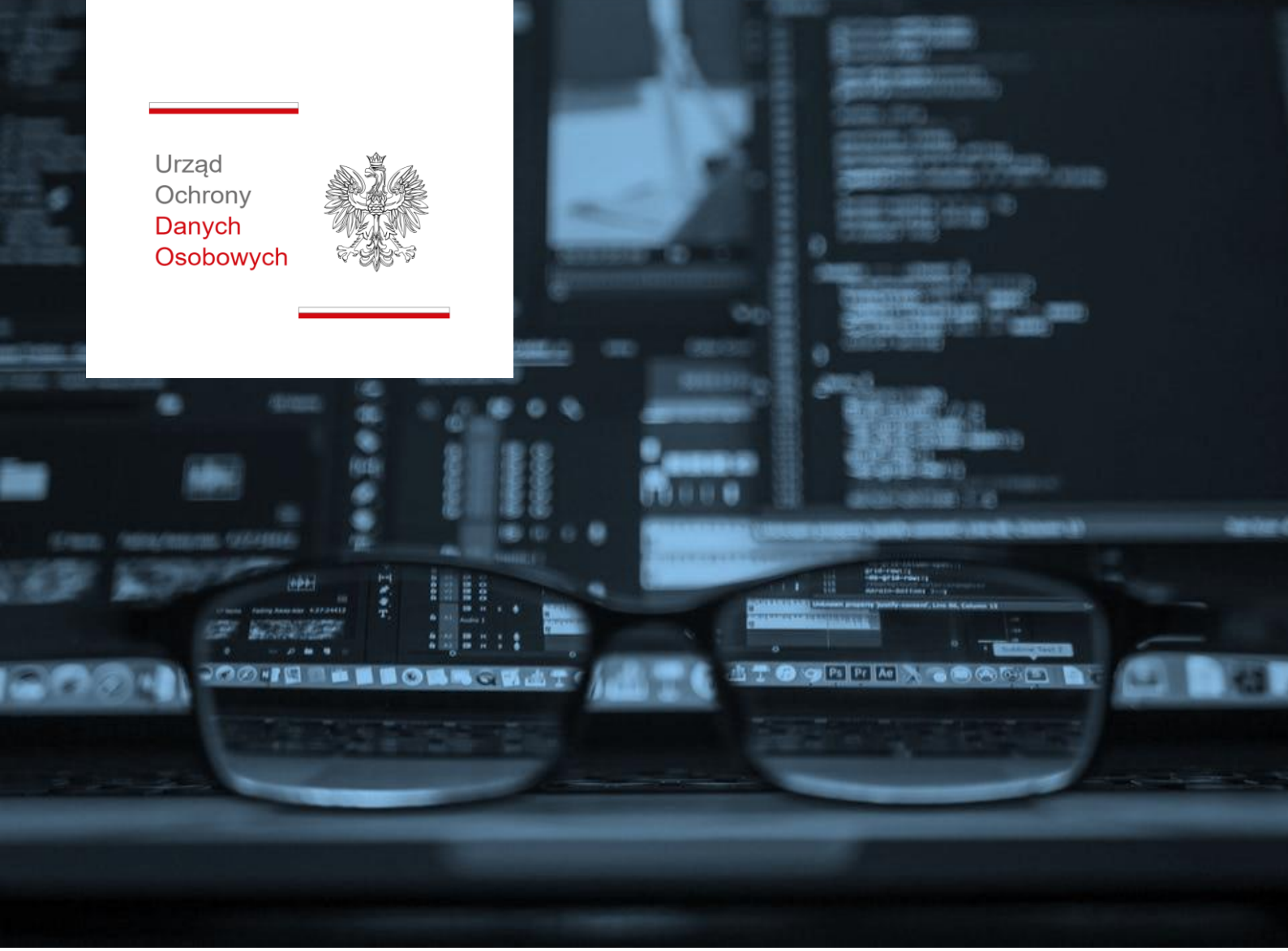
Urząd
Ochrony
Danych
Osobowych



Obowiązki administratorów **związane z naruszeniami ochrony danych osobowych**

www.uodo.gov.pl

wersja 1.0
maj 2019

Spis treści

Pojęcie naruszenia ochrony danych osobowych. Definicja wraz z przykładami.

01.

Przez pojęcie „naruszenia ochrony danych osobowych" należy rozumieć **„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"** (art. 4 pkt 12 RODO).

Żeby zaistniało naruszenie, muszą być spełnione łącznie trzy przesłanki:

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

Jednocześnie - jak wskazuje Grupa Robocza Art. 29 w Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01) - można wyróżnić trzy typy naruszeń ochrony danych osobowych:

1. **NARUSZENIE POUFNOŚCI – polega na ujawnieniu danych osobowych nieuprawnionej osobie**

Przykład I

Przypadkowe wysłanie danych osobowych klienta do niewłaściwego działu firmy lub osoby postronnej.

Przykład II

System informatyczny administratora został zainfekowany złośliwym oprogramowaniem. Po przeprowadzeniu wstępnej analizy administrator stwierdził, że w wyniku działania tego oprogramowania osoba nieupoważniona uzyskała dostęp do danych osobowych.

2. **NARUSZENIE DOSTĘPNOŚCI – polega na czasowej bądź trwałej utracie lub zniszczeniu danych osobowych**

Przykład I

Zgubienie lub kradzież nośnika zawierającego bazy danych klientów administratora przy braku kopii zapasowej.

Przykład II

Pracownik przypadkowo lub osoba nieupoważniona celowo usuwa dane ze zbioru. Administrator próbuje odzyskać dane z kopii zapasowej, jednak jego działania nie przynoszą rezultatu.

Przykład III

W wyniku przerwy w dostawie prądu lub ataku typu „odmowa usługi" (tzw. DDoS), administrator tymczasowo lub trwale traci dostęp do danych osobowych.

W powyższym przykładzie III mamy do czynienia ze zdarzeniem skutkującym utratą dostępności danych osobowych przez pewien czas. Jest to naruszenie, ponieważ brak dostępu do danych może mieć znaczący wpływ na prawa lub wolności osób fizycznych. Jednak **nie każda czasowa niedostępność danych jest naruszeniem**. Jest nią tylko taka niedostępność danych, która może stanowić ryzyko dla praw lub wolności osób fizycznych, np. w przypadku szpitala brak dostępu danych pacjentów może prowadzić do uniemożliwienia przeprowadzenia operacji medycznej, a zatem narażenia życia, co należy zaklasyfikować jako wysokie ryzyko dla praw lub wolności osób fizycznych. W przypadku kilkugodzinnego braku dostępu spółki medialnej do swoich systemów i niemożliwości wysyłania newslettera do abonentów, istnieje natomiast niskie prawdopodobieństwo naruszenia praw lub wolności osób fizycznych. Podobnie w przypadku planowanej konserwacji systemu, dane osobowe mogą być niedostępne przez pewien czas i nie należy traktować tego jako naruszenia bezpieczeństwa.

3. **NARUSZENIE INTEGRALNOŚCI – polega na zmianie treści danych osobowych w sposób nieautoryzowany**.

Przykład

„Pracownik dla żartu zmienia nazwiska klientów poprzez dopisanie litery „s" na końcu każdego z nich."

Jakie obowiązki w związku z naruszeniami ochrony danych osobowych przewiduje RODO?

02.

RODO przewiduje następujące obowiązki administratora związane z naruszeniem ochrony danych osobowych:

- wprowadzenie procedur umożliwiających stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych;

- prowadzenie wewnętrznej ewidencji naruszeń;
- zgłaszanie naruszeń organowi nadzorczemu;
- powiadamianie osoby, której dane dotyczą, o naruszeniu;
- podejmowanie działań mających na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.

Ważnym, jeśli nie najważniejszym, elementem całego procesu związanego ze zgłaszaniem naruszenia ochrony danych, jest szybkość podjęcia niezbędnych działań, zarówno wobec organu nadzorczego, jak i osób, których dane dotyczą.

2.1 Administrator

Żeby zapewnić działania bez zbędnej zwłoki, administratorzy powinni opracować i wdrożyć procedury postępowania na wypadek wystąpienia naruszenia ochrony danych. Taka procedura pomoże ujednolicić, usprawnić oraz przyśpieszyć działania w przypadku wykrycia naruszenia ochrony danych. W tej procedurze powinno się zawrzeć m.in.:

- cel, w jakim procedura została opracowana;
- zakres jej stosowania;
- katalog ewentualnych zagrożeń i naruszeń, jakie mogą wystąpić w związku z przetwarzaniem danych u konkretnego administratora;
- opis etapów zarządzania naruszeniem, począwszy od jego wykrycia, a kończąc na usunięciu;
- opis postępowania personelu administratora w przypadku wystąpienia naruszenia ochrony danych.

Zdolność do zapobiegania naruszeniom w przypadkach, w których jest to możliwe, oraz zdolność do niezwłocznego reagowania na naruszenia w sytuacjach, w których mimo to dojdzie do ich wystąpienia, stanowi kluczowy element każdej polityki w zakresie bezpieczeństwa danych[1].

Dobrze zaprojektowana i wdrożona procedura postępowania na wypadek wystąpienia naruszenia ochrony danych pozwala dokonać klasyfikacji zidentyfikowanych naruszeń ochrony danych, czyli określić poziom wystąpienia ryzyka naruszenia praw i wolności osób fizycznych. W zależności, z jakim poziomem ryzyka naruszenia praw i wolności osób fizycznych administrator ma do czynienia, inaczej kształtują się jego obowiązki w stosunku do organu nadzorczego, a także osób, których dane dotyczą. Jeżeli w wyniku analizy administrator stwierdził, że prawdopodobieństwo zaistnienia ryzyka naruszenia praw i wolności osób fizycznych jest małe, nie jest on zobligowany do zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych Osobowych. Wskazane naruszenie musi jedynie wpisać do wewnętrznej ewidencji naruszeń. W przypadku stwierdzenia ryzyka naruszenia praw i wolności osób fizycznych, obowiązkiem administratora jest zgłoszenie naruszenia ochrony danych Prezesowi UODO, jak również umieszczenie wpisu w wewnętrznej ewidencji naruszeń. Wystąpienie wysokiego ryzyka naruszenia praw i wolności osób fizycznych, oprócz wpisu w ewidencji naruszeń, wymaga od administratora podjęcia odpowiednich działań, zarówno wobec organu nadzorczego (zgłoszenie naruszenia ochrony danych), ale także w niektórych przypadkach również wobec osób, których dane dotyczą. W przypadku naruszeń, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą, RODO wprowadza bowiem dodatkowy obowiązek niezwłocznego

[1] Patrz art. 32 RODO oraz motyw 83 i 87 RODO.

zawiadomienia podmiotu danych przez administratora, chyba że ten podjął działania prewencyjne przed zaistnieniem naruszenia albo działania zaradcze po wystąpieniu naruszenia (art. 34 ust. 3 RODO).

Niezależnie od poziomu ryzyka, administrator zobowiązany jest do wprowadzenia środków zaradczych mających na celu zminimalizowanie **ryzyka i zabezpieczenie danych osobowych.**

2.2 Współadministratorzy

Współadministratorzy, zgodnie z art. 26 RODO, w ramach realizowanego wspólnie przedsięwzięcia, określają zakresy swojej odpowiedzialności, dotyczącej wypełniania obowiązków wynikających z RODO. Wiąże się to z koniecznością ustalenia, która strona będzie odpowiedzialna za wywiązywanie się ze zobowiązań ustanowionych w art. 33 i 34 RODO oraz jakie będą obowiązki pozostałych stron w zakresie wymiany informacji dotyczących naruszeń ochrony danych osobowych. Ważne jest, aby podjęte uzgodnienia zapewniały efektywne wywiązywanie się z obowiązków wynikających z przepisów prawa. Grupa Robocza Art. 29 w Wytycznych dotyczących zgłaszania naruszeń (WP 250 rev. 01) zaleca, aby uzgodnienia umowne między współadministratorami uwzględniały postanowienia wskazujące administratora, który będzie zajmował się dbaniem o wypełnianie ustanowionych w RODO obowiązków w zakresie zgłaszania naruszeń lub który będzie odpowiedzialny za wypełnianie tych obowiązków.

2.3 Podmiot przetwarzający

Administrator ponosi odpowiedzialność prawną za przetwarzanie danych osobowych prowadzone przez niego samego lub w jego imieniu (motyw 74 RODO). Podmiot przetwarzający odgrywa istotną rolę w zapewnianiu administratorowi możliwości wywiązania się ze spoczywających na nim obowiązków. Zgodnie z art. 28 ust. 3 lit. f RODO, umowa lub inny instrument prawny stanowią w szczególności, że **podmiot przetwarzający,** uwzględniając charakter przetwarzania oraz dostępne mu informacje, **pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36 RODO**, a zatem również obowiązków określonych w art. 33 i 34 RODO.

Zgodnie z art. 33 ust. 2 RODO, **podmiot przetwarzający** po stwierdzeniu naruszenia ochrony danych osobowych **bez zbędnej zwłoki zgłasza je administratorowi**. Bez zbędnej zwłoki oznacza najszybciej jak to możliwe i taki termin wywiązywania się z tego obowiązku powinien być nałożony na podmioty przetwarzające w umowach powierzenia. Jeżeli podmiot przetwarzający świadczy usługi na rzecz wielu administratorów, a dany incydent wywiera wpływ na wszystkich z nich, podmiot przetwarzający będzie zobowiązany do zgłoszenia naruszenia bez zbędnej zwłoki każdemu z tych administratorów.

Zgodnie z art. 28 ust. 1 RODO, jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą. **Administrator powinien korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje** – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – **wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia**, w tym wymogom bezpieczeństwa przetwarzania (motyw 81 RODO).

Oznacza to na przykład, że gdy naruszenie ochrony danych osobowych wymaga podjęcia działań mających na celu jak najszybsze zablokowanie nieuprawnionego dostępu do danych osobowych, a dotyczy to danych przetwarzanych w ramach powierzenia, administrator powinien wydać odpowiednie polecenie podmiotowi przetwarzającemu i zadbać o to by żądanie organu nadzorczego zostało jak najszybciej i skutecznie zrealizowane. Pamiętać należy, że brak odpowiedniego działania po stronie podmiotu przetwarzającego w sytuacji naruszenia ochrony danych osobowych może skutkować zastosowaniem przez organ wobec podmiotu przetwarzającego uprawnień określonych w art. 58 RODO. Dotychczasowe doświadczenia Urzędu Ochrony Danych Osobowych wskazują, że nie wszystkie podmioty, przy pomocy których administratorzy przetwarzają dane osobowe, gwarantują odpowiednie bezpieczeństwo danych osobowych oraz szybkie i skuteczne rozwiązania służące prawidłowemu wywiązywaniu się z obowiązków określonych w art. 33 i 34 RODO.

O jakich naruszeniach trzeba powiadomić Prezesa UODO?

03.

W przypadku wykrycia przez administratora naruszenia ochrony danych osobowych konieczne jest, aby w pierwszej kolejności dokonana została analiza pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych. Jeżeli w wyniku przeprowadzonego badania okaże się, że nie ma prawdopodobieństwa wystąpienia ryzyka naruszenia praw i wolności osób fizycznych, administrator zwolniony jest z obowiązku powiadamiania organu nadzorczego o naruszeniu. Trzeba jednakże pamiętać, że organ nadzorczy będzie mógł zwrócić się do administratora o uzasadnienie decyzji o niezgłaszaniu naruszenia, w związku z tym wnioski z przeprowadzonej analizy należy odnotować w wewnętrznej ewidencji naruszeń.

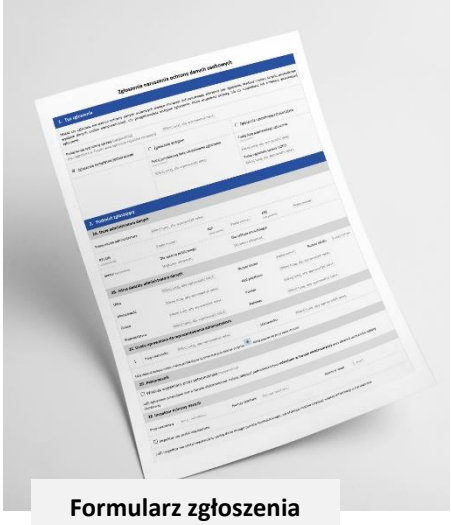
Z ryzykiem naruszenia praw lub wolności osób fizycznych mamy do czynienia wówczas, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np. dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, nadużycia finansowe, straty finansowe, nieuprawnione cofnięcie pseudonimizacji, utrata poufności danych osobowych chronionych tajemnicą zawodową, naruszenie dobrego imienia lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej. Jeżeli naruszenie dotyczy danych osobowych ujawniających pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub danych genetycznych, dotyczących zdrowia lub życia seksualnego, należy uznać, że występuje duże prawdopodobieństwo takiej szkody.

Więcej informacji na temat oceny ryzyka można znaleźć w dwuczęściowym poradniku Prezesa UODO, w którym odpowiedziano na pytania: Jak rozumieć podejście oparte na ryzyku według RODO? oraz Jak stosować podejście oparte na ryzyku?

W jaki sposób powiadomić Prezesa UODO o naruszeniu?

04.

Organem właściwym do zgłaszania naruszeń ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (Prezes UODO).



Formularz zgłoszenia

https://uodo.gov.pl/pl/134/233

Zgłoszenia można dokonać za pomocą formularza dostępnego na stronie uodo.gov.pl na 4 sposoby:

1. **Elektronicznie poprzez wypełnienie dedykowanego formularza dostępnego bezpośrednio na platformie biznes.gov.pl**
2. Elektronicznie poprzez wysłanie wypełnionego formularza na elektroniczną skrzynkę podawczą ePUAP: UODO/SkrytkaESP
3. Elektronicznie poprzez wysłanie wypełnionego formularza za pomocą pisma ogólnego dostępnego na platformie biznes.gov.pl,
4. Tradycyjną pocztą, wysyłając wypełniony formularz na adres Urzędu.

Jeżeli naruszenie dotyczy danych osób w różnych krajach UE, Prezes UODO może być, ale nie musi być wiodącym (czyli właściwym dla administratora lub podmiotu przetwarzającego) organem nadzorczym. W przypadku transgranicznego naruszenia ochrony danych administrator powinien dokonać analizy, czy wiodącym organem nadzorczym w odniesieniu do czynności przetwarzania, które zostały objęte naruszeniem jest Prezes UODO, czy też może inny europejski organ nadzorczy (więcej: Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego (WP 244 rew. 01).

05. Jakie informacje musi zawierać zgłoszenie naruszenia kierowane do Prezesa UODO?

Zgodnie z art. 33 ust. 3 RODO, administrator powinien wskazać w zgłoszeniu naruszenia następujące informacje:

- **opis charakteru naruszenia ochrony danych osobowych**, w tym w miarę możliwości wskazanie **kategorii i przybliżonej liczby osób**, których dane dotyczą, oraz **kategorii i przybliżonej liczby wpisów** danych osobowych, których dotyczy naruszenie;
- wskazanie **imienia i nazwiska oraz danych kontaktowych inspektora ochrony danych** lub **oznaczenia innego punktu kontaktowego**, od którego można uzyskać więcej informacji;
- **opis możliwych konsekwencji** naruszenia ochrony danych osobowych;
- wskazanie **środków, jakie zostały 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.**

Istotne jest, aby opis charakteru naruszenia był na tyle szczegółowy i jasny, aby organ nadzorczy mógł ocenić całość zdarzenia i podjąć skuteczne działania, takie jak np. skierowanie wystąpienia do administratora o zawiadomienie bądź ponowne prawidłowe zawiadomienie osób, których dane dotyczą (gdy administrator zrezygnował z zawiadomienia bądź dokonał zawiadomienia osób w sposób nieprawidłowy). Zbyt lakoniczna informacja nie spełnia tej funkcji, a tym samym nie pozwala organowi nadzorczemu na podjęcie szybkich i właściwych działań mających na celu ochronę praw i wolności osób fizycznych. Przede wszystkim należy pamiętać, aby poinformować organ nadzorczy o zastosowanych środkach zaradczych (np. czy stosowano metody szyfrowaniu w utraconym nośniku elektronicznym zawierającym dane osobowe, a jeśli tak, to jakie to były metody).

06. W jakim terminie należy zgłosić naruszenie Prezesowi UODO?

Zgodnie z art. 33 ust. 1 RODO, 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 RODO, **chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**.

To czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą.

Ponadto administrator musi zgłosić naruszenie nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Według Grupy Roboczej Art. 29, **administrator „stwierdza" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych.**

Należy pamiętać, że podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych zobowiązany jest do zgłoszenia go administratorowi (art. 33 ust. 2 RODO). Administrator, dokonując oceny ryzyka naruszenia praw lub wolności osób fizycznych, decyduje czy zgłosić takie naruszenie organowi nadzorczemu oraz powiadomić osoby, których dane dotyczą.

07. Czy dopuszczalne jest przekazywanie informacji o naruszeniu po upływie 72 godzin od stwierdzenia naruszenia?

Administratorzy nie zawsze będą dysponować wszystkimi wymaganymi informacjami dotyczącymi naruszenia w ciągu 72 godzin od jego stwierdzenia. W związku z tym, zgodnie z art. 33 ust. 4 RODO, **administrator może udzielać informacji sukcesywnie.** W takim przypadku administrator powinien przekazać brakujące informacje, jak tylko wejdzie w ich posiadanie. Zawiadamianie „sukcesywne" jest dopuszczalne, pod warunkiem że administrator poda organowi nadzorczemu przyczyny opóźnienia.

Grupa Robocza Art. 29 w Wytycznych dotyczących zgłaszania naruszeń (WP 250 rev. 01) również niejednokrotnie podkreśla, że np. brak dostępu do szczegółowych informacji (np. informacji o dokładnej liczbie osób, których dane dotyczą, na które naruszenie wywarło wpływ) nie powinien stanowić przeszkody dla terminowego zgłoszenia naruszenia. **Przepisy RODO dopuszczają możliwość wskazywania przybliżonej liczby osób fizycznych**, na które dane naruszenie wywarło wpływ, **oraz przybliżonej liczby wpisów danych osobowych**, których dotyczy to naruszenie.

08. Najczęściej popełniane błędy podczas zgłaszania naruszeń

Administrator danych jest zobowiązany do zgłaszania naruszeń ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych, gdy naruszenie stwarza prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych.

Najczęściej popełniane błędy przy zgłaszaniu naruszeń:

1. **Brak niektórych wymaganych w art. 33 ust. 3 RODO informacji (przekazane w zgłoszeniu informacje są niekompletne).**

Prawidłowo wypełnione zgłoszenie naruszenia ochrony danych powinno zawierać co najmniej:

- opis charakteru naruszenia ochrony danych osobowych - w tym w miarę możliwości wskazywanie kategorii i przybliżonej liczby osób, których dane dotyczą oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opisanie możliwych konsekwencji naruszenia ochrony danych osobowych;
- opisanie środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosowanych przypadkach środków w celu zminimalizowania ewentualnych negatywnych skutków naruszenia.

Przekazanie wszystkich wymaganych informacji ułatwia elektroniczny formularz, który nie jest obowiązkowy, lecz jego usystematyzowany układ pozwala administratorom na sporządzenie prawidłowego zgłoszenia, które zawiera wszystkie wymagane informacje.

Prawidłowo wypełnione zgłoszenie pozwoli organowi nadzorczemu ocenić skalę i charakter naruszenia i – w razie potrzeby - podjąć odpowiednie i szybkie działania naprawcze w związku z jego zaistnieniem. Jeżeli z jakichś względów administrator nie może skorzystać z formularza, powinien zawrzeć wszystkie informacje wskazane w art. 33 ust. 3 RODO w piśmie kierowanym do Prezesa UODO.

Zgłoszenie naruszenia powinno nastąpić w terminie do 72 godzin od jego stwierdzenia. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Gdy w chwili zgłaszania naruszenia administrator nie dysponuje wszystkimi wymaganymi informacjami, to w terminie 72 godzin od wykrycia naruszenia powinien przekazać organowi nadzorczemu te informacje, które na temat naruszenia posiada. Jeśli zgłoszenie następuje na formularzu, należy zaznaczyć pole „Zgłoszenie wstępne" w pkt 1 formularza. W takim przypadku, zgodnie z art. 33 ust. 4 RODO, administrator powinien przekazać brakujące informacje po ich uzyskaniu, bez zbędnej zwłoki.

2. **Niedokładne wypełnianie zgłoszeń (informacje przekazywane w zgłoszeniu są lakoniczne i nierzetelne).**

Brak rzetelnego opisu (np. wpisanie jedynie sformułowania „zagubiono dokument") **rodzi konieczność podejmowania** przez organ **dodatkowych czynności** w celu ustalenia np. rodzaju dokumentu i zakresu danych, jaki on zawiera. Po skontaktowaniu się z inspektorem ochrony danych lub innym wskazanym przez administratora punktem kontaktowym w tej sprawie okazuje się, że dany dokument był np. oryginałem umowy zawierającym podstawowe dane identyfikacyjne wraz z numerem PESEL, adresem zamieszkania, numerem dokumentu tożsamości oraz szczegółowymi informacjami finansowymi wskazującymi na status materialny danej osoby fizycznej. „Charakter naruszenia" powinien więc zawierać szczegółowy opis stanu faktycznego oraz okoliczności naruszenia.

Nierzetelne, zdawkowe przekazywanie informacji uniemożliwia ocenę prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych. Jednym z najważniejszych celów zgłaszania naruszeń ochrony danych jest ograniczenie szkód dla osób fizycznych. Uzyskanie przez organ nadzorczy pełnych, wymaganych w art. 33 ust. 3 RODO informacji o określonym naruszeniu, pozwala mu na właściwą ocenę naruszenia i odpowiednią reakcję polegającą np. na zażądaniu od administratora powiadomienia osób,

których dane dotyczą, w sytuacji, gdy jest to konieczne, a administrator nie uczynił tego z własnej inicjatywy. Brak odpowiedniej i szybkiej reakcji na naruszenia ochrony danych osobowych zwiększa ryzyko urzeczywistnienia się związanych z nimi szkód.

W przypadku braku w zgłoszeniu wymaganych informacji, konieczne jest wezwanie administratora do ich uzupełnienia. Brak reakcji administratora na takie wezwanie może skutkować nałożeniem administracyjnej kary pieniężnej zgodnie z art. 83 ust. 5 lit. e RODO.

3. Wypełnianie zgłoszeń w sposób rutynowy, prowadzący do błędów.

W przypadku administratorów kierujących do urzędu znaczne ilości zgłoszeń, zauważalna jest tendencja do niedbałego i szablonowego sposobu wypełniania formularza zgłoszenia naruszenia. To powoduje, że w zgłoszeniach od tych administratorów często obecne są błędy wynikające z automatycznego przenoszenia informacji dotyczących innych zdarzeń, np. wcześniej zgłoszonych naruszeń. Takie błędne, nieścisłe przekazywanie informacji powoduje konieczność prowadzenia z administratorem dalszej korespondencji lub innej formy kontaktu, a tym samym ponoszenia niepotrzebnych nakładów czasu i pracy zarówno po stronie administratora, jak i organu nadzorczego.

4. Zgłaszanie naruszeń ochrony danych osobowych przez podmiot przetwarzający bądź inny podmiot nie będący administratorem zobowiązanym do zgłoszenia naruszenia.

Podmiot przetwarzający nie zgłasza naruszeń ochrony danych osobowych organowi nadzorczemu. Obowiązek ten ciąży na administratorze. Zgodnie z art. 33 ust. 2 RODO podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. Również art. 28 ust. 3 lit. f RODO zobowiązuje podmiot przetwarzający do pomagania administratorowi w wywiązaniu się z obowiązków określonych w art. 33 RODO (np. poprzez udzielenie dostępnych mu w danej sprawie informacji). Na podstawie zgromadzonych informacji administrator stwierdza naruszenie ochrony danych i podejmuje decyzję o właściwym zaklasyfikowaniu naruszenia w zależności od poziomu ryzyka dla praw lub wolności osób, których dane dotyczą, a tym samym o konieczności zgłoszenia naruszenia Prezesowi UODO oraz zawiadomienia osób, których dane dotyczą.

Naruszenia nie zgłasza również podmiot, który np. w wyniku pomyłki otrzymał od innego podmiotu korespondencję z danymi osobowymi nie kierowaną do niego. W takim przypadku należy niezwłocznie powiadomić ten podmiot o zaistniałym zdarzeniu, który to, będąc administratorem, jest zobowiązany dokonać analizy i podjąć decyzję o ewentualnym zgłoszeniu naruszenia Prezesowi UODO.

09. Jak oceniać ryzyko naruszenia praw lub wolności osób fizycznych na wypadek stwierdzenia naruszenia?

9.1 Wprowadzenie

Uzyskanie informacji przez administratora o zaistnieniu incydentu mającego znaczenie dla ochrony danych osobowych, obliguje go do dokonania rzeczowej analizy w celu **stwierdzenia czy doszło do naruszenia ochrony danych osobowych**, w rozumieniu art. 4 pkt 12 RODO. Według Grupy Roboczej Art. 29 w Wytycznych dotyczących zgłaszania naruszeń (WP 250 rev. 01) **administrator „stwierdza" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych**.

Konsekwencją stwierdzenia naruszenia jest konieczność przeprowadzenia analizy pod kątem ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Analiza ta pozwoli stwierdzić, czy należy wypełnić obowiązek z art. 33 ust. 1 RODO (tj. zgłosić naruszenie organowi nadzorczemu) oraz art. 34 ust. 1 RODO (tj. zawiadomić osoby, których dane dotyczą o naruszeniu).

Uwaga!

Wprowadzenie procedur umożliwiających stwierdzanie i ocenę naruszeń pod kątem wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych jest obowiązkiem administratora niezależnie od zaistnienia naruszenia ochrony danych osobowych.

Podczas oceny ryzyka naruszenia praw lub wolności osób fizycznych powstałego w wyniku wystąpienia naruszenia, kładzie się nacisk na inne kwestie, niż uwzględniane w ocenie skutków dla ochrony danych. W ocenie skutków dla ochrony danych bierze się pod uwagę zarówno ryzyko dla planowego przetwarzania danych, jak i ryzyko powstałe w przypadku wystąpienia naruszenia. **Badając możliwe naruszenie**, **rozpatruje się** w ujęciu ogólnym **prawdopodobieństwo jego wystąpienia oraz szkody dla osób, których dane dotyczą**, jakie mogą z niego wyniknąć. Innymi słowy, jest to ocena wydarzenia hipotetycznego. W przypadku faktycznego naruszenia zdarzenie już nastąpiło, więc nacisk kładzie się w całości na powstałe ryzyko, że naruszenie będzie skutkowało wpływem na osoby fizyczne.

Zgodnie z motywem 76 RODO, mówiąc o ocenie ryzyka naruszenia praw i wolności osób fizycznych konieczne jest uwzględnienie:

- **powagi** tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą oraz
- **prawdopodobieństwa** wystąpienia tego zdarzenia będącego skutkiem naruszenia.

Urzeczywistnienie się określonego zagrożenia może nie spowodować skutków dla praw lub wolności osób, których dane są przetwarzane, spowodować znikome skutki lub skutki katastrofalne. W skrajnych

przypadkach, np. w systemach przetwarzania informacji medycznej, nieuprawniona modyfikacja danych lub niedostępność danych w wyniku złego ich zabezpieczenia może skutkować utratą zdrowia, a nawet życia. Dlatego **oceniając ryzyko naruszenia praw i wolności** osób, których dane dotyczą, **osoby odpowiedzialne za przeprowadzenie tego procesu powinny przyjąć perspektywę osób, których dane są przetwarzane i właśnie z tej perspektywy oceniać stopień dotkliwości w przypadku zmaterializowania się zagrożenia.**

Nie jest konieczne, aby ryzyko się zmaterializowało (by faktycznie doszło do naruszenia praw lub wolności). Administrator, który ocenił wielkość potencjalnej szkody, które naruszenie może spowodować, biorąc pod uwagę kontekst i okoliczności całego zdarzenia, powinien ocenić prawdopodobieństwo jego zaistnienia.

Przykład

*Pracownik administratora porzucił dokumenty kadrowe i finansowe (zawierające m.in. takie dane, jak: imię, nazwisko, PESEL, adres zamieszkania, informacje o wynagrodzeniach) w kontenerze na odpady. Administrator **stwierdził,** że doszło do naruszenia ochrony danych.*
Jednak z uwagi na:
- krótki okres jaki upłynął od zaistnienia do stwierdzenia naruszenia,
- zamknięty teren zakładu pracy,
- monitoring kontenerów na odpady,
- podjęte natychmiastowo działania zaradcze,
*mimo powagi tego zdarzenia, a w szczególności zakresu i kategorii danych, **prawdopodobieństwo** zmaterializowania się szkody dla osób, których te dane dotyczą (np. posłużenia się danymi w celu wyłudzenia ubezpieczenia) **ocenił jako niskie.***

Jeżeli w wyniku przeprowadzonego badania okaże się, że nie ma ryzyka naruszenia praw lub wolności osób fizycznych, administrator zwolniony jest z obowiązku powiadamiania organu nadzorczego o naruszeniu. Należy jednakże pamiętać, że organ nadzorczy będzie mógł zwrócić się do administratora o uzasadnienie decyzji o niezgłaszaniu naruszenia, w związku z tym wnioski z przeprowadzonej analizy należy odnotować w wewnętrznej ewidencji naruszeń.

Przykłady naruszeń, w których nie wystąpiło ryzyko naruszenia praw lub wolności osób fizycznych (brak obowiązku zawiadomienia Prezesa UODO o naruszeniu):

Przykład I

Pracownik kancelarii przez pomyłkę wynosi poza jej obszar teczkę z niezabezpieczonymi danymi osobowymi, wśród których znajdują się również szczególne kategorie danych osobowych. Po chwili orientuje się, że nastąpiła pomyłka i wraca do kancelarii zwracając teczkę. Działanie takie naruszyło zasady ochrony danych, ale nie mogło skutkować naruszeniem praw lub wolności osób fizycznych, gdyż dane nie zostały udostępnione.

Przykład II

Administrator traci bezpiecznie zaszyfrowany pendrive (zgodnie z aktualnym stanem wiedzy technicznej). Klucz szyfrowania pozostaje w posiadaniu administratora i nie jest to jedyna kopia danych osobowych. W takiej sytuacji dane pozostają niedostępne dla złodzieja. Oznacza to małe prawdopodobieństwo, by naruszenie stanowiło zagrożenie dla praw lub wolności osób, których dane dotyczą.

Do każdej sytuacji należy jednak podchodzić z dużą rozwagą i ostrożnością. Zmiana choćby jednego z kluczowych elementów zdarzenia może bowiem doprowadzić do odmiennych wniosków, np. jeżeli w przypadku opisanym w przykładzie II po czasie okaże się, że naruszono bezpieczeństwo klucza lub, że oprogramowanie narażone jest na ataki, wówczas zmieni się ryzyko naruszenia praw i wolności osób, a w związku z tym może powstać obowiązek zgłoszenia naruszenia Prezesowi UODO. Podobna sytuacja może

się zdarzyć, gdy w sytuacji zaistnienia naruszenia administrator nie będzie dysponował kopią zapasową danych osobowych. W takim przypadku będziemy mieli do czynienia z naruszeniem dostępności, stanowiącym ryzyko dla praw i wolności osób fizycznych i w związku z tym sytuacja ta będzie wymagała zgłoszenia naruszenia organowi nadzorczemu.

Uwaga!

W przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna.

Ryzyko naruszenia praw lub wolności osób fizycznych powstaje, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialną szkodą dla osób fizycznych, których dane naruszono. Szkodami takimi są np.:

- dyskryminacja,
- kradzież tożsamości lub oszustwo dotyczące tożsamości,
- nadużycia finansowe,
- straty finansowe,
- nieuprawnione cofnięcie pseudonimizacji,
- utrata poufności danych osobowych chronionych tajemnicą zawodową,
- naruszenie dobrego imienia
- lub inne znaczące skutki gospodarcze lub społeczne dla danej osoby fizycznej.

Jeżeli naruszenie dotyczy danych osobowych ujawniających:

- pochodzenie etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,
- dane genetyczne,
- dane dotyczące zdrowia,
- dane dotyczące życia seksualnego,

należy uznać, że występuje duże prawdopodobieństwo takiej szkody. **Niemniej jednak każde z takich zdarzeń należy rozpatrywać indywidualnie.**

9.2 Kryteria oceny ryzyka dla osób fizycznych będącego wynikiem naruszenia

A. Kryteria zalecane przez Grupę Roboczą Art. 29 (więcej: wytyczne WP250, s. 27).

- ☑ Rodzaj naruszenia (np. naruszenie dostępności danych medycznych może nieść za sobą poważniejsze skutki niż naruszenie ich poufności).
- ☑ Charakter, wrażliwość i ilość danych osobowych (np. ujawnienie imienia i nazwiska oraz adresu danej osoby prawdopodobnie nie wyrządzi jej szkody w normalnej sytuacji. Jednak jeżeli imię i nazwisko oraz adres rodzica adopcyjnego zostaną ujawnione rodzicowi biologicznemu, może mieć to bardzo poważne konsekwencje zarówno dla rodzica adopcyjnego, jak i dziecka).

- ☑ Łatwość identyfikacji osób fizycznych (np. dane osobowe chronione za pomocą odpowiedniego poziomu szyfrowania będą nieczytelne dla osób nieupoważnionych, które nie posiadają klucza deszyfrującego).
- ☑ Waga konsekwencji dla osób fizycznych (fakt, że przypadkowy odbiorca jest zaufany, np. bank, może spowodować, że skutki naruszenia nie będą poważne, nie oznacza, że naruszenie nie miało miejsca; należy również zwrócić uwagę na to, jak trwałe są konsekwencje dla osób fizycznych, gdyż wpływ może być postrzegany jako poważniejszy, jeżeli dotyczy dłuższego okresu).
- ☑ Cechy szczególne danej osoby fizycznej (np. stres wywołany z pozoru nieistotnym naruszeniem może wpłynąć na stan zdrowia osoby w podeszłym wieku; ujawnienie danych osobowych dzieci może narazić ich bliskich na wyłudzenie środków finansowych - tzw. metoda „na wnuczka").
- ☑ Cechy szczególne administratora danych (w przypadku naruszenia danych medycznych, osoby fizyczne są narażone na większe zagrożenie).
- ☑ Liczba osób fizycznych, na które naruszenie wywiera wpływ (należy jednak pamiętać, że charakter zdarzenia może mieć poważne konsekwencje nawet dla jednej osoby).

B. Kryteria z art. 3 ust. 2 rozporządzenia KE nr 611/2013

W art. 3 ust. 2 rozporządzenia nr 611/2013 przedstawiono wytyczne dotyczące czynników, które należy wziąć pod uwagę w związku ze zgłaszaniem naruszeń w sektorze usług łączności elektronicznej – Grupa Robocza Art. 29 wskazuje, że mogą one okazać się przydatne w kontekście dokonywania zgłoszeń zgodnie z RODO:

- ☑ Charakter i treść danych osobowych (np. dane związane z informacjami finansowymi, szczególne kategorie danych, dane dotyczące poczty elektronicznej, dane dotyczące lokalizacji, historie przeglądania stron internetowych czy wykaz wykonanych usług telekomunikacyjnych).
- ☑ Prawdopodobne konsekwencje naruszenia danych osobowych (np. kradzież lub sfałszowanie tożsamości, uszczerbek fizyczny, psychiczny, upokorzenie lub naruszenie dobrego imienia).
- ☑ Okoliczności w jakich doszło do naruszenia (np. gdzie skradziono dane oraz kiedy dostawca dowiedział się, że dane są w posiadaniu nieupoważnionej strony trzeciej).

C. Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych (metodologia ENISA)

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) we współpracy z organami ochrony danych Grecji i Niemiec, w 2013 r. opracowała metodologię oceny stopnia naruszenia ochrony danych (dostępna na stronie ENISA.europa.eu), w której zaproponowano trzy główne kryteria:

- ☑ (KPD) Kontekst przetwarzania danych,
- ☑ (ŁI) Łatwość identyfikacji osoby, które dane dotyczą,
- ☑ (ON) Okoliczności naruszenia, mające dodatkowy wpływ na powagę (dotkliwość) naruszenia.

Końcowy wynik oceny dotkliwości naruszenia (DN), po uwzględnieniu przyjętych wartości punktowych dla poszczególnych kryteriów (przykładowo wskazano je w omawianym dokumencie) można uzyskać korzystając z następującego wzoru: DN = KPD x ŁI x ON.

Uzyskany wynik pozwala określić poziom dotkliwości naruszenia ochrony danych dla osób, których dane dotyczą (w omawianym dokumencie przyjęto 5-stopniową skalę: niskie, średnie, wysokie, bardzo wysokie).

9.3 Praktyka organu nadzorczego

Według części administratorów zgłaszających naruszenia Prezesowi UODO, wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą nie występuje, np. w przypadku zagubienia bądź wręczenia niewłaściwej osobie dokumentacji zawierającej imię i nazwisko oraz nr PESEL. W większości takich sytuacji organ nadzorczy uznaje jednak, że tego typu naruszenie powoduje takie wysokie ryzyko. W takich przypadkach dane mogą być wykorzystane w sposób nieuprawniony np. w celu:

- uzyskania przez osoby trzecie kredytów w instytucjach pozabankowych, na szkodę osoby, której dane dotyczą;
- uzyskania dostępu do danych o stanie zdrowia osoby, której dane dotyczą w przypadku przełamania zabezpieczeń do systemu świadczeń opieki zdrowotnej lub korzystania ze świadczeń opieki zdrowotnej przysługujących tej osobie;
- korzystania z praw obywatelskich osoby, której dane naruszono, np. wykorzystania danych do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego;
- zarejestrowania przedpłaconej karty telefonicznej (pre-paid), która może posłużyć do celów przestępczych[2];
- wyłudzenia ubezpieczenia lub środków z ubezpieczenia;
- zawarcia umów cywilno-prawnych, np. najmu nieruchomości;
- posłużenia się fałszywymi danymi, np. przy otrzymywaniu mandatu.

Jak wskazuje Grupa Robocza Art. 29 w swoich wytycznych, **to, czy administrator wie, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje, może mieć znaczenie dla poziomu potencjalnego ryzyka.** Nie budzi więc żadnych wątpliwości, że np. naruszenie poufności danych będące wynikiem kradzieży dokumentów wiąże się z wysokim ryzykiem dla osób, których dane dotyczą. W każdym przypadku, rozpatrując zgłoszone naruszenie, organ nadzorczy przyjmuje perspektywę osób, których dane dotyczą i właśnie z tej perspektywy ocenia stopień dotkliwości w przypadku zmaterializowania się zagrożenia. W ocenie Prezesa UODO, sytuacja, w której wspomniana w przykładzie korespondencja (zawierająca przynajmniej takie kategorie danych, jak imię, nazwisko i numer PESEL) jest dostarczana osobie znanej bądź nieznanej administratorowi, co do zasady wiąże się z wysokim ryzykiem dla osób, których dane dotyczą. Można przyjąć inne prawdopodobieństwo w sytuacji dostarczenia omyłkowej korespondencji osobie znanej administratorowi (np. innemu klientowi administratora, który poinformował o pomyłce bądź oświadczył, że nie wykorzystał przekazanych omyłkowo informacji do celów prywatnych i/lub niezgodnych z prawem), nie daje to jednak żadnej gwarancji, że intencje takiej osoby obecnie bądź

[2] Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych wprowadziła dla użytkowników wymóg rejestracji prepaidowych kart SIM do 1 lutego 2017 r. Na podstawie przepisów tej ustawy, w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, wprowadzono regulacje zobowiązujące abonentów do podania dostawcy usług telekomunikacyjnych danych umożliwiających ich identyfikację. Zgodnie z Art. 60b ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2018 r. poz. 1954 z późn. zm.) do rejestracji karty wystarczy wskazać imię i nazwisko oraz numer i serię paszportu (nazwę, serię i numer dokumentu potwierdzającego tożsamość).

w przyszłości nie zmienią się, a ewentualne konsekwencje posłużenia się takimi kategoriami danych mogą być znaczące.

Jednym z największych zagrożeń nieuprawnionego wykorzystywania numeru PESEL wraz z imieniem i nazwiskiem jest możliwość łatwego uzyskania dowodu kolekcjonerskiego. Dowód taki trudno na pierwszy rzut oka odróżnić od dowodu będącego autentycznym dokumentem tożsamości i umożliwia on szybkie wyrządzenie szkód i krzywd osobie, której dane dotyczą. Dowód kolekcjonerski może zostać wykorzystany np. do przejęcia karty SIM, co z kolei może poskutkować uzyskaniem dostępu do konta bankowego bądź innych usług powiązanych z numerem (poczta e-mail, serwisy społecznościowe - odzyskiwanie haseł do kont bardzo często opiera się na kodach/hasłach przesyłanych na numer telefonu komórkowego). Za pomocą dowodu kolekcjonerskiego można wyłudzić kredyt bądź sprzedać czyjąś nieruchomość.

Mając świadomość zagrożeń, jakie niesie ze sobą posługiwanie się numerem PESEL wraz z imieniem i nazwiskiem, oraz w związku z tym, że art. 87 RODO upoważnia państwa członkowskie do określenia szczególnych warunków przetwarzania krajowego numeru identyfikacyjnego, jakim w Polsce jest numer PESEL, Prezes UODO podejmuje działania mające na celu ograniczenie dostępu do nr PESEL np. osób pełniących funkcje w organach osób prawnych ujawnionych w rejestrach publicznych (KRS).

Podejście oparte na takiej ocenie należy więc odzwierciedlać w przyjmowanej przez administratora metodologii oceny ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) w swoich zaleceniach dotyczących metod oceny wagi naruszeń wskazuje, że metodologia opiera się na możliwie obiektywnym podejściu, a jednocześnie jest na tyle elastycznym rozwiązaniem, że może zostać z powodzeniem przyjęta przez administratora, dostosowując ją do krajowego systemu prawnego i innych czynników. ENISA wskazuje również, że punktacja kryteriów zaproponowana w tej metodologii powinna być tak dobrana, by pozwalała uzyskać najbardziej odpowiednie wyniki. A zatem musi uwzględniać aktualne, mogące wystąpić w określonych sytuacjach zagrożenia. Jednym z kryteriów proponowanych przez agencję jest okoliczność naruszenia, w którym zła intencja jest jednym z czynników decydujących o przyjętej punktacji. Administratorzy w zgłoszeniach naruszeń przekazywanych do UODO wskazują na tę metodologię i niesłusznie, w ocenie organu, wbrew wyżej wskazanym zagrożeniom, zaniżają to kryterium. Powołują się przy tym na brak złych intencji, co skutkuje uzyskaniem wyniku wskazującego na średnie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, a w konsekwencji brak obowiązku powiadomienia osób o naruszeniu zgodnie z art. 34 ust. 1 RODO.

Jakie naruszenia należy wpisywać do wewnętrznej ewidencji? 10.

Art. 33 ust. 5 RODO nakłada na administratorów obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, czyli prowadzenia wewnętrznej ewidencji naruszeń. Użyte w ww. artykule sformułowanie „wszelkich naruszeń” oznacza, że ewidencja powinna obejmować wszystkie naruszenia spełniające kryteria określone w definicji zawartej w art. 4 pkt 12 RODO. W ewidencji powinny zatem znaleźć

się zarówno naruszenia ochrony danych osobowych podlegające obowiązkowi notyfikacyjnemu Prezesowi UODO, jak i te, które nie podlegają zgłoszeniu organowi nadzorczemu ze względu na to, że mało prawdopodobne jest, by skutkowały one ryzykiem naruszenia praw lub wolności osób fizycznych.

Zgodnie z wymaganiami art. 33 ust. 5 RODO administrator musi rejestrować informacje o naruszeniu obejmujące okoliczności naruszenia ochrony danych osobowych, przebieg i naruszone dane osobowe. Ewidencja powinna obejmować ponadto skutki i konsekwencje naruszenia oraz działania naprawcze podjęte przez administratora.

Prowadzenie ewidencji łączy się z zasadą rozliczalności przewidzianą w art. 5 ust. 2 RODO oraz obowiązkami administratora wynikającymi z art. 24 RODO. Jak wskazuje art. 33 ust. 5 (zdanie 2) RODO organ nadzorczy może zażądać dostępu do dokumentacji (ewidencji) naruszeń i dokumentacja ta powinna pozwolić organowi na weryfikowanie przestrzegania RODO w zakresie tych obowiązków.

Grupa Robocza Art. 29 podkreśla również, że w przypadku podjęcia decyzji o niezgłoszeniu naruszenia, wskazane jest udokumentowanie takiego faktu w ewidencji wraz z podaniem przyczyny, dla której administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne.

Jeżeli chodzi o sposób prowadzenia ewidencji, Grupa Robocza Art. 29 podkreśla, że administrator może zdecydować o dokumentowaniu naruszeń w rejestrze czynności przetwarzania prowadzonym zgodnie z art. 30 RODO. Nie ma wymogu prowadzenia osobnego rejestru naruszeń, jeżeli informacje dotyczące naruszenia można łatwo zidentyfikować i przedłożyć na żądanie.

Brak udokumentowania naruszenia we właściwy sposób może prowadzić do wykonania przez organ nadzorczy uprawnień na mocy art. 58 RODO lub nałożenia administracyjnej kary pieniężnej zgodnie z art. 83 RODO.

11. Jakie działania należy podejmować w celu ograniczenia występowania najczęstszych typów naruszeń ochrony danych osobowych?

1. **Naruszenia polegające na udostępnieniu danych osobowych nieuprawnionym osobom w związku z wysyłaniem poczty elektronicznej.**

W przypadku wysyłania korespondencji do większej liczby osób, należy dbać o to, aby adresy mailowe osób, do których korespondencja jest kierowana, nie były udostępniane wszystkim pozostałym adresatom wiadomości (chyba że takie działanie jest celowe i uzasadnione). Innymi słowy, osoba do której skierowana jest korespondencja, co do zasady nie powinna mieć możliwości zapoznania się z danymi pozostałych adresatów wiadomości. Przy wysyłce jednej wiadomości e-mail do wielu adresatów istnieją proste środki, które pozwalają na ukrycie innych adresatów poprzez zastosowanie tzw. pola UDW (tj. „ukryte do wiadomości", ang. BCC).

Częstymi naruszeniami są też przypadki przesłania danych osobowych do niewłaściwego odbiorcy, tj. na niewłaściwy adres e-mail/adres do korespondencji, na skutek omyłki pracownika. Pomyłka pracownika polega zazwyczaj na użyciu adresu e-mail podobnego w treści do właściwego, bądź jest konsekwencją wprowadzenia do systemu informatycznego niewłaściwych danych (np. wprowadzenie na koncie klienta adresu e-mail/adresu korespondencyjnego innego klienta). Żeby przeciwdziałać takim sytuacjom, należy pouczyć osoby odpowiedzialne za wysyłkę korespondencji, a także osoby wprowadzające dane do systemów informatycznych o konieczności weryfikacji danych dotyczących adresu e-mail/adresu do korespondencji po ich wprowadzeniu bądź wdrożyć odpowiednie rozwiązania techniczne umożliwiające taką weryfikację.

2. Naruszenia polegające na zagubieniu lub kradzieży niezabezpieczonych (niezaszyfrowanych) urządzeń informatycznych z danymi osobowymi (smartfony, komputery przenośne).

Sam fakt utraty danych osobowych w wyniku zagubienia czy kradzieży urządzeń lub nośników nie musi prowadzić do naruszenia praw i wolności osób, których dane dotyczą, jeżeli administrator zastosował skuteczne, adekwatne środki zabezpieczenia.

Takimi środkami mogą być zgodne z aktualnym stanem wiedzy technicznej metody szyfrowania pamięci urządzeń/plików z danymi osobowymi bądź automatyczne wylogowanie użytkownika ze zdalnych zasobów, z których korzysta (np. skrzynek pocztowych po zakończeniu pracy w programie pocztowym, przeglądarce internetowej).

3. Naruszenia polegające na udostępnieniu dokumentacji medycznej osobie nieuprawnionej.

W działalności podmiotów odpowiedzialnych za przechowywanie i udostępnianie dokumentacji medycznej, ważną rolę odgrywają skuteczne i prawidłowe procedury weryfikacji osób zgłaszających się z wnioskiem o dostęp do takiej dokumentacji. Weryfikacji tej należy dokonywać według szczegółowo określonych procedur opracowanych na podstawie szczególnych przepisów prawa (m.in. ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta oraz aktów wykonawczych dotyczących dokumentacji medycznej). Ważna jest również bieżąca weryfikacja aktualności udzielonych upoważnień do dostępu do dokumentacji lub informacji o stanie zdrowia. Ponieważ upoważnienia mogą być w każdej chwili odwoływane, istotna jest stała kontrola ich ważności.

Podmioty lecznicze powinny zapewnić procedury adresowania przesyłek pocztowych zawierających dane medyczne oraz przeszkolić osoby zajmujące się ich przygotowaniem. Ze zgłoszeń naruszeń ochrony danych osobowych wpływających do UODO wynika, że nader często dochodzi do omyłkowego przesłania dokumentów do innego adresata. Z kolei lekarze przy korzystaniu z systemów służących do odnotowywania wizyt pacjentów i sporządzania z nich wydruków powinni zwracać baczną uwagę, czy edytują dane właściwego pacjenta oraz czy przekazują mu właściwy wydruk z dokumentacji (zasada prawidłowości danych).

4. Naruszenia polegające na zablokowaniu dostępu do danych przez złośliwe oprogramowanie (ransomware).

a) Czym jest ransomware i jak mu zapobiegać?

Ransomware to rodzaj złośliwego oprogramowania, które szyfruje dane, uniemożliwiając do nich dostęp, oferując następnie klucz deszyfrujący za opłatą (najczęściej za pomocą kryptowaluty). Z uwagi na charakter usług świadczonych przez wielu administratorów, np. ochrona zdrowia, ważne jest, aby w przypadku wystąpienia incydentu (naruszenia dostępności danych) podmioty miały możliwość dalszego

świadczenia usług osobom, których dane dotyczą. W tym celu **należy posiadać kopie zapasowe danych osobowych odseparowane od środowiska, które może być celem ataku** przez złośliwe oprogramowanie, uniemożliwiając w ten sposób bezpowrotne zaszyfrowanie również tych danych. Ponadto należy:

- używać sprawdzonego oprogramowania antywirusowego oraz oprogramowania kontrolującego dostęp do zasobów z zewnątrz (firewall),
- ustawiać odpowiednio silne hasła a tam gdzie usługa dostępna z zewnątrz jest zbędna, wyłączać ją (np. usługi zdalnego pulpitu – tzw. RDP),
- aktualizować na bieżąco swoje oprogramowanie,
- uświadamiać użytkowników i wprowadzać politykę użytkowania nieznanych nośników zewnętrznych oraz zachowania wzmożonej czujności przy otwieraniu załączników poczty elektronicznej (zwracając szczególną uwagę na pliki z takimi rozszerzeniami jak „exe", „vbs" czy „scr"). Zwracać szczególną uwagę na wiadomości poczty elektronicznej informujące o otrzymaniu faktury czy wyglądające jak powiadomienie z banku, sklepu bądź instytucji publicznej (plik bądź link może zawierać złośliwe oprogramowanie).

b) Co zrobić, jeśli dane zostały zaszyfrowane?

1. W przypadku stwierdzenia działania podejrzanego lub nieznanego procesu natychmiast należy odłączyć urządzenie od sieci, uniemożliwiając w ten sposób potencjalne rozprzestrzenianie się złośliwego oprogramowania.
2. **Nie płacić okupu, jeśli go zażądano.** Wysyłając pieniądze cyberprzestępcom, potwierdza się, że ich oprogramowanie działa. Nie ma żadnej gwarancji, że uzyska się klucz deszyfrujący, potrzebny do odzyskania plików.
3. **Podjąć niezbędne działania w celu przywrócenia kopii zapasowej.**
4. Gromadzić wszelkie informacje na temat incydentu. W przypadku zgłoszenia takiego naruszenia organowi nadzorczemu, Prezes UODO w piśmie do administratora może np. wezwać do wskazania:
   - w jaki sposób stwierdzono brak naruszenia poufności danych (dane nie zostały pobrane przez osobę nieupoważnioną, a jedynie zaszyfrowane w sposób uniemożliwiający uzyskanie do nich dostępu),
   - czy i w jakiej formie oprogramowanie szyfrujące poinformowało o konieczności uiszczenia opłaty w celu odzyskania dostępu do danych (wskazując nazwę złośliwego oprogramowania, sposób poinformowania, żądaną kwotę, kanał komunikacji, sposób zapłaty oraz termin),
   - czy administrator był w posiadaniu kopii zapasowej, a jeśli tak, to w jakim czasie ją przywrócił.

   Co ważne, nie każda czasowa bądź trwała niedostępność do danych jest naruszeniem ochrony danych osobowych. Jest nią tylko taka niedostępność danych, która może stanowić ryzyko dla praw lub wolności osób fizycznych.
5. Zawiadomić organy ścigania o popełnieniu przestępstwa (zaszyfrowanie danych przez ransomware może być przestępstwem z art. 268a Kodeksu karnego oraz w przypadku żądania okupu za odszyfrowanie – z art. 287 Kodeksu karnego).
6. Prezes UODO zachęca do zgłaszania takich zdarzeń również do CERT Polska pod adresem https://incydent.cert.pl/. O fakcie zgłoszenia takiego incydentu do CERT Polska warto poinformować Prezesa UODO, podając datę zgłoszenia oraz jego numer (np. w zgłoszeniu uzupełniającym).

c) Czy mogę odzyskać zaszyfrowane dane bez opłacania okupu?

Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji we współpracy z Europolem oraz organami ścigania z innych państw na stronie https://www.nomoreransom.org/ udostępnia darmowe

narzędzia deszyfrujące, które mogą okazać się pomocne w przypadku niektórych infekcji. Znając nazwę złośliwego oprogramowania, postępując zgodnie ze wskazówkami dołączonymi do narzędzia, można odzyskać zaszyfrowane dane.

Więcej informacji na ten temat i wskazówek dotyczących ransomware znajduje się na stronie https://www.nomoreransom.org/.

5. **Naruszenia polegające na zagubieniu przez pracowników dokumentów zawierających dane osobowe klientów.**

Wiele zgłoszeń kierowanych do Prezesa UODO dotyczy przypadków zagubienia przez pracowników dokumentów zawierających dane osobowe klientów. Dotyczy to w szczególności tych pracowników, których praca polega na kontaktach z klientem w miejscu jego zamieszkania (np. agentów ubezpieczeniowych, doradców finansowych). W celu eliminowania naruszeń tego typu należy przy wyjazdach do klientów ograniczyć ilość przewożonej dokumentacji do niezbędnego minimum (nie zabierać danego dnia dokumentacji klientów, z którymi nie jest na ten dzień umówione spotkanie) albo tam gdzie jest to możliwe przewozić dokumentację w formie elektronicznej (na zaszyfrowanych urządzeniach informatycznych).

6. **Naruszenia polegające na nieprawidłowej wysyłce dokumentów oraz anonimizacji danych osobowych w związku z udostępnianiem informacji publicznej.**

W przypadku podmiotów sektora publicznego, oprócz omyłkowego wysyłania dokumentacji do innego odbiorcy, zdarzają się również sytuacje nieprawidłowej anonimizacji danych. Sytuacje te występowały w przypadku udostępniania danych w trybie dostępu do informacji publicznej, w tym w Biuletynie Informacji Publicznej. Remedium na taki stan rzeczy powinny być regularne szkolenia pracowników z zakresu ochrony danych, w tym bezpieczeństwa danych, wprowadzenie szczegółowych instrukcji postępowania z dokumentami zawierającymi dane osobowe, w tym sposobów anonimizacji danych oraz wzmocnienie kontroli nad procesem wysyłki korespondencji (tradycyjnej i e-mail).

12. Kiedy i w jakim celu trzeba zawiadamiać o naruszeniu osoby, których dane dotyczą?

12.1 Kiedy należy dokonać zawiadomienia?

Zgodnie z art. 34 pkt 1 RODO „Jeżeli **naruszenie** ochrony danych osobowych **może powodować wysokie ryzyko naruszenia praw lub wolności**[3] osób fizycznych, administrator **bez zbędnej zwłoki** zawiadamia osobę, której dane dotyczą, o takim naruszeniu”.

[3] Jak oceniać ryzyko naruszenia praw lub wolności osób fizycznych na wypadek stwierdzenia naruszenia – rozdział 8.

Do takich przypadków należą sytuacje, w których naruszenie prowadzi do dyskryminacji, kradzieży tożsamości, oszustwa, straty finansowej lub uszczerbku na reputacji. Jeżeli naruszenie dotyczy danych wrażliwych, można założyć, że jest prawdopodobne, iż takie naruszenie może prowadzić do wskazanych wyżej szkód. Nie jest konieczne, aby wysokie ryzyko zmaterializowało się, czyli faktycznie doszło do naruszenia praw lub wolności osoby fizycznej.

RODO wymaga, aby osoby fizyczne zostały zawiadomione o naruszeniu ich danych „bez zbędnej zwłoki". Oznacza to, że administrator powinien zrealizować ów obowiązek tak szybko, jak pozwalają na to okoliczności danej sprawy. Należy przyjąć, że im poważniejsze jest ryzyko naruszenia praw lub wolności podmiotu danych, tym szybciej powinno nastąpić zawiadomienie, jak wskazuje motyw 86 RODO.

Jedynie w pewnych okolicznościach, gdy jest to uzasadnione, oraz zgodnie z zaleceniami organów ścigania administrator może opóźnić wysłanie zawiadomienia o naruszeniu do osób fizycznych, na które wywiera ono wpływ, do momentu, w którym takie zawiadomienie nie zaszkodzi takim postępowaniom. Sytuacja taka jest wprost przewidziana w art. 45 ust. 6 ustawy z 14 grudnia o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

12.2 Jaki jest cel zawiadomienia?

Poinformowanie na czas osób fizycznych o zaistniałym naruszeniu ma na celu umożliwienie im podjęcia niezbędnych działań zapobiegawczych dla ochrony przed negatywnymi skutkami naruszenia.

Zgodnie z zaleceniami Grupy Roboczej Art. 29 dotyczącymi zgłaszania naruszeń, administratorzy powinni wybierać metody pozwalające zapewnić jak najszybszą i jak największą szansę właściwego przekazania informacji o naruszeniu wszystkim osobom fizycznym, na które to naruszenie wywiera wpływ. W związku z powyższym administrator nie może zwlekać z zawiadomieniem osób, zwłaszcza kiedy żąda tego od niego organ nadzorczy.

12.3 Kiedy można zrezygnować z zawiadomienia?

W art. 34 ust. 3 RODO określono trzy sytuacje, w których nie ma konieczności zawiadomienia osób fizycznych w przypadku wystąpienia naruszenia.

1. Administrator zastosował przed wystąpieniem naruszenia odpowiednie techniczne i organizacyjne środki w celu ochrony danych osobowych, w szczególności środki uniemożliwiające odczyt danych osobom, które nie są uprawnione do dostępu do tych danych.

Przykład

Dane zabezpieczono za pomocą najnowocześniejszego szyfrowania lub tokenizacji.

2. Natychmiast po wystąpieniu naruszenia administrator podjął działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej.

Przykład I

Administrator natychmiast zidentyfikował osobę fizyczną, która uzyskała dostęp do danych osobowych, i podjął wobec niej działania, zanim mogła ona w jakikolwiek sposób wykorzystać te dane. Mimo to należy odpowiednio uwzględnić możliwe skutki każdego naruszenia poufności, również w tym wypadku biorąc pod uwagę charakter przedmiotowych danych.

Przykład II

Administrator zorientował się, że przesyłka zawierająca dane osobowe została zaadresowana na niewłaściwy adres i skontaktował się operatorem pocztowym, który nie dopuścił do dostarczenia jej wskazanemu początkowo adresatowi.

3. Skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku.

Przykład

Dokumentacja administratora uległa zalaniu, a dokumenty zawierające dane osobowe przechowywano tylko w formie papierowej. W takim przypadku administrator musi wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby fizyczne zostaną poinformowane o naruszeniu w równie skuteczny sposób. Jeżeli wykonanie tego działania wymagałoby niewspółmiernie dużego wysiłku, można również uzgodnić, że informacje na temat naruszenia będą dostępne na żądanie, co może okazać się przydatne dla osób, na które naruszenie mogło wywrzeć wpływ, lecz z którymi administrator nie mógł się w inny sposób skontaktować.

13. Jakie informacje należy przekazać osobom, których dane dotyczą w związku z naruszeniem?

Zgodnie z art. 34 ust. 2 RODO, gdy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator, bez zbędnej zwłoki, jasnym i prostym językiem zawiadamia osoby, których naruszenie dotyczy. Zawiadomienie takie **powinno zawierać wymagane przez przepisy elementy, wskazane poniżej:**

1. charakter naruszenia ochrony danych osobowych,
2. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3. opis możliwych konsekwencji naruszenia ochrony danych osobowych;
4. opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie powinno być napisane przejrzystym, łatwo zrozumiałym językiem zgodnie z art. 12 ust. 1 RODO[4].

Art. 12 ust. 1 RODO - Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą

Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji (…) oraz prowadzić z nią wszelką komunikację na mocy (…) art. 34 w sprawie przetwarzania.

Najlepiej zatem używać zwrotów bezpośrednich, np. „Podajemy informacje o krokach, które może Pani podjąć w związku z incydentem"; Następstwem naruszenia ochrony Pana danych osobowych może być: założenie na Pana dane osobowe konta internetowego (np. w serwisach społecznościowych, poczty elektronicznej)". Grupa Robocza Art. 29 w Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP250rev.01)[5] podkreśla, że „Najważniejsze, aby osoby, których dane dotyczą, **zrozumiały charakter naruszenia** i **wiedziały, co muszą zrobić, aby się zabezpieczyć**." Dlatego komunikat kierowany do osoby musi być jasny i zrozumiały oraz zawierać spójne i logiczne zalecenia dostosowane do konkretnej sytuacji. Taki, aby osoby, do których kierowane jest zawiadomienie, mogły zrozumieć, co się stało z ich danymi osobowymi, dlaczego oraz co to dla nich oznacza. Informacje, które tych cech nie posiadają, są wewnętrznie sprzeczne, nie spełniają tej funkcji, a tym samym nie pozwalają osobom na właściwe zastosowanie się do wskazówek administratora.

Administrator powinien mieć na względzie grupę odbiorców, do której zawiadomienie będzie skierowane i dostosować do niej jego treść. Tytułem przykładu: jeżeli określony podmiot posiada klientów w zbliżonym wieku i poziomie wykształcenia to język komunikatu powinien uwzględniać te okoliczności. Jeżeli natomiast adresaci są zróżnicowani lub administrator nie posiada wystarczających danych dla dokładniejszego określenia grupy odbiorców zawiadomienia, to w takim przypadku punktem odniesienia powinien być przeciętny adresat takiej wiadomości. Celem jest przekazanie odbiorcy komunikatu łatwego do zrozumienia. Ponadto komunikat nie powinien być nadmiernie rozbudowany, gdyż długa informacja z reguły utrudnia zrozumienie istoty przekazu.

By zapewnić przejrzystość zawiadomienia zalecane jest uwzględnienie oddzielenia opisu i charakteru naruszenia od możliwych konsekwencji, środków zaradczych czy danych kontaktowych inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji.

1 Opis charakteru naruszenia

Opis charakteru naruszenia jest istotnym elementem informacji przekazywanej osobom, których dane dotyczą. Powinien on być na tyle szczegółowy i jasny, aby osoby, do których jest kierowany mogły zrozumieć, co się stało z ich danymi osobowymi, dlaczego oraz co to dla nich oznacza. Zbyt lakoniczna informacja nie

[4] więcej wskazówek i przykładów przejrzystego formułowania zawiadomień o naruszeniu ochrony danych w prezentacji „Zasada przejrzystości a zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych – prezentacja" dostępnej pod adresem https://uodo.gov.pl/pl/file/2007

[5] https://www.uodo.gov.pl/pl/10/12

spełnia tej funkcji, a tym samym nie pozwala osobom na właściwe zastosowanie się do wskazówek administratora.

Forma niewystarczająca

Informujemy, że na skutek naruszenia osoba trzecia uzyskała dostęp do Pani/Pana danych osobowych przetwarzanych w systemach naszego urzędu.

Forma oczekiwana

Opis charakteru naruszenia

W dniu 13.05 br. nastąpiło naruszenie poufności Pani danych osobowych. Pani dane w zakresie: imię, nazwisko, numer PESEL, numer telefonu, adres e-mail oraz informacja o udzielonych świadczeniach socjalnych (zapomoga finansowa w wysokości Y przydzielona w związku z trudną sytuacją osobistą) na skutek pomyłki pracownika zostały wysłane listem poleconym innej osobie.

2 Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji

Administratorzy mają największe kompetencje do określenia punktu, który jest najwłaściwszy do kontaktu w sprawie naruszenia ochrony danych osobowych (dla osób, których dane dotyczą). Administrator powinien jednak uważać, aby nie wykorzystywać kanału, który w wyniku naruszenia przestał być bezpieczny, ponieważ kanał ten mogą wykorzystać również atakujący podszywający się pod administratora.

Forma niewystarczająca

Wszelkie informacje można uzyskać pod adresem kontakt@nazwa_administratora.gov.pl
(adres e-mail, pod którym można pisać w każdej sprawie)

Forma oczekiwana

Gdzie może Pani uzyskać więcej informacji?
Jeżeli ma Pani jakiekolwiek pytania lub chciałaby nam Pani przekazać dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt z naszym inspektorem ochrony danych:
Inspektor Ochrony Danych – Jan Kowalski
Adres e-mail: iod@nazwa_administratora.gov.pl
Telefon: 123 456 789

3 Opis możliwych konsekwencji

Posługiwanie się ogólnymi sformułowaniami, które znajdują się w RODO np. „uszczerbek fizyczny”, „strata finansowa”, „kradzież tożsamości” są niewystarczające. Opis możliwych konsekwencji powinien odzwierciedlać ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić jej podjęcie niezbędnych działań zapobiegawczych.

Możliwe konsekwencje powinny mieć charakter opisowy skierowany bezpośrednio do osoby, np.:

- osoby trzecie mogą podjąć próbę uzyskania na Pani/Pana szkodę, pożyczek w instytucjach pozabankowych np. przez Internet lub telefonicznie, bez konieczności okazywania dokumentu tożsamości;
- osoby trzecie mogą podjąć próbę uzyskania dostępu do systemów obsługujących udzielanie świadczeń medycznych i uzyskać wgląd do danych o Pani/Pana stanie zdrowia, ponieważ czasem dostęp do systemów rejestracji pacjenta można uzyskać, potwierdzając swoją tożsamość za pomocą numeru PESEL;
- Pani/Pana dane osobowe mogą zostać wykorzystane np. do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego tym samym skorzystać z Pani/Pana praw obywatelskich;
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osobę trzecią do próby wyłudzenia ubezpieczenia;
- osoby trzecie mogą podjąć próbę zawarcia na Pani/Pana szkodę umów cywilno-prawnych, np. najmu nieruchomości;
- Pani/Pana dane osobowe mogą zostać wykorzystane przez osoby trzecie do ukrycia swojej tożsamości, np. przy otrzymywaniu mandatu.

Forma niewystarczająca

Następstwem naruszenia może być utrata kontroli nad własnymi danymi osobowymi.

Forma oczekiwana

Możliwe konsekwencje naruszenia

Następstwem naruszenia Pana danych osobowych może być:

- *założenie na Pana dane osobowe konta internetowego (np. w serwisach społecznościowych),*
- *podszycie się pod inną osobę lub instytucję w celu wyłudzenia od Pani dodatkowych określonych informacji (np. danych do logowania, szczegółów karty kredytowej),*
- *wykorzystania Pani danych do zarejestrowania karty telefonicznej typu prepaid, która może posłużyć do celów przestępczych*

4 Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu

Administrator zobowiązany jest wskazać, jakie działania podjął bądź proponuje podjąć w związku z naruszeniem ochrony danych osobowych. Samo zapewnienie o braku złych intencji i podjęciu wszelkich działań w celu zaradzenia naruszeniu jest niespełnieniem obowiązku ciążącego na administratorze.

Forma niewystarczająca

W związku z zaistniałym naruszeniem ochrony danych postaramy się, aby do takich zdarzeń nie dochodziło w przyszłości.

Forma oczekiwana

Działania przez nas podjęte:

W związku z zaistniałym naruszeniem ochrony danych osobowych dokonaliśmy zmian w zakresie procedury weryfikacji poprawności adresu korespondencyjnego oraz zwróciliśmy się do niewłaściwego odbiorcy o zwrot dokumentacji. Dokonaliśmy także poprawienia Pani danych kontaktowych w celu uniknięcia wystąpienia podobnego zdarzenia w przyszłości. Naruszenie ochrony danych zgłosiliśmy również Prezesowi UODO.

5

W stosownych przypadkach środki minimalizujące negatywne skutki naruszenia

Obowiązkiem administratora jest zaproponowanie osobie, której dane dotyczą, środków w celu zminimalizowania zaistnienia takiego zdarzenia. Zalecenia te powinny mieć formę konkretnych i adekwatnych do danej sytuacji wskazówek. Niewłaściwe jest ograniczenie zaleceń np. tylko do zachęty poinformowania administratora bądź inspektora ochrony danych o jakichkolwiek próbach wykorzystania danych osobowych przez nieupoważnioną osobę trzecią, w sytuacji kiedy doszło do naruszenia poufności danych przez ich publikację np. na stronie internetowej. W takich sytuacjach należy - uwzględniając związane z konkretnym naruszeniem zagrożenia - przekazać osobie propozycję działań, które pozwolą jej podjąć działania w celu ochrony jej interesów. Na przykład:

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy aby Pan/Pani:

- *skorzystał/a z możliwość założenia konta w systemie informacji kredytowej celem monitorowania prób uzyskania kredytu,*
- *zachował/a ostrożność przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem internetu czy telefonu,*
- *skorzystał z możliwości zastrzeżenia dokumentu tożsamości w systemie dokumenty zastrzeżone (więcej informacji www.dokumentyzastrzezone.pl) i jego wymiany.*

Forma niewystarczająca

Jeżeli dowie się Pan o wykorzystaniu Pana danych przez osobę nieuprawnioną prosimy o jak najszybsze przekazanie nam tej informacji.

Forma oczekiwana

Co może Pan zrobić?

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy aby Pan:

a) *Ignorował nieoczekiwane wiadomości, w szczególności od nieznanych nadawców,*
b) *Zachował ostrożność w sytuacji odbierania połączeń telefonicznych od nieznanych numerów telefonów,*
c) *Założył konto w systemie informacji kredytowej lub gospodarczej w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym wykorzystaniem.*

Jeśli dowie się Pan o wykorzystaniu Pana danych przez osobę nieuprawnioną, prosimy o jak najszybsze przekazanie nam tej informacji.

W jaki sposób informować osoby, których dane dotyczą, o naruszeniu? 14.

Forma, w jakiej podmioty danych powinny być zawiadomione o naruszeniu, nie została wprost wskazana w RODO. Ostateczny jej dobór będzie zależał od rodzaju danych kontaktowych podmiotów danych, którymi dysponuje administrator.

Mając na względzie znaczenie zawiadomienia, powinno być ono sporządzone w formie, która umożliwi podmiotowi danych na wielokrotne zapoznanie się z jego treścią. Wybierając środek komunikacji trzeba pamiętać, że zawiadomienie musi zostać dostarczone adresatowi w możliwie najkrótszym czasie.

W tym kontekście wadą przesyłki nadanej drogą tradycyjną jest czas niezbędny na jej doręczenie podmiotowi danych. Dla porównania zasadniczą zaletą elektronicznej formy komunikacji jest jej szybkość, co jest pożądane z uwagi na obowiązek powiadomienia podmiotu danych bez zbędnej zwłoki (art. 34 ust. 1 RODO). Forma ta umożliwia adresatowi zarówno wielokrotne zapoznanie się z komunikatem, jak i jego wydruk w razie potrzeby.

Co do zasady administrator bezpośrednio powiadamia osoby, których dane naruszono, chyba że wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku administrator wydaje publiczny komunikat lub stosuje podobny środek, aby w równie skuteczny sposób poinformować osoby, których dane dotyczą (art. 34 ust. 3 lit. c RODO).

Do powiadamiania osób, których dane naruszono, administrator powinien stosować komunikaty dedykowane, które nie powinny być przesyłane razem z innymi informacjami, na przykład newsletterem, czy standardową wiadomością. Pomoże to przekazać informacje o naruszeniu w jasny i przejrzysty sposób. Powiadomienia ograniczającego się do komunikatu prasowego czy firmowego bloga nie uznaje się za skuteczne poinformowanie osoby fizycznej o naruszeniu.

Ponadto, jeżeli administrator nie jest w stanie zawiadomić danej osoby fizycznej o naruszeniu, ponieważ przechowywane dane są niewystarczające do skontaktowania się z tą osobą, w takim szczególnym przypadku administrator powinien ją poinformować tak szybko, jak jest to rozsądnie wykonalne (np. jeżeli osoba fizyczna skorzysta z przewidzianego w art. 15 RODO prawa do uzyskania dostępu do swoich danych osobowych i dostarczy administratorowi dodatkowe informacje wymagane do skontaktowania się z nią).

Najczęściej popełniane błędy podczas zawiadamiania osób.

15.

Mimo że art. 34 RODO wprost wskazuje administratorom, jakie wiadomości o zaistniałym naruszeniu muszą przekazać osobom, których dane dotyczą, wśród administratorów wciąż zauważalna jest tendencja do nieprawidłowego lub niedbałego konstruowania zawiadomień kierowanych do ww. osób. Nieprawidłowości dotyczą co do zasady wszystkich elementów składających się na zawiadomienie kierowane do osób, których dane dotyczą.

Opis charakteru naruszenia

Administratorzy niejednokrotnie konstruują ww. opis w oderwaniu od zasad przejrzystości nakazującej tworzenie zawiadomień jasnym i prostym językiem. Często wskazują osobom, których dane dotyczą, jedynie szczątkowe/niepełne/niezrozumiałe informacje na temat okoliczności wystąpienia incydentu, np. „Naruszenie polegało na zagubieniu dokumentacji zawierających Pana dane osobowe.” Opis naruszenia powinien być na tyle szczegółowy i jasny, aby osoby do których kierowane jest zawiadomienie, mogły zrozumieć, co się stało z ich danymi osobowymi, dlaczego oraz co to dla nich oznacza. W związku z powyższym

prawidłowy „opis charakteru naruszenia" powinien zawierać **co najmniej** okoliczności wystąpienia naruszenia wraz z opisem kategorii danych, które uległy naruszeniu.

Dane kontaktowe IOD lub innego punktu kontaktowego, od którego można uzyskać więcej informacji

Nieprawidłowości polegają na podawaniu samych danych teleadresowych IOD, bez jednoczesnego wskazania jego imienia i nazwiska. W przypadku „innych punktów kontaktowych" zauważalne jest zjawisko wyznaczania przez administratorów jako takich punktów swoich infolinii oraz biur obsługi konsumentów (bok). W związku z powyższym administratorzy powinni mieć na uwadze, że „punkt kontaktowy" musi być dla osób, których dane dotyczą, łatwo dostępny, tj. taki kanał komunikacji nie może uniemożliwiać lub utrudniać ww. osobom uzyskanie szczegółowych informacji dotyczących zaistniałego naruszenia - co do zasady punktem kontaktowym nie powinna być więc ogólnodostępna infolinia/bok administratora, ale raczej dedykowana infolinia lub też formularz kontaktowy na stronie administratora.

Opis możliwych konsekwencji naruszenia ochrony danych osobowych

Najczęstszym błędem administratorów jest konstruowanie tego elementu w sposób mało precyzyjny, tj. informowanie, że naruszenie może doprowadzić do utraty poufności ich danych czy utraty kontroli nad danymi osobowymi. **Taka informacja jest niewystarczająca**. Administrator, biorąc pod uwagę charakter naruszenia oraz kategorie danych, które uległy naruszeniu, powinien wskazać osobom, których dane dotyczą, najbardziej prawdopodobne, negatywne konsekwencje naruszenia ich danych osobowych. Np. w przypadku naruszenia takich danych, jak imię, nazwisko oraz nr PESEL, należy wskazać np., że możliwa jest kradzież lub sfałszowanie tożsamości poprzez uzyskanie przez osoby trzecie, na szkodę osób, których dane naruszono, kredytów w instytucjach pozabankowych bądź wyłudzenia ubezpieczenia lub środków z ubezpieczenia co może spowodować negatywne konsekwencje związane z próbą przypisania osobom, których dane dotyczą, odpowiedzialności za dokonanie takiego oszustwa.

Opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosowanych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków

„Wskazówki" administratora nie uwzględniają dosyć często charakteru oraz kategorii danych, które uległy naruszeniu, np. w przypadku utraty takich danych, jak nr PESEL czy seria i nr dowodu osobistego, samo zasugerowanie osobie, aby poinformowała administratora o wykorzystaniu jego danych osobowych nie jest środkiem minimalizującym ewentualne negatywne skutki naruszenia. W takiej sytuacji właściwe będzie wskazanie możliwości założenia konta w systemie informacji kredytowej celem monitorowania prób uzyskania kredytu, czy zgłoszenie faktu naruszenia danych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości".

Czy RODO wymaga podjęcia innych kroków w związku z naruszeniem? 16.

Podobnie jak w przypadku każdego incydentu związanego z bezpieczeństwem, administrator powinien ustalić, czy naruszenie było wynikiem błędu ludzkiego lub problemu systemowego i zobaczyć w jaki sposób można zapobiec powtórce incydentu - czy to poprzez lepsze procesy, dalsze szkolenia lub inne kroki naprawcze. W celu sprawnej realizacji przez administratorów i podmioty przetwarzające obowiązków w zakresie naruszeń ochrony danych zalecane jest wdrożenie wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. Ponadto procedura zgłaszania organowi nadzorczemu naruszeń ochrony danych osobowych oraz zawiadamiania o naruszeniach podmiotów danych, może być elementem kodeksu postępowania, zgodnie z art. 40 ust. 2 lit. i RODO.

Obowiązki dotyczące naruszeń określone w innych aktach prawnych 17.

17.1 Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. 2004.171.1800 z późn. zm.)

Firmy telekomunikacyjne to jedne z podmiotów, które - w przypadku stwierdzenia naruszenia ochrony danych osobowych - są zobowiązane zawiadamiać o tym Prezesa Urzędu Ochrony Danych Osobowych, a czasami również osoby, których ono dotyczy. Poniżej wyjaśniamy, kiedy i jak to robić.

W świetle przepisów:

- unijnego ogólnego rozporządzenia o ochronie danych, czyli RODO,
- Rozporządzenia Komisji (UE) Nr 611/2013 z dnia 24 czerwca 2013 r. w sprawie środków mających zastosowanie przy powiadamianiu o przypadkach naruszenia danych osobowych, na mocy dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady o prywatności i łączności elektronicznej, zwanego dalej też „rozporządzeniem Komisji (UE) Nr 611/2013”,
- ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne,

dostawcy publicznie dostępnych usług telekomunikacyjnych nie tylko muszą chronić dane osobowe osób korzystających z ich usług, ale także w przypadku stwierdzenia naruszenia ochrony danych osobowych zobligowani są powiadomić o tym fakcie krajowe organy nadzorcze, w Polsce - Prezesa Urzędu Ochrony Danych Osobowych (Prezesa UODO). Dodatkowo w niektórych przypadkach konieczne jest również powiadomienie abonenta lub użytkownika końcowego, którego dane zostały naruszone.

Nadrzędnym celem każdego zgłoszenia naruszenia organowi nadzorczemu jest ochrona praw i wolności osób fizycznych. Niezmiernie ważną kwestią w tym przypadku jest czas reakcji administratora, tj. jak najszybsze powiadomienie o naruszeniu organu nadzorczego oraz - jeśli to konieczne - powiadomienie o naruszeniu osób, których dane dotyczą.

Poniżej zamieszczamy zestawienie pomocnych wskazówek dotyczących obowiązku zgłaszania naruszeń danych osobowych w sektorze telekomunikacyjnym.

Co należy rozumieć przez naruszenie danych osobowych?

Przez **naruszenie danych osobowych** rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub bezprawnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych osobowych przekazywanych, przechowywanych lub w inny sposób przetwarzanych w związku ze świadczeniem przez przedsiębiorcę telekomunikacyjnego publicznie dostępnych usług telekomunikacyjnych.

Kto i w jakim terminie powinien powiadomić Prezesa UODO o naruszeniu danych osobowych?

Obowiązek taki został nałożony na **dostawców publicznie dostępnych usług telekomunikacyjnych.** Naruszenie danych osobowych powinno być zgłoszone **niezwłocznie, ale nie później niż 24 godziny po wykryciu naruszenia**. Termin ten wynika z art. 2 ust. 2 rozporządzenia Komisji (UE) Nr 611/2013. Ponieważ jest on krótszy niż termin wskazany w RODO, to przedsiębiorcy telekomunikacyjni powinni dołożyć wszelkich starań, aby przesłać wymagane prawem informacje w terminie 24, a nie 72 godzin.

W jaki sposób można zawiadomić Prezesa UODO o wystąpieniu naruszenia?

Zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO dokonuje się **elektronicznie za pomocą odpowiedniego formularza dostępnego na stronie internetowej urzędu pod linkiem** https://uodo.gov.pl/pl/134/233. Formularz ten zawiera wszystkie wymagane informacje, o których mowa w art. 2 ust. 2 rozporządzenia Komisji (UE) nr 611/2013.

Kiedy i w jakim celu trzeba zawiadomić o naruszeniu osoby, których dane dotyczą?

Zgodnie z art. 174a ust. 3 ustawy prawo telekomunikacyjne, w przypadku gdy naruszenie danych osobowych może mieć niekorzystny wpływ na prawa abonenta lub użytkownika końcowego będącego osobą fizyczną, dostawca publicznie dostępnych usług telekomunikacyjnych, oprócz powiadomienia Prezesa UODO, niezwłocznie zawiadamia o takim naruszeniu również abonenta lub użytkownika końcowego na zasadach określonych w art.3 rozporządzenia Komisji (UE) nr 611/2013. Zawiadomienie abonenta lub osoby fizycznej następuje **bez zbędnej zwłoki po wykryciu naruszenia ochrony danych osobowych** przez administratora.

Co powinno zawierać zawiadomienie skierowane do abonenta?

Zgodnie z art. 3 ust. 4 rozporządzenia Komisji (UE) Nr 611/2013, w powiadomieniu skierowanym do abonenta lub osoby fizycznej dostawca zawiera takie informacje, jak:

1. nazwa dostawcy;
2. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, w którym można uzyskać więcej informacji;
3. streszczenie zdarzenia, w wyniku którego doszło do naruszenia danych osobowych;
4. przybliżona data zdarzenia;
5. charakter i treść danych osobowych, zgodnie z art. 3 ust. 2 rozporządzenia;
6. prawdopodobne konsekwencje naruszenie danych osobowych dla danego abonenta lub osoby fizycznej, zgodnie z art. 3 ust. 2 rozporządzenia;
7. okoliczności naruszenia danych osobowych, zgodnie z art. 3 ust. 2 rozporządzenia;

8. środki wprowadzone przez dostawcę w celu zaradzenia naruszeniu ochrony danych osobowych;
9. środki zalecane przez dostawcę w celu złagodzenia ewentualnych niekorzystnych skutków.

Kiedy nie ma obowiązku informowania osób, których dane dotyczą, o naruszeniu ochrony danych?
„Zawiadomienie abonenta lub użytkownika końcowego będącego osobą fizyczną o naruszeniu nie jest wymagane, jeżeli dostawca publicznie dostępnych usług telekomunikacyjnych **wdrożył odpowiednie techniczne i organizacyjne środki ochrony, które uniemożliwiają odczytanie danych** przez osoby nieuprawnione oraz zastosował je do danych, których ochrona została naruszona (na podstawie art. 174a ust. 5 Prawa telekomunikacyjnego).

Ponadto w wyjątkowych okolicznościach, gdy powiadomienie abonenta lub osoby fizycznej może zaszkodzić należytemu zbadaniu przypadku naruszenia danych osobowych, dostawcy zezwala się, po uprzednim uzyskaniu zgody Prezesa UODO, na powiadomienie abonenta lub osoby fizycznej w późniejszym terminie.

Co w przypadku, gdy administrator nie zawiadomił abonenta o fakcie naruszenia danych?
Jeżeli dostawca publicznie dostępnych usług telekomunikacyjnych nie zawiadomił abonenta lub użytkownika końcowego będącego osobą fizyczną o fakcie naruszenia danych osobowych, Prezes UODO może nałożyć, w drodze **decyzji**, na dostawcę **obowiązek przekazania abonentom lub użytkownikom końcowym będącym osobami fizycznymi takiego zawiadomienia**, biorąc pod uwagę możliwe niekorzystne skutki naruszenia.

Czy dostawca usług telekomunikacyjnych musi prowadzić rejestr naruszeń danych osobowych?
Dostawca publicznie dostępnych usług telekomunikacyjnych prowadzi rejestr naruszeń danych osobowych, w tym faktów towarzyszących naruszeniom, ich skutków i podjętych działań. Rejestr ten powinien obejmować następujące elementy:

1. opis charakteru naruszeń danych osobowych;
2. informacje o zaleconych przez dostawcę publicznie dostępnych usług telekomunikacyjnych środkach mających na celu złagodzenie ewentualnych niekorzystnych skutków naruszeń danych osobowych;
3. informacje o działaniach podjętych przez dostawcę publicznie dostępnych usług telekomunikacyjnych;
4. informacje o fakcie poinformowania lub braku poinformowania abonenta o wystąpieniu naruszenia danych osobowych;
5. opis skutków naruszenia danych osobowych;
6. opis zaproponowanych przez dostawcę publicznie dostępnych usług telekomunikacyjnych środków naprawczych.

17.2 Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. 2019.0.125)

W art. 44 ustawy, na administratorów przetwarzających dane osobowe w związku z zapobieganiem i zwalczaniem przestępczości nałożono taki sam obowiązek, jak na administratorów na podstawie art. 33 ust. 1 RODO. Analogiczne obowiązki są uregulowane w zakresie terminu zawiadomienia Prezesa UODO

o naruszeniu (bez zbędnej zwłoki, nie później niż w ciągu 72 godzin) oraz zakresu informacji jaki należy przekazać organowi nadzorczemu.

Wobec podmiotów przetwarzających (art. 44 ust. 3), nałożono obowiązek przekazywania informacji o naruszeniu administratorowi bez zbędnej zwłoki, nie później jednak niż w ciągu 48 godzin (RODO zobowiązuje administratorów do przekazywania tych informacji bez zbędnej zwłoki, bez wskazania terminu granicznego).

W art. 45 ustawy na administratorów nałożono tożsamy obowiązek jak istnieje na gruncie art. 34 RODO, tj. obowiązek zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Jednakże jedyne opóźnienie, ograniczenie bądź odstępstwo od tego obowiązku może mieć miejsce wyłącznie w przypadku, o którym mowa w art. 26 ust. 1 ustawy tj. przekazanie informacji mogłoby powodować:

1) ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
2) utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3) utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
4) zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
5) zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
6) istotne naruszenie dóbr osobistych innych osób.

17.3 Rozporządzenie eIDAS - Rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

W art 19 ust. 2 rozporządzenia eIDAS nałożono na dostawców usług zaufania wymóg niezwłocznego (nie później niż 24h od otrzymania informacji o wystąpieniu zdarzenia) zawiadamiania organu nadzorczego o wszelkich przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na przetwarzane przez świadczoną usługę zaufania dane osobowe.

Rejestr dostawców usług zaufania prowadzony jest przez Narodowe Centrum Certyfikacji (NCCert) i dostępny jest na stronach:

- https://www.nccert.pl/uslugi.htm (kwalifikowane usługi zaufania)
- https://www.nccert.pl/uslugiNK.htm (niekwalifikowane usługi zaufania).

17.4 Ustawa z dnia 15 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U.2018.1560)

Art. 34 ust. 2 tej ustawy nakłada na Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego (tzw. CSIRT-y), koordynujące obsługę incydentu, który doprowadził do naruszenia ochrony danych osobowych obowiązek współpracy z Prezesem Urzędu Ochrony Danych Osobowych.

Niemniej jednak w przypadku gdy takie incydenty stanowią naruszenie ochrony danych osobowych zgodnie z RODO lub w momencie gdy się nim stają, operatorzy usług kluczowych (o których mowa w art. 5 ust. 1 ustawy) mogą być zobowiązani, zgodnie z art. 33 ust, 1 RODO do zawiadomienia organu nadzorczego niezależnie od wymogów dotyczących zgłoszenia incydentu na podstawie ustawy o krajowym systemie cyberbezpieczeństwa.

Jeżeli naruszenie, zgłaszane przez administratora na podstawie art. 33 RODO do Prezesa UODO, dotyczy podejrzanych załączników, phishingu, szantażu czy działania złośliwego oprogramowania, Prezes UODO zachęca do zgłaszania takich zdarzeń również do CERT Polska pod adresem https://incydent.cert.pl/. O fakcie zgłoszenia takiego incydentu do CERT Polska warto poinformować Prezesa UODO podając datę zgłoszenia oraz jego numer (np. w zgłoszeniu uzupełniającym).

Urząd
Ochrony
Danych
Osobowych

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa