PROCEDURA

NARUSZENIE OCHRONY DANYCH OSOBOWYCH

Szkoły Podstawowej nr 1 w Bytowie,
ul. Mierosławskiego 7, 77-100 Bytów

Data wprowadzenia:	
Wersja:	**1**
Data utworzenia:	**05.03.2026 r.**
Opracował:	**Piotr Przyborowski (IOD)**
Zatwierdził:	

SPIS TREŚCI:

1. Wprowadzenie

1) Incydent ochrony danych osobowych

a) Ustawa o ochronie danych osobowych nie definiuje wprost, czym jest incydent w ochronie danych osobowych. Szczegółowe wyjaśnienie tego pojęcia można odnaleźć w normie PN-ISO/ IEC 27001. Zgodnie z jej treścią przez incydent związany z bezpieczeństwem informacji należy rozumieć pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.

b) Można wyróżnić trzy zasadnicze grupy incydentów w ochronie danych osobowych:

- umyślne incydenty (np. kradzież danych i sprzętu, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie danych, włamanie do systemu informatycznego lub pomieszczeń),
- zdarzenia losowe wewnętrzne (np. awaria komputera/serwera/dysku twardego/oprogramowania, pomyłki informatyków, utrata danych),

- zdarzenia losowe zewnętrzne (np. pożar, zalanie wodą, utrata zasilania, utrata łączności)

2) Naruszenie danych osobowych

a) Aby zaistniało naruszenie, muszą być spełnione łącznie trzy przesłanki:

- naruszenie musi dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez podmiot, którego dotyczy naruszenie,
- skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych,
- naruszenie jest skutkiem złamania zasad bezpieczeństwa danych.

b) Rodzaje naruszeń ochrony danych osobowych:

- naruszenie poufności – polega na ujawnieniu danych osobowych nieuprawnionej osobie,
- naruszenie dostępności – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych,
- naruszenie integralności – polega na zmianie treści danych osobowych w sposób nieautoryzowany.

2. Cel procedury

Niniejsza Procedura (PNO) określa tryb i zasady postępowania osób zatrudnionych przy przetwarzaniu danych osobowych, w przypadku gdy stwierdzono naruszenie ochrony danych osobowych.

3. Zakres stosowania

Procedurę naruszeń ochrony danych osobowych stosuje się do wszelkich czynności, stanowiących w myśl RODO, przetwarzanie danych osobowych.

4. Opis postępowania

W przypadku, gdy w firmie zostaną stwierdzone zagrożenia bezpieczeństwa danych osobowych, należy przeprowadzić postępowanie wyjaśniające, w trakcie którego należy ustalić czy zagrożenie jest incydentem czy naruszeniem ochrony danych osobowych. Po tym ustaleniu należy postępować zgodnie z punktami 5 lub 6 niniejszej procedury.

5. Sposób postępowania przy incydencie ochrony danych osobowych

1) W przypadku stwierdzenia incydentu ochrony danych osobowych, osoba stwierdzająca incydent obowiązana jest niezwłocznie powiadomić o tym Administratora Danych Osobowych lub Inspektora Ochrony Danych.

2) Administrator i Inspektor Ochrony Danych po otrzymaniu powiadomienia:

a) ustalają zakres i przyczyny zagrożenia oraz jego ewentualne skutki,

b) rekomendują działania zmierzające do eliminacji podobnych zagrożeń w przyszłości,

c) Wszystkie incydenty ochrony danych osobowych rejestrowane są w Rejestrze incydentów (Załącznik PNO 5).

6. Sposób postępowania przy naruszeniu ochrony danych osobowych

1) W przypadku stwierdzenia naruszenia ochrony danych osobowych, osoba stwierdzająca naruszenie obowiązana jest niezwłocznie powiadomić o tym Inspektora Ochrony Danych.

2) Inspektor Ochrony Danych po otrzymaniu powiadomienia:

   a) podejmuje niezbędne działania mające na celu uniemożliwienie dalszego naruszenia zabezpieczenia systemu,

   b) zabezpiecza, utrwala wszelkie informacje i dokumenty, które mogą stanowić pomoc przy ustaleniu przyczyn naruszenia,

   c) ustala charakter i rodzaj naruszenia oraz metody działania osób naruszających zabezpieczenie systemu,

   d) dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,

   e) sporządza szczegółowy Raport z naruszenia (Załącznik PNO 1) zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.

3) Raport wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) Inspektor Ochrony Danych przekazuje niezwłocznie kierownikowi jednostki organizacyjnej.

4) Inspektor Ochrony Danych osobowych w porozumieniu z kierownikiem jednostki organizacyjnej podejmuje niezbędne działania w celu zapobieżenia naruszeniom zabezpieczeń systemu w przyszłości.

5) Wszystkie naruszenia ochrony danych osobowych rejestrowane są w Rejestrze naruszeń (Załącznik PNO 4).

6) Inspektor Ochrony Danych po stwierdzeniu, iż naruszenie ochrony danych osobowych spowodowało ryzyko naruszenia praw i wolności osób, których dane podlegały naruszeniu, niezwłocznie informuje o tym fakcie organ nadzorczy, ale nie dłużej niż w ciągu 72 godzin od momentu wykrycia naruszenia, za pomocą interaktywnego pliku (Załącznik PNO 3), który odpowiednio wypełniony wysyłany jest do UODO.

7) Inspektor Ochrony Danych po stwierdzeniu, iż naruszenie ochrony danych osobowych spowodowało ryzyko naruszenia praw i wolności osób, niezwłocznie informuje o tym fakcie osoby, których dane podlegały naruszeniu (Załącznik PNO 2).

8) Zawiadomienie osób, których dane dotyczą o naruszeniu ochrony danych nie jest również wymagane, gdy:

   a) Administrator wdrożył odpowiednie techniczne lub organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, które uniemożliwia odczyt danych przez osoby nieuprawnione,

   b) Administrator, po stwierdzeniu naruszenia, zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osoby, której dane dotyczą,

c) powiadomienie wszystkich osób wymagałoby niewspółmiernego wysiłku – wtedy należy wydać publiczny komunikat o zdarzeniu

7. Załączniki

1) Załącznik PNO 1 – Raport z naruszenia ochrony danych osobowych,
2) Załącznik PNO 2 - Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych,
3) Załącznik PNO 3 – Zgłoszenie naruszenia ochrony danych osobowych,
4) Załącznik PNO 4 - Przykłady potencjalnych incydentów,
5) Załącznik PNO 5 – Rejestr incydentów,
6) Załącznik PNO 6 – Rejestr naruszeń.

Załącznik PNO 1

Raport z naruszenia ochrony danych osobowych ze względu na dostępność, integralność i poufność

Sporządzający opis:……

Stanowisko:……..

1) Miejsce, dokładny czas i data naruszenia ochrony danych osobowych (piętro, nr pokoju, godzina, itp.):

……..
……..
……..
……..

2) Osoby powodujące naruszenie (które swoim działaniem lub zaniechaniem przyczyniły się do naruszenia ochrony danych osobowych):

……..
……..
……..
……..

3) Osoby, które uczestniczyły w zdarzeniu związanym z naruszeniem ochrony danych osobowych:

……..
……..
……..
……..

4) Informacje o danych, które zostały lub mogły zostać ujawnione:

……..
……..
……..
……..

5) Zabezpieczone materiały lub inne dowody związane z wydarzeniem:

……..
……..
……..
……..

6) Krótki opis wydarzenia związanego z naruszeniem ochrony danych osobowych (przebieg zdarzenia, opis zachowania uczestników, podjęte działania korekcyjne, korygujące, zapobiegawcze):

……..
……..
……..
……..

Data:..... Podpis:……

Załącznik PNO 2

Administrator Danych Osobowych

……..

……...

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Szanowny/a Pan/Pani ……

W związku z art. 34 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),

informuję o naruszeniu ochrony Pana/Pani i danych osobowych przetwarzanych przez …….

Charakter naruszenia ochrony danych osobowych	
Możliwe konsekwencje naruszenia ochrony danych osobowych	
Środki zastosowane/proponowane w celu zaradzenia naruszeniu ochrony danych / zminimalizowania negatywnych skutków*	
Imię i nazwisko Inspektora Ochrony Danych / punkt kontaktowy**	

** W zależności od przypadku, który wystąpił.*

*** W zależności od przyjętej struktury organizacyjnej.*

Zgłoszenie naruszenia 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 tekst.

☐ Naruszenie zostało lub zostanie zgłoszone organowi ochrony danych osobowych w innym państwie Jeśli tak, podaj w jakim.

☐ Naruszenie zostało lub zostanie zgłoszone innym organom np. Policja, CSIRT NASK, CSIRT GOV, CSIRT MON (najedź myszką na nazwę organu by dowiedzieć się więcej)

Podaj nazwy tych organów
Kliknij tutaj, aby wprowadzić tekst.

Podaj numer/sygnaturę zgłoszenia do innego organu
Kliknij tutaj, aby wprowadzić tekst.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora Kliknij tutaj, aby wprowadzić tekst.

REGON (opcjonalnie) Podaj numer. NIP (opcjonalnie) Podaj numer. KRS (opcjonalnie) Podaj numer.

Sektor (opcjonalnie) Dla sektora publicznego: Wybierz element. Dla sektora prywatnego: Wybierz element.

2B. Adres siedziby administratora danych

Ulica	Kliknij tutaj, aby wprowadzić tekst.	Numer domu	Podaj numer Numer lokalu Podaj numer
Miejscowość	Kliknij tutaj, aby wprowadzić tekst.	Kod pocztowy	Kliknij tutaj, aby wprowadzić tekst.
Gmina	Kliknij tutaj, aby wprowadzić tekst.	Powiat	Kliknij tutaj, aby wprowadzić tekst.
Województwo	Kliknij tutaj, aby wprowadzić tekst.	Państwo	Kliknij tutaj, aby wprowadzić tekst.

2C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
2.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
3.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

2D. Pełnomocnik

☐ Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** oraz dowód uiszczenia opłaty skarbowej

Zgłoszenie naruszenia ochrony danych osobowych

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.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
2.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
3.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
4.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.
5.	Nazwa i dane kontaktowe	Kliknij tutaj, aby wprowadzić tekst.	Rola	Kliknij tutaj, aby wprowadzić tekst.

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia
Wskaż kiedy dowiedziałeś/aś się o naruszeniu. Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa
Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający (opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h
Kliknij tutaj, aby wprowadzić tekst.

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

Data i czas zakończenia naruszenia (opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.
Kliknij tutaj, aby wprowadzić tekst.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

Zgłoszenie naruszenia ochrony danych osobowych

4B. Na czym polegało naruszenie?

☐ a) Zgubienie lub kradzież nośnika/urządzenia

☐ b) Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

☐ c) Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

☐ d) Nieuprawnione uzyskanie dostępu do informacji

☐ e) Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

☐ f) Złośliwe oprogramowanie ingerujące w poufność, integralność lub dostępność danych

☐ g) Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

☐ h) Nieprawidłowa anonimizacja danych osobowych w dokumencie

☐ i) Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

☐ j) Niezamierzona publikacja

☐ k) Dane osobowe wysłane do niewłaściwego odbiorcy

☐ l) Ujawnienie danych niewłaściwej osoby

☐ m) Ustne ujawnienie danych osobowych

4C. Działanie złośliwego oprogramowania (odpowiedz na poniższe pytania, jeśli w sekcji 4B zaznaczono pole f)

a) Jeśli w ocenie administratora doszło wyłącznie do naruszenia dostępności danych, w jaki sposób stwierdzono, że nie doszło do naruszenia ich poufności? (w sytuacji gdy np. dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu)
Kliknij tutaj, aby wprowadzić tekst.

b) Czy, a jeżeli tak, to w jakiej formie, złośliwe oprogramowanie poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (podaj nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin)
Kliknij tutaj, aby wprowadzić tekst.

c) Jeżeli doszło do utraty dostępności danych, to czy administrator był w posiadaniu kopii zapasowej, jeśli tak to w jakim czasie ją przywrócił?
Kliknij tutaj, aby wprowadzić tekst.

UWAGA: *Jeżeli zgłoszenie naruszenia dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, rozważ zgłoszenie zdarzenia do CERT Polska pod adresem https://incydent.cert.pl/. Dokonanie takiego zgłoszenia jest szczególnie zalecane w przypadku, kiedy odpowiedzi na powyższe pytania są utrudnione bądź niemożliwe.*
O fakcie zgłoszenia incydentu do CERT Polska poinformuj w zgłoszeniu uzupełniającym Prezesa UODO (pkt 1 formularza) podając datę zgłoszenia, jego numer oraz ewentualnie informacje na temat incydentu otrzymane od CERT Polska).

4D. Przyczyna naruszenia

☐ Wewnętrzne działanie niezamierzone ☐ Wewnętrzne działanie zamierzone

☐ Zewnętrzne działanie niezamierzone ☐ Zewnętrzne działanie zamierzone

4E. Charakter

☐ Naruszenie poufności danych
Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

☐ Naruszenie integralności danych
Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

☐ Naruszenie dostępności danych
Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4F. Dzieci

☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku. (opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których dotyczy 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.

Zgłoszenie naruszenia ochrony danych osobowych

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.

6B. Dane szczególnej kategorii

- ☐ Dane o pochodzeniu rasowym lub etnicznym
- ☐ Dane o poglądach politycznych
- ☐ Dane o przekonaniach religijnych lub światopoglądowych
- ☐ Dane o przynależności do związków zawodowych
- ☐ Dane dotyczące seksualności lub orientacji seksualnej
- ☐ Dane dotyczące zdrowia
- ☐ Dane genetyczne
- ☐ Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

6C. Dane, o których mowa w art. 10 RODO

- ☐ Dane dotyczące wyroków skazujących
- ☐ Dane dotyczące czynów zabronionych
- ☐ Inne

Kliknij tutaj, aby wprowadzić tekst.

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.

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.

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

Zgłoszenie naruszenia ochrony danych osobowych

◉ Tak ○ Nie

Uzasadnienie
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.

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.

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

Liczba zawiadomionych osób
Kliknij tutaj, aby wprowadzić tekst.

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.

Zgłoszenie naruszenia ochrony danych osobowych

11. Przetwarzanie transgraniczne

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Islandia	☐ Liechtenstein
☐ Litwa	☐ Luksemburg	☐ Łotwa	☐ Malta
☐ Niemcy	☐ Norwegia	☐ Portugalia	☐ Rumunia
☐ Słowacja	☐ Słowenia	☐ Szwecja	☐ Węgry
☐ Wielka Brytania	☐ Włochy		

_____

Data, miejscowość
(dla zgłoszenia w formie papierowej)

_____

Podpis osoby lub osób upoważnionych do reprezentowania administratora[1]
(dla zgłoszenia w formie papierowej)

[1] Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa

Przykłady potencjalnych incydentów:

1. Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.
2. Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych i sieci.
3. Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych przez nieuprawnione osoby.
4. Nieuprawnione modyfikowanie parametrów systemu i aplikacji.
5. Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.
6. Przechowywanie dokumentów zabezpieczonych w niedostatecznym stopniu przed dostępem osób niepowołanych.
7. Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.
8. Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.
9. Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.
10. Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.
11. Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe
12. Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.
13. Podejrzana treść wiadomości pocztowych (treść lub nadawca).
14. Ujawnianie sposobu działania aplikacji i systemu jej zabezpieczeń osobom niepowołanym.
15. Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej nieuprawnionej osobie.
16. Wyniesienie bez zgody pracodawcy dokumentów zawierających dane osobowe poza teren firmy.
17. Wydanie na makulaturę dokumentów zawierających dane osobowe.
18. Wysłanie wiadomości e-mail zawierającej dane osobowe do osoby, która nie była uprawniona do otrzymywania takich wiadomości.
19. Wysłanie wiadomości e-mail zawierającej dane osobowe do kilku odbiorców tak, że każdy odbiorca może zobaczyć adres skrzynki mailowej innych odbiorców.
20. Niewłaściwa anonimizacja danych, po której dane osobowe można nadal odczytać.

REJESTR INCYDENTÓW

Lp.	Kto zgłosił	Data zgłoszenia	Opis zdarzenia	Działania korygujące i zapobiegawcze	Odpowiedzialny za realizację	Ocena skuteczności	Czy incydent przerodził się w naruszenie
1	2	3	4	6	7	8	9

REJESTR NARUSZEŃ

Lp.	Naruszenie	Źródło zgłoszenia	Data zgłoszenia	Przyczyna niezgodności	Działania korygujące i zapobiegawcze	Odpowiedzialny za realizację	Data zakończenia	Ocena skuteczności
1	2	3	4	5	6	7	8	9