**PROCEDURA NOTYFIKACJI   
NARUSZEŃ DANYCH OSOBOWYCH**

**Spis treści**

[I. Wstęp 3](#_Toc518295465)

[II. Cel procedury 3](#_Toc518295466)

[III. Zakres stosowania 4](#_Toc518295467)

[IV. Postanowienia ogólne 5](#_Toc518295468)

[V. Źródła incydentów 7](#_Toc518295469)

[VI. Naruszenie ochrony danych osobowych 7](#_Toc518295470)

[VII. Notyfikacja naruszeń - podmioty, których powiadomienie może być wymagane na podstawie RODO 8](#_Toc518295471)

[VIII. Ocena ryzyka wystąpienia naruszenia ochrony danych osobowych 9](#_Toc518295472)

[IX. Powiadamianie organu nadzorczego 11](#_Toc518295473)

[X. Jak dokonać zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu 11](#_Toc518295474)

[XI. Podjęcie decyzji, czy zawiadomić osobę, której dane dotyczą 12](#_Toc518295475)

[XII. Jak dokonać zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych 13](#_Toc518295476)

[XIII. Obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych 13](#_Toc518295477)

[Załącznik Nr 1 do Procedury notyfikacji – Wzór zgłoszenia w sprawie naruszenia ochrony danych osobowych 15](#_Toc518295478)

[Załącznik Nr 2 do Procedury notyfikacji – Wzór rejestru naruszeń ochrony danych osobowych 22](#_Toc518295479)

[Załącznik Nr 3 do Procedury notyfikacji – Wzór zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych 23](#_Toc518295480)

[Załącznik nr 4 Schemat procedury notyfikacji naruszeń 25](#_Toc518295481)

[Załącznik nr 5 Przykłady naruszeń danych osobowych 26](#_Toc518295482)

# Wstęp

* 1. Niniejsza procedura powinna być stosowana w przypadku wystąpienia incydentu, który spowodował naruszenie ochrony danych osobowych.
  2. Zgłaszanie organowi nadzorczemu incydentów, w których doszło do naruszenia ochrony danych osobowych jest wymogiem wynikającym   
     z przepisów 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), zwanego dalej RODO lub Rozporządzenie. Zgłoszenie takie musi być dokonane niezwłocznie, w miarę możliwości nie później niż w terminie 72 godzin po jego stwierdzeniu. Zgodnie z RODO zgłoszenie nie jest wymagane, gdy jest mało prawdopodobne aby incydent skutkował ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 RODO).
  3. Dodatkowo, jeśli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności podmiotów danych, Rozporządzenie wymaga ich powiadomienia lub wydania publicznego komunikatu w sprawie incydentu (jeżeli powiadomienie wymagałoby niewspółmiernie dużego wysiłku), lub zastosowania podobnego środka, za pomocą, którego osoby, których dane dotyczą, zostaną w równie skuteczny sposób poinformowane (art. 34 RODO).

# Cel procedury

2.1. Niniejsza procedura ma na celu zapewnienie zgodności zgłaszania naruszeń danych, z wymogami wynikającymi z przepisów RODO, poprzez:

1. zapewnienie odpowiednich mechanizmów pozwalających na zgłaszanie naruszeń do organu nadzorczego w wyznaczonym czasie,
2. ustalenie osób odpowiedzialnych za naruszenia i odpowiednią reakcję na działania niepożądane.

W praktyce oznacza to, że należy:

1. określić czym są naruszenia ochrony danych osobowych;
2. wykryć i zgłosić naruszenia / podejrzenia naruszenia ochrony danych osobowych;
3. rejestrować naruszenia / podejrzenia wystąpienia naruszenia ochrony danych osobowych;
4. określić osoby odpowiedzialne za monitorowanie naruszeń;
5. określić sposób zgłaszania naruszeń do odpowiedniego organu w wyznaczonym czasie;
6. wyznaczyć osoby odpowiedzialne za usuwanie skutków naruszeń ochrony danych osobowych;
7. określić sposób informowania osób, których dane dotyczą   
   o naruszeniach ochrony ich danych osobowych;
8. zastosować działania doraźne w celu zminimalizowania skutków naruszenia;
9. gromadzić i zabezpieczać dowody naruszenia;
10. ustalić i usunąć przyczyny wystąpienia naruszenia.

# Zakres stosowania

1. Niniejsza procedura ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.
2. Procedurą objęte są dane osobowe w rozumieniu art. 4 pkt 1 RODO – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
3. „Przetwarzanie”, zgodnie z art. 4 pkt 2 RODO, oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

# Postanowienia ogólne

1. Administrator jest odpowiedzialny za wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających stopień bezpieczeństwa odpowiadający ryzyku, na które narażone są przetwarzane dane osobowe. Przy ocenie ryzyka uwzględnia się stan aktualny stan wiedzy technicznej, koszty wdrażania oraz charakter, zakres, kontekst i cele przetwarzania,   
   a także ryzyko naruszeń prawa i wolności osób, których dane dotyczą. Ocena uwzględnia również prawdopodobieństwo wystąpienia naruszenia jak i konsekwencje, z jakim wiążą się naruszenia.
2. Odpowiedzialny za nadzór/ realizację procedury notyfikacji naruszeń danych osobowych jest *Inspektor Ochrony Danych Osobowych (dalej „IOD”)*/ *osoba odpowiedzialna wyznaczona przez Administratora (wskazać stanowisko/Dział)*. Osoba odpowiedzialna za nadzór/realizację procedury notyfikacji naruszeń może udzielać dalszych upoważnień w zakresie realizacji poszczególnych uprawnień i obowiązków określonych   
   w procedurze.
3. W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych przez pracownika, pracownik ten ma obowiązek:

* powiadomić niezwłocznie bezpośredniego przełożonego, przesyłając mu drogą mailową informację i zawiadamiając go ponadto drogą telefoniczną o przesłanym zgłoszeniu,
* powstrzymać się od wszelkich działań mogących utrudnić ustalenie okoliczności naruszenia,
* zabezpieczyć pomieszczenie do czasu przybycia bezpośredniego przełożonego,
* podjąć inne działania stosownie do zaistniałej sytuacji, niezbędne do zapobieżenia dalszym zagrożeniom dla danych.

1. Bezpośredni przełożony otrzymując informacje o stwierdzeniu lub podejrzeniu naruszenia ochrony danych osobowych przekazuje je drogą mailową do [IOD/ osoba odpowiedzialna].
2. W razie braku odpowiedzi od [IOD/ osoba odpowiedzialna] w ciągu 4h od wysłania informacji drogą mailową bezpośredni przełożony zobowiązany jest przekazać telefonicznie [IOD/ osoba odpowiedzialna] informacje   
   o stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
3. [IOD/ osoba odpowiedzialna] niezwłocznie po podjęciu informacji o wystąpieniu / podejrzeniu wystąpienia incydentu weryfikuje, czy dane, których dotyczy incydent są przetwarzane jako:
4. administratora danych osobowych – tj. jako podmiot decydujący   
   o celu i zakresie przetwarzanych danych,
5. podmiot przetwarzający dane osobowe – tj. dane przetwarzane są   
   (w tym również np. zbierane) na rzecz realizacji celu i w zakresie zdefiniowanym przez odrębny podmiot.
   1. W przypadku spełnienia warunku 4.6 punkt b) [IOD / osoba odpowiedzialna] podejmuje wyłącznie poniżej wskazane działania   
      i powstrzymuje się od wszelkich innych czynności:
6. niezwłocznie po powzięciu wiadomości o takim zdarzeniu informuje administratora danych osobowych, których dotyczy incydent o takim zdarzeniu oraz zapewnia pomoc i przekazuje wszelkie dalsze informacje dotyczące tego zdarzenia,
7. ustala przyczynę zdarzenia,
8. podejmuje niezwłocznie wszelkie czynności mające na celu usunięcie negatywnych skutków zdarzenia i zabezpieczenie danych osobowych w sposób należyty przed dalszymi takimi zdarzeniami,
9. zbiera wszystkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności wystąpienia zdarzenia i przeciwdziałaniu podobnym zdarzeniom w przyszłości i w tym celu współpracuje z administratorem danych osobowych, których dotyczy incydent na każdym etapie wyjaśniania sprawy.
10. W sytuacji spełnienia warunku 4.6 punkt b należy postępować zgodnie z dalszą częścią procedury począwszy od punktu VII.
11. Do stosowania niniejszej procedury zostają przeznaczone wzory stanowiące załączniku niniejszego dokumentu:
12. Wzór zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu (stanowi Załącznik nr 1 do niniejszej Procedury, aktualny wzór zgłoszenia znajduje się na oficjalnej stronie internetowej Urzędu Ochrony Danych Osobowych pod linkiem <https://uodo.gov.pl/pl/134/233> ),
13. Wzór zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych (stanowi Załącznik nr 3 do niniejszej Procedury),
14. Wykaz naruszeń wraz z wykazem działań korygujących i osoby odpowiedzialne za jej prawidłową realizację (stanowią Załącznik nr 2 do niniejszej Procedury).

# Źródła incydentów

1. Zdarzenia (incydenty) mogące prowadzić do naruszenia ochrony danych osobowych mogą pochodzić z następujących źródeł:
2. podmioty przetwarzające,
3. pracownicy, zleceniobiorcy lub inne osoby działające na rzecz Adminitratora,
4. klienci, pozostałe osoby zgłaszające (źródło: np. adres IOD na stronie www),
5. systemy informatyczne,
6. [inne].

# Naruszenie ochrony danych osobowych

1. Naruszeniem ochrony danych osobowych, w związku z którym konieczne jest zgłoszenie naruszenia do organu może stanowić sytuacja,   
   w której dane osobowe są przetwarzane niezgodnie z prawem lub w sposób niedozwolony; zostały utracone; uległy uszkodzeniu lub zniszczeniu, mimo zastosowania odpowiednich środków technicznych lub organizacyjnych. Naruszeniem jest również utrata, modyfikacja danych oraz nieuprawione ujawnienie lub nieuprawniony dostęp do danych osobowych przestanych, przechowywanych lub przetwarzanych w inny sposób. Poniżej zostało przedstawione objaśnienie pojęć użytych w niniejszej definicji naruszenia ochrony danych osobowych.
   * **Zniszczenie danych osobowych** – oznacza sytuację, w której dane przestają istnieć lub przestają istnieć w formie nadającej się do użytku przez administratora.
   * **Uszkodzenie** – oznacza sytuację, w której dane osobowe uległy zmianie czy zepsuciu lub stały się niekompletne.
   * **Utrata danych osobowych** – sytuacja, w której dane mogą nadal istnieć, ale administrator utracił kontrole nad nimi lub dostęp do nich, lub nie jest już w ich posiadaniu.
   * **Niedozwolone lub niezgodne z prawem przetwarzanie** – obejmuje przypadki ujawnienia lub udostępnienia danych osobowych odbiorcom nieupoważnionym do otrzymania ich lub uzyskania do nich dostępu, a także wszelkie inne formy przetwarzania naruszające postanowienia polityki ochrony danych.
2. Procedura rozróżnia 3 główne rodzaje naruszenia bezpieczeństwa danych osobowych:
   * 1. Naruszenie poufności – niedozwolone lub przypadkowe ujawnienie lub dostęp do danych osobowych;
     2. Naruszenie dostępności – niedozwolone lub przypadkowa utrata dostępu do danych osobowych lub zniszczenie ich;
     3. Naruszenie integralności – niedozwolona lub przypadkowa zmiana danych osobowych.
3. W razie ustalenia, że doszło do naruszenia ochrony danych osobowych, ale nie zachodzą przesłanki zgłoszenia [IOD/ osoba odpowiedzialna] sporządzi notatkę uzasadniającą brak zgłoszenia.

# Notyfikacja naruszeń - podmioty, których powiadomienie może być wymagane na podstawie RODO

* 1. Po podjęciu decyzji, że doszło do naruszenia danych osobowych, na gruncie Rozporządzenia, może być wymagane powiadomienie następujących podmiotów:

1. **Organ nadzorczy** – jeżeli doszło do naruszenia ochrony danych osobowych, któremu towarzyszy ryzyko naruszenia praw lub wolności osób fizycznych,
2. **Osoba, której dane uległy naruszeniu** – jeżeli doszło do naruszenia ochrony danych osobowych, które może skutkować wysokim ryzykiem naruszenia praw lub wolności osób fizycznych.
   1. Nie każde zdarzenie (incydent) stanowi naruszenie ochrony danych osobowych. Poniżej przedstawiono przykładowe zdarzenia (incydenty), które mogą prowadzić do naruszenia ochrony danych osobowych.
   2. Przykładowe zdarzenia (incydenty) mogące prowadzić do wystąpienia naruszenia ochrony danych osobowych:

* stwierdzono naruszenie lub próbę naruszenia zabezpieczenia systemu teleinformatycznego,
* stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie poufności, integralności lub dostępności tych danych,
* stan pomieszczeń lub szaf, bądź innych miejsc przechowywania danych osobowych, zawartość dokumentacji lub nośników informacji mogący wskazywać na uzyskanie dostępu do nich przez osoby nieupoważnione,
* nieautoryzowany dostęp do danych / systemów / lokali (fizyczny),
* inny stan pomieszczeń lub systemu informatycznego niż pozostawiony po zakończeniu pracy lub przerwie w pracy,
* kradzież /utrata urządzeń biznesowych (PC / smartfon / klucze dostępu/ klucze dostępu do lokali),
* nieuprawnione przekazanie lub ujawnienie danych osobowych;
* uszkodzenie dokumentacji,
* zmiana danych zapisanych na kopiach zapasowych dokonana w sposób nieuprawniony lub ich utrata,
* zniszczenie lub próba zniszczenia w sposób nieuprawniony danych osobowych,
* zakażenie systemów informatycznych wirusami / złośliwym oprogramowaniem,
* phishing / spam / ransomware.

W konsekwencji obowiązek notyfikacyjny nie ma charakteru bezwzględnego.

W poniższych sekcjach opisano, w jaki sposób należy podjąć tę decyzję i co zrobić, jeśli wymagane jest zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu oraz zawiadomienie osoby, której dane dotyczą o takim naruszeniu.

# Ocena ryzyka wystąpienia naruszenia ochrony danych osobowych

1. Naruszenie ochrony danych osobowych może skutkować:
2. **Brakiem ryzyka** naruszenia praw lub wolności osób fizycznych,
3. **Ryzykiem** naruszenia praw lub wolności osób fizycznych,
4. **Wysokim ryzykiem** naruszenia praw lub wolności osób fizycznych.
5. Czynniki, które należy brać pod uwagę przy ocenie ryzyka:
6. **Typ/rodzaj naruszenia** – przez rodzaj naruszenia należy rozumieć np. utracenie i utratę dostępności do danych osobowych, ujawnienie nieupoważnionym stronom;
7. **Charakter, wrażliwość i zakres danych osobowych** – należy wziąć pod uwagę, czy naruszenie dotyczy danych osobowych zwykłych lub szczególnych kategorii danych osobowych. Naruszenie dotyczące dużych ilości danych osobowych może mieć wpływ na odpowiednio dużą liczbę osób;
8. **Łatwość identyfikacji osób** – należy rozważyć łatwość identyfikacji osoby, której dane osobowe uległy naruszeniu, czy za pomogą naruszonych danych można zidentyfikować konkretne osoby lub dopasować dane do innych informacji w celu identyfikacji osób;
9. **Rodzaj konsekwencji dla osób, których dane dotyczą** –   
   w zależności charakteru danych osobowych, których dotyczy naruszenie rodzaj konsekwencji dla osób, których dane dotyczą może być różny. W szczególności jeżeli naruszenie dotyczy szczególnych kategorii danych, takie naruszenie może prowadzić do kradzieży tożsamości lub oszustwa, cierpienia psychicznego, upokorzenia lub zniszczenia reputacji;
10. **Szczególne cechy osoby, której dane dotyczą** – należy wziąć pod uwagę, czy naruszenie może dotyczyć danych osobowych dzieci lub innych osób, które w wyniku tego naruszenia mogą zostać narażone na większe ryzyko;
11. **Liczba dotkniętych osób** – należy wziąć pod uwagę liczbę osób, których dane zostały naruszone. Im większa liczba osób, których dane zostały naruszone, tym większy może być wpływ naruszenia. Jednak należy pamiętać, że naruszenie dotyczące danych osobowych wyłącznie jednej osoby fizycznej może mieć poważny wpływ na tę osobę, w zależności od charakteru danych osobowych, które zostały naruszone;
12. **Szczególne cechy administratora danych** - charakter i rola działalności administratora oraz procesy przetwarzania danych występujące u administratora.
    1. Wysokie ryzyko naruszenia praw lub wolności osób fizycznych występuje, gdy naruszenie może prowadzić do materialnych lub niematerialnych szkód dla osób, których dane zostały naruszone np. dyskryminacja, kradzież tożsamości lub oszustwo, straty finansowe i szkody wizerunkowe. Ponadto naruszenie może występować w szczególności, gdy dotyczy danych osobowych, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
    2. Należy wziąć pod uwagę, że Rozporządzenie wprowadza szereg wyjątków, w których nie ma obowiązku dokonywania zawiadomienia   
       o naruszeniu osoby, której dane dotyczą. Są to następujące sytuacje:
13. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie (w szczególności szyfrowanie);
14. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
15. wymagałoby to niewspółmiernie wysokiego wysiłku (w takim przypadku wydany zostanie komunikat lub zastosowany zostanie inny podobny środek, za pomocą którego osoby, których dane dotyczą, zostaną poinformowane w równie skuteczny sposób).
    1. Oceny ryzyka, jej uzasadnienie i wnioski powinny być w pełni udokumentowane. Wynik oceny ryzyka powinien zawierać jeden   
       z następujących wniosków:
16. Brak ryzyka naruszenia praw lub wolności osób fizycznych - naruszenie danych osobowych nie wymaga powiadomienia;
17. Ryzyko naruszenia praw lub wolności osób fizycznych - naruszenie danych osobowych wymaga powiadomienia wyłącznie organu nadzoru;
18. Wysokie ryzyko naruszenia praw lub wolności osób fizycznych - naruszenie danych osobowych wymaga powiadomienia zarówno organu nadzoru, jak i zainteresowanych podmiotów danych.

Wnioski te mogą ulec zmianie na podstawie opinii organu nadzorczego   
i dalszych informacji, które zostaną wykryte w ramach trwającego dochodzenia w sprawie naruszenia.

# Powiadamianie organu nadzorczego

1. W przypadku, gdy rekomendacje wynikające z oceny ryzyka (pkt 8.4.) stanowią, że występuje ryzyko naruszenia praw lub wolności osób fizycznych i naruszenie danych osobowych wymaga powiadomienia organu nadzoru, należy dokonać odpowiedniego zgłoszenia do organu nadzorczego.
2. Treść zgłoszenia przygotowuje IOD, zgodnie ze wzorem udostępnionym przez organ nadzorczy.  
   Zgłoszenia można dokonać formie elektronicznej poprzez:
   1. wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie biznez.gov.pl
   2. elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: /UODO/SkrytkaESP
   3. elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl lub na platformie epuap.gov.pl
   4. tradycyjną pocztą wysyłając wypełniony formularz na adres Urzędu.

Prezes Urzędu Ochrony Danych Osobowych

ul. Stawki 2, 00-193 Warszawa

tel. (22) 531 03 00

elektroniczna skrzynka podawcza: <https://uodo.gov.pl/pl/p/kontakt>

Najnowszy wzór formularza stanowi załącznik nr. 1 do niniejszej procedury

# Jak dokonać zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku podjęcia decyzji o powiadomieniu organu nadzorczego należy niezwłocznie dokonać zgłoszenia naruszenia – jeżeli to możliwe –   
   w ciągu 72 godzin od jego stwierdzenia. Moment, od którego należy liczyć okres 72 godzin wyznaczamy od chwili stwierdzenia naruszenia (rozdział V). W przypadku przekroczenia terminu 72 godzin do zgłoszenia należy dołączyć wyjaśnienia dotyczące przyczyn opóźnienia.
2. W przypadku braku możliwości przekazania wszystkich informacji wskazanych w pkt. 10.4. w terminie 72 godzin po stwierdzeniu naruszenia, w zgłoszeniu zamieszcza się znane informacje, jednocześnie wskazując   
   w nim, że pozostałe informacje zostaną przekazane niezwłocznie po tym, gdy będą znane administratorowi (powiadomienie sukcesywne). W zgłoszeniu należy wskazać przyczynę sukcesywnego przekazywania informacji (np. konieczność przeprowadzenia szczegółowego audytu funkcjonowania systemów informatycznych, w przypadku stwierdzenia przez administratora wielu podobnych naruszeń w krótkim odcinku czasu, wpływających w taki sam sposób na osoby, których dane dotyczą).
3. Zgłoszenie organowi nadzorczemu powinno zostać przekazane za pomocą odpowiednich środków bezpieczeństwa, korzystając z formularza zawiadomienia o naruszeniu danych osobowych (Załącznik nr 1 do Procedury).
4. W ramach zgłoszenia należy podać następujące informacje:
5. 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;

1. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
2. możliwe konsekwencje naruszenia ochrony danych osobowych;
3. środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym   
   w stosownych przypadkach w celu zminimalizowania jego ewentualnych negatywnych skutków;
4. jeżeli zawiadomienia dokonano po upływie 72 godzin od jego stwierdzenia – powody opóźnienia.

# Podjęcie decyzji, czy zawiadomić osobę, której dane dotyczą

* 1. W przypadku, gdy rekomendacje wynikające z oceny ryzyka (pkt 8.4.) stanowią, że występuje wysokie ryzyko naruszenia praw lub wolności osób fizycznych i naruszenie danych osobowych wymaga powiadomienia nie tylko organu nadzorczego, ale również osoby, której dane dotyczą, należy dokonać odpowiedniego powiadomienia tej osoby.

# Jak dokonać zawiadomienia osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

1. Po podjęciu decyzji, że naruszenie uzasadnia zawiadomienie osoby, której dane dotyczą, bez zbędnej zwłoki przekazuje osobie jasnym i prostym językiem, zgodnie ze wzorem stanowiącym załącznik nr 3 do Procedury, następujące informacje:
2. charakter naruszenia ochrony danych osobowych,
3. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
4. możliwe konsekwencje naruszenia ochrony danych osobowych;
5. środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach w celu zminimalizowania jego ewentualnych negatywnych skutków.
6. Zawiadomienie osoby, której dane dotyczą powinno zostać przekazane za pomocą odpowiednich środków bezpieczeństwa, korzystając   
   z formularza zawiadomienia o naruszeniu danych osobowych (Załącznik nr 3 do Procedury).

Możliwe sposoby powiadamiania osób o naruszeniu ochrony danych osobowych to:

1. Powiadomienie za pośrednictwem strony internetowej lub poczty elektronicznej - Administrator danych może umieścić na swojej stronie internetowej informację o naruszeniu ochrony danych osobowych lub poinformować osoby, których dane dotyczą, za pośrednictwem poczty elektronicznej. W tym przypadku ważne jest, aby informacja była dostępna dla wszystkich osób, których dane zostały naruszone, a także była jasna, zwięzła i zrozumiała.
2. Powiadomienie za pośrednictwem mediów społecznościowych - Administrator danych może również wykorzystać media społecznościowe do powiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych. W tym przypadku ważne jest, aby informacja była dostępna dla wszystkich osób, których dane zostały naruszone, a także była jasna, zwięzła i zrozumiała.
3. Powiadomienie za pośrednictwem poczty tradycyjnej - Administrator danych może również powiadomić osoby, których dane dotyczą, za pośrednictwem poczty tradycyjnej. W tym przypadku ważne jest, aby informacja została wysłana na dokładny adres osoby, której dane zostały naruszone, a także była jasna, zwięzła i zrozumiała.

W każdym przypadku ważne jest, aby informacja o naruszeniu ochrony danych osobowych była przekazana w sposób jasny, zrozumiały i dostępny dla osób, których dane zostały naruszone. Ponadto, Administrator danych powinien dokładnie przemyśleć, który sposób powiadomienia jest najodpowiedniejszy w danym przypadku, biorąc pod uwagę charakter i skale naruszenia oraz oczekiwania osób, których dane dotyczą.

# Obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych

1. Zgodnie z Załącznikiem nr 2 do niniejszej Procedury należy dokumentować wszelkie naruszenia ochrony danych osobowych, w tym:
2. okoliczności naruszenia ochrony danych osobowych,
3. skutki naruszenia ochrony danych osobowych, oraz
4. podjęte działania zaradcze.
5. Należy prowadzić dokumentację naruszeń ochrony danych osobowych w taki sposób, by na jej podstawie organ nadzorczy miał możliwość weryfikacji, czy obowiązki wynikające z Rozporządzenia są właściwie realizowane. Prowadzona dokumentacja uwzględnia wszystkie naruszenia ochrony danych osobowych: zarówno te, które zaistniały, jak i te, które zaistniały u jego podmiotu przetwarzającego.
6. W dokumentacji należy odnotować wszelkie naruszenia ochrony danych osobowych. Łącznie z tymi, których nie zgłoszono do organu nadzorczego z uwagi na małe prawdopodobieństwo, by naruszenie skutkowało ryzykiem naruszenia praw lub wolności osoby fizycznej (zgodnie z rekomendacjami wynikającymi z przeprowadzonej oceny ryzyka, o których mowa w pkt 8.4.). W ten sposób organ nadzorczy będzie miał możliwość weryfikacji, czy podjęto prawidłową decyzję o zaniechaniu zgłoszenia naruszenia ochrony danych osobowych.

# Zgłoszenie naruszenia ochrony danych osobowych przez podmiot przetwarzający

* 1. W przypadku wykrycia naruszenia ochrony danych osobowych, podmiot przetwarzający powinien niezwłocznie poinformować administratora danych osobowych o tym fakcie.

Powiadomienie powinno zawierać następujące informacje:

* Opis naruszenia ochrony danych osobowych, w tym datę i godzinę wykrycia naruszenia
* Rodzaj danych osobowych objętych naruszeniem
* Przyczyny i skutki naruszenia
* Działania podejmowane przez podmiot przetwarzający w celu zminimalizowania szkód wynikających z naruszenia ochrony danych osobowych
* Działania, jakie zostaną podjęte przez podmiot przetwarzający w celu zapobieżenia przyszłym naruszeniom ochrony danych osobowych
  1. Administrator danych osobowych powinien niezwłocznie podjąć odpowiednie kroki w celu zminimalizowania skutków naruszenia ochrony danych osobowych oraz poinformować organ nadzorczy o tym fakcie, jeśli naruszenie to może prowadzić do ryzyka dla praw i wolności osoby, której dane dotyczą.
  2. W przypadku gdy naruszenie ochrony danych osobowych jest znaczne lub groźne, Administrator danych osobowych powinien także poinformować osoby, których dane dotyczą, o tym naruszeniu, w sposób określony przez obowiązujące przepisy prawa.
  3. Po rozwiązaniu problemu, Administrator danych osobowych powinien przeprowadzić wewnętrzną analizę zdarzenia, aby ocenić, co można było zrobić, aby zapobiec naruszeniu i jak można wzmocnić procedury w przyszłości.
  4. Zgłoszenie naruszenia ochrony danych osobowych przez podmiot przetwarzający nie wymaga szczególnej formie, może zostać dokonane   
     w formie elektronicznej mailowej lub telefonicznej, chyba, ze jest zastrzeżona   
     w umowie powierzenia.
  5. Czas 72h na zgłoszenie do organu liczy się od chwili stwierdzenia przez Administratora danych osobowych, że doszło do naruszenia.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 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 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. | | | | | | | | | |
| 1. **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** | | | | | | | | | | | | | | | |
|  | Imię i nazwisko | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | Stanowisko | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | Imię i nazwisko | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | Stanowisko | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | Imię i nazwisko | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | Stanowisko | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | Imię i nazwisko | Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | Stanowisko | Kliknij tutaj, aby wprowadzić tekst. | | | |
|  | 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 | | | | | | | | | | | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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. | | |
| 1. **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. | | | | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Charakter naruszenia** | | | | | | | | | | | | | | | |
| **4A. Opisz szczegółowo na czym polegało naruszenie** | | | | | | | | | | | | | | | |
| Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | | | | |
| **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) | | | | | | | | | | | | | | | |
| 1. 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. | | | | | | | | | | | | | | | |
| 1. 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. | | | | | | | | | | | | | | | |
| 1. 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/*](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) | | | | | | | | | | | | | | | |
| 1. **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. | | | | | | |
| 1. **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. | | |
| 1. **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. | | | | | | | | |
| 1. **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?** | | | | | | | | | | | | | | | |
|  | |  | | | | | | | | | | | | | |
| **Uzasadnienie**  Kliknij tutaj, aby wprowadzić tekst. | | | | | | | | | | | | | | | |
| 1. **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. | | | | | | | | | | | | | | | |
| 1. **Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?** | | | | | | | | | | | | | | | |
|  | Pamiętaj, że po powiadomieniu osób, należy przesłać treść zawiadomienia do UODO. | | | | | | | | |  | | | |  | |
| Czy indywidualnie? | | | | | | | | | |  | | | | Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające. | |
| 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. | | | | | | | | | |
| 1. **Przetwarzanie transgraniczne** | | | | | | | | | | | | | | | |
| **☐** Naruszenie ma charakter transgraniczny  Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie: | | | | | | | | | | | | | | | |
| **☐** Austria  **☐** Cypr  **☐** Finlandia  **☐** Holandia  **☐** Litwa  **☐** Niemcy  **☐** Słowacja  **☐** Wielka Brytania | | | | **☐** Belgia  **☐** Czechy  **☐** Francja  **☐** Irlandia  **☐** Luksemburg  **☐** Norwegia  **☐** Słowenia  **☐** Włochy | | | | | | | **☐** Bułgaria  **☐** Dania  **☐** Grecja  **☐** Islandia  **☐** Łotwa  **☐** Portugalia  **☐** Szwecja | | | | **☐** Chorwacja  **☐** Estonia  **☐** Hiszpania  **☐** Liechtenstein  **☐** Malta  **☐** Rumunia  **☐** Węgry |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| * 1. **Kategorie danych osobowych**   **UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.** | | | | | | |
| 1. **Kategorie danych** | | | | | | |
| Szczegółowy opis kategorii danych, których dotyczy naruszenie Wymień jakie dane uległy naruszeniu: np. w przypadku sklepu internetowego profil użytkownika, w skład którego wchodzą: nazwa użytkownika, imię, nazwisko, hasło (zapisane otwartym tekstem lub hashowane), adres e-mail, oraz historia transakcji - kwota, data i nazwa kupionego produktu.  Kliknij tutaj, aby wprowadzić tekst. | | | | | | |
| 1. **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:  Kliknij tutaj, aby wprowadzić tekst. | | | |
| 1. **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 | | | |
| 1. **Dane, o których mowa w art. 10 RODO** | | | | | | |
| Dane dotyczące wyroków skazujących  Dane dotyczące czynów zabronionych  Inne  Opisz poniżej kategorie danych:  Kliknij tutaj, aby wprowadzić tekst. | | | | | | |
| 1. **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) | | | | | Kliknij tutaj, aby wprowadzić tekst. | |
| * 1. **Kategorie osób**   **UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.** | | | | | | |
| 1. **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  Kliknij tutaj, aby wprowadzić tekst. | | | | | | |
| 1. **Liczba osób, których mogło dotyczyć naruszenie** | | | | | | |
| Przybliżona liczba osób, których mogło dotyczyć naruszenie | | | | Kliknij tutaj, aby wprowadzić tekst. | | |
| 1. **Środki bezpieczeństwa zastosowane przed naruszeniem** | | | | | | |
| 1. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przez administratora przed naruszeniem** (opcjonalnie) | | | | | | |
| Kliknij tutaj, aby wprowadzić tekst. | | | | | | |
| 1. **Możliwe konsekwencje** | | | | | | |
| 1. **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. | | | |
| 1. **Ryzyko naruszenia praw i wolności osób fizycznych** | | | | | | |
|  |  | | | | |  |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. **Środki zaradcze** | | | | | | | |
| 1. **Komunikacja z osobami, których dane dotyczą** | | | | | | | |
| Czy osoby, których dane dotyczą, zostały powiadomione o naruszeniu? | | | | | | | |
|  |  | | |  | |  | |
| Czy indywidualnie? | | | | Powód niezawiadomienia osób, których dane dotyczą:    Opis tych środków Kliknij tutaj, aby wprowadzić tekst. | | 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  Kliknij tutaj, aby wprowadzić datę. | | Wskaż datę kiedy zamierzasz powiadomić osoby, których dane dotyczą, o naruszeniu  Kliknij tutaj, aby wprowadzić datę.  Nie znam jeszcze daty kiedy zamierzam powiadomić osoby, których dane dotyczą | |
| Liczba zawiadomionych osób, których dane dotyczą  Kliknij tutaj, aby wprowadzić tekst. | |
| Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą  Kliknij tutaj, aby wprowadzić tekst. | | | |
| Treść zawiadomienia  Kliknij tutaj, aby wprowadzić tekst. | | | |
| 1. **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.  Kliknij tutaj, aby wprowadzić tekst. | | | | | | | |
| 1. **Transgraniczne przetwarzanie i inne powiadomienia** | | | | | | | |
| Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE (oopcjonalnie) | | | | | | | |
| Austria  Cypr  Finlandia  Holandia  Łotwa  Rumunia  Węgry | | | Belgia  Czechy  Francja  Irlandia  Malta  Słowacja  Wielka Brytania | | Bułgaria  Dania  Grecja  Litwa  Niemcy  Słowenia  Włochy | | Chorwacja  Estonia  Hiszpania  Luksemburg  Portugalia  Szwecja |
| Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu spoza UE (oopcjonalnie)  Wymień inne organy nadzorcze spoza UE, którym naruszenie zostało lub zostanie zgłoszone  Kliknij tutaj, aby wprowadzić tekst. | | | | | | | |
| Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu UE z powodu innych zobowiązań prawnych (oopcjonalnie)  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. | | | | | | | |

**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

**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 RODO1 bądź art. 44 ust. 1 – 5 DODO2, podejmowania działań określonych w art. 34 ust. 4 oraz art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, a także prowadzenia przez organ wewnętrznego 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 RODO i art. 58 ust. 2 RODO bądź art. 45 ust. 5 DODO, 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:

1. prawo dostępu do swoich danych oraz otrzymania ich kopii;
2. prawo do sprostowania (poprawiania) swoich danych;
3. 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;
4. prawo do ograniczenia przetwarzania danych;
5. 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.

2 Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości

# Załącznik Nr 2 do Procedury notyfikacji – Wzór rejestru naruszeń ochrony danych osobowych

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Opis naruszenia | Data zgłoszenia | Żródło/ osoba zgłaszajaca | Data naruszenia | Kategoria i przybliżona liczba osób, których dane dotyczą | Możliwe konsekwencje | Działania zaradcze | Data rozpoczęcia działań zaradczych | Data wdrożenia działań zaradczych | Rekomendacja dot. zgłaszania naruszenia organowi nadzorczemu oraz powiadamiania osób, których dotyczy naruszenie | Data powiadomienia organu nadzorczego oraz osoby, której dotyczy naruszenie | Osoba odpowiedzialna za wdrożenie działań |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |

# Załącznik Nr 3 do Procedury notyfikacji – Wzór zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Wzór 1.

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ……………...…….  (miejscowość, data)  **Administrator danych**  u.. xyz  00-001 Miejscowość  **Generalny Inspektor Ochrony danych**  ul. .....  00-000 Warszawa  **ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ, O NARUSZENIU OCHRONY DANYCH OSOBOWYCH**  Niniejszym w trybie art. 34 ogólnego rozporządzenia o ochronie danych, zgłaszam naruszenie ochrony danych osobowych, które miało miejsce w dniu … w … .  W ostatnich dniach doszło do incydentu, wskutek którego Pani/Pana dane osobowe mogły dostać się w niepowołane ręce. Poniżej przekazujemy informacje dotyczące tego incydentu, a także działań, jakie w związku z tym podejmujemy. Podajemy też informacje o krokach, które Pani może podjąć w związku z incydentem. Prosimy o uważną lekturę niniejszego zawiadomienia.   |  |  |  | | --- | --- | --- | | **1.** | **Charakter naruszenia ochrony danych:** |  | | **2.** | **Możliwe konsekwencje naruszenia ochrony danych:** |  | | **3.** | **Środki zastosowane lub proponowane w celu zaradzenia naruszenia ochrony danych osobowych, w tym zastosowane środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych:** |  | | **4.** | **Dane inspektora ochrony danych\*** | Np. Imię Nazwisko nr. telefonu: XXX XXX XXX, adres e-mail: nazwa\_skrzynki@domena.pl |   …………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………….\*\*  ………………………………………………………………………………  *(czytelny podpis administratora danych, zgodnie z reprezentacją podmiotu)*  \* W przypadku niepowołania należy wskazać inny punkt kontaktowy. |
|  |

Wzór 2.

Szanowna Pani/ Szanowny Panie,

Zgodnie z wymaganiami wynikającymi z przepisów dotyczących ochrony danych osobowych informujemy, że doszło do naruszenia bezpieczeństwa danych osobowych przetwarzanych przez naszą firmę, w tym również Pani/Pana dane osobowe.

W wyniku naruszenia zostały odkryte nieuprawnione działania w stosunku do naszej bazy danych, w tym przechowywane dane osobowe, takie jak imię i nazwisko, adres e-mail, adres zamieszkania i numer telefonu. Chociaż nasze środki bezpieczeństwa były w pełni funkcjonalne, przestępcy byli w stanie ominąć zabezpieczenia i uzyskać dostęp do Twoich danych osobowych.

Wszystkie dane osobowe, które zostały naruszone, są aktualnie analizowane,   
a przedsięwzięte zostaną niezbędne kroki w celu poprawy naszych standardów bezpieczeństwa danych.

W związku z wykrytym naruszeniem Twoje dane mogą być wykorzystywane do prób wyłudzeń min. Za pośrednictwem fałszywych wiadomości SMS lub dostarczenia na Twój adres e-mail informacji handlowych, na które nie wyraziłeś/aś zgody.

Jesteśmy przekonani, że jest to niezwykle niepokojąca sytuacja, ale chcemy zapewnić Panią/ Pana, że wraz z naszym zespołem ds. bezpieczeństwa pracujemy nad wzmocnieniem zabezpieczeń, aby przeciwdziałać ewentualnym przyszłym naruszeniom.

W przypadku jakichkolwiek pytań lub wątpliwości, prosimy o kontakt z nami pod adresem e-mail [adres e-mail].

Z poważaniem,

# Załącznik nr 4 Schemat procedury notyfikacji naruszeń

Obraz zawierający diagram

Opis wygenerowany automatycznie

# Załącznik nr 5 Przykłady naruszeń danych osobowych

|  |  |  |  |
| --- | --- | --- | --- |
| **Przykład** | **Czy powiadomić organ nadzorczy?** | **Czy powiadomić osobę, którą dane dotyczą?** | **Notatki/rekomendacje** |
| i. Administrator przechowuje kopię zapasową archiwum danych osobowych zaszyfrowanych na płycie CD. Płyta CD została skradziona podczas włamania. | Nie. | Nie. | Jeżeli dane są zaszyfrowane odpowiednim algorytmem, istnieją kopie zapasowe danych a unikalny klucz szyfrujący nie został złamany, to takie naruszenie może nie podlegać zgłoszeniu. |
| ii. Dane osobowe zostają pozyskane z bezpiecznej strony internetowej zarządzanej przez administratora podczas ataku cybernetycznego. Administrator obsługuje klientów w jednym państwie członkowskim UE. | Tak, należy zgłosić właściwemu organowi nadzorczemu jeżeli może się to wiązać z konsekwencjami wobec osób. | Tak, należy poinformować osoby w zależności od charakteru danych osobowych oraz jeżeli stopień potencjalnych konsekwencji wobec osób jest wysoki. | Jeżeli ryzyko nie jest wysokie, zalecamy aby administrator informował osoby  w zależności od okoliczności danej sprawy. Na przykład, poinformowanie może nie być wymagane jeżeli nastąpi naruszenie poufności w odniesieniu do newslettera związanego z programem telewizyjnym, jednakże poinformowanie może być wymagane jeżeli po charakterze newslettera można poznać poglądy polityczne osób, których dane zostały ujawnione. |
| iii. Krótka, trwająca kilka minut, awaria zasilania call center administratora, oznaczająca, że konsumenci nie mogą zadzwonić do administratora oraz uzyskać dostępu do swoich rekordów. | Nie. | Nie. | Takie naruszenie ochrony danych osobowych nie podlega notyfikacji, jednakże należy je udokumentować zgodnie z art. 33 ust. 5.  Taka dokumentacja powinna być przechowywana przez administratora. |
| iv. Administrator staje się ofiarą oprogramowania szantażującego, które powoduje zaszyfrowanie wszystkich danych. Nie istnieją kopie zapasowe i dane nie mogą być przywrócone. Po zbadaniu sprawy okazuje się, że jedyną funkcjonalnością ww. oprogramowania było zaszyfrowanie danych a w systemie nie ma żadnych innych wirusów. | Tak, należy zgłosić taką sytuację właściwemu organowi nadzorczemu, jeżeli powoduje to ewentualne konsekwencje wobec osób, jako że stanowi to utratę dostępności danych. | Tak, należy zgłosić taką sytuację osobom, w zależności od charakteru danych osobowych oraz możliwego skutku braku dostępności danych oraz innych prawdopodobnych konsekwencji. | Jeżeli istniałaby kopia zapasowa a dane mogłyby być odzyskane w odpowiednim czasie, nie trzeba by było zgłaszać tego organowi nadzorczemu ani osobom, ponieważ nie doszłoby do stałego utracenia dostępności lub poufności. Jednakże organ nadzorczy może rozważyć przeprowadzenie postępowania w celu oceny zgodności  z szerszymi wymogami w zakresie bezpieczeństwa, wynikającymi z art. 32 RODO. |
| v. Osoba dzwoni na infolinię banku w celu zgłoszenia naruszenia ochrony danych. Osoba otrzymała miesięczne zestawienie kogoś innego.  Administrator przeprowadza krótkie postępowanie wyjaśniające (tj. skończone w 24 godziny) oraz ustala z odpowiednim poziomem pewności, że doszło do naruszenia ochrony danych osobowych oraz ustala czy jest to wada systemowa, która może dotknąć innych klientów. | Tak. | Należy poinformować tylko te osoby, których to dotyczy, jeżeli istnieje wysokie ryzyko oraz jasnym jest, że nie dotyczy to innych osób. | Jeżeli, na skutek dalszego wyjaśnienia sprawy okaże się do dotknęło to większej liczby osób, należy ponownie poinformować o tym organ nadzorczy a administrator podejmuje dodatkowe kroki w celu powiadomienia innych osób, jeżeli się okaże, że dotyczy ich to ryzyko. |
| vi. Sklep internetowy działający w wielu krajach pada ofiarą cyber-ataku. Nazwy użytkowników, hasła oraz historia zakupów zostają opublikowane w Internecie przez hakera. | Tak, należy poinformować wiodący organ nadzorczy jeżeli atak dotyczy przetwarzania odbywającego się w różnych krajach. | Tak, ponieważ może to prowadzić do wysokiego ryzyka. | Administrator powinien podjąć działania, np. poprzez wymuszenie zmiany haseł na kontach, których dotyczył atak, jak również inne kroki w celu zaradzenia ryzyku. |
| vii. Spółka hostująca stronę internetową (podmiot przetwarzający) znajduje błąd w kodzie, który administruje uwierzytelnianiem użytkowników. Skutkiem tego błędu jest to, że każdy użytkownik może uzyskać dostęp do informacji o koncie każdego innego użytkownika. | Spółka hostująca, jako podmiot przetwarzający musi poinformować swoich klientów (tzn. administratorów) bez zbędnej zwłoki.  Zakładając, że spółka hostująca stronę przeprowadziła własne postępowanie wyjaśniające administratorzy danych powinni wiedzieć czy wpłynęło to na ich dane i z tego względu należy uznać, że dowiedzieli się oni o naruszeniu w momencie przekazania im informacji przez spółkę hostującą (podmiot przetwarzający). Następnie administrator musi zgłosić naruszenie organowi nadzorczemu. | Jeżeli wystąpienie wysokiego ryzyka dla osób nie jest prawdopodobne nie trzeba ich informować. | Spółka hostująca (podmiot przetwarzający) musi rozważyć, czy nie ciążą na nim żadne inne obowiązki notyfikacyjne (np. na mocy dyrektywy NIS).  Jeżeli nie ma dowodu, że w odniesieniu do tego konkretnego administratora doszło do wyzyskania podatności systemu mogło nie dojść do naruszenia podlegającemu zgłoszeniu, jednakże prawdopodobnym jest, że podlega ono obowiązkowi udokumentowania lub wynikać z braku zgodności z art. 32. |
| viii. Dane medyczne przechowywane w szpitalu stają się niedostępne przez 30 godzin na skutek ataku cybernetycznego. | Tak, szpital ma obowiązek zgłoszenia ponieważ może wystąpić wysokie ryzyka dla dobrostanu oraz prywatności pacjentów. | Tak, należy poinformować osoby, których dane zostały dotknięte atakiem cybernetycznym. |  |
| IX. Dane osobowe 5000 studentów zostały przez przypadek wysłane na złą listę, zawierającą ponad 1000 adresów. | Tak, należy zgłosić naruszenie organowi nadzorczemu. | Tak, należy poinformować osoby w zależności od zakresu oraz rodzaju danych osobowych oraz stopnia poważności ewentualnych konsekwencji. |  |
| x. Email wysłany w ramach marketingu bezpośredniego  w polach „do” lub „do wiadomości” wymienia użytkowników, pozwalając każdemu odbiorcy na poznanie adresów email innych odbiorców. | Tak, poinformowanie organu nadzorczego może być obowiązkowe jeżeli naruszenie dotyczy dużej liczby osób, jeżeli ujawniono dane wrażliwe (np. lista mailingowa psychoterapeuty), lub jeżeli inne czynniki powodują wysokie ryzyko (mail zawiera hasła) | Tak, należy poinformować osoby w zależności od zakresu oraz rodzaju danych osobowych oraz stopnia poważności możliwych konsekwencji. | Zgłoszenie może nie być konieczne jeżeli nie są ujawnione dane wrażliwe lub jeżeli ujawni ono jedynie niewielką liczbę adresów email. |