARUSZEŃ

URZĄD OCHRONY DANYCH OSOBOWYCH

10. Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

- (•) Tak
- ( ) Nie, ale zostaną zawiadomione
  Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO.
- ( ) Nie, nie zostaną zawiadomione, ponieważ:
- ( ) Nie oceniłem jeszcze

Czy indywidualnie?

- (•) Tak
- ( ) Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został bądź zostanie wydany publiczny komunikat lub zastosowany podobny środek, za pomocą którego osoby, których dane dotyczą, zostały bądź zostaną poinformowane w równie skuteczny sposób.

Wskaż datę zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

Wskaż datę planowanego zawiadomienia
Kliknij tutaj, aby wprowadzić datę.

Liczba zawiadomionych osób
Kliknij tutaj, aby wprowadzić tekst.

☐ Nie znam jeszcze daty kiedy zamierzam zawiadomić osoby, których dane dotyczą

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą
Kliknij tutaj, aby wprowadzić tekst.

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.

Pamiętaj, że zawiadomienie powinno:

- opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Kliknij tutaj, aby wprowadzić tekst.

( ) przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

( ) po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

( ) stwierdzono brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (uzasadnienie w pkt. 8B formularza).

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

NAJCZĘŚCIEJ WYSTĘPUJĄCE TYPY NARUSZEŃ W JEDNOSTKACH OŚWIATY

URZĄD OCHRONY DANYCH OSOBOWYCH

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

NAJCZĘŚCIEJ WYSTĘPUJĄCE TYPY NARUSZEŃ W JEDNOSTKACH OŚWIATY

URZĄD OCHRONY DANYCH OSOBOWYCH

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

NAJCZĘŚCIEJ WYSTĘPUJĄCE TYPY NARUSZEŃ W JEDNOSTKACH OŚWIATY

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).

NAJCZĘŚCIEJ WYSTĘPUJĄCE TYPY NARUSZEŃ W JEDNOSTKACH OŚWIATY

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.**

NAJCZĘŚCIEJ WYSTĘPUJĄCE TYPY NARUSZEŃ W JEDNOSTKACH OŚWIATY

URZĄD OCHRONY DANYCH OSOBOWYCH

Naruszenia polegające na zagubieniu przez pracowników dokumentów zawierających dane osobowe klientów

W celu eliminowania naruszeń tego typu należy:

- przy zabieraniu dokumentacji do domu ograniczyć jej ilość do niezbędnego minimum;
- 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;

NAJCZĘŚCIEJ WYSTĘPUJĄCE TYPY NARUSZEŃ W JEDNOSTKACH OŚWIATY

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.

NAJCZĘŚCIEJ WYSTĘPUJĄCE TYPY NARUSZEŃ W JEDNOSTKACH OŚWIATY

URZĄD OCHRONY DANYCH OSOBOWYCH

Naruszenia polegające na udostępnieniu dokumentacji medycznej ucznia nieuprawnionej osobie trzeciej.

URZĄD OCHRONY DANYCH OSOBOWYCH

PRZETWARZANIE NIEZGODNE Z PRAWEM

URZĄD OCHRONY DANYCH OSOBOWYCH

PRZETWARZANIE NIEZGODNE Z PRAWEM

URZĄD OCHRONY DANYCH OSOBOWYCH

PRZETWARZANIE NIEZGODNE Z PRAWEM

URZĄD OCHRONY DANYCH OSOBOWYCH

POSTĘPOWANIE PO WYSTĄPIENIU NARUSZENIA

URZĄD OCHRONY DANYCH OSOBOWYCH

POSTĘPOWANIE PO WYSTĄPIENIU NARUSZENIA

URZĄD OCHRONY DANYCH OSOBOWYCH

POSTĘPOWANIE PO WYSTĄPIENIU NARUSZENIA

URZĄD OCHRONY DANYCH OSOBOWYCH

BARDZO DZIĘKUJEMY ZA UWAGĘ

Tomasz Struk

Andrzej Zielonka