GRUPA ROBOCZA DS. OCHRONY DANYCH NA MOCY ART. 29

17/EN

WP250

Wytyczne w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/679

Przyjęte 3 października 2017 r.

Niniejsza Grupa Robocza została powołana na mocy artykułu 29 dyrektywy 95/46/WE. Jest to niezależny europejski organ doradczy w sprawach ochrony danych i prywatności. Jej zadania zostały opisane w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę Sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej, B-1049 Bruksela, Belgia, Biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

GRUPA ROBOCZA DS. OCHRONY OSÓB FIZYCZNYCH
W ZAKRESIE PRZETWARZANIA DANYCH OSOBOWYCH

powołana na mocy artykułu 29 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.,

uwzględniając postanowienia art. 29 i 30 tej dyrektywy,

uwzględniając regulamin wewnętrzny,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

SPIS TREŚCI

WPROWADZENIE

Ogólne rozporządzenie o ochronie danych (OROD) wprowadza wymóg powiadamiania właściwego krajowego organu nadzorczego[1] o naruszeniu (dalej: „naruszenie") ochrony danych osobowych, a także, w niektórych przypadkach, poinformowania o naruszeniu osób, których dane osobowe ucierpią wskutek takiego naruszenia.

Wymóg powiadamiania o przypadkach naruszeń dotyczy obecnie pewnych organizacji, takich jak podmioty świadczące publicznie dostępne usługi łączności elektronicznej (jak określono w dyrektywie 2009/136/WE i rozporządzeniu (UE) nr 611/2013)[2]. Ponadto niektóre państwa członkowskie UE we własnym zakresie wprowadziły już obowiązek zawiadamiania o naruszeniach na poziomie krajowym. Może to obejmować obowiązek zgłaszania naruszeń z udziałem różnych kategorii administratorów, nie tylko podmiotów świadczących publicznie dostępne usługi łączności elektronicznej (np. w Niemczech i Włoszech), lub obowiązek zgłaszania wszelkich naruszeń związanych z danymi osobowymi (np. w Holandii). Inne państwa członkowskie mogą posiadać stosowne kodeksy postępowania (jak na przykład Irlandia[3]). Mimo że obecnie wiele unijnych organów ochrony danych zachęca administratorów do zgłaszania naruszeń, dyrektywa o ochronie danych 95/46/WE[4], którą OROD zastępuje, nie nakłada konkretnego obowiązku powiadamiania o naruszeniach, a zatem dla wielu organizacji będzie to nowe wymaganie. OROD wprowadza obowiązek powiadamiania dla wszystkich administratorów, chyba że jest mało prawdopodobne, by naruszenie naraziło na ryzyko prawa i wolności osób fizycznych[5]. Podmioty przetwarzające dane również mają ważną rolę do odegrania i muszą zgłaszać wszelkie naruszenia do swoich administratorów[6].

Grupa Robocza na mocy art. 29 (GR29) uważa, że nowy obowiązek powiadamiania przyniesie szereg korzyści. W przypadku powiadomienia organu nadzoru administratorzy mogą otrzymać radę co do konieczności powiadomienia osób, których naruszenie dotyczy. Organ nadzorczy może w istocie zażądać od administratora poinformowania takich osób o naruszeniu[7]. Powiadamianie osób fizycznych o naruszeniu daje administratorowi możliwość przekazania informacji o ryzyku stwarzanym przez naruszenie oraz o krokach, jakie mogą podjąć te osoby, by uchronić się przed jego potencjalnymi konsekwencjami. Każdy plan odpowiedzi na naruszenie powinien skupiać się na ochronie osób fizycznych i ich danych osobowych. W związku z tym powiadomienie o naruszeniu należy postrzegać jako narzędzie pozwalające zapewnić lepszą ochronę danych osobowych. Jednocześnie należy zauważyć, że niezgłoszenie naruszenia osobie fizycznej czy organowi nadzorczemu może prowadzić do nałożenia na administratora sankcji na mocy art. 83.

W związku z powyższym zachęca się administratorów i podmioty przetwarzające dane do planowania z wyprzedzeniem i wdrażania procedur pozwalających im wykrywać naruszenia i niezwłocznie im zaradzać, oceniać ryzyko dla osób fizycznych[8], a następnie określać, czy konieczne jest

---

[1] Patrz art. 4 ust. 21 OROD

[2] Patrz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611

[3] Patrz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[4] Patrz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[5] Prawa zapisane w Karcie praw podstawowych UE, dostępnej pod adresem http://eur- lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[6] Patrz art. 33 ust. 2. Jest to koncepcja zbliżona do art. 5 rozporządzenia (UE) nr 611/2013, który stanowi, że dostawca, któremu zlecono świadczenie części usługi łączności elektronicznej (i nie jest związany z abonentami bezpośrednim stosunkiem umownym), ma obowiązek niezwłocznie powiadomić dostawcę zamawiającego o przypadku naruszenia danych osobowych.

[7] Patrz art. 34 ust. 4 i art. 58 ust. 2 lit. e

[8] Może to zapewnić wymóg kontroli i przeglądu w ramach oceny skutków dla ochrony danych, obowiązkowy w przypadku operacji przetwarzania, które mogą narazić prawa i wolności osób fizycznych na wysokie ryzyko (art. 35 ust. 1 i ust. 11.

powiadomienie właściwego organu nadzorczego, i w razie konieczności informować o naruszeniu osoby, których ono dotknęło. Powiadomienie organu nadzorczego powinno stanowić część planu reakcji na zdarzenie.

OROD zawiera postanowienia wskazujące, kiedy i kogo należy powiadamiać o naruszeniu, a także jakie informacje należy przekazywać w ramach powiadomienia. Informacje wymagane do powiadomienia można podawać sukcesywnie, przy czym administratorzy powinni odpowiednio szybko podejmować działania w związku z każdym naruszeniem.

W opinii 03/2014 w sprawie powiadomień o naruszeniu ochrony danych osobowych[9] GR29 przedstawiła wytyczne dla administratorów mające im pomóc podejmować decyzje o powiadamianiu podmiotów danych w przypadku naruszenia. W opinii rozważano zobowiązanie podmiotów świadczących usługi łączności elektronicznej w związku z dyrektywą 2002/58/WE i podano przykłady z wielu sektorów, w kontekście wówczas dopiero proponowanego OROD, a także przedstawiono dobre praktyki dla wszystkich administratorów.

Niniejsze wytyczne wyjaśniają obowiązek zgłoszenia naruszenia i wymogi dotyczące przekazywania informacji zawarte w OROD, a także niektóre z działań, jakie mogą podjąć administratorzy i podmioty przetwarzające dane w celu wywiązania się ze swoich nowych zobowiązań. Ponadto zawierają przykłady różnych rodzajów naruszeń oraz osób, które należy powiadamiać w zależności od przypadku.

I. Powiadamianie o naruszeniu danych osobowych na mocy OROD

A. Podstawowe względy bezpieczeństwa

Jednym z wymogów stawianych przez OROD jest przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych[10].

„Zniszczenie" danych osobowych powinno być jasne: oznacza sytuację, w której dane przestają istnieć lub przestają istnieć w formie nadającej się do użytku przez administratora. „Uszkodzenie" również powinno być stosunkowo jasne: oznacza sytuację, w której dane osobowe uległy zmianie czy zepsuciu lub stały się niekompletne. „Utratę" danych osobowych należy rozumieć jako sytuację, w której dane mogą nadal istnieć, ale administrator utracił kontrole nad nimi lub dostęp do nich, lub nie jest już w ich posiadaniu. Niedozwolone lub niezgodne z prawem przetwarzanie obejmuje przypadki ujawnienia lub udostępnienia danych osobowych odbiorcom nieupoważnionym do otrzymania ich lub uzyskania do nich dostępu, a także wszelkie inne formy przetwarzania naruszające postanowienia OROD.

Przykład

Przykładem utraty danych osobowych może być zagubienie lub kradzież nośnika zawierającego kopię bazy danych klientów administratora. Innym przykładem utraty może być sytuacja, w której tylko jedna kopia ze zbioru danych osobowych została zaszyfrowana przez oprogramowanie typu ransomware lub przez samego administratora przy użyciu klucza, którym ten już nie dysponuje.

---

[9] Patrz opinia 03/2014 w sprawie powiadomień o naruszeniu ochrony danych osobowych http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] Patrz art. 5 ust. 1 lit. f i art. 32.

W związku z powyższym OROD wymaga zarówno od administratorów, jak i od podmiotów przetwarzających wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, na które narażone są przetwarzane dane osobowe. Powinni przy tym uwzględnić stan techniki, koszty wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw i wolności osób fizycznych[11], zmienne pod względem prawdopodobieństwa i powagi. W związku z tym kluczowym elementem każdej polityki bezpieczeństwa danych jest możliwość – w stosownych przypadkach – zapobiegnięcia naruszeniu lub reagowania na nie w odpowiedni sposób, jeżeli już do niego dojdzie.

B. Czym jest naruszenie ochrony danych osobowych?

1. Definicja

Aby móc podjąć próbę usunięcia naruszenia, administrator powinien najpierw umieć takie naruszenie rozpoznać. Art. 4 ust. 12 OROD definiuje „naruszenie ochrony danych osobowych" jako:

> „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"

Powinno być jasne, że naruszenie stanowi zdarzenie zagrażające bezpieczeństwu. Niemniej zgodnie z art. 4 ust. 12 OROD znajduje zastosowanie tylko w przypadku naruszenia *danych osobowych*. Na skutek takiego naruszenia administrator może nie być w stanie zapewnić poszanowania zasad przetwarzania danych osobowych, określonych w art. 5 OROD. Podkreśla to różnicę pomiędzy zdarzeniem zagrażającym bezpieczeństwu a naruszeniem ochrony danych osobowych – zasadniczo każde naruszenie danych osobowych jest zdarzeniem zagrażającym bezpieczeństwu, ale nie każde zdarzenie zagrażające bezpieczeństwu stanowi naruszenie ochrony danych osobowych.

Potencjalne niekorzystne skutki naruszenia dla osób fizycznych przedstawiono poniżej.

2. Rodzaje naruszeń ochrony danych osobowych

W swojej opinii 03/2014 w sprawie powiadomień o naruszeniu GR29 wyjaśnia, że naruszenia można zaklasyfikować ze względu na trzy powszechnie znane zasady bezpieczeństwa informacji[12]:

- „Naruszenie poufności" – niedozwolone lub przypadkowe ujawnienie lub dostęp do danych osobowych.
- „Naruszenie dostępności" – niedozwolona lub przypadkowa utrata dostępu do danych osobowych lub zniszczenie ich.
- „Naruszenie integralności" – niedozwolona lub przypadkowa zmiana danych osobowych.

Należy również zauważyć, że w zależności od okoliczności naruszenie może dotyczyć jednocześnie poufności, dostępności i integralności danych osobowych lub dowolnej kombinacji tych kategorii.

O ile rozróżnienie między naruszeniem poufności a naruszeniem integralności jest dość jasne, naruszenie dostępności może być pojęciem mniej oczywistym. Naruszenie zawsze uznaje się za naruszenie dostępności w przypadku trwałej utraty lub zniszczenia danych osobowych.

[11] Patrz art. 32 oraz motyw 83.
[12] Patrz opinia 03/2014.

Przykład

Przykłady utraty dostępności to sytuacje, w których doszło do usunięcia danych – przypadkowo lub przez nieupoważnioną osobę – a także utrata klucza deszyfrującego w przypadku bezpiecznie zaszyfrowanych danych. Jeżeli administrator nie jest w stanie odzyskać dostępu do danych np. z kopii zapasowej, uznaje się to za trwałą utratę dostępności.

Utrata dostępności może również mieć miejsce w przypadku znaczącego zakłócenia normalnej działalności organizacji np. w wyniku przerwy w dostawie prądu lub ataku typu blokada usług (ang. denial of service), skutkującego tymczasowym lub trwałym brakiem dostępu do danych osobowych.

Można tu zadać pytanie, czy tymczasową utratę dostępności należy uznać za naruszenie, a jeśli tak, to czy należy takie naruszenie zgłosić. Art. 32 OROD, „bezpieczeństwo przetwarzania", wyjaśnia, że podczas wdrażania odpowiednich środków technicznych i organizacyjnych, mających zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, należy uwzględnić miedzy innymi „zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania" oraz „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego".

W związku z powyższym zdarzenie skutkujące utratą dostępności danych osobowych przez pewien odcinek czasu stanowi naruszenie bezpieczeństwa (i należy je udokumentować[13]), ale w zależności od okoliczności powiadomienie organu nadzorczego czy poszkodowanych osób może, ale nie musi być wymagane. Jeżeli niedostępność danych osobowych może prowadzić do ryzyka naruszenia praw i wolności osób fizycznych, wówczas administrator musi ją zgłosić. Należy to oceniać na podstawie konkretnych przypadków.

Przykłady

W kontekście szpitala brak dostępu do kluczowych informacji na temat pacjentów, nawet tymczasowy, może stanowić ryzyko dla praw i wolności osób fizycznych, np. prowadzić do odwołania operacji.

Natomiast jeżeli z powodu kilkugodzinnego braku dostępu do swoich systemów (np. na skutek przerwy w dostawie prądu) spółka medialna nie może wysłać newslettera do abonentów, istnieje małe prawdopodobieństwo ryzyka naruszenia praw i wolności osób fizycznych.

Ponadto, należy zauważyć, że chociaż utrata dostępu do systemów administratora może być tylko tymczasowa i nie musi pociągać za sobą skutków dla osób fizycznych, to sam fakt, że miało miejsce włamanie do sieci można uznać za potencjalne naruszenie poufności, które wymaga zgłoszenia. Dlatego ważne jest, by administrator rozważył wszystkie możliwe konsekwencje naruszenia.

Przykład

Infekcja oprogramowaniem typu ransomware (złośliwym oprogramowaniem, które szyfruje dane administratora do czasu zapłaty okupu) może prowadzić tylko do tymczasowej utraty dostępu do danych, jeżeli można je odzyskać z kopii zapasowej. Mimo wszystko doszło jednak do włamania, w związku z czym może być wymagane zgłoszenie zdarzenia, jeśli kwalifikuje się ono jako naruszenie poufności (tj. atakujący uzyskał dostęp do danych osobowych) stanowiące ryzyko dla praw i wolności osób fizycznych.

[13] Patrz art. 33 ust. 5.

3. Możliwe konsekwencje naruszenia ochrony danych osobowych

Naruszenie może potencjalnie mieć dla osób fizycznych szereg znaczących negatywnych skutków, które mogą prowadzić do szkód fizycznych, materialnych i niematerialnych. OROD wyjaśnia, że do skutków tych należą utrata kontroli nad danymi osobowymi, ograniczenie praw, dyskryminację, kradzież lub sfałszowanie tożsamości, strata finansowa, nieupoważnione odwrócenie pseudonimizacji, naruszenie dobrego imienia oraz utrata poufności danych osobowych chronionych tajemnicą zawodową. Skutki te obejmują również wszelkie inne znaczne szkody gospodarcze lub społeczne dla osób, których dotyczą dane[14].

OROD zobowiązuje zatem administratora do zgłoszenia naruszenia do właściwego organu nadzorczego, chyba że ryzyko wystąpienia takich negatywnych skutków jest nieznaczne. W przypadku wysokiego ryzyka wystąpienia tego rodzaju negatywnych skutków OROD zobowiązuje administratora do powiadomienia o naruszeniu osób, których ono dotyczy, tak szybko, jak jest to racjonalnie możliwe[15].

Wagę umiejętności rozpoznania naruszenia, oceny ryzyka dla osób fizycznych i zgłoszenia naruszenia w razie konieczności podkreśla motyw 87 OROD:

> „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. Fakt, 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."

Dalsze wytyczne dotyczące oceny ryzyka negatywnego wpływu na osoby fizyczne przedstawiono w pkt. V.

W przypadku, gdy administratorzy nie powiadomią organu nadzorczego i/lub osób, których dane naruszono, nawet jeśli spełnione zostaną wymogi z art. 33 i/lub 34, organ nadzorczy może dokonać wyboru, przy którym musi wziąć pod uwagę wszelkie środki naprawcze, jakimi dysponuje, w tym nałożenie stosownej administracyjnej kary pieniężnej – samej lub łącznie z innym środkiem naprawczym określonym w art. 58 ust. 2. Jeżeli wybrana zostanie administracyjna kara pieniężna, jej wartość nie może przekroczyć 10.000.000 EUR lub 2% całkowitego rocznego obrotu przedsiębiorstwa z całego świata zgodnie z art. 83 ust. 4 lit. a OROD. Należy również pamiętać, że w niektórych przypadkach niezgłoszenie naruszenia może ujawnić brak środków bezpieczeństwa lub nieodpowiedni charakter istniejących środków. W takim przypadku organ nadzorczy ma również możliwość nałożenia sankcji za niepowiadomienie lub niepoinformowanie o naruszeniu (art. 33 i 34) z jednej strony, a za brak (odpowiednich) środków bezpieczeństwa (art. 32) z drugiej, ponieważ są to dwa odrębne naruszenia.

[14] Patrz również motywy 85 i 75.
[15] Patrz również motyw 86.

II. Artykuł 33 – Zgłaszanie naruszenia organowi nadzorczemu

A. Kiedy zgłaszać

1. Wymogi na mocy art. 33

Art. 33 ust. 1 stanowi, co następuje:

> „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. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia."

2. Kiedy administrator „stwierdza" naruszenie?

Zgodnie z tym, co opisano powyżej, w przypadku naruszenia OROD wymaga od administratora niezwłocznego zgłoszenia takiego naruszenia, jeżeli to możliwe – w ciągu 72 godzin od jego stwierdzenia. Tutaj może pojawić się pytanie, kiedy uznaje się, że administrator „stwierdził" naruszenie. Według GR29 należy uznać, że administrator „stwierdził" naruszenie, kiedy ma wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, prowadzące do naruszenia bezpieczeństwa danych osobowych. Zależy to od okoliczności konkretnego naruszenia. W niektórych przypadkach od samego początku stosunkowo jasne jest, że doszło do naruszenia; w innych stwierdzenie naruszenia ochrony danych osobowych może zająć więcej czasu. Główny nacisk należy jednak położyć na szybkie działanie w kierunku zbadania zdarzenia i ustalenia, czy rzeczywiście miało miejsce naruszenie ochrony danych, a jeśli tak – podjęcie działań naprawczych i zgłoszenie naruszenia w razie takiej konieczności.

Przykłady

W przypadku utraty płyty CD z niezaszyfrowanymi danymi często nie da się ustalić, czy osoby nieupoważnione uzyskały do nich dostęp. Taki przypadek należy jednak zgłosić, ponieważ istnieje wystarczający stopień pewności co do tego, że doszło do naruszenia; administrator „stwierdza" naruszenie w chwili zdania sobie sprawy z utraty płyty.

Osoba trzecia informuje administratora o przypadkowym otrzymaniu danych osobowych jednego z jego klientów i przedstawia dowody niedozwolonego ujawnienia danych. Jako że administrator otrzymał jasne dowody naruszenia, nie ma wątpliwości co do tego, że „stwierdził" naruszenie.

Administrator odkrywa, że mogło mieć miejsce włamanie do jego sieci. Sprawdza swoje systemy, aby ustalić, czy doszło do naruszenia bezpieczeństwa przechowywanych w nich danych, i potwierdza, że istotnie tak się stało. Ponownie, jako że administrator uzyskał jasne dowody naruszenia, nie ma wątpliwości co do tego, „stwierdził" naruszenie.

Cyberprzestępca kontaktuje się z administratorem po włamaniu się do jego systemu, aby zażądać okupu. W takim przypadku administrator ma wyraźne dowody, że doszło do naruszenia; nie ma więc wątpliwości co do tego, że stwierdził naruszenie.

Po otrzymaniu pierwszych informacji o możliwym naruszeniu od osoby fizycznej, spółki medialnej czy z innego źródła, lub po samodzielnym odkryciu zdarzenia zagrażającego bezpieczeństwu, administrator może przeprowadzić krótkie dochodzenie, aby ustalić, czy rzeczywiście doszło do naruszenia. W czasie trwania takiego dochodzenia nie można jeszcze uznać, że administrator „stwierdził" naruszenie. Zgodnie z założeniami wstępne dochodzenie powinno rozpocząć się jak najszybciej i pozwolić ustalić z należytą pewnością, czy miało miejsce naruszenie, a określić także

jego możliwe konsekwencje dla osób fizycznych; później może nastąpić bardziej dokładne dochodzenie.

Niezbędną częścią planu reakcji jest ocena możliwego ryzyka dla osób fizycznych, pozwalająca stwierdzić, czy powstał wymóg powiadomienia, a także określić działanie(-a) konieczne do zaradzenia naruszeniu. Istnieje jednak możliwość, że administrator dokonał już wstępnej oceny ryzyka, jakie może stwarzać naruszenie, w ramach oceny skutków dla ochrony danych (DPIA)[16] przeprowadzonej przed wykonaniem danej operacji przetwarzania. Ocena skutków dla ochrony danych może jednak okazać się bardziej ogólna niż konkretne okoliczności naruszenia. które rzeczywiście miało miejsce; dlatego też w każdym przypadku należy przeprowadzić dodatkową ocenę z uwzględnieniem wszelkich okoliczności. Więcej informacji na temat oceny ryzyka znajduje się w pkt. V.

W większości przypadków wstępne czynności należy zakończyć jak najszybciej po wstępnym alercie – mogą one trwać dłużej jedynie w wyjątkowych przypadkach.

Przykład

Osoba fizyczna poinformowała administratora o otrzymaniu wiadomości elektronicznej, w której ktoś się pod niego podszywał; wiadomość zawiera dane osobowe związane z (bieżącym) korzystaniem z usług administratora, co sugeruje, że istnieje zagrożenie dla jego bezpieczeństwa. Administrator przeprowadza krótkie dochodzenie, w toku którego odkrywa, że miało miejsce włamanie do jego sieci, i znajduje dowody nieuprawnionego dostępu do danych osobowych. Od tej chwili uznaje się, że administrator „stwierdził" naruszenie i wymagane jest powiadomienie organu nadzorczego, jeżeli może ono narazić osoby fizyczne na ryzyko. Administrator musi w takiej sytuacji podjąć odpowiednie działania następcze w celu zaradzenia naruszeniu.

W związku z powyższym administrator powinien wdrożyć procedury wewnętrzne pozwalające na wykrywanie naruszeń i zaradzanie im. Na przykład w celu wykrycia pewnego rodzaju nieprawidłowości w zakresie przetwarzania danych administrator lub podmiot przetwarzający może wykorzystać pewnego rodzaju środki techniczne, takie jak przepływ danych czy analizatory rejestru, dzięki którym możliwe jest określenie zdarzeń i alertów poprzez zestawianie danych rejestru[17]. W przypadku wykrycia naruszenia ważne jest, by zgłosić je przełożonym na odpowiednim szczeblu zarządzania, tak aby umożliwić zaradzenie mu, a także w razie konieczności takiego wymogu zgłoszenie go zgodnie z art. 33, a w razie potrzeby także zgodnie z art. 34. Takie środki i mechanizmy zgłaszania można opisać w planach reakcji na incydenty administratora i/lub w zasadach zarządzania. Maja one pomóc administratorowi tworzyć skuteczne plany i ustalać, kto w organizacji ponosi odpowiedzialność operacyjną za usuwanie naruszeń, a także określać zasadność i sposób przekazywanie poszczególnych przypadków na wyższy poziom kompetencji.

Administrator powinien również zawrzeć porozumienia ze wszystkimi podmiotami przetwarzającymi, z usług których korzysta, zaś same te podmioty zobowiązane są powiadamiać administratora o przypadkach naruszenia (patrz niżej).

Co prawda za wdrożenie odpowiednich środków w celu zapobiegania naruszeniom, reagowania na nie i zaradzania im odpowiadają administratorzy i podmioty przetwarzające, istnieją jednak pewne kroki praktyczne, które należy podejmować we wszystkich przypadkach.

- Informacje na temat wszelkich zdarzeń związanych z bezpieczeństwem powinny być kierowane do odpowiedzialnej osoby lub osób, którym powierzono zadanie stwierdzania

[16] Patrz wytyczne GR29 w sprawie oceny skutków dla ochrony danych na stronie: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[17] Należy zauważyć, że dane rejestru ułatwiające przeprowadzenie kontroli, np. przechowywania, modyfikacji lub usunięcia danych, również można uznać za dane osobowe powiązane z osobą, która rozpoczęła operację przetwarzania.

obecności naruszenia oraz oceny ryzyka.

- Należy zatem ocenić, jakie ryzyko dla osób fizycznych wynika z naruszenia (prawdopodobieństwo braku ryzyka, ryzyka lub wysokiego ryzyka) i poinformować odpowiednie działy organizacji.
- W przypadku takiej konieczności należy powiadomić organ nadzorczy i ewentualnie poinformować o naruszeniu osoby fizyczne, których ono dotyczy.
- Jednocześnie administrator powinien podjąć działania w celu zaradzenia naruszeniu i odzyskania danych.

Jasny powinien być również fakt, że na administratorze spoczywa obowiązek zareagowania na pierwsze zgłoszenie i stwierdzenie, czy naruszenie rzeczywiście miało miejsce. Ten krótki okres umożliwia przeprowadzenie dochodzenia w celu zebrania dowodów i ocenienia ryzyka, jeszcze zanim może pojawić się konieczność zgłoszenia naruszenia przez administratora. Jeśli jednak administrator stwierdzi z należytą pewnością, że doszło do naruszenia, i spełnione zostały warunki określone w art. 33 ust. 1, musi bez zbędnej zwłoki powiadomić organ nadzorczy – jeśli to możliwe w ciągu 72 godzin. Jeżeli administrator nie podejmie działań w odpowiednim czasie i stanie się oczywiste, że miało miejsce naruszenie, można to uznać za niewywiązanie się z obowiązku zgłoszenia określonego w art. 33.

Art. 32 wyjaśnia, że administrator i podmiot przetwarzający powinni wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić odpowiedni poziom bezpieczeństwa danych osobowych – umiejętność wykrywania, usuwania i zgłaszania naruszenia w odpowiednim czasie należy uznać za kluczowy aspekt tych środków.

3. Obowiązki podmiotu przetwarzającego

Administrator ponosi co prawda pełną odpowiedzialność za ochronę danych osobowych, podmiot przetwarzający odgrywa jednak ważną rolę wspierania administratora w wywiązywaniu się z obowiązków, włączając w to zgłaszanie naruszeń. Art. 28 ust. 3 wymaga, by przetwarzanie przez podmiot przetwarzający odbywało się na podstawie umowy lub innego instrumentu prawnego. Zgodnie z art. 28 ust. 3 lit. f umowa lub inny instrument prawny powinny stanowić, że podmiot przetwarzający „uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36".

Art. 33 ust. 2 jasno wskazuje, że jeżeli administrator korzysta z usług podmiotu przetwarzającego, podmiot taki po stwierdzeniu naruszenia ochrony danych osobowych musi zgłosić je administratorowi „bez zbędnej zwłoki". Administrator korzysta z usług podmiotu przetwarzającego dla własnych celów; co do zasady należy zatem uznać, że „stwierdza" naruszenie równocześnie z podmiotem przetwarzającym. Zobowiązanie podmiotu przetwarzającego do powiadomienia administratora pozwala administratorowi zająć się naruszeniem i określić, czy musi powiadomić organ nadzoru zgodnie z art. 33 ust. 1 oraz osoby, których dane naruszono, zgodnie z art. 34 ust. 1.

OROD nie podaje wyraźnego terminu, w którym podmiot przetwarzający ma powiadomić administratora, a jedynie stanowi, że musi tego dokonać „bez zbędnej zwłoki". W związku z tym GR29 zaleca, by podmiot przetwarzający natychmiast powiadomił administratora i sukcesywnie przekazywał dalsze informacje na temat naruszenia, kiedy tylko staną się dostępne. Jest to ważne, aby administrator mógł wywiązać się z obowiązku powiadomienia organu nadzorczego w ciągu 72 godzin.

Jeżeli podmiot przetwarzający świadczy usługi na rzecz wielu administratorów, którzy ucierpieli na skutek tego samego incydentu, wówczas musi powiadomić o szczegółach zdarzenia wszystkich administratorów.

Podmiot przetwarzający może dokonać zgłoszenia w imieniu administratora, jeżeli administrator nadał mu odpowiednie upoważnienie i sytuacje taką przewidują ustalenia umowne między

administratorem a podmiotem przetwarzającym. Zgłoszenia należy wówczas dokonać zgodnie z przepisami art. 33 i 34. Niemniej warto zauważyć, że odpowiedzialność prawna w związku ze zgłoszeniem leży po stronie administratora.

Jak wyjaśniono powyżej, administratorzy zobowiązani są określać w umowach z podmiotami przetwarzającymi, w jaki sposób należy wywiązywać się z zobowiązań określonych w art. 33 ust. 2.

B. Przekazywanie informacji organowi nadzorczemu

1. Informacje, które należy przekazać

Art. 33 ust. 3 stanowi, że w przypadku zgłaszania naruszenia organowi nadzorczemu administrator powinien 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."

OROD nie definiuje kategorii osób, których dane dotyczą, ani kategorii wpisów danych osobowych. GR29 sugeruje jednak, że kategorie osób, których dotyczą dane, powinny odwoływać się do rodzajów osób fizycznych, których dane osobowe naruszono – w zależności od użytych deskryptorów mogą to być m.in. dzieci i inne grupy wymagające szczególnej opieki, osoby z niepełnosprawnościami, pracownicy czy klienci. Podobnie, kategorie wpisów danych osobowych mogą odnosić się do różnych typów wpisów, które może przetwarzać administrator, takich jak dane o stanie zdrowia, dokumentacje placówek oświaty, informacje dotyczące opieki społecznej, szczegóły finansowe, numery rachunków bankowych, numery paszportów itd.

Z motywu 85 jasno wynika, że jednym z celów powiadamiania jest ograniczenie szkód u osób fizycznych. W związku z tym, jeżeli naruszenie wiąże się z ryzykiem konkretnej szkody ze względu na rodzaj osób, których dotyczą dane, lub rodzaj samych danych (np. kradzież tożsamości, oszustwo, strata finansowa, zagrożenie dla tajemnicy zawodowej), ważne jest, by zgłoszenie uwzględniało takie kategorie. W ten sposób łączy się to z wymogiem opisania prawdopodobnych konsekwencji naruszenia.

Brak bardziej precyzyjnych informacji (np. dokładnej liczby poszkodowanych osób, których dotyczą dane) nie powinien być przeszkodą dla terminowego zgłoszenia. OROD dopuszcza możliwość podania w przybliżeniu liczby osób fizycznych, których dane naruszono, i liczby objętych naruszeniem wpisów danych osobowych. Nacisk należy kłaść na usuwanie negatywnych skutków naruszenia, a nie na podawanie dokładnych danych liczbowych. Jeśli zatem stanie się jasne, że miało miejsce naruszenie, ale jego zakres nie jest jeszcze znany, bezpiecznym sposobem na wywiązanie się z obowiązku notyfikacyjnego jest powiadamianie sukcesywne (patrz niżej).

Art. 33 ust. 3 stanowi, że administrator „musi co najmniej" przekazać te informacje wraz ze zgłoszeniem, co oznacza, że w razie konieczności administrator może przekazać również dodatkowe szczegóły. Różne rodzaje naruszeń (poufności, integralności lub dostępności) mogą wymagać przekazania dalszych informacji w celu pełnego wyjaśnienia okoliczności poszczególnych spraw.

Przykład

W ramach powiadomienia organu nadzorczego administrator może uznać za przydatne podanie nazwy podmiotu przetwarzającego dane, jeżeli to on jest pierwotną przyczyną naruszenia, zwłaszcza jeśli doprowadził do zdarzenia, które wpłynęło na wpisy danych osobowych wielu innych administratorów korzystających z usług tego samego przedmiotu przetwarzającego.

Organ nadzoru może w każdym przypadku zażądać dalszych informacji w ramach dochodzenia w sprawie naruszenia.

2. Powiadamianie sukcesywne

W zależności od charakteru naruszenia konieczne może okazać się dalsze zbadanie sprawy przez administratora w celu ustalenia wszystkich istotnych faktów związanych ze zdarzeniem. Art. 33 ust. 4 stanowi w związku z tym:

„Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie bez zbędnej zwłoki."

OROD zakłada zatem, iż administratorzy nie zawsze będą dysponować wszystkimi potrzebnymi informacjami dotyczącymi naruszenia w ciągu 72 godzin od stwierdzenia go, jako że pełne, wyczerpujące dane na temat zdarzenia mogą nie zawsze być dostępne w tym początkowym okresie. Dlatego też rozporządzenie dopuszcza możliwość powiadamiania sukcesywnego. Bardziej prawdopodobne jest to w bardziej skomplikowanych przypadkach naruszenia, takich jak zagrożenia cybernetyczne, kiedy może okazać się konieczne podjęcie wnikliwego dochodzenia w celu pełnego ustalenia charakteru naruszenia i zakresu, w jakim narażono bezpieczeństwo danych osobowych. W związku z powyższym w wielu przypadkach administrator będzie musiał przeprowadzić bardziej dogłębne dochodzenie i podjąć działania następcze, kiedy będzie dysponować dodatkowymi informacjami w późniejszym terminie. Jest to dopuszczalne pod warunkiem, że administrator poda przyczyny opóźnienia zgodnie z art. 33 ust. 1. GR29 zaleca, by przy pierwszym powiadomieniu organu nadzorczego administrator poinformował go również o tym, kiedy będzie w stanie podać więcej informacji. Organ nadzorczy powinien uzgodnić sposób i termin podania dodatkowych informacji.

Głównym założeniem wymogu zgłaszania naruszeń jest zachęcanie administratorów do niezwłocznego podejmowania działań w związku z naruszeniem, zaradzania mu i – jeśli to możliwe – odzyskiwania narażonych danych osobowych, a także do zasięgania rady organu nadzorczego. Dzięki powiadomieniu organu nadzorczego w ciągu pierwszych 72 godzin administrator może mieć pewność co do prawidłowości podjętej decyzji o powiadomieniu lub niepowiadomieniu osób, których dotyczą dane.

Niemniej celem powiadomienia organu nadzorczego jest nie tylko uzyskanie wytycznych co do powiadomienia osób fizycznych, których dane naruszono. W pewnych przypadkach jasne jest, że ze względu na charakter naruszenia i powagę ryzyka administrator musi niezwłocznie powiadomić poszkodowane osoby. Przykładowo, w przypadku bezpośredniego zagrożenia kradzieżą tożsamości lub w przypadku ujawnienia szczególnych kategorii danych osobowych[18] w internecie administrator powinien bez zbędnej zwłoki podjąć działania w celu usunięcia naruszenia i powiadomienia o nim osób, których ono dotknęło (patrz pkt. IV). W wyjątkowych okolicznościach może to zrobić nawet przed powiadomieniem organu nadzorczego. Ogólnie rzecz biorąc, powiadomienie organu nadzoru nie może służyć za usprawiedliwienie niepowiadomienia o naruszeniu osoby, której dane dotyczą, pomimo istnienia takiego wymogu.

Powinno być również jasne, że po dokonaniu pierwotnego zgłoszenia administrator może

[18] Patrz art. 9.

przekazywać na bieżąco organowi nadzorczemu aktualne informacje w przypadku uzyskania w toku dochodzenia dowodów na to, że opanowano zdarzenie, a w rzeczywistości żadne naruszenie nie miało miejsca. Informację tę można dodać do informacji przekazanych już organowi nadzorczemu, a następnie zarejestrować odpowiednio zdarzenie jako zdarzenie niestanowiące naruszenia. Za zgłoszenie zdarzenia, które ostatecznie nie okaże się naruszeniem, nie przewiduje się żadnej kary.

Przykład

W ciągu 72 godzin od wykrycia naruszenia administrator powiadamia organ nadzoru o utracie płyty CD zawierającej kopię danych osobowych części jego klientów. Później niewłaściwie oznaczona płyta zostaje odnaleziona w lokalu administratora, a jej zawartość odzyskana. Administrator przekazuje organowi nadzorczemu aktualne informacje i prosi o zmianę powiadomienia.

Należy zauważyć, że podejście sukcesywne do powiadamiania o naruszeniach przewidują już obecne zobowiązania na mocy dyrektywy 2002/58/WE, rozporządzenia 611/2013 i w związku z innymi samodzielnie zgłaszanymi zdarzeniami.

3. Powiadamianie z opóźnieniem

Art. 33 ust. 1 jasno stanowi, że do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin należy dołączyć wyjaśnienie przyczyn opóźnienia. Zgodnie z tym zapisem oraz z pojęciem powiadomienia sukcesywnego uznaje się, że administrator może nie zawsze mieć możliwość zgłoszenia naruszenia w tym terminie, oraz dopuszcza powiadomienie z opóźnieniem.

Taki scenariusz może mieć miejsce w przypadku stwierdzenia przez administratora wielu podobnych naruszeń poufności w krótkim odcinku czasu, wpływających w taki sam sposób na osoby, których dotyczą dane. Administrator może stwierdzić naruszenie i w początkowej fazie dochodzenia, jeszcze przed powiadomieniem, wykryć kolejne, podobne naruszenia o różnych przyczynach. W zależności od okoliczności administratorowi może zająć trochę czasu ustalenie zakresu naruszeń i, zamiast zgłaszać każde naruszenie z osobna, administrator może dokonać jednego, kompleksowego zgłoszenia obejmującego szereg bardzo podobnych naruszeń o potencjalnie różnych przyczynach. Może to prowadzić to opóźnienia powiadomienia organu nadzorczego o więcej niż 72 godziny od czasu stwierdzenia naruszeń przez administratora.

Ściśle rzecz biorąc, każde naruszenie stanowi zdarzenie podlegające obowiązkowi sprawozdawczemu. Aby uniknąć nadmiernie uciążliwych formalności, administrator może dokonać „łącznego" zgłoszenia obejmującego wszystkie te naruszenia, pod warunkiem że dotyczą one tego samego rodzaju danych osobowych naruszonych w ten sam sposób w stosunkowo krótkim odcinku czasu. Jeżeli ma miejsce szereg naruszeń różnego rodzaju danych osobowych naruszonych na różne sposoby, wówczas zgłoszenie powinno nastąpić normalnie, przy czym każde naruszenie należy zgłosić zgodnie z art. 33.

Chociaż OROD dopuszcza możliwość opóźnienia zgłoszenia, nie należy uznawać tej możliwości za rozwiązanie w zwykłym trybie. Warto zaznaczyć, że łączne zgłoszenia mogą dotyczyć również wielu podobnych naruszeń zgłaszanych w ciągu 72 godzin.

C. Naruszenia dotykające osoby fizyczne w więcej niż jednym państwie członkowskim

W przypadkach transgranicznego przetwarzania[19] danych osobowych naruszenie może wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim. Art. 33 ust. 1 jasno stanowi, że w przypadku wystąpienia naruszenia administrator powinien zgłosić je organowi nadzorczemu właściwemu zgodnie z art. 55 OROD[20]. Art. 55 ust. 1 stanowi, co następuje:

[19] Patrz art. 4 ust. 23.
[20] Patrz również motyw 122.

„Każdy organ nadzorczy jest właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z niniejszym rozporządzeniem na terytorium swojego państwa członkowskiego.”

Art. 56 ust. 1 zaś stanowi:

„Bez uszczerbku dla art. 55 organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego jest właściwy do podejmowania działań jako wiodący organ nadzorczy – zgodnie z procedurą przewidzianą w Artykuł 60 – względem transgranicznego przetwarzania dokonywanego przez tego administratora lub ten podmiot przetwarzający.”

Ponadto art. 56 ust. 6 stanowi:

„Administrator lub podmiot przetwarzający komunikują się w sprawie dokonywanego przez nich transgranicznego przetwarzania jedynie z wiodącym organem nadzorczym.”

Oznacza to, że w każdym przypadku, gdy naruszenie dotyczy danych osobowych osób fizycznych w więcej niż jednym państwie członkowskim i wymagane jest zgłoszenie go, administrator musi powiadomić wiodący organ nadzorczy[21]. W związku z tym podczas przygotowywania planu reakcji na naruszenie administrator musi określić wiodący organ nadzorczy, który należy powiadomić[22]. Pozwoli to administratorowi szybko zareagować na naruszenie i wywiązać się z zobowiązań wynikających z art. 33. Jeżeli administrator ma jakiekolwiek wątpliwości w związku z określeniem wiodącego organu nadzorczego, powinien powiadomić przynajmniej lokalny organ nadzorczy właściwy dla miejsca naruszenia. Administrator może również chcieć zgłosić zdarzenie organowi nadzorczemu niebędącemu organem wiodącym, np. jeżeli wie, że naruszenie dotknęło również osoby fizyczne w innym państwie członkowskim. Jeżeli jednak administrator zdecyduje powiadomić jedynie wiodący organ nadzorczy, zaleca się, by w odpowiednich przypadkach określił, czy naruszenie dotyczy zakładów położonych w innych państwach członkowskich, a także w których państwach członkowskich naruszenie prawdopodobnie miało wpływ na osoby, których dane dotyczą.

D. Okoliczności, w których nie wymaga się powiadomienia

Art. 33 ust. 1 jasno stanowi, że przypadki, gdy „jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych”, nie wymagają powiadamiania organu nadzorczego. Przykładem może być sytuacja, w której dane osobowe są już ogólnodostępne, a ich ujawnienie nie stwarza ryzyka dla osoby fizycznej. Jest to niezgodne z obecnymi wymaganiami dotyczącymi zgłaszania naruszeń obowiązujących dostawców ogólnie dostępnych usług łączności elektronicznej zawartymi w dyrektywie 2009/136/WE, zgodnie z którymi wszystkie istotne naruszenia należy zgłaszać właściwemu organowi.

W swojej opinii 03/2014 w sprawie powiadomień o naruszeniu[23] GR29 wyjaśnia, że naruszenie poufności danych osobowych zaszyfrowanych algorytmem zgodnym z aktualnym stanem techniki nadal stanowi naruszenie danych osobowych i podlega obowiązkowi zgłoszenia. Jeśli jednak zachowano poufność klucza – tj. nie naruszono jego bezpieczeństwa i wygenerowano go w sposób niepozwalający na ustalenie jego treści przy pomocy dostępnych środków technicznych przez jakąkolwiek osobę nieupoważnioną do dostępu do niego – wówczas dane są co do zasady nieczytelne.

[21] Patrz wytyczne GR29 w sprawie określania wiodącego organu nadzorczego administratora lub podmiotu przetwarzającego dane, dostępne na stronie http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[22] Listę danych kontaktowych wszystkich europejskich krajowych organów ochrony danych można znaleźć na stronie: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[23] GR29, opinia 03/2014 w sprawie powiadomień o naruszeniu, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

W związku z tym istnieje więc niewielkie prawdopodobieństwo, ze naruszenie wpłynie na osoby fizyczne, a zatem nie wymaga się zawiadamiania ich[24]. Jednak nawet utrata lub zmiana zaszyfrowanych danych może mieć negatywne konsekwencje dla osób, których te dane dotyczą, jeżeli administrator nie ma odpowiednich kopii zapasowych. W takim przypadku wymagane jest poinformowanie osób, których dotyczą dane, nawet jeśli same dane zostały odpowiednio zaszyfrowane.

GR29 wyjaśniła również, że to samo tyczy się przypadków, w których dane osobowe, takie jak hasła, zostały bezpiecznie zaszyfrowane funkcją skrótu i ciągiem zaburzającym (solą), wartość skrótu określono za pomocą zgodnej ze stanem techniki kryptograficznej funkcji skrótu, klucz użyty do zaszyfrowania danych nie był zagrożony w związku z żadnym naruszeniem oraz został wygenerowany w sposób uniemożliwiający jego ustalenie przy pomocy dostępnych środków technicznych przez osobę nieupoważnioną do dostępu do danych.

Jeżeli więc dane osobowe stały się zasadniczo niemożliwe do odczytu dla osób nieupoważnionych i jeśli dane stanowią kopię lub istnieje dla nich kopia zapasowa, wówczas nie ma obowiązku zgłaszania organowi nadzorczemu naruszenia poufności odpowiednio zaszyfrowanych danych osobowych. Powodem jest tu małe prawdopodobieństwo, by naruszenie takie stwarzało ryzyko dla praw i wolności osób fizycznych. Oczywiście oznacza to, że nie trzeba również informować osoby fizycznej, ponieważ najprawdopodobniej nie występuje wysokie ryzyko. Należy mieć jednak na uwadze, że nawet jeśli powiadomienie nie jest początkowo wymagane ze względu na prawdopodobny brak ryzyka dla praw i wolności osób fizycznych, stan ten może z czasem ulec zmianie, prowadząc do konieczności ponownej oceny ryzyka. Na przykład jeżeli w późniejszym czasie okaże się, że narażono bezpieczeństwo klucza lub że oprogramowanie szyfrujące jest podatne na ataki, powiadomienie o naruszeniu może stać się konieczne.

Ponadto należy zauważyć, że w przypadku naruszenia w sytuacji braku kopii zapasowej szyfrowanych danych osobowych mamy do czynienia z naruszeniem dostępności, które może narazić osoby fizyczne na ryzyko i w związku z tym wymagać zgłoszenia. Podobnie przypadek naruszenia obejmującego utratę zaszyfrowanych danych, nawet jeśli istnieje kopia zapasowa danych osobowych, może podlegać obowiązkowi zgłoszenia w zależności od czasu potrzebnego do odtworzenia danych z kopii zapasowej i skutków niedostępności danych dla osób, których dotyczą. Zgodnie z art. 32 ust. 1 lit. c ważnym czynnikiem bezpieczeństwa jest „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego".

Przykład

Przykładem naruszenia niewymagającego powiadomienia organu nadzorczego może być utrata bezpiecznie zaszyfrowanego urządzenia mobilnego używanego przez administratora i jego personel. Jeżeli klucz szyfrowania pozostaje w posiadaniu administratora i jego personelu i nie jest to jedyna kopia danych osobowych, to dane te pozostają niedostępne dla atakującego. Oznacza to małe prawdopodobieństwo, by naruszenie stanowiło zagrożenie dla praw lub wolności osób, których dotyczą naruszone dane. Jeżeli w późniejszym czasie stanie się jasne, że naruszono bezpieczeństwo klucza szyfrowania lub że oprogramowanie czy algorytm są narażone na ataki, wówczas zmieni się ryzyko naruszenia praw i wolności osób fizycznych, a w związku z tym może powstać obowiązek zgłoszenia.

Jednakże do niespełnienia wymagań art. 33 dochodzi w przypadku, gdy administrator nie powiadomi organu nadzorczego, pomimo że danych nie zaszyfrowano bezpiecznie. W związku z tym przy wybieraniu oprogramowania szyfrującego administratorzy powinni uważnie przyjrzeć się jakości i właściwemu wdrożeniu oferowanego mechanizmu szyfrującego, zapoznać się z rzeczywistym zapewnianym poziomem ochrony i ocenić, czy jest odpowiedni dla istniejącego ryzyka. Administratorzy powinni również znać specyfikę działania produktów umożliwiających szyfrowania.

[24] Patrz również art. 4 ust. 1 i 2 rozporządzenia 611/2013.

Na przykład urządzenie może ulegać szyfrowaniu po wyłączeniu, ale nie przy przejściu w tryb czuwania. Niektóre produkty stosujące szyfrowanie mają „domyślny klucz", który należy zmieniać dla każdego klienta, aby zapewnić jego skuteczność. Nawet jeśli specjaliści ds. bezpieczeństwa uznają szyfrowanie za odpowiednie zgodnie z aktualnymi standardami, po kilku latach może się ono stać przestarzałe, co przekłada się na wątpliwości co do tego, czy produkt zapewnia wystarczające szyfrowanie i odpowiedni poziom ochrony.

III. **Artykuł 34 – Zawiadamianie osoby, której dane dotyczą**

A. Informowanie osób fizycznych

W niektórych przypadkach poza powiadomieniem organu nadzoru administrator zobowiązany jest powiadomić również osoby fizyczne, których dane naruszono.

Art. 34 ust. 1 stanowi:

> „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."

Administratorzy powinni pamiętać, że powiadomienie organu nadzorczego jest obowiązkowe w przypadku, gdy naruszenie może narazić osoby fizyczne na ryzyko. Ponadto w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych w konsekwencji naruszenia należy poinformować także te osoby. Próg, od którego zależy obowiązek powiadomienia osób fizycznych o naruszeniu ich danych, jest zatem wyższy niż próg, od którego zależy obowiązek zgłoszenia naruszenia organom nadzorczym; osób fizycznych nie trzeba powiadamiać o wszystkich naruszeniach, co pozwala chronić je przed zbędnym obciążeniem związanym z powiadomieniem.

OROD stanowi, że osoby fizyczne należy informować o naruszeniu ich danych „bez zbędnej zwłoki", czy tak szybko, jak to możliwe. Głównym celem powiadamiania osób fizycznych jest przekazanie im konkretnych informacji dotyczących kroków, jakie powinny podjąć, by zapewnić sobie bezpieczeństwo[25]. Jak zauważono powyżej, w zależności od charakteru naruszenia i stwarzanego przez nie ryzyka poinformowanie na czas osób fizycznych może pomóc im ochronić się przed negatywnymi skutkami naruszenia.

Załącznik B do niniejszych wytycznych zawiera niewyczerpującą listę przypadków, w których naruszenie może narazić osoby fizyczne na wysokie ryzyko, a zatem nakładających na administratora obowiązek powiadomienia osób, których dane naruszono.

B. Informacje, które należy przekazać

W kwestii zawiadamiania osób fizycznych art. 34 ust. 2 stanowi, co następuje:

> „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 Artykuł 33 ust. 3 lit. b), c) i d)."

Zgodnie z tym przepisem administrator powinien podać przynajmniej następujące informacje:

- opis charakteru naruszenia;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego;

[25] Patrz również motyw 86.

- opis prawdopodobnych skutków naruszenia;
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Przykładowo w ramach kroków podejmowanych w celu zaradzenia naruszeniu i ograniczenia jego potencjalnych negatywnych skutków administrator może oświadczyć, że po zgłoszeniu naruszenia właściwemu organowi nadzorczemu otrzymał radę w sprawie zaradzenia naruszeniu i zmniejszenia jego skutków. W stosownych przypadkach administrator powinien również przekazać odpowiednią poradę osobom, których dane naruszono, tak aby mogły się ochronić przed potencjalnymi negatywnymi skutkami naruszenia, np. zresetować hasła w przypadku naruszenia bezpieczeństwa ich danych dostępu. Ponownie administrator może postanowić przekazać więcej informacji niż jest to wymagane.

C. Kontaktowanie się z osobami fizycznymi

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

Do powiadamiania osób, których dane naruszono, należy stosować komunikaty dedykowane, których nie należy przesyłać razem z innymi informacjami, takimi jak bieżące informacje, newslettery czy standardowe wiadomości. Pomoże to przekazać informacje o naruszeniu w jasny i przejrzysty sposób.

Przykładami przejrzystych metod komunikacji są: bezpośrednie wiadomości (np. e-mail, SMS, bezpośrednia wiadomość), widoczne banery na stronach internetowych lub powiadomienia, przesyłki pocztowe i widoczne reklamy w prasie. Powiadomienia ograniczającego się do komunikatu prasowego czy firmowego bloga nie uznaje się za skuteczne poinformowanie osoby fizycznej o naruszeniu. GR29 zaleca administratorom wybranie środków zwiększających szansę właściwego przekazania informacji wszystkim osobom, których dane naruszono. W zależności od okoliczności może to oznaczać, że administrator zastosuje kilka sposobów komunikacji zamiast korzystać z jednego kanału kontaktu.

Administratorzy mogą również stanąć przed koniecznością zapewnienia dostępności komunikatu w odpowiedniej formie zamiennej i we właściwym języku, tak aby osoby, których dane naruszono, mogły zrozumieć przekazywane informacje. Przykładowo komunikacja w języku ojczystym odbiorcy pozwoli mu zrozumieć charakter naruszenia i kroki, które może podjąć, by zapewnić sobie ochronę.

Administratorzy mają największe możliwości określenia najbardziej odpowiedniego kanału komunikacji do poinformowania osób fizycznych o naruszeniu, zwłaszcza w przypadku częstych kontaktów z klientami. Administrator powinien jednak podchodzić z ostrożnością do kanału komunikacji, którego bezpieczeństwo zostało narażone, ponieważ mogą z niego korzystać również osoby niepowołane, podszywające się pod administratora.

Ponadto zgodnie z motywem 86:

„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.”

Administratorzy mogą zatem chcieć skontaktować się z organem nadzorczym, by zasięgnąć rady nie tylko w sprawie informowania o naruszeniu osób, których dotyczą dane, zgodnie z art. 34, ale również w sprawie treści wiadomości dla takich osób i najodpowiedniejszej drogi ich przekazania.

D. Okoliczności, w których nie wymaga się powiadomienia

Art. 34 ust. 3 podaje trzy warunki, których spełnienie znosi wymóg powiadomienia osób fizycznych o naruszeniu ich danych. Są one następujące:

- Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony danych osobowych, których dotyczy naruszenie, w szczególności środki uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych. Dotyczy to na przykład przypadków zabezpieczenia danych osobowych za pomocą szyfrowania zgodnego z aktualnym stanem techniki.
- Natychmiast po naruszeniu administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej, której dane dotyczą. Na przykład, w zależności od okoliczności sprawy administrator może niezwłocznie zidentyfikować osobę, która uzyskała dostęp do danych osobowych, i podjąć działania przeciwko takiej osobie jeszcze zanim zdoła ona cokolwiek zrobić z danymi. Należy odpowiednio rozważyć możliwe konsekwencje każdego przypadku naruszenia poufności – ponownie w zależności od charakteru danych.
- Skontaktowanie się z osobami, których dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku[26], na przykład w sytuacji, gdy ich dane kontaktowe zostały utracone w wyniku naruszenia lub nie były nigdy znane. Przykład: magazyn urzędu statystycznego uległ zalaniu, a dokumenty zawierające dane osobowe przechowywano jedynie w formie papierowej. Administrator musi zatem przekazać odpowiednie informacje do wiadomości publicznej lub podjąć podobne działania, aby równie skutecznie poinformować osoby, których dane dotyczą. W przypadku niewspółmiernie dużego wysiłku można również wdrożyć środki techniczne zapewniające dostępność informacji o naruszeniu na żądanie, co może okazać się przydatne dla osób, których dane naruszono, a z którymi administrator nie może skontaktować się w inny sposób.

Zgodnie z zasadą rozliczalności administratorzy powinni być w stanie wykazać przed organem nadzorczym, że spełnili przynajmniej jeden z powyższych warunków[27]. Należy mieć na uwadze, że nawet jeśli powiadomienie nie jest początkowo wymagane ze względu na brak zagrożenia dla praw i wolności osób fizycznych, stan ten może z czasem ulec zmianie, prowadząc do konieczności ponownej oceny ryzyka.

Jeżeli administrator postanowi nie powiadamiać osoby, której naruszenie dotyczy, zgodnie z art. 34 ust. 4 organ nadzorczy może od niego tego zażądać w przypadku uznania, że naruszenia może narazić te osoby na wysokie ryzyko. Ewentualnie może uznać, że zostały spełnione warunki określone w art. 34 ust. 3, a zatem powiadomienie osób fizycznych nie jest wymagane. Jeżeli organ nadzorczy uzna decyzję o niepowiadamianiu osób, których dotyczą dane, za nieuzasadnioną, może rozważyć skorzystanie z dostępnych mu uprawnień i sankcji.

IV. **Ocena ryzyka i wysokiego ryzyka**

A. Ryzyko jako czynnik warunkujący zgłoszenie

Mimo że OROD wprowadza obowiązek zgłoszenia naruszenia, nie jest ono wymagane w każdych okolicznościach:

[26] Więcej informacji znajdzie się w nadchodzących wytycznych GR29 w sprawie przejrzystości, które uwzględnią kwestię niewspółmiernie dużego wysiłku.
[27] Patrz art. 5 ust. 2.

- Powiadomienie właściwego organu nadzorczego jest wymagane tylko w przypadku prawdopodobieństwa wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych.
- Powiadomienie osoby fizycznej o naruszeniu jest wymagane tylko w przypadku prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia praw lub wolności tej osoby.

Oznacza to, że jest niezwykle ważne, by natychmiast po stwierdzeniu naruszenia administrator nie tylko starał się opanować zdarzenie, ale także ocenił ryzyko, jakie może ono stworzyć. Są ku temu dwie ważne przyczyny: po pierwsze, znajomość prawdopodobieństwa i powagi potencjalnych skutków dla osoby, której dane dotyczą, pomoże administratorowi podjąć skuteczne działania w celu opanowania naruszenia i zaradzeniu mu; po drugie, pomoże mu to ustalić, czy konieczne jest powiadomienie organu nadzorczego, a w stosownych przypadkach także samych osób.

Jak wyjaśniono powyżej, głównym czynnikiem warunkującym konieczność zgłoszenia naruszenia jest potencjalne ryzyko naruszenia praw i wolności osób fizycznych, zaś głównym czynnikiem warunkującym konieczność zgłoszenia naruszenia osobom fizycznym jest *wysokie* ryzyko naruszenia praw lub wolności tych osób. Ryzyko jest obecne, kiedy naruszenie może skutkować fizyczną, materialną lub niematerialna szkodą dla osób fizycznych, których dane naruszono. Przykłady takich szkód to dyskryminacja, kradzież tożsamości lub oszustwo dotyczące tożsamości, naruszenie dobrego imienia. 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, wyroków skazujących i naruszeń prawa lub związanych z nimi środków bezpieczeństwa, należy uznać, że występuje duże prawdopodobieństwo takiej szkody[28].

B. Czynniki do wzięcia pod rozwagę przy ocenie ryzyka:

Zgodnie z motywami 75 i 76 OROD przy ocenie ryzyka należy ogólnie rzecz biorąc uwzględnić zarówno prawdopodobieństwo, jak i potencjalną powagę ryzyka naruszenia praw i wolności osób, których dotyczą dane. Ponadto stanowią one, że ryzyko należy szacować na podstawie obiektywnej oceny.

Należy zauważyć, że ocena ryzyka dla praw i wolności w wyniku naruszenia skupia się na innych zagadnieniach niż ocena skutków dla ochrony danych[29]. Ocena skutków dla ochrony danych dotyczy zarówno ryzyka związanego z przetwarzaniem danych zgodnie z planem, jak i ryzyka w przypadku naruszenia. Biorąc pod rozwagę potencjalne naruszenie, administrator dokonuje ogólnej oceny prawdopodobieństwa jego wystąpienia oraz szkody, jaką może ponieść osoba, którą dotyczą dane; innymi słowy – oceny hipotetycznego zdarzenia. W przypadku rzeczywistego naruszenia zdarzenie już miało miejsce, a zatem należy całkowicie skupić się na wynikającym z naruszenia ryzyku dla osób fizycznych.

[28] Patrz motyw 75 i motyw 85.

[29] Patrz wytyczne GR w sprawie oceny skutków dla ochrony danych na stronie: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Przykład

Zgodnie z wytycznymi oceny skutków dla ochrony danych proponowane stosowanie konkretnego oprogramowania bezpieczeństwa do ochrony danych osobowych jest odpowiednim środkiem zapewniającym poziom ochrony adekwatny do ryzyka, na jakie przetwarzanie danych narażałoby w przeciwnym razie osoby fizyczne. Jeśli jednak słaby punkt stanie się znany, może to sprawić, że oprogramowanie nie będzie już odpowiednie do opanowania ryzyka naruszenia chronionych danych osobowych, w związku z czym konieczna będzie ponowna jego ocena w ramach bieżącej oceny skutków dla ochrony danych.

Słabość produktu zostaje później wykorzystana i ma miejsce naruszenie. Administrator powinien ocenić szczególne okoliczności naruszenia, naruszone dane i poziom potencjalnych skutków dla osób fizycznych, a także prawdopodobieństwo materializacji ryzyka.

Podobnie przy ocenie ryzyka dla osób fizycznych administrator weźmie pod uwagę szczególne okoliczności naruszenia, w tym jego powagę i potencjalne skutki. GR29 zaleca zatem, by przy ocenie ryzyka wziąć pod rozwagę następujące kryteria[30]:

- Rodzaj naruszenia

Rodzaj naruszenia może mieć wpływ na poziom ryzyka dla osób fizycznych. Na przykład naruszenie poufności, w wyniku którego osobom nieupoważnionym ujawniono informacje medyczne, może mieć inne konsekwencje dla osób poszkodowanych niż naruszenie polegające na utracie danych medycznych lub dostępu do nich.

- Charakter, wrażliwość i rozmiar danych osobowych

Kluczowym czynnikiem przy ocenie ryzyka jest oczywiście rodzaj i wrażliwość danych osobowych narażonych na niebezpieczeństwo w wyniku naruszenia. Zazwyczaj ryzyko szkody dla osób poszkodowanych rośnie wraz ze wzrostem wrażliwości danych, jednak należy mieć na uwadze również inne dane osobowe na temat tych osób, które mogą być już publicznie dostępne. Na przykład, w zwyczajnych okolicznościach jest mało prawdopodobne, by ujawnienie nazwiska i adresu osoby fizycznej mogło doprowadzić do istotnej szkody. Z kolei ujawnienie nazwiska i adresu rodzica przysposabiającego rodzicowi biologicznemu może mieć bardzo poważne konsekwencje zarówno dla rodzica przysposabiającego, jak i dla dziecka.

Naruszenia dotyczące danych o stanie zdrowia, dokumentów tożsamości lub danych finansowych, np. danych karty kredytowej, mogą spowodować szkodę także z osobna, ale w połączeniu mogą posłużyć do kradzieży tożsamości. Połączenie danych osobowych jest zazwyczaj bardziej problematyczne niż pojedynczy typ danych.

Niektóre rodzaje danych osobowych mogą początkowo wydawać się nieszkodliwe, jednakże należy dobrze zastanowić się, co określone dane mogą ujawnić na temat osób, których dotyczą. Lista klientów odbierających regularnie dostawy nie musi stanowić szczególnie wrażliwych danych, ale te same informacje dotyczące klientów, którzy poprosili o wstrzymanie dostaw na czas ich urlopu, mogą okazać się użyteczne dla przestępców.

Z kolei mała ilość bardzo wrażliwych danych może mieć duży wpływ na osobę, której dotyczą, zaś duży zakres danych może doprowadzić do ujawnienia jeszcze większej ilości informacji na jej temat.

[30] Art. 3 ust. 2 rozporządzenia 611/2013 podaje wytyczne dotyczące czynników, które należy brać pod uwagę w związku ze zgłaszaniem naruszeń w sektorze usług łączności elektronicznej, użytecznych w kontekście powiadomień zgodnie z OROD.

Ponadto naruszenie obejmujące duże ilości danych osobowych może mieć wpływ na odpowiednio dużą liczbę osób.

- Łatwość identyfikacji osób fizycznych

Ważnym czynnikiem do wzięcia pod uwagę przy określaniu łatwości, z jaką osoba trzecia może wykorzystać dane osobowe, do których uzyskała dostęp, by ustalić tożsamość poszczególnych osób fizycznych lub dopasować te dane do innych informacji w tym samym celu. W zależności od okoliczności ustalenie tożsamości może okazać się możliwe bezpośrednio na podstawie danych osobowych bez konieczności dalszego dochodzenia, zaś z drugiej strony dopasowanie danych osobowych do konkretnej osoby może być wyjątkowo trudne, ale nadal możliwe w określonych warunkach. Identyfikacja może okazać się możliwa bezpośrednio lub pośrednio na podstawie naruszonych danych, ale może również zależeć od kontekstu konkretnego naruszenia i publicznej dostępności powiązanych danych osobowych. Zagadnienie to jest bardziej istotne w przypadku naruszeń poufności i dostępności. Jak stwierdzono powyżej, dane osobowe chronione odpowiednim poziomem szyfrowania będą nieczytelne dla nieupoważnionych osób nieposiadających klucza deszyfrującego. Pseudonimizacja, czyli proces pozbawiania danych elementów pozwalających na identyfikację, w ramach którego do wpisu dołącza się zakodowany znacznik lub pseudonim pozwalający na powiązanie go z daną osobą bez identyfikowania jej, może zminimalizować prawdopodobieństwo ustalenia tożsamości osób poszkodowanych w wyniku naruszenia.

- Skala konsekwencji dla osób fizycznych.

W zależności od charakteru danych osobowych objętych naruszeniem (np. specjalne kategorie danych) potencjalna szkoda dla osób fizycznych może okazać się nadzwyczaj dotkliwa, zwłaszcza w przypadku naruszeń prowadzących do kradzieży lub sfałszowania tożsamości, szkody fizycznej, stresu psychicznego, upokorzenia lub naruszenia dobrego imienia. Jeżeli naruszenie obejmuje dane osobowe dotyczące osób w szczególne trudnej sytuacji, jego skutkiem może być narażenie ich na jeszcze większe ryzyko szkody.

Wpływ na poziom potencjalnego ryzyka może mieć również to, czy zgodnie z wiedzą administratora dane osobowe znajdują się w rękach osób o nieznanych lub wrogich zamiarach. Może wystąpić naruszenie poufności, polegające na przypadkowym ujawnieniu danych osobowych osobie trzeciej w rozumieniu art. 4 ust. 10 lub innemu odbiorcy. Ma to miejsce na przykład w sytuacji przypadkowego przesłania danych osobowych do niewłaściwego działu organizacji lub do powszechnie stosowanego dostawcy. Administrator może wówczas poprosić odbiorcę o zwrot lub bezpieczne zniszczenie otrzymanych w taki sposób danych. W obu przypadkach, jeżeli administrator jest z odbiorcą w trwających stosunkach zna stosowane przez niego procedury, jego historię i inne istotne szczegóły, odbiorcę można uznać za „zaufanego". Innymi słowy, administrator może mieć uzasadnioną pewność co do odbiorcy i w związku z tym spodziewać się, że nie odczyta on ani nie skorzysta z dostępu do przesłanych niewłaściwie danych, lecz postąpi zgodnie z instrukcjami dotyczącymi ich zwrotu. Nawet jeśli uzyskano dostęp do danych, administrator może mimo wszystko mieć co do odbiorcy zaufanie, że nie podejmie on żadnych dalszych działań w związku z danymi, niezwłocznie zwróci je administratorowi i będzie współpracować przy ich odzyskiwaniu. Takie przypadki można uwzględnić w ocenie ryzyka przeprowadzanej przez administratora w następstwie naruszenia – zaufanie do odbiorcy może zmniejszyć dotkliwość skutków naruszenia, ale nie oznacza, że naruszenie nie miało miejsca. Może jednak skutkować wyeliminowaniem prawdopodobieństwa ryzyka dla osób fizycznych, w związku z czym nie wymaga się już powiadamiania organu nadzorczego ani osób, których dane naruszono. Ponownie, zależy to od konkretnego przypadku. Administrator musi jednak zachować informacje dotyczące naruszenia w ramach ogólnego obowiązku prowadzenia ewidencji naruszeń (patrz pkt. VI poniżej).

Należy również wziąć pod rozwagę czas trwania konsekwencji naruszenia dla osób fizycznych, jako że skutki długoterminowe uznaje się za bardziej dotkliwe.

- Cechy szczególne osoby fizycznej

Naruszenie może dotyczyć danych dzieci lub innych osób wymagających szczególnej opieki, które w wyniku naruszenia mogą zostać narażone na większe ryzyko. Również inne cechy osoby poszkodowanej mogą warunkować skutki naruszenia dla tych osób.

- Liczba osób poszkodowanych

Naruszenie może dotyczyć zaledwie jednej czy kilku osób fizycznych lub kilku tysięcy, a nawet większej ich liczby. Ogólnie rzecz biorąc, im większa liczba osób poszkodowanych, tym poważniejsze skutki może mieć naruszenie. Naruszenie może mieć poważne skutki dla tylko jednej osoby w zależności od rodzaju i kontekstu danych osobowych, które naruszono.

- Cechy szczególne administratora danych

Rodzaj i rola administratora mogą mieć wpływ na poziom ryzyka wynikającego z naruszenia dla osób fizycznych. Na przykład zakład opieki zdrowotnej przetwarza szczególne kategorie danych osobowych, co oznacza, że naruszenie takich danych będzie stanowić większe zagrożenie dla osób poszkodowanych niż ujawnienie listy dystrybucyjnej czasopisma.

- Zagadnienia ogólne

W związku z powyższym przy ocenie ryzyka będącego prawdopodobnym skutkiem naruszenia administrator powinien rozważyć powagę możliwych skutków dla praw i wolności osób fizycznych w połączeniu z prawdopodobieństwem ich wystąpienia. Jasne jest, że w przypadku poważniejszych konsekwencji naruszenia ryzyko jest wyższe; podobnie ryzyko jest podwyższone w przypadku większego prawdopodobieństwa ich wystąpienia. W przypadku wątpliwości administrator powinien wykazać się raczej nadmierną ostrożnością niż jej brakiem i zgłosić naruszenie. Załącznik B podaje przydatne przykłady różnych rodzajów naruszeń narażających osoby fizyczne na ryzyko lub wysokie ryzyko.

Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA) wydała zalecenia dotyczące metodologii oceny powagi naruszenia, które administratorzy i podmioty przetwarzające dane mogą uznać za przydatne podczas tworzenia planu reakcji na naruszenie[31].

V. **Rozliczalność i prowadzenie rejestru**

A. Dokumentowanie naruszeń

Niezależnie od tego, czy naruszenia wymaga zgłoszenia organowi nadzorczemu, administrator musi prowadzić dokumentację wszystkich naruszeń zgodnie z art. 33 ust. 5:

> „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."

Łączy się to z zasadą rozliczalności przewidzianą w art. 5 ust. 2 OROD. Zachęca się zatem administratorów do zakładania wewnętrznej ewidencji naruszeń, niezależnie od obowiązku ich zgłaszania lub jego braku[32].

[31] ENISA, Zalecenia w sprawie metodologii oceny powagi naruszeń danych osobowych, https://www.enisa.europa.eu/publications/dbn-severity

[32] Administrator może postanowić udokumentować naruszenia we własnym rejestrze czynności przetwarzania prowadzonej zgodnie z art. 30. Nie wymaga się prowadzenia osobnego rejestru, jeżeli informacje dotyczące naruszenia można łatwo zidentyfikować i przedłożyć na żądanie.

Chociaż to administrator określa sposób i strukturę dokumentacji naruszeń, istnieją pewne zasadnicze zasady dotyczące rejestrowanych informacji, które muszą zostać zawarte w każdym przypadku. Zgodnie z wymaganiami art. 33 ust. 5 administrator musi rejestrować informacje o naruszeniu obejmujące jego przyczyny, przebieg i naruszone dane osobowe. Powinny one również zawierać skutki i konsekwencje naruszenia oraz działania naprawcze podjęte przez administratora.

Oprócz tych informacji GR29 zaleca również dokumentowanie uzasadnienia decyzji podjętej w odpowiedzi na naruszenie. W szczególności należy udokumentować powody decyzji w przypadku niezgłoszenia naruszenia. Należy podać przyczyny, dla których administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne[33]. Ewentualnie, jeżeli administrator uzna, że spełniony jest któryś z warunków opisanych w art. 34 ust. 3, powinien być w stanie przedstawić odpowiednie dowody takiego stanu rzeczy.

W przypadku gdy administrator zgłosi naruszenie organowi nadzorczemu, ale zrobi to z opóźnieniem, musi być w stanie przedstawić przyczyny takiego opóźnienia; powiązana dokumentacja może pomóc wykazać, że było ono uzasadnione i nienadmierne.

Przy powiadamianiu osób fizycznych o naruszeniu ich danych administrator powinien przedstawić naruszenie w przejrzysty sposób i poinformować o nim skutecznie i terminowo. Ponadto zachowanie dowodów powiadomienia pomoże mu to wykazać rozliczalność i zgodność z przepisami.

Z punktu widzenia zgodności z art. 33 i 34 korzystne jest, by zarówno administratorzy, jak i podmioty przetwarzające stosowały udokumentowana procedurę zgłoszeń określającą zasady postępowania na wypadek wykrycia naruszenia, w tym sposoby opanowania incydentu i zaradzenia mu, jak również obejmującą ocenę ryzyka i zgłaszanie naruszenia. Z tego względu do wykazania zgodności z przepisami OROD może być również przydatne wykazanie, że pracownicy zostali poinformowani o istnieniu tego rodzaju procedur i mechanizmów oraz wiedzą, jak powinni reagować na naruszenia.

Należy zauważyć, że nieudokumentowanie naruszenia we właściwy sposób może prowadzić do wykonania przez organ nadzorczych uprawnień na mocy art. 58 lub nałożenia administracyjnej kary pieniężnej zgodnie z art. 83.

B. Rola inspektora ochrony danych

Administrator lub podmiot przetwarzający dane może mieć swojego inspektora ochrony danych (IOD)[34] zgodnie z wymaganiami art. 37 lub dobrowolnie w ramach dobrych praktyk. Art. 39 OROD określa szereg obowiązkowych zadań IOD, ale nie zabrania przydzielania kolejnych zadań administratorowi w przypadku takiej potrzeby.

Do najistotniejszych zadań IOD w zakresie zgłaszania naruszeń należą: współpraca z organem nadzorczym oraz działanie w charakterze punktu kontaktowego dla organu nadzorczego i osób, których dotyczą dane. Należy również zauważyć, że w przypadku zgłoszenia naruszenia danych organowi nadzorczemu zgodnie z art. 33 ust. 3 lit. b administrator zobowiązany jest podać nazwisko i dane kontaktowe swojego IOD lub innego punktu kontaktowego. Oznacza to, że IOD może odgrywać ważną rolę przy zgłaszaniu naruszenia i podczas dalszego dochodzenia prowadzonego przez organ nadzorczy.

VI. Obowiązki notyfikacyjne na mocy innych instrumentów prawnych

Poza obowiązkiem zgłaszania i informowania o naruszeniach zgodnie z OROD administratorzy powinni znać również dotyczące ich wymagania w zakresie zgłaszania konkretnych naruszeń danych osobowych na mocy obowiązujących przepisów, które mogą się różnić w zależności od państwa członkowskiego, np.:

[33] Patrz motyw 85.
[34] Patrz wytyczne GR w sprawie IOD: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

- Rozporządzenie (EU) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS)[35].

Rozporządzenie nakłada na dostawców usług zaufania obowiązek zgłaszania naruszeń do właściwego organu nadzorczego.

- Dyrektywa (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[36].

Zarówno podmioty świadczące usługi podstawowe, jak i dostawcy usług cyfrowych zobowiązani są do zgłaszania właściwemu organowi nadzorczemu zdarzeń naruszających ochronę, które mogą dotyczyć danych osobowych.

Przykład

Dostawca usługi w chmurze zgłaszający naruszenie na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji może również stanąć przed koniecznością powiadomienia administratora, jeżeli naruszenie dotyczy danych osobowych. Podobnie od dostawcy usług zaufania zgłaszającego naruszenie zgodnie z rozporządzeniem eIDAS może być wymagane powiadomienie właściwego organu ochrony danych.

- Dyrektywa 2009/136/WE (dyrektywa o prawach obywateli) i rozporządzenie 611/2013 (rozporządzenie w sprawie powiadamiania o naruszeniu).

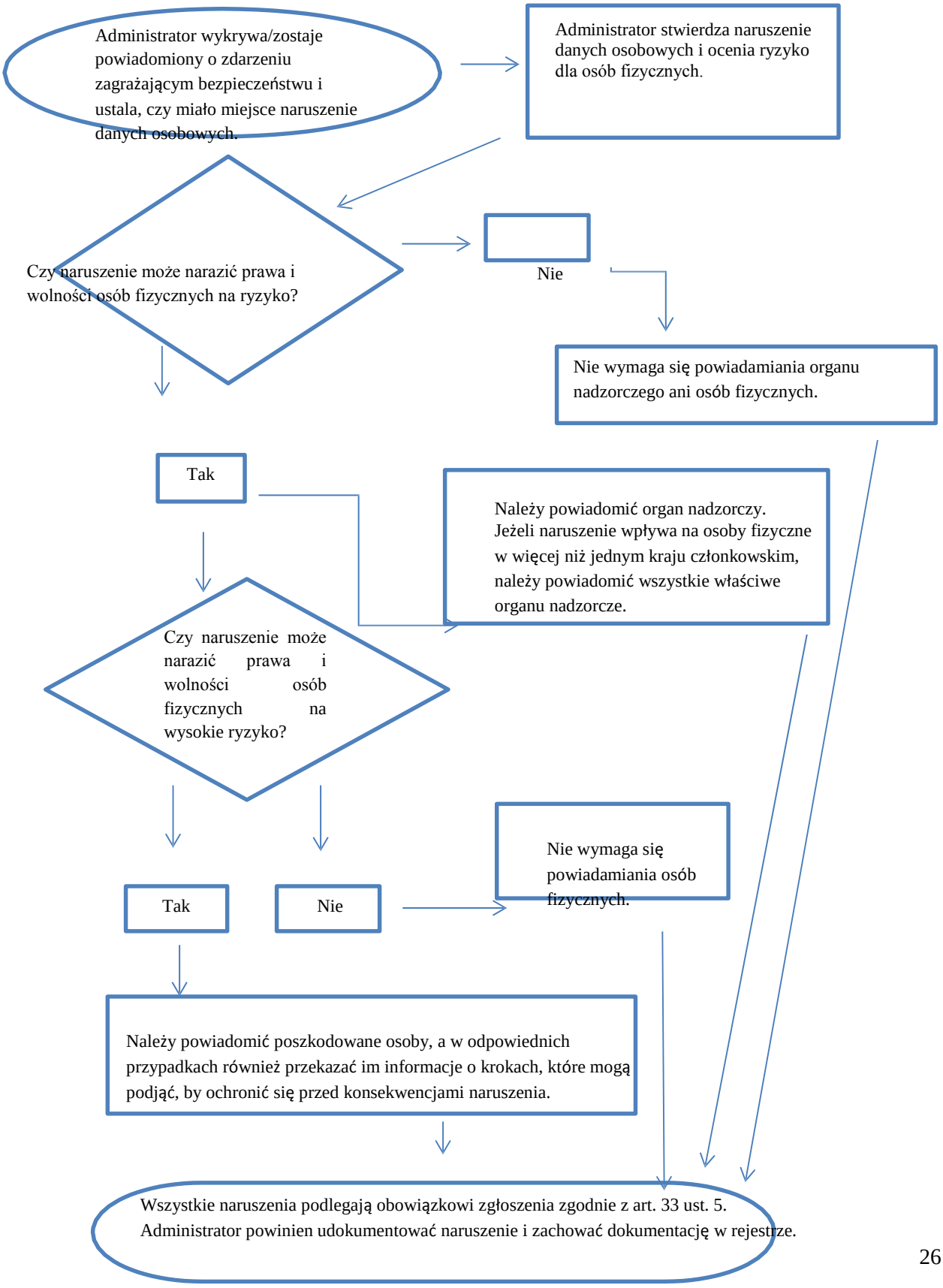
Dostawcy ogólnie dostępnych usług łączności elektronicznej w rozumieniu dyrektywy 2002/58/WE[37] muszą zgłaszać naruszenia właściwym organom krajowym.

Administratorzy powinni również znać wszelkie dodatkowe obowiązki notyfikacyjne o charakterze prawnym, medycznym lub zawodowym wynikające z obowiązujących przepisów prawa.

[35] Patrz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG
[36] Patrz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG
[37] 10 stycznia 2017 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia o prywatności i łączności elektronicznej, które zastąpi dyrektywę 2009/136/WE i zniesie wymóg powiadamiania. Jednakże do czasu zatwierdzenia wniosku przez Parlament Europejski w mocy pozostają obecne wymagania dotyczące powiadamiania – patrz https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic- communications

VII. **Załącznik**

A. Schemat przedstawiający wymagania dotyczące powiadamiania



A. Przykłady naruszeń danych osobowych i podmioty, którym należy je zgłaszać

Poniższa niewyczerpująca lista przykładów pomoże administratorom określić, czy muszą zgłosić naruszenie danych osobowych w zależności od przypadku. Przykłady mogą stanowić pomoc przy rozróżnianiu przypadków ryzyka i wysokiego ryzyka naruszenia praw i wolności osób fizycznych.

Przykład	**Czy należy powiadomić organ nadzorczy?**	**Czy należy powiadomić osobę, której dotyczą dane?**	**Uwagi/zalecenia**
i. Administrator przechowywał kopię zapasową archiwum danych osobowych zaszyfrowaną na płycie CD. Płytę skradziono podczas włamania.	Nie.	Nie.	Jeżeli dane są zaszyfrowane za pomocą algorytmu zgodnego ze stanem techniki, istnieją kopie zapasowe danych, a unikalny klucz jest bezpieczny, może to być naruszenie niepodlegające obowiązkowi zgłoszenia. Jeżeli jednak w późniejszym czasie coś zagrozi temu bezpieczeństwu, powiadomienie będzie wymagane.
ii. Dane osobowe osób fizycznych wyprowadzono w wyniku cyberataku z bezpiecznej strony internetowej zarządzanej przez administratora. Administrator ma klientów w jednym kraju członkowskim.	Tak, należy powiadomić właściwy organ nadzorczy, jeżeli istnieje możliwość konsekwencji dla osób fizycznych.	Tak, należy powiadomić osoby fizyczne w zależności od rodzaju naruszonych danych osobowych, jeżeli potencjalne konsekwencje dla tych osób są poważne.	Jeżeli ryzyko nie jest wysokie, zalecamy administratorom powiadomienie osób, których dotyczą dane, w zależności od okoliczności sprawy. Na przykład, powiadomienie może nie być konieczne w przypadku naruszenia poufności związanego z newsletterem programu telewizyjnego, ale będzie wymagane, jeżeli newsletter może doprowadzić do ujawnienia poglądów politycznych osób, których dotyczą dane.
iii. Z powodu krótkotrwałej przerwy w dostawie prądu w centrum telefonicznym administratora klienci nie mogli się dodzwonić i uzyskać dostęp do swoich danych.	Nie.	Nie.	To nie jest naruszenie danych osobowych podlegające obowiązkowi zgłoszenia; niemniej, zdarzenie należy zarejestrować zgodnie z art. 33 ust. 5. Administrator

Przykład	Czy należy powiadomić organ nadzorczy?	Czy należy powiadomić osobę, której dotyczą dane?	Uwagi/zalecenia
			powinien prowadzić odpowiedni rejestr.
iv. Na administratora przeprowadzono atak za pomocą oprogramowania typu ransomware, w wyniku którego wszystkie dane zostały zaszyfrowane. Nie istnieją kopie zapasowe i nie można odzyskać danych. W toku dochodzenia staje się jasne, że oprogramowanie jedynie szyfruje dane, a w systemie nie wykryto żadnego innego złośliwego oprogramowania.	Tak, należy powiadomić właściwy organ nadzorczy, jeżeli istnieje możliwość konsekwencji dla osób fizycznych, ponieważ doszło do utraty dostępności.	Tak, należy powiadomić osoby fizyczne w zależności od charakteru naruszonych danych osobowych i możliwych skutków braku dostępu do danych oraz innych prawdopodobnych konsekwencji.	Jeżeli istniały kopie zapasowe i możliwe jest odzyskanie danych w odpowiednim czasie, o zdarzeniu nie trzeba powiadamiać organu nadzorczego ani osób fizycznych, ponieważ nie doszło do trwałej utraty dostępności lub poufności. Niemniej organ nadzorczy może rozważyć przeprowadzenie dochodzenia w celu oceny zgodności z szerszymi wymogami bezpieczeństwa wynikającymi z art. 32.
v. Osoba fizyczna dzwoni na infolinię banku, by zgłosić naruszenie danych. Osoba ta otrzymała miesięczny wyciąg z rachunku przeznaczony dla kogoś innego. Administrator przeprowadza krótkie dochodzenie (tj. zakończone w ciągu 24 godzin) i stwierdza z należytą pewnością, że doszło do naruszenia danych osobowych i może istnieć błąd w systemie, w związku z którym mogło ucierpieć więcej osób.	Tak.	Należy powiadomić tylko poszkodowane osoby – jeżeli występuje wysokie ryzyko i jasne jest, że nie naruszono danych pozostałych osób.	Jeżeli w toku dalszego dochodzenia okaże się, że ucierpiało więcej osób, należy dostarczyć organowi nadzorczemu aktualne informacje, a administrator musi dodatkowo powiadomić także inne osoby, jeżeli są narażone na wysokie ryzyko.
vi. Na międzynarodowy targ internetowy przeprowadzono cyberatak, w wyniku którego w internecie opublikowano nazwy	Tak, należy powiadomić wiodący organ nadzorczy, jeżeli w grę wchodzi przetwarzanie transgraniczne.	Tak, ponieważ może to prowadzić do wysokiego ryzyka.	Administrator powinien podjąć działania, np. wymusić zmianę haseł zagrożonych kont, a także inne kroki mające na celu

Przykład	Czy należy powiadomić organ nadzorczy?	Czy należy powiadomić osobę, której dotyczą dane?	Uwagi/zalecenia
użytkownika, hasła i historię zakupów.			zmniejszenie ryzyka.
vii. Firma hostingowa (podmiot przetwarzający) wykryła błąd w kodzie kontrolującym autoryzację użytkowników. Na skutek usterki każdy użytkownik ma dostęp do danych kont wszystkich pozostałych użytkowników.	Firma hostingowa, jako podmiot przetwarzający, musi niezwłocznie powiadomić swoich poszkodowanych klientów (oraz administratorów). Zakładając, że firma hostingowa przeprowadziła własne dochodzenie, poszkodowani administratorzy powinni mieć dostateczną pewność co do tego, czy wszyscy stali się ofiarami naruszenia, a zatem, czy można uznać, że „stwierdzili" naruszenie w chwili otrzymania powiadomienia od firmy hostingowej (podmiotu przetwarzającego). Administrator musi powiadomić organ nadzorczy.	Jeżeli nie ma wysokiego ryzyka dla osób fizycznych, nie trzeba ich powiadamiać.	Firma hostingowa (podmiot przetwarzający) musi rozważyć inne obowiązki notyfikacyjne (np. na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji). Jeżeli nie ma dowodów na wykorzystanie słabego punktu u tego konkretnego administratora, mogło nie dojść do naruszenia podlegającego obowiązkowi zgłoszenia, ale prawdopodobnie miało miejsce zdarzenie do zarejestrowania lub przypadek niezgodności z przepisami art. 32.
viii. Z powodu cyberataku dane medyczne szpitala są niedostępne przez 30 godzin.	Tak, szpital jest zobowiązany zgłosić naruszenie, ponieważ może pojawić się wysokie ryzyko zagrożenia dobrostanu i prywatności pacjentów.	Tak, należy powiadomić osoby fizyczne, których dane naruszono	
ix. W wyniku pomyłki rozesłano dane osobowe 5 tys. studentów do ponad tysiąca odbiorców za pomocą niewłaściwej listy dystrybucyjnej.	Tak, należy powiadomić organ nadzorczy.	Tak, należy powiadomić osoby fizyczne w zależności od zakresu i rodzaju naruszonych danych osobowych oraz powagi możliwych konsekwencji.	
x. W ramach marketingu bezpośredniego rozesłano pocztą	Tak, powiadomienie organu nadzorczego może być obowiązkowe, jeżeli ucierpiała duża liczba	Tak, należy powiadomić osoby fizyczne w zależności od zakresu i rodzaju	Powiadomienie nie musi być konieczne, jeżeli nie ujawniono żadnych danych

Przykład	Czy należy powiadomić organ nadzorczy?	Czy należy powiadomić osobę, której dotyczą dane?	Uwagi/zalecenia
elektroniczną wiadomości do odbiorców wpisanych w polu „do”, a nie w polu „do wiadomości” („cc”), dając tym samym każdemu odbiorcy wgląd w adresy e-mail pozostałych odbiorców.	osób fizycznych, ujawniono dano wrażliwe (np. lista dystrybucyjna psychoterapeuty) lub wystąpiły inne czynniki wysokiego ryzyka (np. wiadomość zawierała wstępne hasła).	naruszonych danych osobowych oraz powagi możliwych konsekwencji	wrażliwych i ujawniono jedynie niewielką liczbę adresów e-mail.