

Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych

Spis treści

I. Istota naruszenia danych osobowych	2
II. Postępowanie w przypadku naruszenia danych osobowych.....	2
III. Naruszenie danych osobowych - odpowiedzialność	4
IV. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu	4
V. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych	4
Załącznik nr 1	6
Załącznik nr 2	7
Załącznik nr 3	8

I. Istota naruszenia danych osobowych

§ 1

Incydentem w zakresie danych osobowych jest sytuacja powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Naruszeniem danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:

- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.

II. Postępowanie w przypadku naruszenia danych osobowych

§ 2

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza fakt Inspektorowi ochrony danych.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić Inspektora ochrony danych:
 - a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
 - b) dokumentacja jest niszczone bez użycia niszczarki;
 - c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
 - d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), zdjęciach, płytach CD w formie niezabezpieczonej itp.
 - e) nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem;
 - f) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
 - g) wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
 - h) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
 - i) stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
 - j) telefoniczne próby wyłudzenia danych osobowych;
 - k) kradzież komputerów lub twardych dysków z danymi osobowymi;
 - l) utrata kontroli nad kopią danych osobowych;

- m) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
- n) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
- o) istnienie nieautoryzowanych kont dostępu do danych;
- p) hasła do systemów przechowywane są w pobliżu komputera.

§ 3

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

§ 4

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora ochrony danych lub innej osoby upoważnionej przez Administratora danych.

§ 5

Każdy pracownik jest zobowiązany do informowania Administratora (Inspektora ochrony danych) o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 6

Inspektor ochrony danych podejmuje następujące kroki:

- zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
- odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
- nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

§ 7

Inspektor ochrony danych dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - Załącznik nr 1.

§ 8

Inspektor ochrony danych zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz

terminu wznowienia przetwarzania danych osobowych) - Załącznik nr 2 - rejestr incydentów i działań korygujących i zapobiegawczych

III. Naruszenie danych osobowych - odpowiedzialność

§ 9

Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

IV. Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu

§ 10

1. 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 Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorcemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – *Załącznik nr 3*.
2. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu weryfikowanie przestrzegania niniejszego artykułu.

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

§ 11

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje o których mowa w *Załączniku nr 3*

3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
- a) administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
 - b) administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;
 - c) wymagałoby ono niewspółmiernie dużego wysiłku.
- W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą, którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Raport z naruszenia ochrony danych

Data Godzina

Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):

.....

1. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):

.....
.....

2. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:

.....
.....

3. Podjęte działania:

.....
.....

4. Wstępna ocena przyczyn wystąpienia naruszenia:

.....
.....

5. Postępowanie wyjaśniające i naprawcze:

.....
.....

.....
(podpis pracownika)

.....
(data i podpis Inspektora ochrony danych)

Załącznik nr 2

Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych								
Zadanie / problem / incydent	Źródło zgłoszenia	Data rozpoczęcia	Data zakończenia	Czy koniec?	Odpowiedzialny za realizację	Przyczyna niezgodności	Działanie korygujące / zapobiegawcze	Ocena skuteczności
podać opis incydentu	podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.			czy incydent się zakończył Tak/Nie	podać dane osoby lub funkcje osoby odpowiedzialnej	podać przyczynę powstania incydentu	opisać działania jaki podjęto w celu przywrócenia bezpieczeństwa	opisać jakie skutki przyniosło działanie korygujące

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.](#)

	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.

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:

[Wpisz nazwę sektora](#)

Dla sektora prywatnego:

[Wpisz nazwę sektora](#)

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.
4.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
5.	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** (zgodnie z art. 33a KPA) oraz dowód uiszczenia opłaty skarbowej

2E. Inspektor ochrony danych

Imię i nazwisko Numer telefonu Adres e-mail

☐ Inspektor nie został wyznaczony

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

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, współadministrator, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe		Rola	
2.	Nazwa i dane kontaktowe		Rola	
3.	Nazwa i dane kontaktowe		Rola	
4.	Nazwa i dane kontaktowe		Rola	

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.

Sposób stwierdzenia naruszenia
Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu
Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Data i czas zakończenia naruszenia
(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

Kliknij tutaj, aby wprowadzić tekst.

4B. Na czym polegało naruszenie?

- | | |
|---|--|
| ☐ Zgubienie lub kradzież nośnika/urządzenia | ☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie |
| ☐ Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji | ☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora |
| ☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy | ☐ Niezamierzona publikacja |
| ☐ Nieuprawnione uzyskanie dostępu do informacji | ☐ Dane osobowe wysłane do niewłaściwego odbiorcy |
| ☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń | ☐ Ujawnienie danych niewłaściwej osoby |
| ☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych | ☐ Ustne ujawnienie danych osobowych |
| ☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing) | |

4C. Przyczyna naruszenia

- ☐ Wewnętrzne działanie niezamierzone
- ☐ Wewnętrzne działanie zamierzone
- ☐ Zewnętrzne działanie niezamierzone
- ☐ Zewnętrzne działanie zamierzone

4D. 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

4E. 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 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.

6. Kategorie danych osobowych

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

6A. Dane podstawowe

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

[Kliknij tutaj, aby wprowadzić tekst.](#)

6B. Dane szczególnej kategorii

- | | |
|---|---|
| ☐ Dane o pochodzeniu rasowym lub etnicznym | ☐ Dane dotyczące seksualności lub orientacji seksualnej |
| ☐ Dane o poglądach politycznych | ☐ Dane dotyczące zdrowia |
| ☐ Dane o przekonaniach religijnych lub światopoglądowych | ☐ Dane genetyczne |
| ☐ Dane o przynależności do związków zawodowych | ☐ 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 | ☐ Klienci (obecni i potencjalni) |
| ☐ Użytkownicy | ☐ Klienci podmiotów publicznych |
| ☐ Subskrybenci | ☐ Pacjenci |
| ☐ Studenci | ☐ Dzieci |
| ☐ Uczniowie | ☐ Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.) |
| ☐ Służby mundurowe (np. wojsko, policja) | |

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

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

[Kliknij tutaj, aby wprowadzić tekst.](#)

8B. Ryzyko naruszenia praw i wolności osób fizycznych

☐ Niskie

☐ Średnie

☒ Wysokie

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 zminimalizowania ryzyka ponownego wystąpienia naruszenia

Kliknij tutaj, aby wprowadzić tekst.

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

Kliknij tutaj, aby wprowadzić tekst.

10. Zawiadamianie osób, których dane dotyczą

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

☒ Tak

☐ Nie, ale zostaną zawiadomione

Pamiętaj, że po zawiadomieniu osób, należy przesłać treść zawiadomienia do UODO.

☐ Nie, nie zostaną zawiadomione

☐ Nie oceniłem jeszcze

Czy indywidualnie?

☒ Tak

☐ Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został wydany publiczny komunikat lub zastosowano podobny środek, za pomocą którego osoby, których dane dotyczą, zostały poinformowane w równie skuteczny sposób.

Wskaż datę kiedy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

Liczba zawiadomionych osób, których dane dotyczą

Kliknij tutaj, aby wprowadzić tekst.

Wskaż datę kiedy zamierzasz zawiadomić osoby, których dane dotyczą, o naruszeniu

Kliknij tutaj, aby wprowadzić datę.

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

Powód niezawiadomienia osób, których dane dotyczą:

☐ 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.

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

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.

11. Przetwarzanie transgraniczne i inne powiadomienie

☐ 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 | | |

☐ Naruszenie zostało lub zostanie zgłoszone innemu organowi ochrony danych osobowych (opcjonalnie)

Wymień inne organy nadzorcze ochrony danych osobowych, którym naruszenie zostało lub zostanie zgłoszone

Kliknij tutaj, aby wprowadzić tekst.

☐ Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorcemu z powodu innych zobowiązań prawnych (opcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

Kliknij tutaj, aby wprowadzić tekst.

Data, miejscowość

(dla zgłoszenia w formie papierowej)

Podpis osoby lub osób upoważnionych
do reprezentowania administratora¹

(dla zgłoszenia w formie papierowej)

¹ Jeżeli zgłoszenie podpisuje pełnomocnik, należy pamiętać o załączeniu pełnomocnictwa

Informacja:

Administrator danych osobowych.

Administratorem Państwa danych osobowych będzie Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO) z siedzibą w Warszawie, przy ul. Stawki 2.

Można się z nami kontaktować w następujący sposób:

- a) listownie: ul. Stawki 2, 00-193 Warszawa
- b) przez elektroniczną skrzynkę podawczą dostępną na stronie <https://www.uodo.gov.pl/p/kontakt>
- c) telefonicznie: (22) 531 03 00

Inspektor ochrony danych.

Możecie się Państwo kontaktować również z wyznaczonym przez Prezesa UODO inspektorem ochrony danych pod adresem email IOD@uodo.gov.pl

Cele i podstawy przetwarzania.

Będziemy przetwarzać Państwa dane osobowe zawarte w formularzu w celu przyjmowania zgłoszeń o naruszeniu ochrony danych osobowych zgodnie z art. 33 ust 1, 3 i 4 RODO, podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO¹, a także prowadzenia przez organ wewnętrzny rejestru naruszeń na podstawie art. 57 ust. 1 lit. u RODO. Następnie Państwa dane będziemy przetwarzać w celu wypełnienia obowiązku archiwizacji dokumentów wynikającego z ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach.

Odbiorcy danych osobowych.

Odbiorcami Państwa danych osobowych będą Minister Cyfryzacji w związku z zamieszczeniem formularza na platformie E-PUAP bądź Minister Przedsiębiorczości i Technologii w związku z zamieszczeniem formularza na platformie biznes.gov.pl

Okres przechowywania danych.

Będziemy przechowywać Państwa dane przez czas realizacji uprawnień Prezesa UODO wskazanych w art. 34 ust. 4 i art. 58 ust. 2 RODO, a następnie - zgodnie z obowiązującą w Urzędzie Prezesa UODO Instrukcją kancelaryjną oraz przepisami o archiwizacji dokumentów - przez okres 10 lat od końca roku, w którym zgłoszono naruszenie ochrony danych, lub - w przypadku skierowania wystąpienia lub wydania decyzji administracyjnej – wieczyście.

Prawa osób, których dane dotyczą.

Zgodnie z RODO przysługuje Państwu:

- a) prawo dostępu do swoich danych oraz otrzymania ich kopii;
- b) prawo do sprostowania (poprawiania) swoich danych;
- c) prawo do usunięcia danych osobowych, w sytuacji, gdy przetwarzanie danych nie następuje w celu wywiązania się z obowiązku wynikającego z przepisu prawa lub w ramach sprawowania władzy publicznej;
- d) prawo do ograniczenia przetwarzania danych;
- e) prawo do wniesienia skargi do Prezesa UODO (na adres Prezesa Urzędu Ochrony Danych Osobowych, ul. Stawki 2, 00 - 193 Warszawa)

Informacja o wymogu podania danych.

Podanie przez Państwa danych osobowych w niniejszym formularzu jest obowiązkiem wynikającym z art. 33 ust. 3 RODO oraz z art. 63 § 2-3a ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego.

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 (RODO) oraz podjętych działań.