URZĄD OCHRONY DANYCH OSOBOWYCH

Poradnik na gruncie RODO

v2

Obowiązki administratorów związane z naruszeniami ochrony danych osobowych

Luty 2025

Poradnik Prezesa UODO
opracowany przez pracowników UODO po przeprowadzeniu konsultacji społecznych, w tym konsultacji z członkami Społecznego Zespołu Ekspertów przy PUODO

Opracowanie i tekst:
Bartłomiej Kowalski

Konsultacje merytoryczne i wsparcie redakcyjne:
Jacek Młotkiewicz, Bartłomiej Bitkowski, Tomasz Struk, Anna Dutkiewicz

Wersja 1.0 poradnika „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych" pochodzi z czerwca 2019 roku.
Niniejsza publikacja poradnika „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych. Poradnik na gruncie RODO" to wersja 2.0, która ukazała się w lutym 2025 roku.

URZĄD OCHRONY DANYCH OSOBOWYCH

Spis treści

1. Wprowadzenie

1.1. O czym jest ten poradnik?

Ochrona danych osobowych nabiera coraz większego znaczenia w scyfryzowanym świecie, w którym zagrożenia dla informacji i prywatności stały się codziennością. **Naruszenia ochrony danych osobowych** mogą powodować poważne konsekwencje zarówno dla osób, których dane dotyczą, jak i dla podmiotów zobowiązanych do ich zabezpieczenia. **Właściwe reagowanie** na takie incydenty jest kluczowe dla ochrony podstawowych praw i wolności oraz spełniania wymogów prawnych.

Niniejszy poradnik skierowany jest szczególnie do administratorów, podmiotów przetwarzających i inspektorów ochrony danych. Jego celem jest **wyjaśnienie i uporządkowanie** kwestii związanych z zarządzaniem naruszeniami ochrony danych osobowych w ramach RODO oraz **dostarczenie praktycznych wskazówek** w tym zakresie. Poradnik przekazuje aktualną wiedzę, uwzględniając nowe doświadczenia organów nadzorczych, publikacje Europejskiej Rady Ochrony Danych (EROD) oraz orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (TSUE).

Należy podkreślić, że poradnik ten **nie zastępuje przepisów ani oficjalnych wytycznych** – ma charakter pomocniczy i służy lepszemu zrozumieniu zasad postępowania. Wszelkie **wątpliwości należy rozstrzygać przede wszystkim w oparciu o źródła prawa oraz wskazówki i zalecenia organu nadzorczego**, dostosowane do konkretnych sytuacji.

1.2. Gdzie znaleźć dodatkowe informacje?

Jeśli informacje zawarte w poradniku okażą się niewystarczające, warto zapoznać się z następującymi materiałami:

- Rozporządzenie 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)
- Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych
- Wytyczne dotyczące inspektorów ochrony danych („DPO")
- Wyznaczenie i status IOD
- Jak rozumieć i stosować podejście oparte na ryzyku?
- Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony
- Wytyczne nr 4/2019 dotyczące artykułu 25. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych
- Wytyczne 7/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO
- Decyzja wykonawcza Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych pomiędzy administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725
- Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych
- Zgłaszanie naruszeń ochrony danych osobowych (uodo.gov.pl)
- Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO
- Narodowe Standardy Cyberbezpieczeństwa

2. Naruszenia ochrony danych osobowych

2.1. Czym jest „naruszenie ochrony danych osobowych”?

Każde działanie z użyciem informacji o osobach, które można zidentyfikować, jest **przetwarzaniem danych osobowych**[1]. Należy jednak pamiętać, że RODO nie ma zastosowania m.in. do czynności o czysto osobistym lub domowym charakterze[2].

Przykład 2.1.1.

Przetwarzaniem danych osobowych jest m.in.:

- wykorzystywanie przez sklep internetowy informacji o kupujących w celu realizacji zamówień;
- przechowywanie przez placówkę edukacyjną informacji o uczniach w celu śledzenia ich postępów w nauce;
- przeglądanie przez biuro rachunkowe informacji o klientach w celu prowadzenia księgowości i rozliczeń podatkowych.

Przykład 2.1.2.

Przepisy o ochronie danych osobowych **nie dotyczą** czynności wykonywanych wyłącznie na użytek osobisty lub domowy, takich jak m.in.:

- porządkowanie informacji o kontaktach w prywatnym telefonie komórkowym, który nie jest wykorzystywany do celów służbowych czy prowadzonej działalności gospodarczej;
- rozpowszechnianie w sieci prywatnych informacji na swój temat;
- usuwanie ze swojego komputera plików zawierających informacje o prywatnych wynikach badań lekarskich.

[1] Patrz → Art. 4 pkt 1 i 2 RODO
[2] Patrz → Art. 2 ust. 2 lit. c) RODO

Wszędzie tam, gdzie przetwarzane są dane osobowe, może dojść do **naruszenia ochrony danych osobowych**.

Jest nim **zakłócenie bezpieczeństwa przetwarzanych danych osobowych, które może wpłynąć na ich poufność, integralność lub dostępność**[3]. Dochodzi do niego bez względu na to, czy wystąpi:

- przez przypadek (np. w wyniku błędu, zaniedbania lub nieprzewidzianej awarii technicznej);
- na skutek celowego, bezprawnego działania (np. oszustwa, kradzieży lub włamania)[4].

Naruszenie ochrony danych osobowych pojawia się więc **zawsze**, gdy dochodzi do **zdarzenia**, które:

- jest **incydentem bezpieczeństwa**;
- dotyczy **przetwarzanych danych osobowych**;
- może doprowadzić do ich nieuprawnionego **zniszczenia**, **utracenia**, **zmodyfikowania**, **ujawnienia** lub **dostępu** do nich.

Tym samym naruszeniem ochrony danych osobowych **nie jest** zdarzenie, które nie spełnia któregoś z tych warunków.

> **Art. 4 pkt 12 RODO**
>
> **Definicje**
>
> *„naruszenie ochrony danych osobowych" oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;*

[3] Więcej → 2.3. Na czym polegają naruszenia poufności, integralności i dostępności danych osobowych?
[4] Więcej → 2.4. Skąd się biorą naruszenia ochrony danych osobowych?

Przykład 2.1.3.

Naruszeniem ochrony danych osobowych może być m.in.:

- strawienie przez pożar jedynego egzemplarza dokumentów kadrowych (**zniszczenie**);
- zagubienie pendrive'a będącego jedynym nośnikiem bazy informacji o klientach (**utracenie**);
- przekształcenie w ramach żartu nazwisk studentów w systemie informatycznym uczelni (**zmodyfikowanie**);
- wysłanie do niewłaściwego odbiorcy przesyłki pocztowej zawierającej niezabezpieczoną przed dostępem umowę o świadczenie usług (**ujawnienie**);
- przejęcie internetowego konta bankowego przez oszusta (**dostęp**).

Przykład 2.1.4.

Naruszeniem ochrony danych osobowych **nie będzie** m.in.:

- chwilowy brak dostępu do danych osobowych związany z zaplanowaną aktualizacją systemu informatycznego (zdarzenie **nie jest** incydentem bezpieczeństwa);
- zagubienie dokumentacji niezawierającej danych osobowych, np. dokumentów zawierających dane finansowe, których nie można powiązać z osobą fizyczną (zdarzenie **nie dotyczy** danych osobowych);
- omyłkowe wysłanie e-maila zawierającego dane osobowe do niewłaściwego – ale uprawnionego – odbiorcy wewnątrz organizacji (zdarzenie **nie prowadzi** do nieuprawnionego ujawnienia danych osobowych[5]).

Uwaga!

Jeżeli osoba, której dane dotyczą, jest zidentyfikowana lub możliwa do zidentyfikowania, pozostałe informacje o niej **nie muszą być prawdziwe**, aby mogło dojść do naruszenia ochrony danych osobowych. Przetwarzanie (np.

[5] Więcej → 2.3. Naruszenia poufności danych osobowych

wykorzystywanie, przekazywanie lub rozpowszechnianie) fałszywych danych osobowych również może prowadzić do naruszenia praw lub wolności osób, których dane te dotyczą.

Wiedza na temat naruszeń ochrony danych osobowych jest szczególnie ważna dla **administratorów**, czyli podmiotów, które decydują o celach i sposobach przetwarzania[6]. To na nich spoczywa największa odpowiedzialność za ochronę danych osobowych.

Istotną rolę w zapewnieniu bezpieczeństwa przetwarzania odgrywają również **podmioty przetwarzające**[7] i **inspektorzy ochrony danych**[8].

Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[6] Więcej → 3.1. Kim jest „administrator”?
[7] Więcej → 3.3. Kim jest „podmiot przetwarzający”?
[8] Więcej → 3.5. Kim jest „inspektor ochrony danych”?

2.2. Dlaczego naruszenia ochrony danych osobowych są niebezpieczne?

Czasami trudno dokładnie określić, **do jakich konsekwencji doprowadzi incydent bezpieczeństwa**. W niektórych przypadkach ostatecznego wpływu zdarzenia na przetwarzane dane, a w konsekwencji na osoby, których dane dotyczą, nie da się przewidzieć nie tylko na początku, ale nawet przez cały czas jego trwania.

> **Przykład 2.2.1.**
>
> Zainfekowanie systemu informatycznego uczelni złośliwym oprogramowaniem ransomware[9] może doprowadzić do zablokowania dostępu do zgromadzonych w nim zasobów (**utracenie**). W wyniku zdarzenia hakerzy mogą uzyskać także wgląd do danych osobowych pracowników i studentów (**dostęp**), a nawet skopiować je i sprzedać lub publicznie udostępnić w sieci (**ujawnienie**). Jeżeli uczelnia nie posiada kopii zapasowej bazy danych, z czasem może odzyskać dostęp jedynie do części informacji w pierwotnej lub zmienionej formie (**zmodyfikowanie**), a nawet utracić je na zawsze (**zniszczenie**).

Choć różne szczegóły dotyczące przebiegu incydentów mogą być ważne dla procesów przetwarzania, istotą naruszeń ochrony danych osobowych jest ich **potencjalnie niekorzystny wpływ na sytuację osób, których dane dotyczą**. Sama możliwość wystąpienia negatywnych skutków dla osób fizycznych powinna więc wywołać natychmiastową reakcję tych, którzy są zobligowani do ochrony danych osobowych.

> **Przykład 2.2.2.**
>
> W trakcie rutynowego audytu w siedzibie organizacji odkryto, że archiwum dokumentów zawierających m.in. dane osobowe nie było odpowiednio zabezpieczone, ponieważ drzwi do pomieszczenia pozostawały otwarte przez

[9] **Ransomware** jest rodzajem cyberataku, który m.in. blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, wysuwając następnie żądanie zapłaty w zamian za pomoc w przywróceniu stanu pierwotnego.

bliżej nieokreślony czas. Choć w pierwszych chwilach nie było wiadomo, kto w tym czasie mógł uzyskać nieuprawniony dostęp do archiwum, przy okazji potencjalnie niszcząc dokumenty, wynosząc je, zmieniając ich treść lub ją ujawniając, kierownictwo organizacji natychmiast zidentyfikowało zdarzenie jako potencjalne naruszenie ochrony danych osobowych. Miało bowiem świadomość wystąpienia incydentu bezpieczeństwa, który stworzył realne zagrożenie dla przetwarzanych danych osobowych[10].

Ewentualne **skutki** naruszeń ochrony danych osobowych, z jakimi mogą spotkać się osoby, których dane dotyczą, to m.in.:

- uszczerbek fizyczny;
- szkody majątkowe;
- szkody niemajątkowe.

Motyw 85. RODO

Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. (…)

Mimo że następstwa te bywają bardzo poważne, **należy również zwracać uwagę na pozornie nieistotne uciążliwości** dla osób, których dane są przetwarzane, takie jak dyskomfort, niepokój czy stres. Organizacje powinny uwzględniać **szeroki katalog możliwych skutków** naruszeń ochrony danych osobowych.

[10] Więcej → 5. Identyfikowanie naruszeń ochrony danych osobowych

Przykład 2.2.3.

Na skutek awarii sprzętu szpital utracił dostęp do danych medycznych pacjenta, który uległ wypadkowi i przebywał nieprzytomny na jednym z oddziałów. W rezultacie lekarka nie dysponowała informacją o konieczności regularnego podawania pacjentowi leków na nadciśnienie, o czym wcześniej zawiadamiała jego rodzina. Nieprzyjęcie leków doprowadziło do gwałtownego wzrostu ciśnienia u pacjenta, co zakończyło się zawałem. W tym przypadku naruszenie ochrony danych osobowych wywołało skutek w postaci **uszczerbku fizycznego**.

Przykład 2.2.4.

Bank omyłkowo przekazał dane jednego ze swoich klientów, w tym informacje umożliwiające dostęp do bankowości internetowej, niewłaściwej osobie. Nieuprawniony odbiorca, korzystając z otrzymanych danych, przez kilka miesięcy regularnie dokonywał drobnych zakupów, płacąc środkami klienta. Przez długi czas właściciel konta nie zauważał tych transakcji, a gdy w końcu odkrył nieprawidłowości, okazało się, że odzyskanie utraconych pieniędzy nie było już możliwe. W tym przypadku naruszenie ochrony danych osobowych wywołało skutek w postaci **szkód majątkowych**.

Przykład 2.2.5.

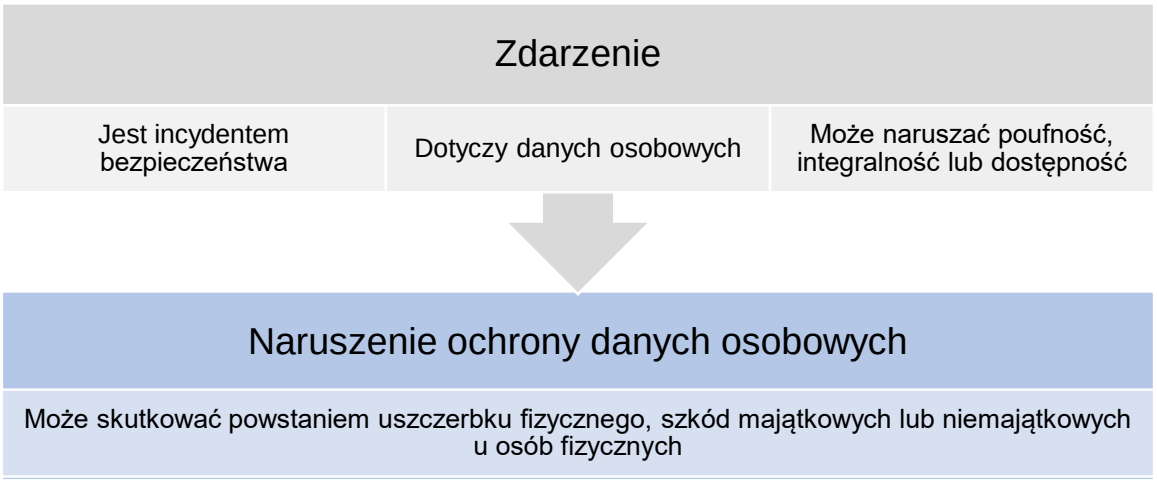
Firma rekrutacyjna przez pomyłkę opublikowała dane jednego z kandydatów, w tym historię zatrudnienia, list motywacyjny oraz notatki z rozmowy kwalifikacyjnej, na ogólnodostępnej stronie internetowej. Informacje były widoczne przez kilka tygodni i zostały przypadkowo odkryte przez samego kandydata, który zauważył, że jego dane były szeroko komentowane w mediach społecznościowych. W efekcie kandydat doświadczył stresu, poczucia wstydu i obawy o swoją reputację zawodową, co miało negatywny wpływ na jego samopoczucie oraz zaufanie do bezpieczeństwa procesów rekrutacyjnych. W tym przypadku naruszenie ochrony danych osobowych wywołało skutek w postaci **szkód niemajątkowych**.

Do naruszenia ochrony danych osobowych dochodzi **niezależnie od tego**, czy niepożądane konsekwencje dla osób fizycznych rzeczywiście wystąpią. Ocena dotycząca tego, **czy taka sytuacja może się wydarzyć i jak może być**

dotkliwa dla jednej lub więcej osób, stanowi jeden z kluczowych obowiązków administratorów związanych z naruszeniami ochrony danych osobowych[11].

Zapamiętaj

Infografika 2.2.1.



Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[11] Więcej → 7. Ocena ryzyka związanego z naruszeniami ochrony danych osobowych

2.3. Na czym polegają naruszenia poufności, integralności i dostępności danych osobowych?

Przetwarzanie musi być **bezpieczne**[12], a naruszenia ochrony danych osobowych mogą zakłócać bezpieczeństwo przetwarzania w różny sposób. Ze względu na ich charakter wyróżnia się:

- naruszenia **poufności** danych;
- naruszenia **integralności** danych;
- naruszenia **dostępności** danych.

> **Uwaga!**
>
> Naruszenia ochrony danych osobowych mogą wpływać równolegle na **więcej niż jeden** aspekt bezpieczeństwa[13].

Naruszenia poufności danych osobowych

Poufność danych osobowych oznacza, że mogą się z nimi zapoznać wyłącznie osoby do tego **uprawnione**, czyli takie, które posiadają odpowiednie upoważnienie lub podstawę prawną do podejmowania określonych działań z użyciem danych osobowych.

Naruszenie **poufności** danych osobowych występuje w przypadku:

- nieuprawnionego **ujawnienia** danych osobowych;
- nieuprawnionego uzyskania **dostępu** do danych osobowych.

[12] Patrz → Art. 32 ust. 1 i 2 RODO
[13] Patrz → Przykład 2.2.1.

Do nieuprawnionego **ujawnienia** danych osobowych dochodzi, gdy ten, kto przetwarza dane osobowe, umożliwi zapoznanie się z nimi osobom nieuprawnionym.

Nieuprawniony **dostęp** do danych osobowych ma miejsce, gdy osoba nieuprawniona samodzielnie (np. bez upoważnienia) uzyska możliwość ich przetwarzania.

Uwaga!

Działanie grupy osób w ramach jednej organizacji nie oznacza, że każda z tych osób jest uprawniona do przetwarzania wszystkich posiadanych przez organizację danych osobowych na wszelkie możliwe sposoby. Naruszenie ochrony danych osobowych, w tym ich poufności, może wystąpić także **wewnątrz struktury** administratora lub podmiotu przetwarzającego.

Przykład 2.3.2.

Naruszeniem **poufności** danych osobowych może być m.in.[14]:

- ustne przekazanie osobom nieuprawnionym informacji będących danymi osobowymi, powziętych w związku z wykonywanym zawodem lub sprawowaną funkcją;
- omyłkowe wysłanie e-maila zawierającego dane osobowe do niewłaściwego (i nieuprawnionego) odbiorcy (chyba że administrator ma dowód niedostarczenia wiadomości);
- wyrzucenie do śmieci dokumentów zawierających dane osobowe lub pozostawienie ich w miejscu, do którego dostęp mają osoby postronne (nieuprawnione);
- sprzedaż starych telefonów, komputerów lub innych nośników bez uprzedniego trwałego usunięcia danych osobowych zapisanych w ich pamięciach;

[14] Więcej → Przykład 2.4.1., Przykład 2.4.2., Przykład 2.4.3., Przykład 2.4.6., Przykład 2.4.8., Przykład 2.5.1., Przykład 3.2.1., Przykład 5.2.1., Przykład 7.1.1., Przykład 7.1.2., Przykład 7.1.3., Przykład 7.1.4., Przykład 11.1.2.

- nieodebranie byłemu pracownikowi dostępu do systemu informatycznego umożliwiającego przeglądanie danych osobowych;
- włamanie się przez nieuprawnione osoby do pomieszczenia, w którym przechowywane są dokumenty zawierające dane osobowe (chyba że administrator ma dowód braku dostępu do dokumentów);
- przełamanie przez cyberprzestępców zabezpieczeń systemu informatycznego umożliwiającego wgląd do danych osobowych.

Naruszenia integralności danych osobowych

Naruszenie **integralności** danych osobowych występuje w przypadku nieuprawnionego **zmodyfikowania** danych osobowych.

Może do niego dojść w przypadku:

- dokonania jakiejkolwiek zmiany przez osobę **nieuprawnioną**;
- dokonania nieprawidłowej (np. przypadkowej, błędnej, niedokładnej, niekompletnej, nieaktualnej) zmiany przez osobę **uprawnioną** (lub niedokonania przez nią odpowiedniej zmiany).

Przykład 2.3.3.

Naruszeniem **integralności** danych osobowych może być m.in.[15]:

- wprowadzenie do dokumentacji błędnych danych osobowych;
- niewprowadzenie do bazy danych zmian informacji, które powinny być zaktualizowane;
- wystąpienie awarii sprzętu elektronicznego skutkującej przekształceniem przetwarzanych za jego pomocą danych osobowych;
- działanie złośliwego oprogramowania dokonującego zmiany w plikach zawierających dane osobowe;

[15] Więcej → Przykład 2.4.4., Przykład 2.4.7., Przykład 2.5.3., Przykład 3.4.1., Przykład 5.2.2., Przykład 7.1.5.

- włamanie się osoby nieuprawnionej do systemu kadrowego i podmienienie numerów rachunków bankowych pracowników na inne;
- odtworzenie z kopii zapasowej danych osobowych i brak ich aktualizacji.

Naruszenia dostępności danych osobowych

Dostępność danych osobowych oznacza, że mogą być one bez przeszkód przetwarzane zgodnie z ich przeznaczeniem przez osoby do tego **uprawnione**.

Naruszenie **dostępności** danych osobowych występuje w przypadku:

- nieuprawnionego **utracenia** danych osobowych;
- nieuprawnionego **zniszczenia** danych osobowych.

Nieuprawnione **utracenie** danych osobowych dotyczy sytuacji, w której czasowo lub trwale nie da się z nich skorzystać, choć istnieje możliwość ich odzyskania lub odtworzenia.

Do nieuprawnionego **zniszczenia** danych osobowych dochodzi wtedy, gdy przepadają one nieodwracalnie, ponieważ administrator nie ma możliwości ich ponownego odtworzenia (np. z kopii zapasowej).

Przykład 2.3.4.

Naruszeniem **dostępności** danych osobowych może być m.in.[16]:

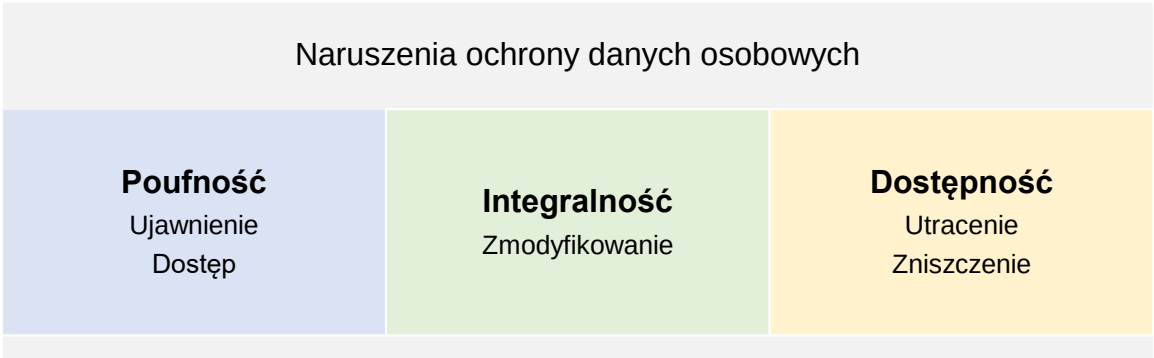
- zagubienie papierowej dokumentacji lub elektronicznego nośnika (np. pendrive'a, dysku SSD, płyty CD) zawierającego dane osobowe (jedynego egzemplarza);
- trwała lub czasowa utrata dostępu do danych osobowych z powodu awarii systemu informatycznego lub cyberataku;

[16] Więcej → Przykład 2.4.5., Przykład 2.4.9., Przykład 5.2.3., Przykład 7.1.2., Przykład 7.1.6., Przykład 10.1.1., Przykład 11.1.1.

- utrata dostępu do danych osobowych na skutek zablokowania lub usunięcia konta użytkownika;
- utrata dostępu do danych osobowych w wyniku problemów technicznych dostawcy chmury obliczeniowej;
- zniszczenie infrastruktury przechowującej dane osobowe (np. pomieszczenia archiwum, serwerów) bez możliwości przywrócenia dostępu do danych w zaplanowanym czasie.

Zapamiętaj

Infografika 2.3.1.



Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

2.4. Skąd się biorą naruszenia ochrony danych osobowych?

Naruszenia ochrony danych osobowych **mogą pojawiać się w każdej organizacji**, bez względu na jej wielkość, zakres przetwarzanych danych osobowych czy środki przeznaczone na ich ochronę. Zrozumienie źródeł tych zjawisk pomaga w skutecznym zapobieganiu im i odpowiednim reagowaniu w przypadku ich występowania.

Przyczynami powstawania naruszeń ochrony danych osobowych mogą być:

- zdarzenia **przypadkowe**;
- celowe, **bezprawne działania**.

Oznacza to, że do naruszenia ochrony danych osobowych dochodzi niezależnie od czynników, jakie miały wpływ na jego wystąpienie, o ile sam incydent **spełnia warunki określone w RODO**[17].

> **Uwaga!**
>
> Naruszenie ochrony danych osobowych **nie musi** wynikać z winy administratora lub podmiotu przetwarzającego. Celem regulacji jest przede wszystkim **ochrona praw i wolności osób fizycznych**, dlatego **każdy** incydent bezpieczeństwa danych osobowych, niezależnie od tego, kto go spowodował, powinien być traktowany poważnie.

Najczęściej spotykane **przyczyny** występowania naruszeń ochrony danych osobowych to m.in.:

- błędy ludzkie;
- niewystarczające zabezpieczenia lub procedury;
- cyberprzestępczość;

[17] Więcej → 2.1. Czym jest „naruszenie ochrony danych osobowych”?

- zamierzone nadużycia wewnętrzne;
- czynniki fizyczne lub środowiskowe.

Nie jest to jednak lista wyczerpująca. W rzeczywistości źródła incydentów bywają nieszablonowe i wielowarstwowe, a scenariusze wydarzeń różnią się od siebie w zależności od specyfiki i okoliczności przetwarzania.

Błędy ludzkie

Pomimo że administratorzy i podmioty przetwarzające nieustannie powinni dążyć do ograniczania występowania błędów, szkodliwe działania lub zaniechania (np. pracowników) to **jedna z najczęstszych przyczyn** powstawania naruszeń ochrony danych osobowych.

Wiele z nich wynika z:

- przyczyn **losowych** (spowodowanych np. zwykłą pomyłką, zaniedbaniem czy nieszczęśliwym zbiegiem okoliczności);
- **braku świadomości** (spowodowanego np. brakiem odpowiednich szkoleń).

> **Przykład 2.4.1.**
>
> Pracownik działu kadr administratora zapisał plik z wrażliwymi danymi osobowymi na firmowym dysku w chmurze obliczeniowej. Przez przypadkowy ruch kursorem umieścił go jednak w ogólnodostępnej lokalizacji, zamiast w specjalnym folderze o ograniczonym dostępie. W rezultacie z informacjami mogły zapoznać się osoby, które nie były do tego uprawnione.
>
> Do naruszenia ochrony danych osobowych doszło więc w wyniku **błędu pracownika administratora**.

Nieumyślnie zakłócać bezpieczeństwo danych osobowych mogą także osoby, które w jakiś sposób uczestniczą w działaniach związanych z przetwarzaniem,

mimo że pozostają **poza wewnętrzną strukturą** administratora lub podmiotu przetwarzającego.

> **Przykład 2.4.2.**
>
> Firma ubezpieczeniowa, jako administrator, wysłała do swojego klienta list zawierający polisę ubezpieczeniową. Kurier przypadkowo doręczył przesyłkę sąsiadowi adresata, który zapoznał się z jej zawartością.
>
> W tej sytuacji naruszenie ochrony danych osobowych wystąpiło w wyniku **błędu pracownika operatora pocztowego**.

> **Przykład 2.4.3.**
>
> Klient sklepu internetowego podczas składania zamówienia przypadkowo wpisał do formularza nieprawidłowy adres e-mail (zamienił miejscami dwa znaki w adresie). W konsekwencji potwierdzenie zamówienia wraz z fakturą zawierającą jego dane osobowe zostało wysłane do niewłaściwej osoby.
>
> Powyższe naruszenie ochrony danych osobowych powstało w wyniku **błędu osoby, której dane dotyczą**.

Nie wszystkie błędy są spowodowane wyłącznie niefortunnymi okolicznościami. Na ich występowanie może wpływać też **brak świadomości** lub lekceważenie zasad ochrony danych osobowych czy też zagrożeń wynikających z nieprzestrzegania wewnętrznych procedur bezpieczeństwa.

> **Przykład 2.4.4.**
>
> Wolontariusz, który nie został odpowiednio przeszkolony w zakresie ochrony danych osobowych, pełnił dyżur w biurze organizacji charytatywnej. Podczas swojej pracy odebrał telefon od osoby fałszywie podającej się za jednego z beneficjentów, która poprosiła o zmienienie informacji na jej temat w bazie organizacji. Wolontariusz, nieświadomy obowiązujących procedur dotyczących weryfikacji tożsamości klienta oraz modyfikacji danych osobowych, wprowadził nowe, nieprawidłowe dane osobowe do systemu.

Działanie wolontariusza, skutkujące naruszeniem ochrony danych osobowych, było błędem wynikającym z **braku świadomości** na temat zasad i procedur dotyczących ochrony danych osobowych.

Niewystarczające zabezpieczenia lub procedury

Zdarza się, że podmioty odpowiedzialne za bezpieczeństwo przetwarzania nie wykonują prawidłowo nałożonych na nie obowiązków. W sytuacji, gdy organizacja przetwarzająca dane osobowe nie dysponuje odpowiednimi:

- **zabezpieczeniami** technicznymi;
- wewnętrznymi **procedurami** bezpieczeństwa;

staje się ona bardziej podatna na incydenty.

Problem ten polega nie tylko na niewdrażaniu niezbędnych środków bezpieczeństwa, ale także na **nieprawidłowej konfiguracji** wykorzystywanych narzędzi informatycznych (polegającej np. na zachowaniu domyślnych ustawień), utrzymywaniu **nieskutecznych metod** postępowania czy stosowaniu **praktyk sprzecznych z zasadami** ochrony danych osobowych.

Dobór właściwych rozwiązań w każdym przypadku powinien być wynikiem **oceny ryzyka** związanego z przetwarzaniem[18].

Przykład 2.4.5.

Stowarzyszenie sportowe przechowywało dane osobowe swoich członków na lokalnym komputerze w siedzibie organizacji. Komputer nie był jednak wyposażony w odpowiednie systemy ochrony danych, takie jak automatyczne tworzenie kopii zapasowych. Gdy doszło do awarii dysku twardego, jego zawartość stała się niedostępna. Stowarzyszenie nie zdołało odzyskać utraconych informacji.

Naruszenie ochrony danych osobowych wywołane zostało **brakiem odpowiednich zabezpieczeń**.

[18] Więcej → 4.1. Na czym polega „podejście oparte na ryzyku”?

Przykład 2.4.6.

Po odejściu pracownika działu kadr instytucji publicznej odpowiedzialnej za obsługę świadczeń społecznych pracodawca nie odebrał mu uprawnień do systemów informatycznych, takich jak platforma do zarządzania danymi pracowników i organizowania podróży służbowych. Stało się tak, ponieważ w organizacji brakowało procedury dotyczącej odbierania dostępu byłym pracownikom. W efekcie były pracownik nadal miał dostęp do danych kadrowych i informacji o podróżach służbowych innych pracowników.

Naruszenie ochrony danych osobowych spowodowane było **brakiem odpowiednich procedur**.

Cyberprzestępczość

Dane osobowe są coraz częściej przetwarzane w formie cyfrowej, a jednym z największych zagrożeń dla ich bezpieczeństwa są **nielegalne działania prowadzone z wykorzystaniem technologii informatycznych i sieci komputerowych**. Z tego powodu do wielu naruszeń ochrony danych osobowych dochodzi w wyniku działań cyberprzestępców, takich jak m.in.:

- phishing[19];
- wykorzystywanie złośliwego oprogramowania (np. ransomware[20]);
- eksploatacja luk w zabezpieczeniach informatycznych.

Przykład 2.4.7.

Cyberprzestępca za pomocą ataku *phishingowego* wprowadził do systemu firmy telekomunikacyjnej złośliwe oprogramowanie, które automatycznie zmodyfikowało bazę danych klientów, zmieniając plany taryfowe i wprowadzając do nich losowe, nieprawdziwe informacje.

[19] **Phishing** jest oszustwem technicznym i socjotechnicznym polegającym na podszyciu się pod zaufaną osobę lub instytucję w celu wyłudzenia wrażliwych informacji lub uzyskania dostępu do systemu informatycznego. Opiera się zazwyczaj na sfałszowanych stronach internetowych, SMS-ach, e-mailach lub wiadomościach wysyłanych poprzez inne komunikatory internetowe.
[20] Więcej → Ransomware

Do naruszenia ochrony danych osobowych doszło na skutek **nielegalnego działania cyberprzestępcy**.

Zamierzone nadużycia wewnętrzne

Niewłaściwe działania personelu administratora lub podmiotu przetwarzającego nie zawsze są przypadkowe i nieumyślne. Czasami osoby posiadające dostęp do danych osobowych celowo wykorzystują swoje uprawnienia do **zachowań sprzecznych z przepisami prawa i zasadami ochrony danych osobowych**. Takie postępowanie może wynikać ze zwykłej ciekawości, potrzeby realizacji osobistych interesów, a nawet działalności przestępczej. Bez względu na motywacje, tego rodzaju nadużycia mogą prowadzić do poważnych konsekwencji.

Przykład 2.4.8.

Pracownik banku, posiadający uprawnienia do przeglądania danych osobowych klientów, z ciekawości postanowił sprawdzić stan konta swojego znajomego. Chociaż nie ujawnił tych informacji nikomu innemu, jego działanie było niezgodne z wewnętrznymi procedurami banku i zasadami ochrony danych osobowych.

W takim przypadku naruszenie ochrony danych osobowych wystąpiło w wyniku **zamierzonego nadużycia uprawnień** w ramach organizacji administratora.

Czynniki fizyczne lub środowiskowe

Niektóre naruszenia ochrony danych osobowych mogą być spowodowane przez **czynniki niezależne**. Zalicza się do nich m.in.:

- katastrofy naturalne (np. powodzie, pożary czy trzęsienia ziemi);
- awarie infrastruktury technicznej (np. przerwy w dostawie prądu, uszkodzenia sieci telekomunikacyjnych);

- oraz inne zdarzenia losowe (np. kradzieże, włamania, przypadkowe zniszczenie nośników danych).

Pomimo losowości takich zdarzeń, podmioty odpowiedzialne za bezpieczeństwo przetwarzania muszą być świadome ich występowania i przygotowane na różne niecodzienne sytuacje.

Przykład 2.4.9.

W szpitalu doszło do awarii systemu chłodzenia w serwerowni, co spowodowało przegrzanie serwerów i ich awaryjne wyłączenie, uniemożliwiając wgląd do baz danych dotyczących pacjentów. Choć szpital był zabezpieczony przez trwałą utratą danych, awaria spowodowała kilkugodzinną przerwę w dostępie do ważnych informacji medycznych.

Powyższe naruszenie ochrony danych osobowych wystąpiło na skutek niespodziewanej **awarii infrastruktury technicznej**.

Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

2.5. Czym się różni „naruszenie ochrony danych osobowych” od „naruszenia przepisów RODO”?

Wystąpienie **naruszenia ochrony danych osobowych** nie oznacza samo w sobie, że administrator lub podmiot przetwarzający dopuścił się **naruszenia przepisów RODO**.

Choć obydwa te zjawiska określa się potocznie mianem „naruszeń”, ich znaczenie jest inne.

Naruszenie przepisów RODO wynika z postępowania niezgodnego z określonymi wymogami przewidzianymi w tym akcie prawnym, które może – ale nie musi – wpływać na powstawanie incydentów bezpieczeństwa.

> **Przykład 2.5.1.**
>
> Szpital zapewnił najwyższy standard ochrony danych osobowych i zgodnie z zasadami RODO wdrożył odpowiednie środki bezpieczeństwa przetwarzania[21]. Mimo to padł ofiarą zaawansowanego cyberataku wykorzystującego nieznaną wcześniej lukę w oprogramowaniu (tzw. atak typu zero-day[22]). Przestępcy uzyskali dostęp do bazy danych pacjentów i skopiowali wrażliwe informacje medyczne.
>
> W tym przypadku naruszenie ochrony danych osobowych **wystąpiło**, choć administrator **nie naruszył** przepisów RODO.

> **Przykład 2.5.2.**
>
> Firma marketingowa gromadziła dane osobowe klientów, nie uzyskawszy na to wyraźnej zgody (i nie definiując przy tym innej przesłanki legalizującej proces przetwarzania), oraz nie informowała ich o celach przetwarzania. Dane były jednak przechowywane w bezpieczny sposób, a w organizacji nie dochodziło do incydentów bezpieczeństwa. Po pewnym czasie nowo zatrudniony

[21] Więcej → 4.2. Jak zapobiegać naruszeniom ochrony danych osobowych?

[22] **Zero-day** to luka lub błąd w oprogramowaniu, której twórcy jeszcze nie wykryli. Z tego powodu użytkownicy nie mają możliwości odpowiedniego zabezpieczenia się, co pozwala hakerom na wykorzystanie podatności, zanim zostanie usunięta. Ataki tego typu są szczególnie niebezpieczne, ponieważ twórcy oprogramowania dopiero opracowują działania zapobiegawcze.

inspektor ochrony danych poinformował kierownictwo firmy o naruszaniu przez nią zasady legalności przetwarzania i braku realizacji obowiązków informacyjnych. W odpowiedzi organizacja w pełni dostosowała swoją działalność do wymogów RODO.

W tej sytuacji **nie doszło** do naruszenia ochrony danych osobowych, mimo że administrator **naruszył** przepisy RODO.

Przykład 2.5.3.

Jedna z partii politycznych nie wdrożyła odpowiednich środków bezpieczeństwa danych osobowych wymaganych przez RODO i nie zabezpieczyła się na wypadek nieoczekiwanych zdarzeń. W wyniku błędu technicznego podczas aktualizacji systemu informatycznego członek zespołu IT nieświadomie zmodyfikował dane osobowe w bazie sympatyków partii.

W tym przypadku **doszło** do naruszenia ochrony danych osobowych, a administrator **naruszył** przepisy RODO. Ponadto okoliczności zdarzenia wskazują, że incydent bezpieczeństwa **mógł być** wynikiem praktyk administratora niezgodnych z RODO, a jego wystąpieniu dało się zapobiec.

Mimo że RODO nakłada na administratorów i podmioty przetwarzające obowiązek zapewnienia **bezpieczeństwa** przetwarzania, **nie da się całkowicie wyeliminować ryzyka** pojawiania się naruszeń ochrony danych osobowych[23]. Działanie nawet najlepiej zabezpieczonych systemów informatycznych może zostać zakłócone przez nieprzewidziane zdarzenia, takie jak pomyłki, katastrofy naturalne czy zaawansowane cyberataki[24].

Celem RODO **nie jest** zapewnienie absolutnej nienaruszalności danych osobowych, ale zagwarantowanie, że organizacje podejmą wszelkie **adekwatne kroki**, aby minimalizować ryzyko oraz chronić prawa i wolności osób, których dane dotyczą, na najwyższym możliwym poziomie[25], a także **odpowiednio zareagują** w razie wystąpienia incydentu[26].

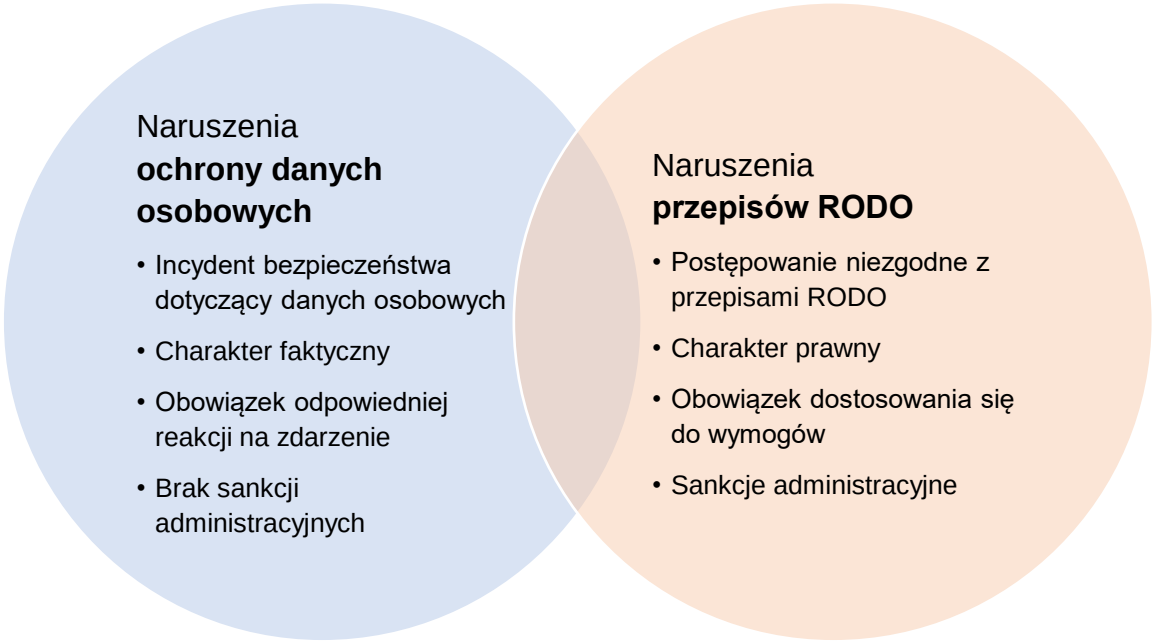
[23] Więcej → 4.1. Na czym polega „podejście oparte na ryzyku”?
[24] Więcej → 2.4. Skąd się biorą naruszenia ochrony danych osobowych?
[25] Więcej → 4.2. Jak zapobiegać naruszeniom ochrony danych osobowych?
[26] Więcej → 3. Obowiązki związane z naruszeniami ochrony danych osobowych

Uwaga!

RODO **nie przewiduje** obowiązku zapobiegania **wszelkim możliwym** naruszeniom ochrony danych osobowych. Jeżeli takie zdarzenie wystąpiło **pomimo** prawidłowego realizowania obowiązków przez podmioty zobowiązane do zapewnienia bezpieczeństwa przetwarzania, nie muszą się one obawiać zastosowania wobec nich sankcji administracyjnych.

Zapamiętaj

Infografika 2.5.1.



3. Obowiązki związane z naruszeniami ochrony danych osobowych

3.1. Kim jest „administrator”?

Możliwość przetwarzania danych osobowych wiąże się z szeregiem **obowiązków**. Ich głównym celem jest **ochrona osób, których dane dotyczą,** przed niepożądanymi konsekwencjami przetwarzania.

Za prawidłowe stosowanie przepisów RODO – w tym bezpieczeństwo przetwarzania – odpowiadają przede wszystkim **administratorzy**, czyli **podmioty, które decydują „po co” i „jak” będą podejmowane działania z użyciem danych osobowych**. W niektórych przypadkach cele i sposoby przetwarzania oraz fakt bycia administratorem wyznaczane są w przepisach prawa, np. w ustawie.

> **Art. 4 pkt 7 RODO**
>
> **Definicje**
>
> *„administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;*

> **Uwaga!**
>
> Status administratora **nie jest kwestią umowną**. Nawet jeżeli strony określą w umowie, który podmiot jest administratorem, ostatecznie jest nim ten, kto **faktycznie** określa cele i sposoby przetwarzania.

Dowiedz się więcej

> → Wytyczne 7/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO

3.2. Jakie obowiązki mają administratorzy w związku z naruszeniami ochrony danych osobowych?

Obowiązki, które administratorzy muszą realizować **stale** w związku z możliwością występowania naruszeń ochrony danych osobowych, to:

- **zapobieganie** powstawaniu naruszeń ochrony danych osobowych (poprzez zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzania[27]);
- **wykrywanie** i „stwierdzanie" naruszeń ochrony danych osobowych[28].

W przypadku „stwierdzenia" naruszenia ochrony danych osobowych administratorzy muszą zrealizować **dodatkowe** obowiązki. Są to:

- **zaradzenie** naruszeniu ochrony danych osobowych oraz jego ewentualnym negatywnym skutkom[29];
- **ocenienie ryzyka** naruszenia praw lub wolności osób fizycznych, jakie może wynikać z naruszenia ochrony danych osobowych[30];
- **zgłoszenie** naruszenia ochrony danych osobowych organowi nadzorczemu (w przypadku **ryzyka** naruszenia praw lub wolności osób fizycznych)[31];
- **zawiadamianie** osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych (w przypadku **wysokiego ryzyka** naruszenia praw lub wolności tych osób)[32];
- **dokumentowanie** naruszenia ochrony danych osobowych[33].

[27] Więcej → 4. Zapobieganie powstawaniu naruszeń ochrony danych osobowych
[28] Więcej → 5. Identyfikowanie naruszeń ochrony danych osobowych
[29] Więcej → 6. Zaradzanie naruszeniom ochrony danych osobowych
[30] Więcej → 7. Ocena ryzyka związanego z naruszeniami ochrony danych osobowych
[31] Więcej → 9. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu
[32] Więcej → 10. Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych
[33] Więcej → 8. Dokumentowanie naruszeń ochrony danych osobowych

Odpowiednie postępowanie z incydentami, w tym naruszeniami ochrony danych osobowych, ma kluczowe znaczenie dla poprawy bezpieczeństwa przetwarzania.

Starannie zaplanowane zarządzanie tym procesem pozwala nie tylko na **szybkie i skuteczne reagowanie** na incydenty, ale także na wyciąganie z nich wniosków, które pomagają **usprawniać** stosowane środki bezpieczeństwa.

Każde takie zdarzenie stanowi okazję do poprawy zabezpieczeń i **minimalizowania ryzyka** występowania podobnych incydentów w przyszłości.

> **Przykład 3.2.1.**
>
> Duża instytucja finansowa zabezpieczyła oraz regularnie monitorowała bezpieczeństwo swoich systemów, aby **zapobiegać** naruszeniom ochrony danych osobowych. Pewnego dnia odkryła, że dostęp do bazy klientów uzyskała osoba nieuprawniona. Instytucja „**stwierdziła**" naruszenie ochrony danych osobowych i natychmiast podjęła działania **zaradcze**, naprawiając lukę w zabezpieczeniach, a następnie **oceniła ryzyko** dla osób, których dane dotyczyły. Ponieważ ryzyko istniało, **zgłosiła** naruszenie ochrony danych osobowych do Prezesa UODO, a jako że ryzyko było wysokie, **zawiadomiła** o tym zdarzeniu także podmioty danych. Instytucja na bieżąco **dokumentowała** przebieg procesu, a po jego zakończeniu wdrożyła dodatkowe zabezpieczenia, aby unikać podobnych problemów w przyszłości i skuteczniej **zapobiegać** naruszeniom ochrony danych osobowych.

Odpowiedzialność i rozliczalność

Odpowiedzialność administratorów dotycząca naruszeń ochrony danych osobowych – podobnie jak w przypadku innych obowiązków wynikających z RODO – opiera się na **zasadzie rozliczalności**[34]. Oznacza to, że administratorzy **muszą być w stanie wykazać**, że prawidłowo wykonują swoje obowiązki.

Z tego powodu administratorzy powinni dbać o gromadzenie (dokumentowanie) **dowodów**, które w razie potrzeby (np. na wezwanie organu nadzorczego lub w

[34] Patrz → Art. 5 ust. 2 RODO

przypadku kontroli) potwierdzą zgodność ich działań z przepisami o ochronie danych osobowych. Mogą to być m.in.:

- tradycyjne dokumenty (np. notatki, instrukcje i korespondencja);
- wyciągi z systemów;
- raporty z audytów czy testów bezpieczeństwa[35].

> **Uwaga!**
>
> To **niewykonywanie** lub **nieprawidłowe wykonywanie** przedstawionych wyżej obowiązków – a nie samo w sobie występowanie naruszeń ochrony danych osobowych – świadczy o **naruszaniu przepisów RODO**[36].

Współadministratorzy

W przypadku **współadministrowania** danymi, czyli **gdy dwie lub więcej organizacji wspólnie ustalają cele i sposoby przetwarzania danych osobowych**, odpowiedzialność za zarządzanie naruszeniami ochrony danych osobowych jest wspólna.

Współadministratorzy **muszą uzgodnić swoje obowiązki** dotyczące postępowania w takich sytuacjach. Ważne jest, aby ustalić jasne zasady współpracy, które określą m.in., który z administratorów – i w jakim zakresie – odpowiada za zgłaszanie naruszeń ochrony danych osobowych Prezesowi UODO czy też zawiadamianie o nich osób fizycznych. Przejrzysty **podział ról** zapewnia sprawniejsze działanie w sytuacjach kryzysowych i pomaga współadministratorom zachować zgodność z przepisami RODO[37].

[35] Więcej → 8. Dokumentowanie naruszeń ochrony danych osobowych
[36] Więcej → 2.5. Czym się różni „naruszenie ochrony danych osobowych" od „naruszenia przepisów RODO"?
[37] Patrz → Art. 26 RODO

Zapamiętaj

Infografika 3.2.1.

<table>
<tr><td rowspan="2">Stałe obowiązki administratora</td><td colspan="2">Zapobieganie powstawaniu naruszeń ochrony danych osobowych</td></tr>
<tr><td colspan="2">Wykrywanie i „stwierdzanie” naruszeń ochrony danych osobowych</td></tr>
<tr><td rowspan="5">Obowiązki administratora w przypadku wystąpienia naruszenia ochrony danych osobowych</td><td colspan="2">Zaradzenie naruszeniu ochrony danych osobowych i jego ewentualnym negatywnym skutkom</td></tr>
<tr><td colspan="2">Ocenienie ryzyka naruszenia praw lub wolności osób fizycznych w związku z naruszeniem ochrony danych osobowych</td></tr>
<tr><td>Ryzyko</td><td>Wysokie ryzyko</td></tr>
<tr><td rowspan="2">Zgłoszenie naruszenia ochrony danych osobowych Prezesowi UODO</td><td>Zgłoszenie naruszenia ochrony danych osobowych Prezesowi UODO</td></tr>
<tr><td>Zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych</td></tr>
<tr><td colspan="2">Dokumentowanie naruszenia ochrony danych osobowych</td></tr>
<tr><td rowspan="2">Stałe obowiązki administratora</td><td colspan="2">Zapobieganie powstawaniu naruszeń ochrony danych osobowych</td></tr>
<tr><td colspan="2">Wykrywanie i „stwierdzanie” naruszeń ochrony danych osobowych</td></tr>
</table>

Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

3.3. Kim jest „podmiot przetwarzający”?

Chociaż to administratorzy ustalają cele i sposoby przetwarzania danych osobowych, często angażują inne podmioty do wykonywania konkretnych czynności w ich imieniu. Takie podmioty nazywane są **podmiotami przetwarzającymi**.

Podmioty przetwarzające działają na podstawie umów z administratorami (lub innych instrumentów prawnych) i przetwarzają dane wyłącznie **zgodnie z ich instrukcjami**. Rola podmiotów przetwarzających jest bardzo ważna, ponieważ również na nich – nie tylko na administratorów – przepisy prawa nakładają **obowiązki** związane z ochroną danych osobowych.

> **Art. 4 pkt 8 RODO**
>
> **Definicje**
>
> *„podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;*

Role administratorów i podmiotów przetwarzających **czasami nakładają się lub zacierają**. Zdarza się, że jedna organizacja może pełnić jednocześnie obie te funkcje. Z tego powodu zawsze należy odpowiednio precyzyjnie określać obowiązki poszczególnych stron w kontekście konkretnych okoliczności przetwarzania (np. celów przetwarzania, kategorii przetwarzanych danych).

Dowiedz się więcej

> → Wytyczne 7/2020 dotyczące pojęć administratora i podmiotu przetwarzającego zawartych w RODO

3.4. Jakie obowiązki mają podmioty przetwarzające w związku z naruszeniami ochrony danych osobowych?

Obowiązki, które podmioty przetwarzające muszą realizować **stale** w związku z możliwością występowania naruszeń ochrony danych osobowych, to:

- **zapobieganie** powstawaniu naruszeń ochrony danych osobowych (poprzez zapewnienie odpowiedniego poziomu bezpieczeństwa przetwarzania oraz postępowanie zgodne z instrukcjami administratorów)[38];
- **wykrywanie** naruszeń ochrony danych osobowych[39].

W reakcji na naruszenia ochrony danych osobowych podmioty przetwarzające muszą realizować **dodatkowe** obowiązki. Są to:

- **zgłoszenie** „stwierdzonego" naruszenia ochrony danych osobowych administratorowi[40];
- **pomaganie** administratorowi w wykonywaniu przez niego zadań związanych z zarządzaniem naruszeniem ochrony danych osobowych[41].

Choć główna odpowiedzialność za obsługę naruszeń ochrony danych osobowych spoczywa na administratorach, podmioty przetwarzające muszą **aktywnie** uczestniczyć w tym procesie. Nie mogą ograniczać się wyłącznie do wykonywania zleconych im zadań.

Utrzymywanie przez nich wysokich standardów ochrony danych, odpowiednie reagowanie na incydenty oraz gotowość do wsparcia administratorów jest niezbędne dla zapewnienia bezpieczeństwa przetwarzania.

---

[38] Więcej → 4. Zapobieganie powstawaniu naruszeń ochrony danych osobowych
[39] Więcej → 5.1. Wykrywanie naruszeń ochrony danych osobowych przez podmioty przetwarzające
[40] Więcej → 5.2. „Stwierdzanie" naruszeń ochrony danych osobowych przez podmioty przetwarzające
[41] Więcej → 3.2. Jakie obowiązki mają administratorzy w związku z naruszeniami ochrony danych osobowych?

Przykład 3.4.1.

Firma IT, która świadczyła usługi przetwarzania danych dla urzędu miasta, zabezpieczyła i regularnie monitorowała bezpieczeństwo swoich systemów, aby **zapobiegać** naruszeniom ochrony danych osobowych. Pewnego dnia **wykryła** błąd w systemie, który doprowadził do niezamierzonej modyfikacji danych mieszkańców. Firma natychmiast **zgłosiła** naruszenie ochrony danych osobowych administratorowi, informując go o szczegółach zdarzenia, a następnie aktywnie **współpracowała** z nim w ograniczaniu skutków incydentu i jego analizie. Po zakończeniu procesu firma wdrożyła dodatkowe zabezpieczenia, aby unikać podobnych problemów w przyszłości i skuteczniej **zapobiegać** naruszeniom ochrony danych osobowych.

Zapamiętaj

Infografika 3.4.1.

Stałe obowiązki podmiotu przetwarzającego	**Zapobieganie** powstawaniu naruszeń ochrony danych osobowych
	Wykrywanie naruszeń ochrony danych osobowych
Obowiązki podmiotu przetwarzającego **w przypadku wystąpienia** naruszenia ochrony danych osobowych	**Zgłoszenie** naruszenia ochrony danych osobowych administratorowi
	Pomaganie administratorowi w realizowaniu przez niego zadań związanych z zarządzaniem naruszeniem ochrony danych osobowych
Stałe obowiązki podmiotu przetwarzającego	**Zapobieganie** powstawaniu naruszeń ochrony danych osobowych
	Wykrywanie naruszeń ochrony danych osobowych

Dowiedz się więcej

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

3.5. Kim jest „inspektor ochrony danych”?

„**Inspektorzy ochrony danych”** (IOD) to profesjonalni doradcy wspierający administratorów i podmioty przetwarzające w zapewnieniu zgodności z przepisami RODO. Niektóre podmioty mają obowiązek wyznaczenia IOD w swojej organizacji[42].

Aby prawidłowo wykonywać swoje zadania, IOD muszą być **niezależni**, a zakres ich odpowiedzialności powinien być **wolny od konfliktu interesów**[43].

Zadania IOD to przede wszystkim:

- **doradzanie** organizacji i personelowi w zakresie ochrony danych osobowych;
- **monitorowanie** przestrzegania przepisów RODO w organizacji;
- **podnoszenie świadomości** personelu na temat ochrony danych osobowych;
- **współpraca z organem nadzorczym**;
- **pełnienie funkcji punktu kontaktowego** dla organu nadzorczego i osób, których dane dotyczą[44].

Dowiedz się więcej

→ Wytyczne dotyczące inspektorów ochrony danych („DPO”)

→ Wyznaczenie i status IOD

[42] Więcej → Art. 37 RODO i art. 8-11a ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych
[43] Patrz → Art. 38 ust. 3 i 6 RODO i motyw 97. RODO
[44] Patrz → Art. 38 ust. 4 RODO i art. 39 RODO

3.6. Jaką rolę odgrywają inspektorzy ochrony danych w procesie obsługi naruszeń ochrony danych osobowych?

IOD powinni być włączani we **wszystkie sprawy** dotyczące ochrony danych osobowych, w tym w sprawy dotyczące naruszeń ochrony danych osobowych. O zaistnieniu naruszenia IOD powinien być niezwłocznie informowany, aby umożliwić mu monitorowanie procesu jego obsługi od najwcześniejszego etapu.

> **Przykład 3.6.1.**
>
> Działania IOD w sprawie naruszeń ochrony danych osobowych to m.in.:
>
> - pomoc w **zapobieganiu** naruszeniom, np. poprzez promowanie w organizacji wiedzy o ochronie danych osobowych, organizowanie szkoleń oraz formułowanie zaleceń dotyczących bezpieczeństwa przetwarzania danych;
> - udzielanie wskazówek dotyczących odpowiedniego reagowania na naruszenia ochrony danych osobowych, w tym **zaradzania** im[45], **zgłaszania** ich Prezesowi UODO[46] oraz **zawiadamiania** osób, których dane dotyczą[47];
> - doradztwo w zakresie **dokumentowania** naruszeń i zarządzania dokumentacją[48];
> - przekazywanie dodatkowych **informacji** o naruszeniach organowi nadzorczemu i osobom, których dane dotyczą.

IOD nie mogą jednak wykonywać zadań, za które odpowiadają wyłącznie administratorzy lub podmioty przetwarzające. W praktyce oznacza to, że IOD – z uwagi na potrzebę unikania konfliktu interesów i zapewnienia niezależności (patrz poniżej) – **nie powinni**:

[45] Więcej → 6. Zaradzanie naruszeniom ochrony danych osobowych
[46] Więcej → 9. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu
[47] Więcej → 10. Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych
[48] Więcej → 8. Dokumentowanie naruszeń ochrony danych osobowych

- **zgłaszać** naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń;
- **zawiadamiać** w imieniu administratorów osób, których dane dotyczą, o naruszeniach ochrony danych osobowych;
- **dokumentować** naruszeń ochrony danych osobowych w imieniu administratorów (w szczególności jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określaniem działań zaradczych);
- **podejmować zobowiązań** dotyczących bezpieczeństwa przetwarzania w imieniu administratorów lub podmiotów przetwarzających;
- **działać na podstawie pełnomocnictwa** w sprawach dotyczących ochrony danych osobowych.

Niewłaściwy podział ról może powodować problemy, dlatego warto pamiętać, że:

- gdy IOD wykonują obowiązki spoczywające na administratorach lub podmiotach przetwarzających mogą tracić obiektywizm i **popadać w konflikt interesów**[49];
- pełnomocnictwo wymaga ścisłego wykonywania poleceń, co **może naruszać niezależność IOD**[50].

> **Uwaga!**
>
> Naruszenie zasad dotyczących statusu IOD może skutkować **sankcjami administracyjnymi** ze strony Prezesa UODO, w tym karami pieniężnymi.

[49] Patrz → Art. 38 ust. 6 RODO
[50] Patrz → Art. 38 ust. 3 RODO i motyw 97. RODO

Dowiedz się więcej

→ Wytyczne dotyczące inspektorów ochrony danych („DPO”)

→ Wyznaczenie i status IOD

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

4. Zapobieganie powstawaniu naruszeń ochrony danych osobowych

4.1. Na czym polega „podejście oparte na ryzyku”?

„**Podejście oparte na ryzyku**” to koncepcja będąca podstawą RODO. Zakłada, że środki ochrony danych osobowych powinny być dostosowane do **ryzyka, jakie przetwarzanie stwarza dla praw i wolności osób fizycznych**.

> **Motyw 75. RODO**
>
> *Ryzyko naruszenia praw lub wolności osób fizycznych, o różnym prawdopodobieństwie i wadze, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych i niemajątkowych (…)*

Specyfika przetwarzania jest **inna w każdym przypadku** – różnice wynikają z jego charakteru, zakresu, kontekstu oraz celów.

> **Motyw 76. RODO**
>
> *Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania wiąże się ryzyko lub wysokie ryzyko.*

Z tego powodu **każdy administrator podlega nieco innym wymaganiom**, które z czasem mogą się zmieniać. Administratorzy muszą więc **samodzielnie oceniać ryzyko** wiążące się z przetwarzaniem, aby decydować, jak w konkretnych warunkach zapewnić stosowanie przepisów.

> **Art. 24 ust. 1 RODO**
>
> **Obowiązki administratora**
>
> *Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.*

Administratorzy powinni oceniać i uwzględniać ryzyko **zarówno na etapie planowania przetwarzania, jaki i w jego trakcie**. Umożliwia to dostosowywanie sposobów postępowania z danymi osobowymi do zmieniających się okoliczności.

> **Art. 25 ust. 1 RODO**
>
> **Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych**
>
> *Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.*

Przepisy nie wskazują wprost wymaganych środków bezpieczeństwa. Administratorzy i podmioty przetwarzające, znając najlepiej specyfikę danego przetwarzania, **muszą samodzielnie dobrać odpowiednie zabezpieczenia**, kierując się wynikami oceny ryzyka[51].

[51] Więcej → 4.2. Jak zapobiegać naruszeniom ochrony danych osobowych?

Gdy przetwarzanie może wiązać się z **wysokim ryzykiem** dla osób, których dane dotyczą, administratorzy powinni przeprowadzić **ocenę skutków dla ochrony danych** (DPIA[52]), aby zidentyfikować potencjalne zagrożenia i dobrać odpowiednie środki ochronne.

Art. 35 ust. 1 RODO

Ocena skutków dla ochrony danych

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. (…)

Uwaga!

Nie należy mylić ryzyka związanego z samym **przetwarzaniem** z ryzykiem wynikającym z **naruszenia ochrony danych osobowych**.

W przypadku ryzyka związanego z **przetwarzaniem** administratorzy analizują hipotetyczne zagrożenia dla przetwarzanych danych i ich wpływ na prawa i wolności osób, których dane dotyczą, aby odpowiednio się przygotować lub zapobiec ryzyku, jeśli jest ono nieakceptowalne (bądź zrezygnować z przetwarzania).

W przypadku ryzyka związanego z **naruszeniem ochrony danych osobowych** administratorzy oceniają zagrożenia wynikające z rzeczywistego incydentu, aby przeanalizować jego potencjalne skutki i zdecydować o dalszych działaniach[53].

Uwaga!

Wystąpienie naruszenia ochrony danych osobowych nie przesądza o tym, że ocena ryzyka przeprowadzona dla procesu przetwarzania, w ramach którego wystąpiło naruszenie, została przeprowadzona błędnie. W takim przypadku

[52] *Data Protection Impact Assessement.*
[53] Więcej → 7.1. Jak oceniać ryzyko związane z naruszeniami ochrony danych osobowych?

warto jednak dokonać jej **przeglądu i aktualizacji**, aby uwzględnić w analizie dodatkową wiedzę uzyskaną przy okazji obsługi zaistniałego naruszenia.

Uwaga!

Administratorzy (oraz w pewnych sytuacjach podmioty przetwarzające) **muszą być gotowi wykazać**[54], że właściwie **ocenili ryzyko** związane z przetwarzaniem.

Dowiedz się więcej

→ Jak rozumieć i stosować podejście oparte na ryzyku?

→ Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony

→ Wytyczne nr 4/2019 dotyczące artykułu 25. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

[54] Więcej → 3.2. Odpowiedzialność i rozliczalność

4.2. Jak zapobiegać naruszeniom ochrony danych osobowych?

Administratorzy i podmioty przetwarzające są **zobowiązani** do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez wdrożenie odpowiednich **środków technicznych i organizacyjnych**.

Właściwy **dobór** tych środków ma kluczowe znaczenie dla skutecznej ochrony danych i powinien uwzględniać stan wiedzy technicznej, koszt wdrażania, a także charakter, zakres, kontekst i cele przetwarzania oraz związane z nim **ryzyko**[55].

Ponieważ okoliczności te zmieniają się w czasie, organizacje powinny regularnie **oceniać i doskonalić** stosowane rozwiązania.

> **Art. 32 ust. 1 RODO**
>
> **Bezpieczeństwo przetwarzania**
>
> *Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:*
>
> *a) pseudonimizację i szyfrowanie danych osobowych;*
>
> *b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;*
>
> *c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;*
>
> *d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.*

[55] Więcej → 4.1. Na czym polega „podejście oparte na ryzyku”?

Aby zapewnić bezpieczeństwo przetwarzania, administratorzy i podmioty przetwarzające muszą aktywnie **zapobiegać** powstawaniu naruszeń ochrony danych osobowych, czyli incydentów, które to bezpieczeństwo zakłócają[56].

> **Art. 32 ust. 2 RODO**
>
> **Bezpieczeństwo przetwarzania**
>
> *Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.*

Wdrożenie skutecznych środków bezpieczeństwa wymaga uwzględnienia charakteru przetwarzania i specyfiki organizacji. Oznacza to, że **nie istnieje uniwersalna lista środków bezpieczeństwa odpowiednich w każdej sytuacji**.

Podmioty odpowiedzialne za ochronę danych osobowych mogą rozważyć wykorzystanie uznanych standardów postępowania. Ważne jednak, by stosować je w sposób **indywidualny i elastyczny**.

> **Przykład 4.1.1.**
>
> Środkami **organizacyjnymi** służącymi zapobieganiu naruszeniom ochrony danych osobowych są m.in.
>
> - wdrożenie **procedur dotyczących ochrony danych osobowych** oraz ich bezpiecznego przetwarzania;
> - wdrożenie **procedur reagowania na incydenty bezpieczeństwa**, w tym planów odzyskiwania danych osobowych i przywracania ich ochrony w sytuacjach nadzwyczajnych;

[56] Więcej → 2.1. Czym jest „naruszenie ochrony danych osobowych”?

- wdrożenie **procedur monitorowania i analizy ruchu sieciowego**, w tym wykrywania prób nieuprawnionego dostępu do systemów lub korzystania z urządzeń w sposób niezgodny z ich przeznaczeniem

- przyjęcie **zasad bezpiecznego korzystania z haseł**, w tym szczegółowych wymagań dotyczących ich tworzenia, przechowywania i regularnej weryfikacji ich bezpieczeństwa;

- przyjęcie **zasad zarządzania użytkownikami i kontroli dostępu**, które zapewniają, dostęp do danych osobowych mają wyłącznie osoby upoważnione, a uprawnienia użytkowników są regularnie weryfikowane oraz dezaktywowane, gdy stają się nieaktualne;

- określenie **dobrych praktyk dotyczących bezpieczeństwa informatycznego**, uwzględniających:

    - zasady ochrony danych w fazie projektowania *(privacy by design)*[57];

    - zasady domyślnej ochrony danych *(privacy by default)*[58];

    - analizę ryzyka związanego z przetwarzaniem[59];

- przeprowadzanie **regularnych audytów bezpieczeństwa informatycznego i testów penetracyjnych**, aby identyfikować luki w systemach, wskazywać obszary wymagające poprawy oraz podnosić świadomość użytkowników na temat zagrożeń;

- weryfikowanie **wdrożenia i skuteczności wdrożonych środków bezpieczeństwa oraz ich aktualizowanie**, zwłaszcza w przypadku zmian technologii, procesów przetwarzania lub pojawienia się nowych ryzyk;

- niezwłoczne **dokumentowanie i korygowanie wykrytych podatności**, obejmujące wskazanie działań naprawczych i harmonogramu ich realizacji;

- **promowanie zasad ochrony prywatności i bezpieczeństwa danych osobowych wśród personelu** poprzez regularne szkolenia dostosowane do specyfiki pracy, aby ograniczyć ryzyko błędów ludzkich;

- dokonywanie **okresowej oceny technicznych i organizacyjnych środków bezpieczeństwa** oraz ich modyfikowanie w razie potrzeby.

[57] Patrz → Art. 25 ust. 1 RODO
[58] Patrz → Art. 25 ust. 2 RODO
[59] Więcej → 4.1. Na czym polega „podejście oparte na ryzyku”?

Przykład 4.1.2.

Środkami **technicznymi** służącymi zapobieganiu naruszeniom ochrony danych osobowych są m.in.:

A. Uwierzytelnianie

- korzystanie z **bezpiecznych danych logowania**, zgodnych z aktualnymi standardami dotyczącymi długości, unikalności i złożoności;
- wdrażanie **uwierzytelniania wieloskładnikowego**, szczególnie w przypadku dostępu do wrażliwych informacji, systemów zdalnych lub uprawnień użytkowników o podwyższonym ryzyku;
- regularne **weryfikowanie ważności danych uwierzytelniających** i ich cykliczna aktualizacja w celu zapobiegania przejęciu kont.

B. Infrastruktura i systemy

- regularne **aktualizowanie systemów operacyjnych, aplikacji oraz urządzeń sieciowych**, w tym przeglądarek i wtyczek;
- **izolacja procesów przetwarzania danych** oraz **segmentowanie systemów i sieci informatycznych** w celu minimalizowania ryzyka rozprzestrzeniania się zagrożeń;
- zwiększanie bezpieczeństwa serwerów i stacji roboczych, w tym:
    - blokowanie dostępu do stron stanowiących potencjalne źródło zagrożeń;
    - natychmiastowe blokowanie złośliwego oprogramowania i podejrzanych aplikacji;
    - monitorowanie użytkowania oprogramowania oraz prowadzenie dzienników zdarzeń (logów);
    - weryfikowanie dostępu na podstawie adresów IP oraz zmiana domyślnych ustawień portów (np. RDP).

C. Poczta elektroniczna

- wyraźne określenie **polityk i procedur dotyczących wysyłania wiadomości e-mail** z danymi osobowymi, w tym:
    - korzystanie z pola „**UDW**” (ukryte do wiadomości) przy wielu odbiorcach;

- zapewnienie, że załączniki zawierają wyłącznie dane przeznaczone do przesłania;

- **szyfrowanie e-maili i załączników** za pomocą unikalnych haseł dostępnych jedynie dla odbiorcy;

- wdrożenie **narzędzi antyspamowych i antyphishingowych**[60] w celu blokowania potencjalnie złośliwych wiadomości;

D. Ochrona przed złośliwym oprogramowaniem

- stosowanie **rozwiązań antywirusowych i antyransomware**[61], które umożliwiają skanowanie i wykrywanie zagrożeń w czasie rzeczywistym;

- tworzenie bezpiecznych **systemów kopii zapasowych**, odseparowanych od głównych baz danych;

E. Wykorzystywanie urządzeń zewnętrznych

- przechowywanie danych w systemach wewnętrznych z zabezpieczeniem zdalnego dostępu poprzez **VPN**[62];

- **szyfrowanie danych** na urządzeniach zewnętrznych oraz stosowanie funkcji „zdalne czyszczenie” w razie utraty sprzętu;

- **blokowanie kont użytkowników** po kilku nieudanych próbach logowania;

F. Przechowywanie dokumentów papierowych

- przechowywanie dokumentów w **zamkniętych, ognioodpornych miejscach odpornych na zalanie**, z kontrolą dostępu i dokumentowaniem tożsamości osób uzyskujących wgląd w dane;

- **niszczenie dokumentów** przy użyciu specjalistycznego sprzętu gwarantującego „bezpieczne” niszczenie.

G. Transport informacji zawierających dane osobowe

- **szyfrowanie danych** na nośnikach (np. CD, DVD, pendrive) oraz stosowanie środków zapobiegających ich nieautoryzowanemu odczytowi, zmianie lub usunięciu podczas transportu.

[60] Więcej → Phishing
[61] Więcej → Ransomware
[62] **VPN** *(Virtual Private Network)* to wirtualna sieć prywatna umożliwiająca bezpieczne i szyfrowane połączenie z siecią publiczną lub prywatną, zapewniając ochronę przesyłanych danych oraz anonimowość użytkownika.

Powyższe rozwiązania to jedynie **przykłady środków bezpieczeństwa**, które mogą być wykorzystane w zależności od potrzeb i specyfiki danej organizacji. Lista ta **nie jest wyczerpująca** – każdy administrator i podmiot przetwarzający powinien samodzielnie dobrać odpowiednie zabezpieczenia, uwzględniając charakter procesów przetwarzania, ich skalę oraz potencjalne zagrożenia dla ochrony danych osobowych.

> **Uwaga!**
>
> Administratorzy i podmioty przetwarzające **muszą być gotowi wykazać**[63], że wdrożyli **odpowiednie** środki bezpieczeństwa w celu **zapobiegania** naruszeniom ochrony danych osobowych.

Dowiedz się więcej

> → Wytyczne nr 4/2019 dotyczące artykułu 25. Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych
>
> → Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

[63] Więcej → 3.2. Odpowiedzialność i rozliczalność

5. Identyfikowanie naruszeń ochrony danych osobowych

5.1. Jak wykrywać naruszenia ochrony danych osobowych?

Identyfikowanie naruszeń ochrony danych osobowych jest kluczowe dla właściwego stosowania przepisów RODO. Aby prawidłowo realizować swoje obowiązki[64], administratorzy muszą być w stanie oceniać, **czy w danych okolicznościach rzeczywiście doszło do zdarzenia**, które należy klasyfikować jako naruszenie ochrony danych osobowych. Wymaga to wykorzystania skutecznych metod wykrywania i analizy incydentów.

Administratorzy mogą pozyskiwać informacje o potencjalnych naruszeniach ochrony danych osobowych z różnych źródeł. Najczęściej dzieje się to w wyniku:

- zgłoszeń dokonywanych przez **członków personelu** (np. pracowników, wolontariuszy);
- zgłoszeń dokonywanych przez **podmioty przetwarzające** (np. dostawców usług IT, biura rachunkowe, firmy ochroniarskie);
- informacji przekazywanych przez **osoby, których dane dotyczą** (np. klientów, studentów, pacjentów);
- powiadomień generowanych przez **systemy informatyczne** (np. IDS[65], IPS[66] czy DLP[67]);

[64] Więcej → 3.2. Jakie obowiązki mają administratorzy w związku z naruszeniami ochrony danych osobowych?

[65] **IDS** *(Intrusion Detection System)* to system, który wykrywa i zgłasza podejrzaną aktywność w sieci lub systemach, informując administratorów o potencjalnych zagrożeniach.

[66] **IPS** *(Intrusion Prevention System)* to system, który nie tylko wykrywa podejrzaną aktywność, ale także automatycznie blokuje i zapobiega potencjalnym zagrożeniom, chroniąc systemy przed atakami w czasie rzeczywistym.

[67] **DLP** (*Data Loss Prevention*) to strategia ochrony danych, która obejmuje technologie (systemy IT), procesy i polityki mające na celu zapobieganie przypadkowemu lub celowemu wyciekowi lub

- wniosków z **działań kontrolnych** (np. audytów, przeglądów zgodności).

Identyfikowanie naruszeń ochrony danych osobowych opiera się na połączeniu środków technicznych i organizacyjnych. Należą do nich zarówno narzędzia monitorujące, jak i odpowiednio przygotowane procedury.

Przykład 5.1.1.

Środkami **technicznymi** służącymi wykrywaniu naruszeń ochrony danych osobowych są m.in.:

- **programy antywirusowe i firewall**, które chronią przed złośliwym oprogramowaniem oraz informują o wykrytych zagrożeniach;
- **logi systemowe**, które umożliwiają analizę aktywności użytkowników i urządzeń w czasie rzeczywistym;
- **automatyczne systemy powiadamiania o podejrzanej aktywności**, które sygnalizują nietypowe działania w systemie (np. logowania z nieznanych źródeł);
- **narzędzia detekcji oraz zapobiegania atakom cybernetycznym i wyciekom danych**, takie jak IDS, które wykrywają podejrzaną aktywność, IPS, które dodatkowo blokują nieautoryzowane próby dostępu, czy DLP, które chronią przed wyciekami lub utratą danych;
- **systemy typu IAM**[68], które pozwalają kontrolować, kto i w jaki sposób uzyskuje dostęp do zasobów informacyjnych (danych, systemów, aplikacji);
- **systemy typu SIEM**[69], które monitorują i analizują dane z różnych źródeł w celu kompleksowego wykrywania zagrożeń oraz incydentów bezpieczeństwa.

utracie danych z organizacji poprzez monitorowanie aktywności użytkowników lub urządzeń w sieciach komputerowych czy telekomunikacyjnych.

[68] **IAM** *(Identity and Access Management)* to system zarządzania tożsamościami i dostępem w organizacji, który służy do kontrolowania, kto ma dostęp do jakich zasobów, w jaki sposób i na jakich warunkach.

[69] **SIEM** *(Security Information and Event Management)* to oprogramowanie służące do zbierania i korelacji danych z różnych systemów IT, pozwalające na monitorowanie i analizę zagrożeń w czasie rzeczywistym.

Przykład 5.1.2.

Środkami **organizacyjnymi** służącymi wykrywaniu naruszeń ochrony danych osobowych są m.in.:

- **szkolenia dla personelu i symulacje zagrożeń**, które uczą, jak rozpoznawać i postępować z incydentami bezpieczeństwa;
- **procedury zgłaszania incydentów**, które pozwalają na szybkie i skuteczne informowanie o podejrzanych zdarzeniach;
- **wyznaczenie osób**, które będą odpowiedzialne za monitorowanie systemów oraz wykrywanie i analizę naruszeń ochrony danych osobowych;
- **regularna analiza** logów i narzędzi monitorujących zdarzenia oraz aktywność użytkowników w sieciach i systemach komputerowych;
- **regularne testy bezpieczeństwa i audyty systemów IT**, które pomagają w identyfikowaniu słabych punktów systemu, potencjalnych luk w zabezpieczeniach czy błędów w konfiguracji.

Wykrywanie naruszeń ochrony danych osobowych przez podmioty przetwarzające

Ponieważ incydenty mogą występować u różnych podmiotów zaangażowanych we wspólne przetwarzanie danych, **administratorzy i podmioty przetwarzające powinni ustalić jasne zasady wymiany informacji na temat potencjalnych naruszeń ochrony danych osobowych**. Ważne jest sprecyzowanie, kto, kiedy i w jaki sposób powinien powiadomić pozostałe strony, aby umożliwić szybkie podjęcie działań i realizację obowiązków wynikających z RODO.

Dowiedz się więcej

→ Klauzula 9 „Zgłaszanie naruszenia ochrony danych osobowych" decyzji wykonawczej Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725

5.2. Na czym polega „stwierdzenie” naruszenia ochrony danych osobowych?

Zidentyfikowanie naruszenia ochrony danych osobowych wiąże się z jego „**stwierdzeniem**”.

Termin ten określa **moment, w którym administrator zdobywa wystarczającą wiedzę o incydencie, aby uznać go za naruszenie ochrony danych osobowych.**

> **Motyw 87. RODO**
>
> *Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. (…)*

Administrator „stwierdza” więc naruszenie ochrony danych osobowych w momencie, gdy staje się **świadomy**, że wykryte **zdarzenie**:

- jest **incydentem bezpieczeństwa**;
- dotyczy przetwarzanych **danych osobowych**;
- może doprowadzić do ich przypadkowego lub niezgodnego z prawem **zniszczenia**, **utracenia**, **zmodyfikowania**, nieuprawnionego **ujawnienia** lub **dostępu** do nich[70].

Z chwilą „stwierdzenia” naruszenia ochrony danych osobowych administrator powinien rozpocząć realizację obowiązków związanych z wystąpieniem takiego zdarzenia[71].

[70] Więcej → 2.1. Czym jest „naruszenie ochrony danych osobowych”?
[71] Więcej → 3.2. Jakie obowiązki mają administratorzy w związku z naruszeniami ochrony danych osobowych?

Przykład 5.2.1.

System monitorujący w firmie e-commerce wykrył nieautoryzowany dostęp do serwera, na którym przechowywano informacje o klientach. Powiadomienie o zdarzeniu zostało natychmiast przesłane do działu IT, który przeprowadził wstępną analizę logów systemowych, aby ustalić źródło i zakres problemu. Wyniki analizy trafiły do inspektora ochrony danych oraz zarządu firmy. Następnie do działań przystąpił zespół ds. zarządzania incydentami, który szczegółowo ocenił sytuację, ustalając, które dane i w jakim stopniu zostały ujawnione osobom nieuprawnionym. Zespół potwierdził, że doszło do nieautoryzowanego dostępu do danych klientów, skutkującego naruszeniem poufności danych osobowych. Z chwilą zgromadzenia tych informacji administrator „**stwierdził**" naruszenie ochrony danych osobowych i przystąpił do realizacji związanych z nim kolejnych obowiązków.

Przykład 5.2.2.

Osoba składająca wniosek o przyznanie zasiłku zauważyła, że w decyzji wydanej przez urząd pojawiły się błędne informacje dotyczące jej danych osobowych. Telefonicznie poinformowała o tym pracownika zajmującego się weryfikacją wniosków. Zgłoszenie zostało niezwłocznie przekazane do zespołu ds. bezpieczeństwa informacji. Wstępna analiza wykazała, że doszło do błędnego przepisania danych z formularza. Wyniki analizy zostały przesłane inspektorowi ochrony danych oraz kierownictwu urzędu. Dalsza weryfikacja potwierdziła wystąpienie naruszenia integralności danych osobowych. Zebrane informacje pozwoliły administratorowi „**stwierdzić**" naruszenie ochrony danych osobowych i przystąpić do realizacji związanych z nim obowiązków.

Uwaga!

Administrator **nie musi** wykonać żadnych dodatkowych czynności, aby formalnie „stwierdzić" naruszenie ochrony danych osobowych. Powinien jednak dokładnie odnotować czas, w jakim do tego doszło. Informacja ta jest istotna przy ewentualnym **zgłaszaniu** naruszenia Prezesowi UODO[72]. Stanowi ona także element obowiązkowej **dokumentacji**[73].

[72] Więcej → 9. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu
[73] Więcej → 8. Dokumentowanie naruszeń ochrony danych osobowych

„Stwierdzanie” naruszeń ochrony danych osobowych przez podmioty przetwarzające

Podmioty przetwarzające mają **obowiązek** niezwłocznego zgłaszania administratorom wszystkich „stwierdzonych” naruszeń ochrony danych osobowych[74].

> **Art. 33 ust. 2 RODO**
>
> **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**
>
> *Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.*

> **Przykład 5.2.3.**
>
> Podmiot przetwarzający odpowiedzialny za zarządzanie infrastrukturą IT firmy ubezpieczeniowej wykrył awarię zasilania, która spowodowała przerwanie działania serwera przechowującego dane klientów. Przeprowadzona analiza potwierdziła, że awaria uniemożliwiła dostęp do danych osobowych i bieżącą obsługę klientów. Po zbadaniu problemu podmiot przetwarzający „**stwierdził**” naruszenie dostępności danych osobowych. Następnie, wypełniając swój obowiązek, natychmiast przekazał informacje administratorowi. Na tej podstawie firma mogła „**stwierdzić**” naruszenie ochrony danych osobowych i przystąpić do realizacji związanych z nim zadań.

> **Przykład 5.2.4.**
>
> Budynek podmiotu przetwarzającego odpowiedzialnego za przechowywanie kopii zapasowych firmy ubezpieczeniowej został objęty pożarem, w wyniku czego spłonęły serwery przechowujące dane osobowe. Przeprowadzona analiza potwierdziła, że nośniki danych uległy całkowitemu zniszczeniu. W wyniku tych ustaleń podmiot przetwarzający **„stwierdził”** naruszenie dostępności danych osobowych. Następnie, wypełniając swój obowiązek, natychmiast przekazał informację administratorowi. Firma ubezpieczeniowa

[74] Więcej → 3.4. Jakie obowiązki mają podmioty przetwarzające w związku z naruszeniami ochrony danych osobowych?

niezwłocznie przystąpiła do analizy własnych zasobów danych, przechowywanych w jej siedzibie. Administrator, po ustaleniu, że dysponuje własną, kompletną kopią zapasową danych objętych pożarem, słusznie **nie „stwierdził”** naruszenia ochrony danych osobowych.

Szczegółowe zasady realizacji tego obowiązku, w tym terminy i sposoby przekazywania informacji, powinny być jasno **określone w umowie** pomiędzy stronami.

Uwaga!

Mimo że administratorzy co do zasady „**stwierdzają**” naruszenia ochrony danych osobowych z chwilą otrzymania informacji od podmiotu przetwarzającego, pozostają oni odpowiedzialni za ich weryfikację oraz ostateczną analizę i kwalifikację incydentu jako naruszenie ochrony danych osobowych.

Dowiedz się więcej

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

6. Zaradzanie naruszeniom ochrony danych osobowych

6.1. Jak zaradzać naruszeniom ochrony danych osobowych i ich ewentualnym skutkom?

Po wykryciu i „stwierdzeniu” naruszenia ochrony danych osobowych jednym z głównych obowiązków administratorów jest podjęcie natychmiastowych **działań zaradczych**[75].

Zaradzenie naruszeniu ochrony danych osobowych polega przede wszystkim na:

- **powstrzymaniu i ograniczeniu incydentu**, aby jak najszybciej przerwać jego przebieg i uniemożliwić dalsze rozprzestrzenianie się;
- **zminimalizowaniu jego skutków**, aby zmniejszyć potencjalne szkody, które mogą dotknąć osoby, których dane zostały naruszone;
- **przywróceniu bezpieczeństwa**, aby ustabilizować sytuację po incydencie i zabezpieczyć objęte nim zasoby.

Skuteczne realizowanie tego zadania wymaga od administratorów zastosowania odpowiednich środków technicznych i organizacyjnych, dostosowanych do specyfiki sytuacji.

Warto być przygotowanym na różne scenariusze, ponieważ szybkie i adekwatne reakcje mogą wpłynąć na **zmniejszanie skali incydentów** i **złagodzenie wynikającego z nich ryzyka** dla osób fizycznych[76].

[75] Patrz → Art. 32 ust. 1 lit. b) RODO i art. 33 ust. 3 lit. d) RODO
[76] Więcej → 7. Ocena ryzyka związanego z naruszeniami ochrony danych osobowych

Przykład 6.1.1.

Metodami **powstrzymywania i ograniczania** naruszeń ochrony danych osobowych są m.in.:

- przeniesienie niezabezpieczonych dokumentów lub nośników danych do bezpiecznego miejsca, aby zapobiec dostępowi osób nieuprawnionych oraz uniemożliwić dalsze rozpowszechnianie informacji;
- zatrzymanie błędnie skonfigurowanej funkcji automatycznej wysyłki e-maili, aby powstrzymać wysyłanie kolejnych wiadomości zawierających dane osobowe do niewłaściwych odbiorców;
- odłączenie od sieci lub odseparowanie urządzeń lub systemów objętych naruszeniem, aby uniemożliwić dalszy nieuprawniony dostęp do danych (np. w przypadku cyberataku lub zainfekowania złośliwym oprogramowaniem);
- zablokowanie kont użytkowników, którzy mogli przyczynić się do powstania incydentu, aby zapobiec dalszemu przetwarzaniu przez nie danych osobowych;
- poprawienie błędnych danych osobowych (np. klientów), aby wyeliminować błędy mogące prowadzić do dalszego ich naruszania.

Przykład 6.1.2.

Metodami **minimalizowania skutków** dla praw lub wolności osób, których dane dotyczą, w związku z naruszeniami ochrony danych osobowych są m.in.:

- poinformowanie o naruszeniu osób, których dane dotyczą, aby mogły samodzielnie podjąć odpowiednie środki ostrożności (np. zmienić hasło, zastrzec numer PESEL, monitorować podejrzane transakcje)[77];
- skontaktowanie się z nieuprawnionym odbiorcą danych, aby uzyskać zapewnienie o niewykorzystywaniu tych informacji oraz zobowiązać go do ich usunięcia;
- odzyskanie korespondencji lub dokumentów zawierających dane osobowe, które zostały omyłkowo wysłane do niewłaściwej osoby lub instytucji;

[77] Więcej → 10. Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

- nawiązanie współpracy z odpowiednimi organami, takimi jak policja, CERT lub UODO, aby zapobiec ewentualnym nadużyciom i zapewnić odpowiednią reakcję na incydent.

Przykład 6.1.3.

Metodami **przywracania bezpieczeństwa** po naruszeniach ochrony danych osobowych są m.in.:

- odtworzenie lub przywrócenie utraconych danych z kopii zapasowej, aby odzyskać informacje utracone w wyniku incydentu;
- usunięcie przyczyn incydentu, takich jak luki w zabezpieczeniach lub błędy proceduralne, które umożliwiły wystąpienie naruszenia, poprzez ich aktualizację lub wdrożenie dodatkowych zabezpieczeń;
- przeprowadzenie szczegółowej analizy incydentu, aby upewnić się, że sytuacja jest opanowana, a dane osobowe są bezpieczne.

Uwaga!

Administratorzy **muszą być gotowi wykazać**[78], że właściwie **zaradzili** naruszeniu ochrony danych osobowych.

Zaradzanie naruszeniom ochrony danych osobowych przez podmioty przetwarzające

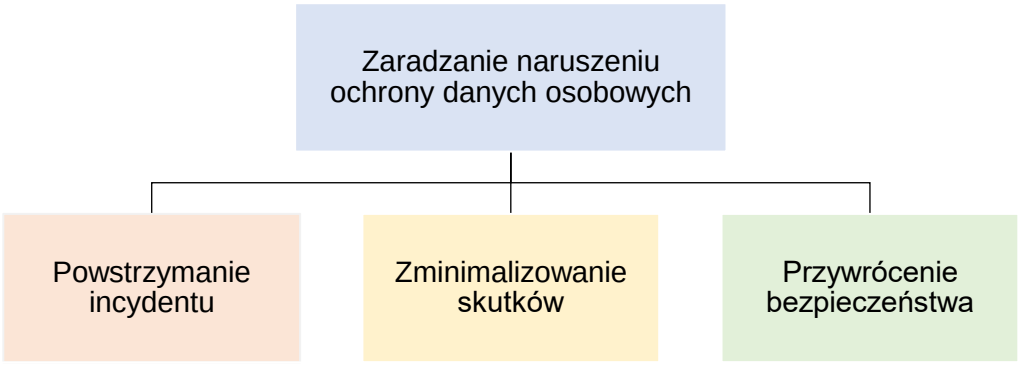
Obowiązek zaradzania naruszeniom ochrony danych osobowych **dotyczy także podmiotów przetwarzających**. Powinny one we własnym zakresie podejmować działania w celu powstrzymywania „stwierdzonych" naruszeń i łagodzenia ich skutków, a także niezwłocznie zgłaszać je administratorom[79]. W całym procesie podmioty przetwarzające zobowiązane są do **ścisłej współpracy z**

[78] Więcej → 3.2. Odpowiedzialność i rozliczalność
[79] Więcej → 5.2. „Stwierdzanie" naruszeń ochrony danych osobowych przez podmioty przetwarzające

administratorami i **postępowania zgodnie z ich wytycznymi**, aby skutecznie opanowywać incydenty i zapewnić ochronę danych osobowych[80].

Zapamiętaj

Infografika 6.1.1.



Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[80] Więcej → 3.4. Jakie obowiązki mają podmioty przetwarzające w związku z naruszeniami ochrony danych osobowych?

7. Ocena ryzyka związanego z naruszeniami ochrony danych osobowych

7.1. Jak oceniać ryzyko związane z naruszeniami ochrony danych osobowych?

Niektóre naruszenia ochrony danych osobowych mogą negatywnie wpływać na sytuację osób, których dane dotyczą, stwarzając **ryzyko naruszenia ich praw lub wolności**[81].

Skutki incydentów mogą być różne. Z tego powodu administratorzy zobowiązani są do przeprowadzania indywidualnej **oceny ryzyka** naruszenia praw lub wolności osób fizycznych za każdym razem, gdy „stwierdzą" naruszenie ochrony danych osobowych[82]. Wyniki tej oceny przesądzają o dalszych krokach podejmowanych przy każdym incydencie.

> **Uwaga!**
>
> Może się okazać, że naruszenie ochrony danych osobowy finalnie nie spowoduje naruszenia praw lub wolności osób fizycznych. Ocenie administratorów podlega wyłącznie **ryzyko** wystąpienia takiej sytuacji, a nie faktycznie powstałe szkody.

Aby prawidłowo ocenić ryzyko, administratorzy powinni oszacować:

- **wagę** potencjalnych konsekwencji;
- oraz **prawdopodobieństwo** ich wystąpienia;

uwzględniając następujące okoliczności zdarzenia:

[81] Więcej → 2.2. Dlaczego naruszenia ochrony danych osobowych są niebezpieczne?
[82] Więcej → 5.2. Na czym polega „stwierdzenie" naruszenia ochrony danych osobowych?

- **rodzaj** naruszenia ochrony danych osobowych[83];
- **charakter, wrażliwość i zakres** danych osobowych;
- **łatwość identyfikacji** osób, których dane dotyczą;
- **dotkliwość konsekwencji** dla osób, których dane dotyczą;
- **cechy szczególne** osób, których dane dotyczą;
- **cechy szczególne** administratora;
- **liczbę osób**, których dane dotyczą.

> **Uwaga!**
>
> RODO dotyczy wyłącznie **praw i wolności osób fizycznych**. Podczas oceny ryzyka związanego z naruszeniem ochrony danych osobowych nie ma więc znaczenia, jakie konsekwencje incydentu poniesie przetwarzająca te dane organizacja jako taka (np. osoba prawna). Administratorzy powinni przyjąć w tym procesie **perspektywę osób, których dane dotyczą**.

Administratorzy muszą ustalić, czy naruszenie ochrony danych osobowych może wiązać się z:

- **brakiem ryzyka**;
- **ryzykiem**, co wymaga **zgłoszenia** go Prezesowi UODO[84];
- lub **wysokim ryzykiem**, co oznacza obowiązek **zgłoszenia** go Prezesowi UODO oraz **zawiadomienia** osób, których dane dotyczą[85].

[83] Więcej → 2.3. Na czym polegają naruszenia poufności, integralności i dostępności danych osobowych?
[84] Więcej → 9. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu
[85] Więcej → 10. Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

Pozostałe obowiązki, takie jak **zaradzanie** naruszeniom ochrony danych osobowych[86] i ich **dokumentowanie**[87], dotyczą **wszystkich** „stwierdzonych" naruszeń, niezależnie od wyników **oceny ryzyka**[88].

Istnieje wiele różnych metod szacowania ryzyka, jednak **żadna nie daje gwarancji właściwych wyników**. Nic nie zastąpi pełnego zrozumienia specyfiki przetwarzania ani świadomości istniejących zagrożeń. Administratorzy powinni znać ten proces na tyle dobrze, aby móc nadzorować jego przebieg i w każdym przypadku samodzielnie podejmować ostateczne decyzje dotyczące oceny ryzyka.

> **Uwaga!**
>
> Administratorzy **muszą być gotowi wykazać**[89], że właściwie **ocenili ryzyko** związane z naruszeniem ochrony danych osobowych i na tej podstawie podjęli odpowiednie działania.

Brak ryzyka

Choć co do zasady naruszenia ochrony danych osobowych stwarzają pewne ryzyko naruszenia praw lub wolności osób fizycznych, zdarzają się sytuacje, w których można jednoznacznie stwierdzić, że takie ryzyko prawdopodobnie **nie wystąpi**.

Są to przede wszystkim przypadki dotyczące:

- ujawnienia danych, które są już **publicznie dostępne**;
- ujawnienia lub utracenia danych **zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych** (jeżeli są one

[86] Więcej → 6. Zaradzanie naruszeniom ochrony danych osobowych
[87] Więcej → 8. Dokumentowanie naruszeń ochrony danych osobowych
[88] Więcej → 3. Obowiązki związane z naruszeniami ochrony danych osobowych
[89] Więcej → 3.2. Odpowiedzialność i rozliczalność

zabezpieczone kluczem, który nie został naruszony, a administrator ma dostęp do ich kopii zapasowej);

- incydentów, którym administratorzy definitywnie **zaradzili**.

Przykład 7.1.1.

Pracownik wydawnictwa omyłkowo przesłał osobie nieuprawnionej szczegóły dotyczące choroby znanego pisarza, które miały znaleźć się w jego autobiografii. Informacje te były jednak wcześniej opisane przez samego pisarza w telewizyjnym w wywiadzie oraz w mediach społecznościowych, gdzie publicznie dzielił się historią swojej choroby. W takim przypadku można było jednoznacznie stwierdzić **brak ryzyka** naruszenia praw lub wolności osoby, której dane dotyczą.

Przykład 7.1.2.

Laptop pracownika kliniki dentystycznej zawierający dane pacjentów został zgubiony. Urządzenie było zabezpieczone szyfrowaniem przy użyciu niezawodnej metody (przy ówczesnym stanie wiedzy technicznej), a klucz szyfrowania nie został utracony ani złamany. Ponadto klinika dysponowała kopią zapasową wszystkich informacji o pacjentach. W takim przypadku można było jednoznacznie stwierdzić **brak ryzyka** naruszenia praw lub wolności osób, których dane dotyczą.

Przykład 7.1.3.

Pracownik firmy budowlanej wyrzucił dokumenty kadrowe i finansowe (zawierające m.in. imiona, nazwiska, numery PESEL i informacje o wynagrodzeniach) do kontenera na odpady znajdującego się na zamkniętym, monitorowanym terenie firmy. Po upływie około godziny pracownik zdał sobie sprawę z błędu, a administrator podjął natychmiastowe działania, odzyskując i zabezpieczając dokumenty. Mimo że początkowo zdarzenie mogło doprowadzić do poważnych konsekwencji, nagrania potwierdziły brak dostępu osób nieuprawnionych oraz skuteczne **zaradzenie** incydentowi. W takim przypadku można było jednoznacznie stwierdzić **brak ryzyka** naruszenia praw lub wolności osób, których dane dotyczą.

Należy pamiętać, że z czasem lub w miarę zdobywania nowych informacji **ocena ryzyka może wymagać aktualizacji**.

Wysokie ryzyko

Administratorzy mogą stwierdzić, że z naruszeniem ochrony danych osobowych wiąże się **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych. Oznacza to, że potencjalne konsekwencje incydentu mogą mieć:

- znaczną **wagę**;
- i/lub duże **prawdopodobieństwo** wystąpienia.

Choć każdy incydent należy analizować indywidualnie, uwzględniając różne kryteria, o **wysokim ryzyku** mogą świadczyć określone okoliczności zdarzenia, w tym m.in.:

- objęcie incydentem **wrażliwych danych osobowych** (takich jak informacje ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane finansowe, dane genetyczne, dane biometryczne, dane dotyczące zdrowia, seksualności, orientacji seksualnej, wyroków skazujących, czynów zabronionych), a także informacje powszechnie wykorzystywane do potwierdzania tożsamości lub zawierania umów, takie jak seria i numer dowodu osobistego oraz numer PESEL;
- **szeroki zakres** danych osobowych objętych incydentem (im szerszy, tym wyższe ryzyko);
- **szczególna dotkliwość** możliwych skutków incydentu (takich jak kradzież tożsamości, oszustwa finansowe, straty finansowe, problemy zawodowe, uszczerbek na zdrowiu, silny stres, lęk i obniżone poczucie bezpieczeństwa);
- **szczególny charakter** osób objętych incydentem (takich jak dzieci, osoby starsze i osoby potrzebujące lub znajdujące się w trudnej sytuacji życiowej);

- **duża liczba** osób objętych incydentem (im większa, tym wyższe prawdopodobieństwo wystąpienia negatywnego skutku).

Przykład 7.1.4.

Cyberatak na biuro podróży spowodował ujawnienie danych tysięcy klientów, w tym numerów PESEL, adresów zamieszkania, numerów telefonów, numerów paszportów oraz historii podróży. Połączenie numerów PESEL i innych danych identyfikacyjnych niesie ze sobą poważne ryzyko, ponieważ może umożliwić zawieranie umów, zaciąganie pożyczek lub uzyskiwanie usług na cudze nazwisko. Będąc w posiadaniu takich danych, przestępcy mogą próbować uzyskać dostęp do kont bankowych, tworzyć fałszywe rezerwacje lub manipulować danymi w systemach finansowych. W efekcie osoby dotknięte naruszeniem poufności mogą być narażone na kradzież tożsamości, oszustwa finansowe oraz długotrwałe trudności związane z wyjaśnianiem i unieważnianiem fałszywych zobowiązań. Z uwagi na szerokie możliwości nadużyć administrator uznał, że incydent stworzył **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych.

Przykład 7.1.5.

Błąd systemowy w szpitalu spowodował błędne zaktualizowanie danych medycznych pacjentów, w tym informacji o alergiach i przyjmowanych lekach. Błędy te przez dłuższy czas pozostały niewykryte, co stanowiło poważne zagrożenie dla zdrowia i życia pacjentów. W przypadku kolejnej hospitalizacji lub nagłego zabiegu mogliby oni otrzymać niewłaściwe leki lub przejść nieodpowiednie procedury medyczne, co mogłoby prowadzić do poważnych reakcji alergicznych, niebezpiecznych interakcji leków, a nawet śmiertelnych powikłań. W takiej sytuacji naruszenie integralności może skutkować bezpośrednim uszczerbkiem na zdrowiu i znacznym obniżeniem bezpieczeństwa pacjentów, którzy ufają, że dokumentacja medyczna odzwierciedla ich rzeczywisty stan zdrowia. Z uwagi na poważne zagrożenie zdrowia administrator uznał, że incydent stworzył **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych.

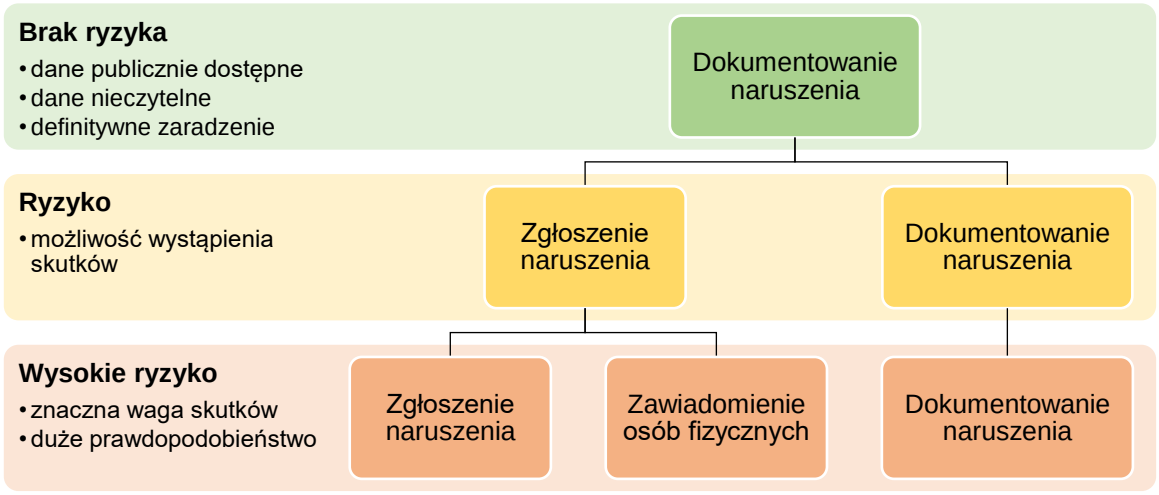
Przykład 7.1.6.

Awaria bazy danych osób z niepełnosprawnościami korzystających ze specjalistycznego transportu publicznego spowodowała, że usługa ta była niedostępna przez kilka dni. Użytkownicy nie mogli rezerwować przejazdów ani telefonicznie, ani osobiście, co było szczególnie dotkliwe dla osób

zależnych od tej formy transportu. Naruszenie dostępności spowodowało, że wiele osób straciło możliwość dotarcia do pracy lub skorzystania z innych niezbędnych usług, co znacząco wpłynęło na ich codziennie funkcjonowanie. Z uwagi na szczególną zależność osób od tej usługi administrator uznał, że incydent stworzył **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych.

Zapamiętaj

Infografika 7.1.1.



Dowiedz się więcej

→ Jak rozumieć i stosować podejście oparte na ryzyku?

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

7.2. Kim jest „zaufany odbiorca”?

Podczas **oceny ryzyka** związanego z naruszeniami poufności danych osobowych znaczenie może mieć to, komu je ujawniono[90].

Podmioty, którym przez pomyłkę udostępniono dane osobowe, mogą pozostawać niezidentyfikowane lub – pomimo prób kontaktu – bliżej nieznane administratorom. Co więcej, nawet istnienie relacji z takim odbiorcą może nie wystarczać, aby łagodniej oszacować ryzyko wystąpienia negatywnych konsekwencji.

„**Zaufany odbiorca**” to **podmiot, który przypadkowo otrzymał dane osobowe, ale dzięki dotychczasowej, pozytywnej współpracy z administratorem można uznać go za godny zaufania**. Istnieje bowiem wystarczająca pewność, że zareaguje on na zdarzenie właściwie i przyczyni się do **ograniczenia ryzyka** naruszenia praw lub wolności osób, których dane dotyczą.

Aby stwierdzić, że nieuprawniony odbiorca danych jest „zaufany”, administratorzy muszą co najmniej:

- **pozostawać z nim w stałych stosunkach** (np. w bliskiej współpracy biznesowej lub wspólnej strukturze organizacyjnej);
- **znać istotne szczegóły dotyczące odbiorcy** (np. procedury bezpieczeństwa i historię dotychczasowej, pozytywnej współpracy w podobnych sytuacjach).

> **Przykład 7.3.1.**
>
> **Zaufanym odbiorcą** może być m.in.:
>
> - inny dział w organizacji administratora;
> - sprawdzony, długoletni dostawca administratora;
> - profesjonalny i blisko współpracujący z administratorem podmiot przetwarzający.

[90] Więcej → 2.3. Naruszenia poufności danych osobowych

Koncepcja „zaufanego odbiorcy” pozwala administratorom dokładniej **ocenić ryzyko** wystąpienia po incydencie skutków dla osób, których dane dotyczą. Istniejąca relacja może złagodzić tę ocenę, ale nie wpływa na zaklasyfikowanie zdarzenia jako naruszenie ochrony danych osobowych[91].

Należy pamiętać, że każdy przypadek wymaga indywidualnej analizy i **żadnego podmiotu nie można z góry uznać za „zaufanego odbiorcę”**.

> **Uwaga!**
>
> Uznanie nieuprawnionego odbiorcy za „zaufanego” za każdym razem odbywa się w ramach oceny ryzyka naruszenia praw lub wolności osób fizycznych dotyczącej konkretnego naruszenia poufności danych osobowych. W związku z tym **status „zaufanego odbiorcy” należy monitorować**, co w uzasadnionych przypadkach może oznaczać konieczność zmiany oceny ryzyka.

> **Uwaga!**
>
> Administratorzy **muszą być gotowi wykazać**[92], że odpowiednio zastosowali koncepcję „zaufanego odbiorcy” w **ocenie ryzyka** związanego z naruszeniem ochrony danych osobowych.

Dowiedz się więcej

> → Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[91] Więcej → 2.1. Czym jest „naruszenie ochrony danych osobowych"?
[92] Więcej → 3.2. Odpowiedzialność i rozliczalność

8. Dokumentowanie naruszeń ochrony danych osobowych

8.1. Jak dokumentować naruszenia ochrony danych osobowych?

Dokumentowanie naruszeń ochrony danych osobowych jest nie tylko obowiązkiem administratorów, ale też istotnym narzędziem służącym do analizy przyczyn i skutków incydentów oraz skuteczności działań organizacji. Pozwala to na utrzymanie przejrzystości w postępowaniu i spełnienie wymogów **rozliczalności**[93].

Każde „stwierdzone" naruszenie ochrony danych osobowych[94], niezależnie od jego rodzaju, charakteru czy **ryzyka** negatywnych skutków[95], powinno zostać dokładnie **udokumentowane**, tak aby w razie potrzeby móc przedstawić szczegółowy przebieg wydarzeń oraz podjęte kroki. Dzięki temu administratorzy mogą **wykazać** przed organem nadzorczym, że właściwie przeanalizowali sytuację i skutecznie zadbali o interesy osób, których naruszenie dotyczy.

> **Art. 33 ust. 5 RODO**
>
> **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**
>
> *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 nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.*

[93] Więcej → 3.2. Odpowiedzialność i rozliczalność
[94] Więcej → 5.2. Na czym polega „stwierdzenie" naruszenia ochrony danych osobowych?
[95] Więcej → 7.1. Jak oceniać ryzyko związane z naruszeniami ochrony danych osobowych?

Uwaga!

Obowiązek dokumentowania dotyczy przede wszystkim „stwierdzonych” **naruszeń ochrony danych osobowych**. Mimo to, aby prawidłowo realizować zasadę rozliczalności, administratorzy powinni dokumentować także przypadki incydentów bezpieczeństwa, które zdecydowali się zaklasyfikować jako zdarzenia niebędące takimi naruszeniami, w tym w szczególności – przyczyny takiej decyzji[96].

W realizacji tego obowiązku może pomóc **wewnętrzny rejestr naruszeń ochrony danych osobowych**. Prowadzenie odrębnej ewidencji nie jest jednak obowiązkowe. Ważne, by informacje na ten temat były wyraźnie oznaczone i w razie potrzeby dostępne do wglądu.

Dokumentacja powinna uwzględniać m.in.:

- **okoliczności** naruszenia ochrony danych osobowych (takie jak data i czas wystąpienia, „stwierdzenia” i zakończenia naruszenia, sposób wykrycia naruszenia, przyczyny naruszenia, rodzaj naruszenia, przebieg naruszenia, rodzaj i zakres danych objętych naruszeniem, liczba i kategorie osób, których dane dotyczą);
- **skutki** (jeżeli wystąpiły) i/lub **możliwe skutki** naruszenia ochrony danych osobowych dla osób, których dane dotyczą;
- **uzasadnienie oceny ryzyka**;
- **podjęte działania zaradcze**[97] (w celu powstrzymania i ograniczenia naruszenia ochrony danych osobowych oraz zminimalizowania jego skutków) i **zapobiegawcze**[98] (w celu zminimalizowania wystąpienia podobnych naruszeń ochrony danych osobowych w przyszłości);

[96] Więcej → 2.1. Czym jest „naruszenie ochrony danych osobowych”?
[97] Więcej → 6.1. Jak zaradzać naruszeniom ochrony danych osobowych i ich ewentualnym skutkom?
[98] Więcej → 4.2. Jak zapobiegać naruszeniom ochrony danych osobowych?

- **szczegóły dotyczące zgłoszenia** naruszenia ochrony danych osobowych Prezesowi UODO[99] (takie jak data zgłoszenia, ewentualne przyczyny opóźnienia w zgłoszeniu, inne istotne informacje zawarte w zgłoszeniu; jeżeli administrator je zgłosił) lub **uzasadnienie decyzji o niezgłoszeniu** naruszenia ochrony danych osobowych Prezesowi UODO (art. 33 ust. 1 RODO)[100];

- **szczegóły dotyczące zawiadomienia osób, których dane dotyczą**, o naruszeniu ochrony danych osobowych[101] (takie jak data zawiadomienia, treść zawiadomienia, metoda zawiadomienia, liczba zawiadomionych osób; jeżeli administrator je zawiadomił) lub – w stosownym przypadku – **uzasadnienie decyzji o niezawiadomieniu osób, których dane dotyczą**, o naruszeniu ochrony danych osobowych (art. 34 ust. 3 RODO)[102].

Dokumentacja naruszeń ochrony danych osobowych powinna być regularnie **aktualizowana**. Każda nowa informacja o incydencie, jego skutkach lub działaniach zaradczych może wpływać na **ocenę ryzyka** i poprawność rejestru.

> **Uwaga!**
>
> RODO nie przewiduje okresów, po których informacje o naruszeniach ochrony danych osobowych mogą zostać usunięte. Administratorzy powinni więc przechowywać je **jak najdłużej**. Z tego powodu **nie jest wymagane ani zalecane umieszczanie w wewnętrznym rejestrze jakichkolwiek danych osobowych** (dotyczących np. osób zaangażowanych w proces zarządzania naruszeniem lub osób, których dotyczy naruszenie).
>
> Jeżeli jednak takie dane znajdą się w **ewidencji** naruszeń, należy pamiętać o zasadach dotyczących przetwarzania danych osobowych, takich jak **zasada minimalizacji**[103].

[99] Więcej → 9.3. Jakie informacje należy przekazać w zgłoszeniu naruszenia ochrony danych osobowych?
[100] Więcej → 9.1. Wyjątek od obowiązku zgłaszania naruszeń ochrony danych osobowych
Więcej → 7.1. Brak ryzyka
[101] Więcej → 10.3. Jakie informacje należy przekazać osobom, których dane dotyczą?
[102] Więcej → 10.1. Wyjątki od obowiązku zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych
[103] Patrz → Art. 5 ust. 1 RODO

Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

9. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu

9.1. Czym jest „zgłoszenie naruszenia ochrony danych osobowych”?

„**Zgłoszenie naruszenia ochrony danych osobowych**” to **oficjalne poinformowanie organu nadzorczego o naruszeniu**, które może wpłynąć na poufność, integralność lub dostępność danych osobowych.

Celem zgłoszenia jest **ograniczenie potencjalnych szkód** dla osób, których dane dotyczą[104], poprzez szybką reakcję administratora i współpracę z Prezesem UODO.

Działania te pomagają **zminimalizować konsekwencje** incydentu, a także umożliwiają organowi nadzorczemu **monitorowanie**, czy administratorzy właściwie realizują swoje obowiązki.

Administratorzy mają **obowiązek** zgłaszać Prezesowi UODO **naruszenia ochrony danych osobowych, które mogą stwarzać ryzyko** naruszenia praw lub wolności osób fizycznych[105].

> **Motyw 85. RODO**
>
> *(…) natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.*

[104] Więcej → 2.2. Dlaczego naruszenia ochrony danych osobowych są niebezpieczne?
[105] Więcej → 7.1. Jak oceniać ryzyko związane z naruszeniami ochrony danych osobowych?

Uwaga!

Samo **zgłoszenie** naruszenia ochrony danych osobowych **nie świadczy o winie** zgłaszającego, **nie przesądza** o naruszeniu przez niego przepisów RODO i **nie wszczyna** automatycznie żadnego formalnego postępowania[106]. Administratorzy zgłaszają incydenty, ponieważ mają największą wiedzę o procesach przetwarzania danych, a dokonanie zgłoszenia jest przede wszystkim przejawem odpowiedzialności i troski o ochronę praw osób, których prawa lub wolności mogą być zagrożone.

Wyjątek od obowiązku zgłaszania naruszeń ochrony danych osobowych

Naruszenia ochrony danych osobowych, w przypadku których ryzyko prawdopodobnie **nie wystąpi**, nie wymagają zgłoszenia. Są to jednak **wyjątkowe** sytuacje, a administratorzy muszą być w stanie **wykazać brak ryzyka**[107].

Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[106] Więcej → 2.5. Czym się różni „naruszenie ochrony danych osobowych" od „naruszenia przepisów RODO"?
[107] Więcej → 7.1. Brak ryzyka

9.2. Jak zgłaszać naruszenia ochrony danych osobowych?

Naruszenie ochrony danych osobowych należy zgłosić **jak najszybciej**, nie później niż w ciągu **72 godzin** od jego „stwierdzenia”[108], niezależnie od dni wolnych od pracy.

> **Art. 33. ust. 1 RODO**
>
> **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**
>
> *W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. (…)*

W celu zgłoszenia naruszenia ochrony danych osobowych warto skorzystać z **formularza** dostępnego na stronie internetowej UODO.

Zgłoszenia można dokonać na kilka sposobów:

- Elektronicznie, poprzez wypełnienie dedykowanego formularza elektronicznego dostępnego bezpośrednio na platformie biznes.gov.pl;
- Elektronicznie, poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą na platformie epuap.gov.pl: **/UODO/SkrytkaESP**
- Elektronicznie, poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl lub platformie epuap.gov.pl;
- Pocztą tradycyjną, poprzez wysłanie wypełnionego formularza na adres UODO.

[108] Więcej → 5.2. Na czym polega „stwierdzenie” naruszenia ochrony danych osobowych?

Uwaga!

W wyjątkowych sytuacjach (np. w przypadku awarii systemów umożliwiających zgłoszenie elektroniczne) administratorzy mogą tymczasowo przesłać zgłoszenie **mailowo** na adres: kancelaria@uodo.gov.pl

Należy wówczas w najbliższym możliwym terminie (np. po ustaniu awarii) **potwierdzić zgłoszenie** jedną ze standardowych metod.

Zgłaszanie naruszeń ochrony danych osobowych przez inne podmioty

Co do zasady to **administratorzy** zgłaszają naruszenia ochrony danych osobowych. Jeżeli administratorów jest więcej, powinni oni ustalić podział obowiązków w tym zakresie[109].

Podmioty przetwarzające[110] mogą zgłaszać naruszenia ochrony danych osobowych **wyłącznie** po uzyskaniu pisemnego **zezwolenia** od administratora, a kwestia ta powinna być precyzyjnie **uregulowana w umowie** między stronami. Ustalenia te **nie zwalniają** jednak administratorów z ostatecznej odpowiedzialności za zgłoszenie.

Zgłoszenia wstępne, uzupełniające i kompletne

Administratorzy nie zawsze dysponują **wszystkimi** niezbędnymi informacjami o naruszeniu ochrony danych osobowych[111] w ciągu pierwszych **72 godzin** od jego „stwierdzenia".

Dlatego istnieją **3 rodzaje zgłoszeń**:

[109] Więcej → 3.2. Współadministratorzy
[110] Więcej → 3.3. Kim jest „podmiot przetwarzający"?
[111] Więcej → 9.3. Jakie informacje należy przekazać w zgłoszeniu naruszenia ochrony danych osobowych?

- **zgłoszenia wstępne**, pozwalające przekazać podstawowe informacje w wymaganym terminie, z obowiązkiem późniejszego uzupełnienia;
- **zgłoszenia uzupełniające**, umożliwiające aktualizowanie informacji o incydencie w miarę ich gromadzenia;
- **zgłoszenia kompletne**, zawierające wszystkie wymagane informacje już przy pierwszym zgłoszeniu.

> **Art. 33 ust. 4 RODO**
>
> **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**
>
> *Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.*

Zgłaszanie naruszeń ochrony danych osobowych z opóźnieniem

Jeżeli zgłoszenie naruszenia ochrony danych osobowych przekazywane jest Prezesowi UODO **po upływie 72 godzin** od jego „stwierdzenia", administratorzy powinni dołączyć do niego **uzasadnienie opóźnienia**.

> **Art. 33 ust 1 RODO**
>
> **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**
>
> *(…) Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.*

Ponieważ wdrożenie procedur umożliwiających niezwłoczne, terminowe zgłaszanie naruszeń ochrony danych osobowych jest obowiązkiem

administratorów[112], opóźnienia powinny wynikać wyłącznie z **wyjątkowych sytuacji**.

Przykład 9.2.1.

Opóźnienie w zgłoszeniu naruszenia ochrony danych osobowych **nie powinno** być usprawiedliwiane m.in. tym, że:

- termin zgłoszenia przypadł na **weekend lub inny dzień wolny od pracy**, a kluczowy personel był niedostępny (przepisy RODO nie przewidują wstrzymywania biegu terminu z takiego powodu);
- osoba odpowiedzialna za zgłoszenie była na **urlopie lub zwolnieniu lekarskim**, a administrator nie zapewnił odpowiedniego zastępstwa;
- kierownictwo organizacji **nie miało czasu na zatwierdzenie zgłoszenia**, mimo że wewnętrzne procedury powinny uwzględniać konieczność niezwłocznego działania;
- administrator czekał na zakończenie **wewnętrznego dochodzenia** w sprawie incydentu (by dokonać jego kwalifikacji)[113] lub procesu **oceny ryzyka** związanego z naruszeniem ochrony danych osobowych[114];
- administrator potrzebował dodatkowego czasu na **zgromadzenie wszystkich wymaganych informacji** (w takich przypadkach można skorzystać ze zgłoszenia **wstępnego** i późniejszego **uzupełnienia**).

Dowiedz się więcej

→ Zgłaszanie naruszeń ochrony danych osobowych (uodo.gov.pl)

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[112] Patrz → Motyw 87. RODO
[113] Więcej → 5.2. Na czym polega „stwierdzenie" naruszenia ochrony danych osobowych?
[114] Więcej → 7.1. Jak oceniać ryzyko związane z naruszeniami ochrony danych osobowych?

9.3. Jakie informacje należy przekazać w zgłoszeniu naruszenia ochrony danych osobowych?

Administratorzy powinni przekazywać Prezesowi UODO **wszystkie istotne informacje** dotyczące naruszeń ochrony danych osobowych. Przepisy określają **minimalne wymagania** w tym zakresie.

> **Art. 33 ust. 3 RODO**
>
> **Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu**
>
> *Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:*
>
> *a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;*
>
> *b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;*
>
> *c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;*
>
> *d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.*

W praktyce warto uwzględnić w zgłoszeniu następujące informacje:

- podstawowe **informacje o administratorze** i **innych podmiotach** mających związek z incydentem (np. współadministratorach, podmiotach przetwarzających lub podmiotach trzecich);
- **okoliczności** naruszenia ochrony danych osobowych (takie jak data i czas wystąpienia, „stwierdzenia" i zakończenia naruszenia, sposób wykrycia naruszenia, przyczyny naruszenia, rodzaj naruszenia, przebieg naruszenia,

rodzaj i zakres danych objętych naruszeniem, liczba i kategorie osób, których dane dotyczą);

- **skutki** (jeżeli wystąpiły) i/lub **możliwe skutki** naruszenia ochrony danych osobowych dla osób, których dane dotyczą;
- **uzasadnienie oceny ryzyka**;
- podjęte działania **zaradcze** (jeżeli administrator je podjął) lub zaplanowane działania **zaradcze** wraz z deklarowaną datą ich realizacji (jeżeli administrator jeszcze ich nie podjął)[115];
- wdrożone (jeżeli administrator je wdrożył) lub zaplanowane **środki bezpieczeństwa** służące **zapobieganiu** występowania podobnych incydentów w przyszłości wraz z deklarowaną datą ich wdrożenia (jeżeli administrator jeszcze ich nie wdrożył)[116];
- **szczegóły dotyczące zawiadomienia osób, których dane dotyczą**, o naruszeniu ochrony danych osobowych[117] (takie jak data zawiadomienia, treść zawiadomienia, metoda zawiadomienia, liczba zawiadomionych osób; jeżeli administrator je zawiadomił) lub – w stosownym przypadku – **uzasadnienie decyzji o niezawiadomieniu osób, których dane dotyczą**, o naruszeniu ochrony danych osobowych (art. 34 ust. 3 RODO)[118];
- imię i nazwisko oraz **dane kontaktowe IOD**[119] lub informacje o innym punkcie kontaktu wyznaczonym w organizacji administratora.

W prawidłowym zgłoszeniu naruszenia ochrony danych osobowych może pomóc uważne wypełnienie **formularza** dostępnego na stronie internetowej UODO[120].

[115] Więcej → 6.1. Jak zaradzać naruszeniom ochrony danych osobowych i ich ewentualnym skutkom?
[116] Więcej → 4.2. Jak zapobiegać naruszeniom ochrony danych osobowych?
[117] Więcej → 10.3. Jakie informacje należy przekazać osobom, których dane dotyczą?
[118] Więcej → 10.1. Wyjątki od obowiązku zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych
[119] Więcej → 3.6. Jaką rolę odgrywają inspektorzy ochrony danych w procesie obsługi naruszeń ochrony danych osobowych?
[120] Więcej → 9.2. Jak zgłaszać naruszenia ochrony danych osobowych?

Uwaga!

Należy **starannie** i **rzetelnie** wypełniać zgłoszenia naruszeń ochrony danych osobowych. Umieszczanie w nich zarówno informacji niepełnych, jak i nadmiarowych, może prowadzić do wydłużania procesu ich weryfikowania oraz opóźniania reakcji na incydenty, a w konsekwencji przyczyniać się do **zwiększania ryzyka** negatywnego wpływu tych zdarzeń na osoby, których dane dotyczą.

Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

10. Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

10.1. Czym jest „zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych”?

„**Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych**” to **oficjalne poinformowanie osoby fizycznej o naruszeniu**, które może wpłynąć na poufność, integralność lub dostępność jej danych osobowych.

Administratorzy mają **obowiązek** zawiadamiać o **naruszeniach ochrony danych osobowych, które mogą powodować wysokie ryzyko** naruszenia praw lub wolności osób fizycznych[121].

Celem zawiadomienia jest **ograniczenie potencjalnych szkód** dla osób, których dane dotyczą, poprzez przekazanie im istotnych informacji o zdarzeniu oraz rekomendowanych środkach ostrożności.

> **Art. 34 ust. 1 RODO**
>
> **Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych**
>
> *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.*

Informowanie osób fizycznych o zdarzeniach, które **nie stwarzają** wysokiego ryzyka **nie jest zalecane**. Nadmiar komunikatów w tym zakresie może skutkować niepotrzebnym stresem lub przeciążeniem informacyjnym,

[121] Więcej → 7.1. Wysokie ryzyko

prowadzącym do ignorowania przez odbiorców podobnych wiadomości, co w konsekwencji mogłoby osłabić znaczenie zawiadomień.

> **Uwaga!**
>
> Jeżeli naruszenie ochrony danych osobowych wywołuje **wysokie ryzyko** wobec tylko niektórych osób nim objętych, administratorzy powinni zawiadomić **wyłącznie te osoby**.

Wyjątki od obowiązku zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

O naruszeniach ochrony danych osobowych, które mogą powodować **wysokie ryzyko** naruszenia ich praw lub wolności **nie trzeba zawiadamiać** osób, których dane dotyczą, jeżeli:

- **przed wystąpieniem** naruszenia ochrony danych osobowych zastosowano **środki ochrony eliminujące wysokie ryzyko** (np. w przypadku ujawnienia lub utracenia danych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych, jeżeli są one zabezpieczone kluczem, który nie został naruszony, a administrator ma dostęp do ich kopii zapasowej[122]);
- **po wystąpieniu** naruszenia ochrony danych osobowych **natychmiast** zastosowano **środki ochrony eliminujące wysokie ryzyko** (np. w przypadku incydentów, którym administratorzy definitywnie **zaradzili**[123]);
- zawiadomienie wymagałoby **niewspółmiernie dużego wysiłku**, ale wyłącznie pod warunkiem, że administrator wyda **publiczny komunikat** lub **poinformuje osoby fizyczne w podobny, równie skuteczny sposób** (w

[122] Patrz → Przykład 7.1.2.
[123] Patrz → Przykład 7.1.3.

tym przypadku wyjątek wyłącza obowiązek **tylko w zakresie zawiadomienia indywidualnego**[124]).

Art. 34 ust. 3 RODO

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

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.

Przykład 10.1.1.

Dokumentacja papierowa dotycząca kilku tysięcy klientów administratora uległa zniszczeniu w wyniku pożaru. Ponieważ organizacja nie posiadała żadnych kopii dokumentów, nie była w stanie odtworzyć danych kontaktowych osób, których dane dotyczą, w celu indywidualnego zawiadomienia ich o zdarzeniu. Zgromadzenie ich na nowo z pewnością **wymagałoby niewspółmiernie dużego wysiłku**, dlatego administrator wydał **publiczny komunikat**, dostępny na jego stronie internetowej oraz na łamach lokalnych gazet.

[124] Więcej → 10.2. Odpowiednie metody zawiadamiania osób, których dane dotyczą

Uwaga!

Administratorzy **muszą być gotowi wykazać**[125], że odpowiednio zastosowali **wyjątek od obowiązku** zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych.

Dowiedz się więcej

→ Wytyczne 1/2021 w sprawie przykładów dotyczących zgłaszania naruszeń ochrony danych osobowych

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[125] Więcej → 3.2. Odpowiedzialność i rozliczalność

10.2. Jak zawiadamiać osoby, których dane dotyczą, o naruszeniach ochrony danych osobowych?

Administratorzy mają **obowiązek** zadbać o to, aby osoby, których dane zostały objęte naruszeniem, były o tym zawiadamiane:

- niezwłocznie;
- zrozumiale;
- odpowiednimi środkami komunikacji.

Zawiadamianie osób, których dane dotyczą, przez inne podmioty

Co do zasady to **administratorzy** zawiadamiają osoby, których dane dotyczą, o naruszeniach ochrony danych osobowych. Jeżeli administratorów jest więcej, powinni oni ustalić podział obowiązków w tym zakresie[126].

Podmioty przetwarzające[127] mogą dokonywać zawiadomień **wyłącznie** po uzyskaniu pisemnego **zezwolenia** od administratora, a kwestia ta powinna być precyzyjnie **uregulowana w umowie** między stronami. Ustalenia te **nie zwalniają** jednak administratorów z ostatecznej odpowiedzialności za zawiadomienie.

> **Uwaga!**
>
> Jeżeli to **podmiot przetwarzający** zawiadamia osobę fizyczną o incydencie, musi jasno wskazać w treści komunikatu, kto w danym przypadku jest **administratorem** danych, a kto **podmiotem przetwarzającym** działającym w jego imieniu[128].

[126] Więcej → 3.2. Współadministratorzy
[127] Więcej → 3.3. Kim jest „podmiot przetwarzający”?
[128] Więcej → 10.3. Jakie informacje należy przekazać osobom, których dane dotyczą?

Niezwłoczne zawiadomienie osób, których dane dotyczą

Zawiadomienia powinny być przekazywane **jak najszybciej**, aby osoby, których dane dotyczą, miały szansę uchronić się przed potencjalnymi skutkami takich zdarzeń.

> **Motyw 86. RODO**
>
> *Administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej osobie podjęcie niezbędnych działań zapobiegawczych. (…) Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie.*

> **Motyw 87. RODO**
>
> *(…) To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją organu nadzorczego, zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu.*

> **Uwaga!**
>
> Administratorzy mogą **wyjątkowo** zrezygnować z **niezwłocznego** przekazania zawiadomienia osobom fizycznym, gdy taka konieczność wynika z prawnie uzasadnionego interesu organów ścigania badających okoliczności naruszenia

ochrony danych osobowych, zgodnie z zaleceniami tych organów, do momentu zakończenia takich działań[129].

Zrozumiałe zawiadamianie osób, których dane dotyczą

Zawiadomienia powinny być przekazywane w **zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie** oraz formułowane **jasnym i prostym językiem**, dostosowanym do konkretnego odbiorcy, tak aby osoby, których dane dotyczą, mogły bez problemu **znaleźć i zrozumieć potrzebne informacje**[130].

Odpowiednie metody zawiadamiania osób, których dane dotyczą

Zawiadomienia powinny być **indywidualne i bezpośrednie**. Naruszenia ochrony danych osobowych nie zawsze wpływają w jednakowy sposób na wszystkie osoby (np. ze względu na różnice w zakresie naruszonych danych lub szczególny charakter niektórych osób). Administratorzy muszą więc **dostosowywać treść komunikatów do konkretnych osób bądź ich poszczególnych grup** (jeżeli da się takie wyodrębnić).

Ponadto odbiorcy muszą mieć możliwość wielokrotnego zapoznania się z treścią zawiadomienia, dlatego zasadniczo powinny przyjmować one **formę pisemną**. Zrezygnować z niej można wyłącznie na żądanie osoby, której dane dotyczą[131].

Przykład 10.2.1.

Środki komunikacji, które można wykorzystać do zawiadomienia osób fizycznych o naruszeniu ochrony danych osobowych to m.in.:

- SMS;
- e-mail;

[129] Patrz → Motyw 88. RODO
[130] Patrz → Art. 12 ust. 1 RODO
[131] Tamże.

- poczta tradycyjna;
- osobiste przekazanie informacji.

Uwaga!

Zawiadomienia powinny być przekazywane za pomocą **specjalnie do tego przeznaczonych wiadomości**. Administratorzy nie mogą łączyć treści zawiadomień z innymi komunikatami (np. reklamami, biuletynami, inną korespondencją).

Jeżeli indywidualne i bezpośrednie zawiadomienie **wymaga niewspółmiernie dużego wysiłku**, administratorzy mogą przekazać informacje osobom, których dane dotyczą, za pośrednictwem:

- publicznego komunikatu;
- podobnego, równie skutecznego środka[132].

Uwaga!

Takie zawiadomienia muszą gwarantować każdej osobie, której dane dotyczą, **realną szansę** na zapoznanie się z ich treścią (np. dzięki umieszczeniu komunikatu w widocznym miejscu oraz zapewnienie jego długotrwałej dostępności).

Administratorzy, którzy nie są w stanie **skutecznie** zawiadomić osoby, której dane dotyczą, przy użyciu wybranej metody, **powinni skorzystać z innych środków komunikacji**, a gdy te również okażą się nieskuteczne – zadbać o możliwość przekazania zawiadomienia w przyszłości, **przy najbliższej możliwej okazji** (np. w przypadku wznowienia kontaktu przez osobę fizyczną).

[132] Więcej → 10.1. Wyjątki od obowiązku zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych
Patrz → Przykład 10.1.1.

Uwaga!

W przypadku zastosowania jakiegokolwiek odstępstwa od reguł dotyczących prawidłowego zawiadamiania osób, których dane dotyczą, o naruszeniach ochrony danych osobowych, administratorzy **muszą być gotowi wykazać**[133], że podjęte przez nich działania były w danym przypadku uzasadnione okolicznościami sprawy.

Dowiedz się więcej

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[133] Więcej → 3.2. Odpowiedzialność i rozliczalność

10.3. Jakie informacje należy przekazać osobom, których dane dotyczą?

Administratorzy powinni przekazywać osobom fizycznym informacje**,** które umożliwią im zrozumienie zaistniałych naruszeń ochrony danych osobowych oraz podjęcie skutecznych działań **zaradczych**.

> **Motyw 86. RODO**
>
> *(…) Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. (…)*

Przepisy określają **minimalne wymagania** w tym zakresie.

> **Art. 34 ust. 2 RODO**
>
> **Zawiadamianie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych**
>
> *Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d).*

W praktyce warto uwzględnić w zawiadomieniu następujące informacje:

- podstawowe **informacje o administratorze** i **innych podmiotach** mających związek z incydentem (np. współadministratorach, podmiotach przetwarzających lub podmiotach trzecich);
- **okoliczności** naruszenia ochrony danych osobowych (data i czas wystąpienia i zakończenia naruszenia, przyczyna naruszenia, rodzaj naruszenia, przebieg naruszenia, rodzaj i zakres danych objętych naruszeniem);

- **skutki** (jeżeli wystąpiły) i/lub **możliwe skutki** naruszenia ochrony danych osobowych dla osób, których dane dotyczą;
- podjęte działania **zaradcze** (jeżeli administrator je podjął) lub zaplanowane działania **zaradcze** (jeżeli administrator jeszcze ich nie podjął)[134];
- **zalecenia** dotyczące środków **zaradczych**, które we własnym zakresie może podjąć osoba, której dane dotyczą;
- imię i nazwisko oraz **dane kontaktowe IOD**[135] lub informacje o innym punkcie kontaktu wyznaczonym w organizacji administratora.

> **Uwaga!**
>
> Należy **starannie** i **rzetelnie** przygotowywać zawiadomienia o naruszeniach ochrony danych osobowych. Umieszczanie w nich informacji **nielogicznych i niespójnych** (jak np. skutki, które nie mają związku z zakresem danych objętych naruszeniem), **niekompletnych** (jak np. brak konkretnych kategorii danych objętych naruszeniem), **nieskutecznych** (jak np. dane kontaktowe, które nie gwarantują szybkiej i łatwej komunikacji), **nieprecyzyjnych** (jak np. zbyt ogólny opis możliwych konsekwencji naruszenia) lub w inny sposób niezgodne z wymaganiami dotyczącymi formy i treści zawiadomienia[136] może opóźniać reakcje na incydenty i przyczyniać się do **zwiększania ryzyka** negatywnego wpływu tych zdarzeń na osoby, których dane dotyczą.

Dowiedz się więcej

> → Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

[134] Więcej → 6.1. Jak zaradzać naruszeniom ochrony danych osobowych i ich ewentualnym skutkom?
[135] Więcej → 3.6. Jaką rolę odgrywają inspektorzy ochrony danych w procesie obsługi naruszeń ochrony danych osobowych?
[136] Więcej → 10.2. Jak zawiadamiać osoby, których dane dotyczą, o naruszeniach ochrony danych osobowych?

11. Transgraniczne naruszenia ochrony danych osobowych

11.1. Czym jest „transgraniczne naruszenie ochrony danych osobowych”?

„**Transgraniczne naruszenie ochrony danych osobowych**” to incydent bezpieczeństwa, który:

- może wpłynąć na poufność, integralność lub dostępność danych osobowych przetwarzanych w więcej niż jednym państwie UE; **lub**
- może **znacznie** wpłynąć na poufność, integralność lub dostępność danych osobowych dotyczących osób fizycznych w więcej niż jednym państwie UE.

> **Art. 4 pkt 23 RODO**
>
> **Definicje**
>
> *„transgraniczne przetwarzanie” oznacza:*
>
> *a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo*
>
> *b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;*

Główna różnica pomiędzy krajowymi a transgranicznymi naruszeniami ochrony danych osobowych polega na **zakresie terytorialnym incydentu** i wynikającej z tego potrzeby współpracy między organami nadzorczymi.

Kluczową rolę odgrywa wśród nich **organ wiodący**, czyli organ nadzorczy państwa UE, w którym:

- znajduje się główna jednostka organizacyjna administratora; **lub**
- podejmowane są kluczowe decyzje dotyczące przetwarzania[137].

> **Motyw 36. RODO**
>
> *Główną jednostką organizacyjną administratora w Unii powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, chyba że decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej administratora w Unii, w którym to przypadku za główną jednostkę organizacyjną należy uznać tą drugą jednostkę organizacyjną. Główną jednostkę organizacyjną administratora w Unii należy określać na podstawie obiektywnych kryteriów; powinna ona oznaczać skuteczne i faktyczne zarządzanie za pośrednictwem stabilnych struktur polegające na podejmowaniu najważniejszych decyzji co do celów i sposobów przetwarzania. Kryterium to nie powinno zależeć od faktu, czy przetwarzanie danych osobowych odbywa się w tej lokalizacji. Obecność i wykorzystywanie środków technicznych i technologii do przetwarzania danych osobowych lub do czynności przetwarzania nie stanowią same w sobie o głównej jednostce organizacyjnej, nie są więc kryteriami decydującymi o jej określeniu. Główną jednostką organizacyjną podmiotu przetwarzającego powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli nie ma on centralnej administracji w Unii – miejsce, w którym odbywają się główne czynności przetwarzania w Unii. Jeżeli sprawa dotyczy zarówno administratora, jak i podmiotu przetwarzającego, właściwym wiodącym organem nadzorczym powinien pozostać organ nadzorczy państwa członkowskiego, w którym administrator ma główną jednostkę organizacyjną, ale organ nadzorczy podmiotu przetwarzającego powinien być uznawany za organ nadzorczy, którego sprawa dotyczy, i powinien uczestniczyć w procedurze współpracy przewidzianej w niniejszym rozporządzeniu. (…) Jeżeli przetwarzania dokonuje grupa przedsiębiorstw, za jej główną jednostkę organizacyjną należy uznać główną jednostkę organizacyjną przedsiębiorstwa sprawującego kontrolę, chyba że cel i sposoby przetwarzania określa inne przedsiębiorstwo.*

[137] Więcej → Art. 56 RODO

W przypadku **przetwarzania transgranicznego** administratorzy powinni przygotować się na to (np. poprzez wdrożenie odpowiednich procedur), by w razie potrzeby:

- **określić**, czy naruszenie ochrony danych osobowych ma **charakter transgraniczny**;
- **zidentyfikować wiodący organ nadzorczy**, któremu należy **zgłosić** naruszenie ochrony danych osobowych[138] oraz prowadzić dalszą komunikację w tej sprawie;
- **dostosować formę i treść zawiadomień** przekazywanych osobom, których dane dotyczą[139], do sytuacji, w której odbiorcy pochodzą z różnych państw UE (np. zwracając uwagę na język zawiadomienia, specyficzne przepisy lokalne i inne istotne różnice, które mogą wpływać na sposób, w jaki osoby fizyczne odbierają komunikat).

Uwaga!

W razie wątpliwości co do tożsamości **wiodącego organu nadzorczego** administrator powinien zgłosić naruszenie ochrony danych osobowych lokalnemu organowi **w miejscu, w którym doszło do incydentu** i postępować zgodnie z jego wskazówkami.

Przykład 11.1.1.

Spółka handlująca odzieżą posiadała oddziały w kilku państwach UE, a każdy z nich prowadził internetową sprzedaż detaliczną, dostarczając klientom ubrania na terenie państwa, w którym się znajdował. Systemy sprzedażowe oddziałów były zintegrowane i oparte na wspólnych serwerach, co umożliwiało dostęp do jednolitej bazy klientów. W wyniku poważnej awarii oprogramowania odpowiedzialnego za bazę danych doszło do trwałej utraty danych osobowych wszystkich klientów spółki. Kopie zapasowe danych również uległy uszkodzeniu, co uniemożliwiło przywrócenie bazy. W efekcie firma nie mogła

[138] Więcej → 9. Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu
[139] Więcej → 10. Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

realizować zamówień, przetwarzać reklamacji ani obsługiwać zwrotów. Ponieważ incydent dotknął klientów w kilku krajach UE, spółka musiała zgłosić naruszenie ochrony danych osobowych wiodącemu organowi nadzorczemu oraz skoordynować zawiadomienie osób fizycznych w każdym z państw.

Przykład 11.1.2.

Laboratorium zajmujące się badaniami genetycznymi na potrzeby potwierdzania pokrewieństwa (np. na zlecenie osób chcących zweryfikować ojcostwo) miało swoja siedzibę w jednym z państw UE, ale klienci z innych krajów UE również przesyłali do niego próbki DNA do analizy. W wyniku cyberataku doszło do ujawnienia danych osobowych klientów laboratorium, w tym wyników testów na ojcostwo – zarówno pozytywnych, jak i negatywnych. Hakerzy opublikowali te dane na oficjalnej stronie internetowej laboratorium, gdzie przez kilka dni były one dostępne dla każdego odwiedzającego. Ponieważ incydent dotknął klientów w kilku krajach UE, spółka musiała zgłosić naruszenie ochrony danych osobowych wiodącemu organowi nadzorczemu oraz skoordynować zawiadomienie osób fizycznych w każdym z państw.

Dowiedz się więcej

→ Wytyczne 8/2022 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego

→ Wytyczne 9/2022 dotyczące zgłaszania naruszeń ochrony danych osobowych na podstawie RODO

www.uodo.gov.pl