

# Zgłoszenie naruszenia ochrony danych osobowych

## 1. Dane wnioskodawcy

### A. Podaj 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.

Zgłoszenie kompletne/jednorazowe

Zgłoszenie wstępne

Podaj datę poprzedniego zgłoszenia (opcjonalnie – jeśli zgłoszenie jest uzupełniające/zmieniające)

Zgłoszenie uzupełniające/zmieniające

## 2. Podmiot zgłaszający

### A. Dane administratora danych

Pełna nazwa administratora

REGON – jeśli został podany (opcjonalnie)

Sektor (opcjonalnie)

Dla sektora publicznego:

Dla sektora prywatnego:

### B. Adres siedziby administratora danych

Państwo

Miejscowość

Województwo

Ulica

Powiat

Kod pocztowy


Gmina

Numer domu  Numer lokalu

### C. Osoby uprawnione do reprezentowania administratora

1. Imię i nazwisko

Stanowisko

(Aby dopisać kolejne osoby, należy po kliknięciu na powyższe pole kliknąć przycisk , który pojawi się po prawej stronie)

### D. Pełnomocnik

Wniosek wypełniany przez pełnomocnika (opcjonalnie)

Pełnomocnictwo udzielone w formie elektronicznej oraz dowód uiszczenia opłaty skarbowej należy załączyć podczas składania wniosku przez portal [biznes.gov.pl](https://biznes.gov.pl). Pełnomocnictwo opatrzone kwalifikowanym podpisem elektronicznym osoby udzielającej pełnomocnictwa.

### E. 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.

## F. 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

Kliknij tutaj, aby wprowadzić tekst.

## 3. Czas naruszenia

### A. 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 wypełnienia formularza jest dłuższy niż 72h

Kliknij tutaj, aby wprowadzić tekst.

### B. Czas naruszenia

#### Data i czas zaistnienia/rozpoczęcia naruszenia

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

#### Trwające naruszenie

Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.

#### Data i czas zakończenia naruszenia

(opcjonalnie)  
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

### C. Komentarz do czasu naruszenia (opcjonalnie)

Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.

Kliknij tutaj, aby wprowadzić tekst.

## 4. Charakter naruszenia

### A. 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

### B. Na czym polegało naruszenie?

Zgubienie lub kradzież nośnika/urządzenia

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

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

Nieuprawnione uzyskanie dostępu do informacji

Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

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

Nieprawidłowa anonimizacja danych osobowych w dokumencie

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

Niezamierzona publikacja

Dane osobowe wystane do niewłaściwego odbiorcy

Ujawnienie danych niewłaściwej osoby

Ustne ujawnienie danych osobowych

Opisz na czym polegało naruszenie.

### C. Dzieci

Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

(opcjonalnie)

### D. Przyczyna naruszenia

Wewnętrzne działanie niezamierzone

Wewnętrzne działanie zamierzone

Zewnętrzne działanie niezamierzone

Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznanne)

## 4.1. Kategorie danych osobowych

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

### A. Kategorie danych

#### Szczegółowy opis kategorii danych, których dotyczy naruszenie

Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzi: nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub hashowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu.

### B. Dane podstawowe

Dane identyfikacyjne

np. imię, nazwisko, nr dowodu osobistego, adres IP

Krajowy numer identyfikacyjny

np. PESEL, SSN

Dane kontaktowe

np. e-mail, numer telefonu, adres korespondencyjny

Dane ekonomiczne i finansowe

np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

Oficjalne dokumenty

np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

Dane lokalizacyjne

np. GPS, dane o przemieszczaniu, miejsce zamieszkania

Inne

Opisz poniżej kategorie danych:

### C. 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

### D. Dane, o których mowa w art. 10 RODO

Dane dotyczące wyroków skazujących

Dane dotyczące czynów zabronionych

Inne

Opisz poniżej kategorie danych:

### E. Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

#### 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)

## 4.2. Kategorie osób

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

### A. Kategorie osób, których dane dotyczą

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

## B. Liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba osób, których mogło dotyczyć naruszenie

Kliknij tutaj, aby wprowadzić tekst.

## 5. Środki bezpieczeństwa zastosowane przed naruszeniem

### A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez administratora przed naruszeniem (opcjonalnie)

Kliknij tutaj, aby wprowadzić tekst.

## 6. Możliwe konsekwencje

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

- |  |   |
|--|---|
| <input type="checkbox"/> Utrata kontroli nad własnymi danymi osobowymi               | <input type="checkbox"/> Strata finansowa   |
| <input type="checkbox"/> Ograniczenie możliwości realizowania praw z art. 15-22 RODO | <input type="checkbox"/> Naruszenie dobrego imienia                                       |
| <input type="checkbox"/> Ograniczenie możliwości realizowania praw                   | <input type="checkbox"/> Utrata poufności danych osobowych chronionych tajemnicą zawodową |
| <input type="checkbox"/> Dyskryminacja   | <input type="checkbox"/> Nieuprawnione odwrócenie pseudonimizacji                         |
| <input type="checkbox"/> Kradzież lub sfalszowanie tożsamości                        | <input type="checkbox"/> Inne   |

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

Kliknij tutaj, aby wprowadzić tekst.

### B. Ryzyko naruszenia praw i wolności osób fizycznych

Niskie

Średnie

Wysokie

## 7. Środki zaradcze

### A. Komunikacja z osobami, których dane dotyczą

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

<input checked="" type="radio"/> Tak	<input type="radio"/> Nie, ale zostaną powiadomione	<input type="radio"/> Nie, nie zostaną powiadomione	<input type="radio"/> Nie oceniłem jeszcze
Czy indywidualnie? <input type="radio"/> Tak  <input checked="" type="radio"/> Nie, gdyż indywidualne powiadomienie 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.		Powód niezawiadomienia osób, których dane dotyczą:  <input checked="" type="radio"/> Przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiający odczyt osobom nieuprawnionym do dostępu do tych danych  <input type="radio"/> Po naruszeniu zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.	Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić podmioty danych, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.
Wskaż datę kiedy osoby, których dane dotyczą, zostały powiadomione o naruszeniu <input type="text" value="Kliknij tutaj, aby wprowadzić datę."/>	Wskaż datę kiedy zamierzasz powiadomić osoby, których dane dotyczą, o naruszeniu <input type="text" value="Kliknij tutaj, aby wprowadzić datę."/> <input type="checkbox"/> Nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą	Opis tych środków <input type="text" value="Kliknij tutaj, aby wprowadzić tekst."/>	
Liczba zawiadomionych osób, których dane dotyczą <input type="text" value="Kliknij tutaj, aby wprowadzić tekst."/>			
Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą <input type="text" value="Kliknij tutaj, aby wprowadzić tekst."/>			
Treść zawiadomienia <input type="text" value="Kliknij tutaj, aby wprowadzić tekst."/>			

### B. Środki w celu zaradzenia naruszeniu ochrony danych osobowych

Opisz dodatkowe środki (poza poinformowaniem osób) zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia.

### C. Transgraniczne przetwarzanie i inne powiadomienia

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorcemu UE (opcjonalnie)

- |                                    |  |                                   |                                     |
|------------------------------------|--|-----------------------------------|-------------------------------------|
| <input type="checkbox"/> Austria   | <input type="checkbox"/> Belgia          | <input type="checkbox"/> Bułgaria | <input type="checkbox"/> Chorwacja  |
| <input type="checkbox"/> Cypr      | <input type="checkbox"/> Czechy          | <input type="checkbox"/> Dania    | <input type="checkbox"/> Estonia    |
| <input type="checkbox"/> Finlandia | <input type="checkbox"/> Francja         | <input type="checkbox"/> Grecja   | <input type="checkbox"/> Hiszpania  |
| <input type="checkbox"/> Holandia  | <input type="checkbox"/> Irlandia        | <input type="checkbox"/> Litwa    | <input type="checkbox"/> Luksemburg |
| <input type="checkbox"/> Łotwa     | <input type="checkbox"/> Malta           | <input type="checkbox"/> Niemcy   | <input type="checkbox"/> Portugalia |
| <input type="checkbox"/> Rumunia   | <input type="checkbox"/> Słowacja        | <input type="checkbox"/> Słowenia | <input type="checkbox"/> Szwecja    |
| <input type="checkbox"/> Węgry     | <input type="checkbox"/> Wielka Brytania | <input type="checkbox"/> Włochy   |                                     |

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorcemu spoza UE (opcjonalnie)

Wymień inne organy nadzorcze spoza UE, którym naruszenie zostało lub zostanie zgłoszone

Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorcemu UE 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.

## 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/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](mailto: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 RODO<sup>1</sup>, 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 wniosku na platformie E-PUAP oraz Wojewoda Podlaski w związku z korzystaniem przez Prezesa UODO z systemu elektronicznego zarządzania dokumentacją (EZD PUW).

### 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.

<sup>1</sup> 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.