GRUPA ROBOCZA ART. 29 DS. OCHRONY DANYCH

18/EN

WP250rev.01

Wytyczne dotyczące zgłaszania naruszenia ochrony danych osobowych na mocy rozporządzenia 2016/679

Przyjęte w dniu 3 października 2017 r.

Ostatnio zmienione i przyjęte w dniu 6 lutego 2018 r.

Grupa Robocza została powołana na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE oraz art. 15 dyrektywy 2002/58/WE.

Sekretariat zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii) Komisji Europejskiej, Dyrekcja Generalna ds. Sprawiedliwości, 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 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r.

uwzględniając postanowienia art. 29 i 30 tej dyrektywy,

uwzględniając swój regulamin wewnętrzny,

PRZYJĘŁA NASTĘPUJĄCE WYTYCZNE:

SPIS TREŚCI

WPROWADZENIE

Ogólne rozporządzenie o ochronie danych (RODO) wprowadza wymóg zgłaszania naruszenia ochrony danych osobowych (zwanego dalej „naruszeniem") do właściwego krajowego organu nadzorczego[1] (lub w przypadku naruszenia transgranicznego - organu wiodącego), a także, w niektórych przypadkach, zawiadomienia o naruszeniu osób, których dane osobowe ucierpią wskutek takiego naruszenia.

Wymóg zgłaszania 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]. Niektóre państwa członkowskie UE we własnym zakresie wprowadziły już obowiązek zgłaszania naruszeń na poziomie krajowym Może to obejmować obowiązek zgłaszania naruszeń dotyczących różnych kategorii administratorów oprócz podmiotów świadczących publicznie dostępne usługi łączności elektronicznej (np. w Niemczech i Włoszech), lub obowiązek zgłaszania wszelkich naruszeń związanych z ochroną danych osobowych (np. w Holandii). Inne państwa członkowskie posiadaj 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 RODO zastępuje, nie przewiduje żadnego konkretnego obowiązku zgłaszania naruszeń, dlatego też dla wielu organizacji będzie to nowy wymóg. Na mocy RODO zgłoszenie naruszenia jest obowiązkowe dla wszystkich administratorów, chyba że jest mało prawdopodobne, by naruszenie stanowiło ryzyko dla praw i wolności osób fizycznych[5]. Ważną rolę do odegrania mają także podmioty przetwarzające dane, które są zobowiązane zgłaszać wszelkie naruszenia swoim administratorom[6].

Grupa Robocza Art. 29 (GR Art. 29) jest zdania, że nowy obowiązek zgłaszania naruszeń przyniesie szereg korzyści. Przy zgłaszaniu naruszenia organowi nadzorczemu administratorzy mogą uzyskać porady odnośnie konieczności zawiadomienia osób, których naruszenie dotyczy. Organ nadzorczy może zażądać od administratora zawiadomienia tych osób o naruszeniu[7]. Zawiadamianie osób fizycznych o naruszeniu daje administratorowi możliwość przekazania informacji o ryzyku zaistniałym w konsekwencji naruszenia oraz o krokach, jakie mogą podjąć te osoby w celu ochrony przed jego możliwymi konsekwencjami. Kluczowym elementem każdego planu reagowania na naruszenie powinna być ochrona osób fizycznych i ich danych osobowych. W związku z tym zgłaszanie naruszenia należy postrzegać jako narzędzie pozwalające zapewnić lepszą zgodność z wymogami odnośnie ochrony danych osobowych. Jednocześnie należy zauważyć, że niezawiadomienie o naruszeniu osoby fizycznej lub niezgłoszenie go organowi nadzorczemu może prowadzić do nałożenia na administratora sankcji na mocy art. 83.

Dlatego też zachęca się administratorów i podmioty przetwarzające dane do tworzenia z wyprzedzeniem planów i wdrażania procedur pozwalających na wykrycie naruszenia i niezwłoczne zaradzenie mu, ocenę ryzyka dla osób fizycznych[8], a następnie określania, czy konieczne jest zgłoszenie naruszenia do właściwego organu nadzorczego, i w razie konieczności zawiadamianie o naruszeniu

[1] Patrz art. 4 ust. 21 RODO

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

[3] Patrz https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[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 ochrony danych osobowych.

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

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

osób, których ono dotyczy. Zgłoszenie organowi nadzorczemu powinno stanowić część takiego planu reagowania na zdarzenia.

RODO określa kiedy i do kogo należy dokonać zgłoszenia naruszenia, a także jakie informacje należy przekazywać w ramach zgłoszenia. Wymagane do zgłoszenia informacje mogą być przekazywane sukcesywnie, niemniej administratorzy powinni odpowiednio szybko podejmować działania w związku z każdym naruszeniem.

W opinii 03/2014 dotyczącej zgłaszania naruszeń ochrony danych osobowych[9] GR Art. 29 przedstawiła wytyczne dla administratorów, aby zapewnić im pomoc przy podejmowaniu decyzji o zawiadamianiu podmiotów danych w przypadku naruszenia. W opinii tej wzięto pod uwagę obowiązki podmiotów świadczących usługi łączności elektronicznej ustanowione dyrektywą 2002/58/WE i podano przykłady z wielu sektorów w kontekście będącego wówczas jeszcze projektem RODO, a także zaprezentowano dobre praktyki dla wszystkich administratorów.

Niniejsze wytyczne wyjaśniają obowiązek zgłoszenia naruszenia i wymogi dotyczące zawiadamiania na mocy RODO oraz niektóre z działań, jakie mogą podjąć administratorzy i podmioty przetwarzające dane w celu wywiązania się ze swoich nowych obowiązków. Ponadto zawierają przykłady różnych rodzajów naruszeń oraz osób, które należy zawiadamiać w zależności od konkretnego przypadku.

I. Zgłaszanie naruszenia ochrony danych osobowych na mocy RODO

A. Podstawowe względy bezpieczeństwa

Jednym z wymogów nałożonych przez RODO jest przetwarzanie danych osobowych w sposób zapewniający, poprzez wykorzystanie odpowiednich środków technicznych lub organizacyjnych, odpowiednie bezpieczeństwo tychże danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem[10].

Co za tym idzie, RODO wymaga tak 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 oni także uwzględnić najnowszy stan techniki, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania, jak również ryzyko, związane z różnym prawdopodobieństwem i powagą, dla praw i wolności osób fizycznych[11]. RODO wymaga także wdrożenia wszystkich odpowiednich środków technicznych i organizacyjnych, aby możliwe było niezwłoczne ustalenie, czy doszło do naruszenia, co następnie pozwala określić, czy istnieje obowiązek zgłoszenia[12].

W związku z tym kluczowym elementem każdej polityki bezpieczeństwa danych jest możliwość zapobiegania naruszeniu w miarę możliwości lub odpowiedniego reagowania, jeżeli już do niego dojdzie.

[9] Patrz opinia 03/2014 dotycząca zgłaszania naruszeń 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 oraz 32.
[11] Art. 32; patrz także Motyw 83
[12] Patrz Motyw 87.

B. Czym jest naruszenie ochrony danych osobowych?

1. Definicja

Podejmując próbę zaradzenia naruszeniu administrator powinien najpierw umieć takie naruszenie rozpoznać. W art. 4 ust. 12 RODO „naruszenie ochrony danych osobowych" zdefiniowane jest 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."

„Zniszczenie" danych osobowych oznacza sytuację, w której dane przestają istnieć lub przestają istnieć w formie umożliwiającej ich wykorzystanie przez administratora. „Uszkodzenie" oznacza sytuację, w której dane osobowe zostały zmodyfikowane, zepsute lub nie są już kompletne. „Utratę" danych osobowych należy rozumieć jako sytuację, w której dane mogą nadal istnieć, ale administrator utracił kontrolę nad nimi lub dostęp do nich, lub nie jest już w ich posiadaniu. Nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych może obejmować ujawnienie danych osobowych (lub udostępnienia ich) odbiorcom, którzy nie są uprawnieni do otrzymania ich (lub uzyskania do nich dostępu), lub jakąkolwiek inną formę przetwarzania, która narusza RODO.

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 jedyna kopia zbioru danych osobowych została zaszyfrowana przez oprogramowanie typu ransomware lub przez administratora przy użyciu klucza, który nie jest już w jego posiadaniu.

Naruszenie stanowi zatem rodzaj zdarzenia zagrażającego bezpieczeństwu. Niemniej zgodnie z art. 4 ust. 12 RODO ma zastosowanie tylko w przypadku naruszenia ochrony *danych osobowych*. W konsekwencji takiego naruszenia administrator nie jest w stanie zapewnić przestrzegania zasad dotyczących przetwarzania danych osobowych wyszczególnionych w art. 5 RODO. Uwypukla to różnicę pomiędzy zdarzeniem zagrażającym bezpieczeństwu a naruszeniem ochrony danych osobowych – zasadniczo każde naruszenie ochrony danych osobowych jest zdarzeniem zagrażającym bezpieczeństwu, ale nie każde zdarzenie zagrażające bezpieczeństwu stanowi naruszenie ochrony danych osobowych[13].

Możliwe niekorzystne skutki naruszenia dla osób fizycznych przedstawiono poniżej.

2. Rodzaje naruszeń ochrony danych osobowych

W opinii 03/2014 dotyczącej zgłaszania naruszeń ochrony danych osobowych GR Art. 29 wyjaśnia, że naruszenia można skategoryzować ze względu na trzy powszechnie znane zasady bezpieczeństwa informacji[14]:

- „Naruszenie poufności" - nieuprawnione lub przypadkowe ujawnienie lub udostępnienie danych osobowych.
- „Naruszenie integralności" - nieuprawniona lub przypadkowa modyfikacja danych osobowych.
- „Naruszenie dostępności"- przypadkowa lub nieuprawiona utrata dostępu[15] do danych

[13] Należy zauważyć, że zdarzenie zagrażające bezpieczeństwu nie ogranicza się wyłącznie do modeli zagrożeń, w których atak dokonywany jest na organizację z zewnątrz, ale obejmuje także dotyczące wewnętrznego przetwarzania, które naruszają zasady bezpieczeństwa.

[14] Patrz opinia 03/2014

[15] Powszechnie uważa się, że „dostęp" jest zasadniczo częścią „dostępności". Patrz na przykład NIST SP800- 53rev4, gdzie „dostępność" definiowana jest jako: „Zapewnienie terminowego i niezawodnego dostępu do informacji i ich wykorzystywania", dostępne na .http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf CNSSI-

osobowych lub ich zniszczenie.

Należy również zauważyć, że zależnie od okoliczności naruszenie może dotyczyć jednocześnie poufności, integralności i dostępności danych osobowych lub dowolnego połączenia tych kategorii.

O ile określenie, czy doszło do naruszenia poufności czy naruszenia integralności jest dość jasne, naruszenie dostępności może być mniej oczywiste. Naruszenie jest zawsze uznawane za naruszenie dostępności, jeśli nastąpiła trwała utrata lub zniszczenie danych osobowych.

Przykład

Przykłady utraty dostępności obejmują sytuacje, gdy dane zostały usunięte przypadkowo lub przez osobę nieupoważnioną, lub w przypadku danych bezpiecznie zaszyfrowanych gdy klucz deszyfrujący został utracony. Jeśli administrator nie jest w stanie przywrócić dostępu do danych na przykład wykorzystując kopię zapasową, wówczas uznaje się, że nastąpiła trwała utrata dostępności.

Utrata dostępności może również nastąpić w przypadku znaczącego zakłócenia normalnej działalności organizacji np. w wyniku przerwy w dostawie zasilania lub ataku typu DoS (blokada usług), prowadzącego do przejściowej lub trwałej niedostępności danych osobowych.

Może nasunąć się pytanie o to, czy przejściowa utrata dostępności danych osobowych powinna być uznana za naruszenie, a jeśli tak, czy wiązałaby się z obowiązkiem zgłoszenia. Art. 32 RODO, „bezpieczeństwo przetwarzania", objaśnia, że podczas wdrażania odpowiednich środków technicznych i organizacyjnych w celu zapewnienia stopnia bezpieczeństwa odpowiadającego 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 zagrażające bezpieczeństwu skutkujące utratą dostępności danych osobowych na pewien czas stanowi rodzaj naruszenia, ponieważ brak dostępu do danych może mieć znaczący wpływ na prawa i wolności osób fizycznych. Niedostępność danych osobowych z powodu planowanej konserwacji systemu nie stanowi „naruszenia bezpieczeństwa" określonego w art. 4 ust. 12.

Podobnie jak trwała utrata lub zniszczenie danych osobowych (lub jakiekolwiek naruszenie innego rodzaju), naruszenie polegające na przejściowej utracie dostępności powinno zostać udokumentowane zgodnie z art. 33 ust. 5 Pomaga to administratorowi w udowodnieniu rozliczalności wobec organu nadzorczego, który może poprosić o wgląd do tych dokumentów[16].W zależności od okoliczności naruszenia, zgłoszenie go organowi nadzorczemu i zawiadomienie osób, których ono dotyczy, może być lub nie być wymagane. Administrator musi ocenić prawdopodobieństwo i wagę możliwego wpływu niedostępności danych osobowych na prawa i wolności osób fizycznych. Zgodnie z art. 33 administrator zobowiązany jest zgłosić naruszenie, chyba że niedostępność danych osobowych najprawdopodobniej nie doprowadzi do ryzyka naruszenia praw i wolności osób fizycznych. Ocenę tego należy jednak przeprowadzać każdorazowo.

4009 mówi także o: „Właściwość bycia dostępnym i użytecznym na żądanie uprawnionego podmiotu." Patrz .https://rmf.org/images/4-CNSS-Publications/CNSSI-4009.pdf ISO/IEC 27000:2016 także definiuje „dostępność" jako „właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

[16] Patrz art. 33 ust. 5.

Przykłady
W kontekście szpitala jeśli krytyczne dane medyczne dotyczące pacjentów są niedostępne nawet przejściowo, może to stanowić ryzyko dla praw i wolności osób fizycznych - na przykład może to skutkować odwołaniem zabiegów chirurgicznych i narażeniem życia.

Analogicznie w przypadku, gdy systemy spółki z branży medialnej są niedostępne przez kilka godzin (np. z powodu przerwie w zasilaniu) a w konsekwencji spółka ta nie może rozesłać biuletynu do abonentów, nie jest prawdopodobne, aby stanowiło to ryzyko dla praw i wolności osób fizycznych.

Należy podkreślić, że nawet jeśli utrata dostępności systemów administratora jest przejściowa i nie ma wpływu na osoby fizyczne, istotne jest, aby administrator wziął pod uwagę wszystkie możliwe konsekwencje naruszenia, jako że może ono wciąż wymagać zgłoszenia z innych powodów.

Przykład

Infekcja oprogramowaniem typu ransomware (złośliwym oprogramowaniem, które szyfruje dane administratora do czasu zapłaty okupu) może prowadzić do przejściowej utraty dostępności, jeżeli dane można odzyskać z kopii zapasowej. Niemniej jednak doszło do włamania do sieci, w związku z czym może być wymagane zgłoszeniem, jeśli incydent zostanie uznany za naruszenie poufności (tj. atakujący uzyskał dostęp do danych osobowych) stanowiące ryzyko dla praw i wolności osób fizycznych.

3. Możliwe konsekwencje naruszenia ochrony danych osobowych

Naruszenie może mieć szereg istotnych negatywnych skutków dla osób fizycznych, prowadząc do szkód fizycznych, materialnych i niematerialnych. RODO objaśnia, że może to obejmować utratę kontroli nad swoimi danymi osobowymi, ograniczenie przysługujących praw, dyskryminację, kradzież lub sfałszowanie tożsamości, straty finansowe, nieupoważnione odwrócenie pseudonimizacji, naruszenie dobrego imienia oraz utratę poufności danych osobowych chronionych tajemnicą zawodową. Może to także mieć znaczący niekorzystny wpływ ekonomiczny lub społeczny na takie osoby fizyczne[17].

RODO zobowiązuje administratora do zgłoszenia naruszenia do właściwego organu nadzorczego, chyba że ryzyko wystąpienia takich negatywnych skutków jest niskie. W przypadku wysokiego ryzyka wystąpienia negatywnych skutków RODO wymaga od administratora zawiadomienia o naruszeniu osób fizycznych, na które ma ono wpływ tak szybko, jak jest to racjonalnie możliwe[18].

Motyw 87 RODO podkreśla wagę możliwości stwierdzenia naruszenia, oceny ryzyka dla osób fizycznych oraz zgłoszenia naruszenia, jeśli jest to wymagane:

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

Dalsze wytyczne dotyczące oceny ryzyka negatywnych skutków dla osób fizycznych omówiono w pkt. IV.

Jeśli administratorzy nie dokonają zgłoszenia organowi nadzorczemu i/lub nie zawiadomią osób

[17] Patrz także Motywy 85 i 87.
[18] Patrz także Motyw 86.

fizycznych o naruszeniu ochrony danych osobowych, nawet jeśli spełnione zostały wymogi art. 33 i/lub 34, organ nadzorczy dokonuje wyboru, który musi uwzględniać wszystkie środki naprawcze, jakimi dysponuje, w tym nałożenie stosownej administracyjnej kary pieniężnej[19], wyłącznie lub w połączeniu z innym środkiem naprawczym określonym w art. 58 ust. 2. W przypadku wybrania administracyjnej kary pieniężnej, jej wartość nie może przekroczyć 10 000 000 euro lub 2% całkowitego rocznego światowego obrotu przedsiębiorstwa zgodnie z art. 83 ust. 4 lit. a RODO. Należy także mieć na uwadze, że w niektórych przypadkach niezgłoszenie naruszenia może ujawnić brak lub nieodpowiedni charakter istniejących środków bezpieczeństwa. Wytyczne GR Art. 29 w sprawie administracyjnych kar pieniężnych stanowią, że: „Występowanie kilku różnych naruszeń popełnionych łącznie w konkretnym pojedynczym przypadku oznacza, że organ nadzorczy może nakładać administracyjne kary pieniężne w sposób, który jest zarazem skuteczny, proporcjonalny i odstraszający na poziomie najpoważniejszego naruszenia." W takim przypadku organ nadzorczy ma również możliwość nałożenia sankcji za niezgłoszenie lub niezawiadomienie 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.

II. Artykuł 33 - Zgłaszanie organowi nadzorczemu

A. Kiedy należy zgłaszać naruszenie ochrony danych osobowych

1. Wymogi art. 33

Art. 33 ust. 1 stanowi, że:

> „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."

Motyw 87 określa, że[20]:

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

2. Kiedy administrator „stwierdza" naruszenie ochrony danych osobowych?

Jak opisano powyżej w przypadku naruszenia RODO nakłada na administratora obowiązek zgłoszenia go bez zbędnej zwłoki, w miarę możliwości nie później niż 72 godziny po jego stwierdzeniu. Może to nasuwać pytanie o to, kiedy uznaje się, że administrator „stwierdził" naruszenie. Według GR Art. 29 należy uznać, że administrator „stwierdził" naruszenie, kiedy ma on wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych osobowych.

Jak zaznaczono wcześniej RODO wymaga od administratora wdrożenia wszystkich odpowiednich środków technicznych i organizacyjnych w celu natychmiastowego stwierdzenia, czy doszło do

[19] Więcej szczegółów: patrz Wytyczne GR Art. 29 w sprawie nakładania i ustalania wysokości administracyjnych kar pieniężnych: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Istotny w tym kontekście jest także Motyw 85.

naruszenia, i bezzwłocznego zgłoszenia naruszenia organowi nadzorczemu i zawiadomienia osób, których ono dotyczy. Stanowi także, że fakt, że 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[21]. Nakłada to na administratora obowiązek zapewnienia, że w odpowiednim czasie „stwierdzi" wszelkie naruszenia, aby móc podjąć odpowiednie działania.

To kiedy dokładnie można uznać, że administrator „stwierdził" konkretne naruszenie, zależy od okoliczności danego naruszenia. W niektórych przypadkach od samego początku względnie jasne jest, że doszło do naruszenia, podczas gdy w innych stwierdzenie naruszenia ochrony danych osobowych może wymagać więcej czasu. Priorytetem jest szybkie podjęcie działań w celu zbadania zdarzenia i ustalenia, czy rzeczywiście doszło do naruszenia ochrony danych, a jeśli tak – podjęcie działań naprawczych i zgłoszenie naruszenia, jeśli jest to wymagane.

Przykłady

1. W przypadku utraty nośnika danych USB z niezaszyfrowanymi danymi osobowymi często nie da się ustalić, czy osoby nieupoważnione uzyskały dostęp do tych danych. Mimo że administrator danych może nie być wstanie stwierdzić, czy doszło do naruszenia poufności, taki przypadek wymaga zgłoszenia, ponieważ istnieje wystarczający stopień pewności co do tego, że doszło do naruszenia dostępności; administrator „stwierdza" naruszenie w chwili, gdy zdaje sobie sprawę z utraty nośnika danych USB.

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

3. Administrator wykrywa, że mogło dojść do włamania do jego sieci. Sprawdza swoje systemy, aby ustalić, czy doszło do naruszenia bezpieczeństwa przechowywanych w nich danych, i potwierdza, że miało to miejsce. Administrator ponownie ma jasne dowody naruszenia poufności, nie ma zatem wątpliwości co do tego, że „stwierdził" naruszenie.

4. Cyberprzestępca kontaktuje się z administratorem po włamaniu się do jego systemu z żądaniem okupu. W takim przypadku administrator, po uprzednim sprawdzeniu systemu i potwierdzeniu, że doszło do ataku, ma jasne dowody, że doszło do naruszenia, nie ma zatem wątpliwości co do tego, że stwierdził naruszenie.

Po otrzymaniu informacji o możliwym naruszeniu od osoby fizycznej, podmiotu z sektora mediów czy z innego źródła, lub po samodzielnym wykryciu zdarzenia zagrażającego bezpieczeństwu, administrator może przez krótki czas prowadzić postępowanie, aby ustalić, czy rzeczywiście doszło do naruszenia. W czasie trwania takiego postępowania nie można jeszcze uznać, że administrator „stwierdził" naruszenie. Wstępne postępowanie powinno rozpocząć się jak najszybciej i pozwolić na ustalenie z należytą pewnością, czy doszło do naruszenia. Bardziej dokładne postępowanie może zostać przeprowadzone w późniejszym czasie.

Po stwierdzeniu naruszenia przez administratora, zgłoszenie – w przypadku naruszenia wymagającego zgłoszenia – musi nastąpić bez zbędnej zwłoki, a jeżeli to możliwe, nie później niż w ciągu 72 godzin. W tym czasie administrator powinien dokonać oceny ryzyka dla osób fizycznych, w celu określenia, czy zgłoszenie jest wymagane, a także określić działanie(-a) konieczne do zaradzenia naruszeniu. Administrator może mieć już wyniki wstępnej oceny ryzyka wynikającego z naruszenia przeprowadzonej w ramach oceny skutków dla ochrony danych[22] sporządzonej przed wykonaniem

[21] Patrz Motyw 87.
[22] Patrz wytyczne GR Art. 29 dotyczące oceny skutków dla ochrony danych na stronie http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

danej operacji przetwarzania. Ocena skutków dla ochrony danych może jednak mieć charakter bardziej ogólny w porównaniu z konkretnymi okolicznościami naruszenia, które rzeczywiście miało miejsce, dlatego też w każdym przypadku należy przeprowadzić dodatkową ocenę z uwzględnieniem wspomnianych okoliczności. Więcej informacji na temat oceny ryzyka, patrz pkt. IV.

W większości przypadków opisane wstępne działania powinny zostać zakończone jak najszybciej po powzięciu pierwszych odnośnych informacji (tj. kiedy administrator lub podmiot przetwarzający podejrzewa, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które mogło dotyczyć danych osobowych). Mogą one trwać dłużej jedynie w wyjątkowych przypadkach.

Przykład

Osoba fizyczna informuje administratora o otrzymaniu wiadomości elektronicznej, w której ktoś podszywał się pod administratora, zawierającej dane osobowe związane z (bieżącym) korzystaniem przez tę osobę z usług administratora, co sugeruje, że istnieje zagrożenie dla bezpieczeństwa administratora. Administrator przeprowadza krótkie postępowanie i wykrywa włamanie do swojej sieci oraz znajduje dowody nieuprawnionego dostępu do danych osobowych. Uznaje się, że administrator „stwierdza" wówczas naruszenie i wymagane jest zgłoszenie go organowi nadzorczemu, chyba że nie stanowi ono ryzyka dla praw i wolności osób fizycznych. W takiej sytuacji administrator musi podjąć odpowiednie działania naprawcze w celu zaradzenia naruszeniu.

Dlatego też administrator powinien wdrożyć procedury wewnętrzne pozwalające na wykrywanie naruszeń i zaradzanie im. Na przykład w celu wykrycia niektórych nieprawidłowości w zakresie przetwarzania danych administrator lub podmiot przetwarzający może wykorzystać określone środki techniczne, takie jak analizatory przepływu danych lub analizatory plików dziennika, dzięki którym możliwe jest zdefiniowanie zdarzeń i alertów na podstawie korelacji pomiędzy określonymi danymi z dziennika[23]. W przypadku wykrycia naruszenia ważne jest, by zgłosić je przełożonym na odpowiednim szczeblu zarządczym, tak aby umożliwić podjęcie odpowiednich kroków, oraz jeśli jest to wymagane zgłoszenie go zgodnie z art. 33, a w razie potrzeby także zgodnie z art. 34. Opis takich środków i mechanizmów zgłaszania może być zawarty w planach reagowania na incydenty i/lub zasadach zarządzania administratora. Pomogą one administratorowi w tworzeniu skutecznych planów i ustaleniu zakresu odpowiedzialności operacyjnej w organizacji za zarządzanie przypadkami naruszeń, a także określeniu tego, kiedy i czy zasadne jest eskalowanie danego incydentu.

Administrator powinien również dokonać stosownych ustaleń ze wszystkimi podmiotami przetwarzającymi, z usług których korzysta, którzy są zobowiązani do zgłaszania naruszeń do administratora (patrz niżej).

Za wdrożenie odpowiednich środków w celu zapobiegania naruszeniom, reagowania na nie i zaradzania im odpowiedzialność ponoszą administratorzy i podmioty przetwarzające, jednak istnieją pewne kroki praktyczne, które należy podjąć we wszystkich przypadkach.

- Informacje odnośnie wszelkich zdarzeń związanych z bezpieczeństwem powinny być kierowane do odpowiedzialnej osoby lub osób, którym powierzono zadanie stwierdzania naruszenia oraz oceny ryzyka.
- Następnie powinna zostać przeprowadzona ocena stopnia ryzyka dla osób fizycznych wynikającego z naruszenia (prawdopodobieństwo braku ryzyka, ryzyka lub wysokiego ryzyka) a odpowiednie działy organizacji powinny zostać o tym poinformowane.
- Jeśli jest to wymagane, należy dokonać zgłoszenia organowi nadzorczemu i potencjalnie zawiadomienia o naruszeniu osób fizycznych, których ono dotyczy.
- Administrator powinien jednocześnie prowadzić działania w celu zaradzenia naruszeniu i

[23] Należy zauważyć, że dane z dziennika umożliwiające przeprowadzenie audytu, np. informacje na temat przechowywania, modyfikacji lub usunięcia danych, również można uznać za dane osobowe powiązane z osobą, która rozpoczęła daną operację przetwarzania.

naprawienia jego konsekwencji.

- Naruszenie powinno być dokumentowane w miarę rozwoju zdarzeń.

Na administratorze spoczywa zatem obowiązek reagowania na wszelkie ostrzeżenia i stwierdzania, czy naruszenie rzeczywiście miało miejsce. Ten krótki okres umożliwia zbadanie zaistniałej sytuacji, a administratorowi umożliwia zebranie dowodów i innych ważnych informacji. Gdy administrator stwierdzi z należytą pewnością, że doszło do naruszenia, i spełnione zostały warunki określone w art. 33 ust. 1, jest on zobowiązany do zgłoszenia go naruszenia organowi nadzorczemu bez zbędnej zwłoki, a jeśli to możliwe w ciągu 72 godzin[24]. Niepodjęcie przez administratora działań w odpowiednim czasie w przypadku, gdy ewidentnie doszło do naruszenia, może zostać uznane za niewywiązanie się z obowiązku zgłaszania naruszenia określonego w art. 33.

Art. 32 stanowi, że administrator i podmiot przetwarzający powinni wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych osobowych. Możliwość wykrywania, usuwania i zgłaszania naruszenia w odpowiednim czasie należy uznać za kluczowy element tych środków.

3. Współadministratorzy

Art. 26 odnosi się do współadministratorów i stanowi, że współadministratorzy określają zakres swojej odpowiedzialności za przestrzeganie RODO[25]. Obejmuje to ustalenie, która strona będzie odpowiedzialna za wypełnienie zobowiązań wynikających z art. 33 i 34. GR Art. 29 zaleca, aby uzgodnienia umowne między współadministratorami zawierały postanowienia określające, który administrator będzie odgrywał główną rolę w wypełnianiu obowiązków zgłaszania naruszenia wynikających z RODO lub odpowiadał za ich przestrzeganie.

4. Obowiązki podmiotu przetwarzającego

Administrator ponosi ogólną odpowiedzialność za ochronę danych osobowych, podmiot przetwarzający odgrywa jednak ważną rolę umożliwiając administratorowi wywiązanie się z nałożonych na niego 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. Art. 28 ust. 3 lit. f stanowi, że umowa lub inny instrument prawny powinny określać, 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 wskazuje, że w przypadku, gdy administrator korzysta z usług podmiotu przetwarzającego, podmiot taki po stwierdzeniu naruszenia ochrony danych osobowych musi zgłosić je administratorowi „bez zbędnej zwłoki". Należy zauważyć, że podmiot przetwarzający nie musi najpierw dokonać oceny prawdopodobieństwa ryzyka wynikającego z naruszenia przed zgłoszeniem go do administratora; to administrator musi dokonać tej oceny, gdy stwierdzi naruszenie. Podmiot przetwarzający musi jedynie ustalić, czy doszło do naruszenia, a następnie zgłoszenia go administratorowi. Administrator korzysta z usług podmiotu przetwarzającego dla osiągnięcia własnych celów. Co do zasady należy zatem uznać, że „stwierdza" naruszenie równocześnie przekazaniem mu odnośnych informacji przez podmiot przetwarzający. Spoczywający na podmiocie przetwarzającym obowiązek zgłaszania naruszenia administratorowi pozwala administratorowi zaradzić naruszeniu i określić, czy konieczne jest zgłoszenie go organowi nadzorczemu zgodnie z art. 33 ust. 1 oraz zawiadomienie osób, których ono dotyczy zgodnie z art. 34 ust. 1. Administrator może również chcieć zbadać naruszenie, jako że podmiot przetwarzający może nie być w stanie poznać wszystkich istotnych faktów dotyczących sprawy, na przykład stwierdzić, czy administrator jest wciąż w posiadaniu kopii lub kopii zapasowej danych osobowych zniszczonych lub utraconych przez podmiot przetwarzający. Może to mieć wpływ to, czy administrator będzie zobowiązany do zgłoszenia naruszenia.

[24] Patrz rozporządzenie nr 1182/71 określające zasady mające zastosowanie do okresów, dat i terminów, dostępne na stronie: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] Patrz także Motyw 79.

RODO nie podaje wyraźnego terminu, w którym podmiot przetwarzający ma zgłosić naruszenie administratorowi, a jedynie stanowi, że musi to nastąpić „bez zbędnej zwłoki". W związku z tym GR Art. 29 zaleca, aby podmiot przetwarzający natychmiast zgłosił naruszenie administratorowi i sukcesywnie przekazywał dalsze informacje na temat naruszenia, kiedy tylko staną się one dostępne. Jest to istotne, aby administrator mógł wywiązać się z obowiązku zgłoszenia naruszenia organowi nadzorczemu w ciągu 72 godzin.

Jak wyjaśniono powyżej umowa zawarta pomiędzy administratorem a podmiotem przetwarzającym powinna określać, w jaki sposób należy spełnić wymogi określone w art. 33 ust. 2, w uzupełnieniu do innych zapisów zawartych w RODO. Może to obejmować wymogi dotyczące wczesnego zgłaszania przez podmiot przetwarzający, co z kolei wspiera administratora w wypełnianiu jego obowiązków odnośnie zgłaszania naruszenia organowi nadzorczemu w ciągu 72 godzin.

Jeżeli podmiot przetwarzający świadczy usługi na rzecz wielu administratorów, na których wpływ ma to samo zdarzenie, wówczas musi przekazać jego szczegóły wszystkim administratorom.

Podmiot przetwarzający może dokonać zgłoszenia w imieniu administratora, jeżeli administrator nadał mu odpowiednie upoważnienie i jest to przewidziane w ustaleniach umownych pomiędzy administratorem a podmiotem przetwarzającym. Zgłoszenia należy wówczas dokonać zgodnie z art. 33 i 34. Niemniej jednak należy podkreślić, że odpowiedzialność prawna za zgłoszenie spoczywa na administratorze.

B. Informowanie organu nadzorczego

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."

RODO nie określa kategorii osób, których dane dotyczą, ani wpisów danych osobowych. GR Art. 29 sugeruje jednak, że kategorie osób, których dane dotyczą, powinny odzwierciedlać rodzaje 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 dotyczące stanu zdrowia, dokumentacja placówek oświaty, informacje dotyczące opieki społecznej, informacje finansowe, numery rachunków bankowych, numery paszportów itd.

Z Motywu 85 jasno wynika, że jednym z celów zgłaszania jest ograniczenie szkód dla osób fizycznych. W związku z tym, jeżeli naruszenie wiąże się z ryzykiem konkretnej szkody dla danej kategorii osób, których dane dotyczą, lub rodzaju danych osobowych (np. kradzież tożsamości, oszustwo, strata finansowa, zagrożenie dla tajemnicy zawodowej), ważne jest, by zgłoszenie uwzględniało informację o takich kategoriach. W ten sposób łączy się to z wymogiem opisania prawdopodobnych konsekwencji naruszenia.

Brak bardziej precyzyjnych informacji (np. dokładnej liczby poszkodowanych osób, których dane dotyczą) nie powinien być przeszkodą dla terminowego zgłoszenia. RODO dopuszcza możliwość podania w przybliżeniu liczby osób fizycznych, których dane naruszono, i liczby objętych naruszeniem wpisów danych osobowych. Priorytetem powinno być usuwanie negatywnych skutków naruszenia, a nie podawanie dokładnych danych liczbowych.

Gdy staje się jasne, że doszło do naruszenia, ale jego zakres nie jest jeszcze znany, bezpiecznym sposobem na wywiązanie się z obowiązku zgłoszenia naruszenia jest zgłaszanie 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 zgłaszania naruszenia organowi nadzorczemu administrator może uznać za przydatne podanie nazwy podmiotu przetwarzającego dane, jeżeli to on jest pierwotną przyczyną naruszenia, zwłaszcza jeśli doprowadziło to do zdarzenia, które wpłynęło na wpisy danych osobowych wielu innych administratorów korzystających z usług tego samego przedmiotu przetwarzającego.

Organ nadzorczy może w każdym przypadku zażądać dalszych informacji w ramach swojego postępowania w sprawie naruszenia.

2. Zgłaszanie sukcesywne

W zależności od charakteru naruszenia konieczne może okazać się dalsze zbadanie sprawy przez administratora w celu ustalenia wszystkich istotnych faktów związanych ze zdarzeniem. Dlatego też art. 33 ust. 4 stanowi, że:

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

RODO uznaje, że administratorzy nie zawsze dysponują 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 początkowym okresie. Tym samym dopuszczone jest zgłaszanie sukcesywne. Ten rodzaj zgłaszania jest bardziej prawdopodobny w przypadku bardziej złożonych naruszeń, takich jak niektóre rodzaje zagrożeń dla cyberbezpieczeństwa, kiedy może okazać się konieczne podjęcie dogłębnego dochodzenia w celu pełnego ustalenia charakteru naruszenia i zakresu, w jakim naruszono ochronę danych osobowych. W związku z powyższym w wielu przypadkach administrator będzie musiał przeprowadzić bardziej dogłębne postępowanie 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. GR Art. 29 zaleca, by przy pierwszym zgłoszeniu organowi nadzorczemu administrator poinformował go również, jeśli nie ma jeszcze wszystkich wymaganych informacji, oraz że będzie w stanie podać więcej szczegółów w późniejszym terminie. Organ nadzorczy powinien uzgodnić sposób i termin podania dodatkowych informacji. Nie oznacza to, że administrator nie może podać dalszych informacji na dowolnym innym etapie, jeżeli pozna dodatkowe istotne szczegóły dotyczące naruszenia, które należy przekazać organowi nadzorczemu.

Głównym celem wymogu zgłaszania naruszeń jest zachęcanie administratorów do niezwłocznego podejmowania działań w związku z naruszeniem, zaradzania mu i – jeżeli to możliwe – odzyskiwania naruszonych danych osobowych, a także do zasięgania rady organu nadzorczego. Zgłoszenie naruszenia organowi nadzorczemu w ciągu pierwszych 72 godzin pozwala administratorowi upewnić się, że podjęta decyzja o zawiadomieniu lub niezawiadomieniu osób, których dane dotyczą była słuszna.

Celem zgłoszenia naruszenia organowi nadzorczemu jest nie tylko uzyskanie wytycznych co do zawiadomienia osób fizycznych, których dane naruszono. W niektórych przypadkach ze względu na charakter naruszenia i wagę ryzyka administrator musi niezwłocznie zawiadomić osoby, których dotyczy naruszenie. Przykładowo w przypadku bezpośredniego zagrożenia kradzieżą tożsamości lub w przypadku ujawnienia szczególnych kategorii danych osobowych[26] w Internecie, administrator powinien bez zbędnej zwłoki podjąć działania w celu zaradzenia naruszeniu i zawiadomienia o nim osób, których ono dotyczy (patrz pkt. III). W wyjątkowych okolicznościach może to nastąpić nawet przed zgłoszeniem naruszenia organowi nadzorczemu. Co do zasady zgłoszenie naruszenia organowi nadzorczemu nie może służyć za usprawiedliwienie niezawiadomienia o naruszeniu osoby, której dane dotyczą, jeśli jest to wymagane.

Należy podkreślić, że po dokonaniu pierwszego zgłoszenia administrator może uaktualnić informacje przekazane organowi nadzorczemu, jeśli w toku postępowania uzyska dowody na to, że opanowano zdarzenie zagrażające bezpieczeństwu, a w rzeczywistości żadne naruszenie nie miało miejsca. Informacje te można potem dodać do informacji przekazanych uprzednio organowi nadzorczemu, a dane zdarzenie zostanie odpowiednio zarejestrowane jako 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 zgłasza organowi nadzorczemu utratę nośnika danych USB zawierającego kopię danych osobowych części jego klientów. Później niewłaściwie oznaczony nośnik danych USB zostaje odnaleziony w lokalu administratora, a jego zawartość odzyskana. Administrator przekazuje organowi nadzorczemu aktualne informacje i wnosi o zmianę zgłoszenia.

Należy zauważyć, że podejście sukcesywne do zgłaszania naruszeń jest już przewidziane odnośnie obowiązków wynikających z dyrektywy 2002/58/WE, rozporządzenia 611/2013 i w związku z innymi samodzielnie zgłaszanymi zdarzeniami.

3. Zgłaszanie z opóźnieniem

Art. 33 ust. 1 wyraźnie stanowi, że do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Powyższe oraz koncepcja zgłaszania sukcesywnego stanowią uznanie faktu, że administrator może nie zawsze mieć możliwość zgłoszenia naruszenia w tym terminie, oraz dopuszczenie zgłaszania 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 dane dotyczą. Administrator może stwierdzić naruszenie i rozpoczynając badanie jego szczegółów, jeszcze przed zgłoszeniem, wykryć kolejne, podobne naruszenia o różnych przyczynach. W zależności od okoliczności administratorowi może zająć pewien okres czasu ustalenie zakresu naruszeń i, zamiast zgłaszać każde naruszenie z osobna, administrator może dokonać jednego istotnego zgłoszenia obejmującego szereg bardzo podobnych naruszeń o potencjalnie różnych przyczynach. Może to skutkować opóźnieniem zgłoszenia naruszenia organowi nadzorczemu o więcej niż 72 godziny od czasu stwierdzenia tych naruszeń przez administratora.

Ściśle rzecz ujmując każde naruszenie stanowi zdarzenie podlegające obowiązkowi zgłoszenia. 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 okresie czasu. Jeżeli ma miejsce szereg naruszeń różnego rodzaju danych osobowych dokonywanych na różne sposoby, wówczas zgłoszenie powinno nastąpić normalnie, przy czym każde naruszenie należy zgłosić zgodnie z art. 33.

[26] Patrz art. 9.

Mimo iż RODO dopuszcza możliwość opóźnienia zgłoszenia, nie należy postrzegać tego jako rozwiązania, które należy stosować regularnie. Warto zaznaczyć, że zgłoszenia łączne mogą dotyczyć również wielu podobnych naruszeń zgłaszanych w ciągu 72 godzin.

C. Naruszenia transgraniczne i naruszenia w jednostkach organizacyjnych poza UE

1. Naruszenia transgraniczne

W przypadkach transgranicznego przetwarzania danych osobowych[27] naruszenie może wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim. Art. 33 ust. 1 jasno stanowi, że w przypadku naruszenia administrator powinien zgłosić je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO[28]. Art. 55 ust. 1 stanowi, że:

> „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 art. 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 ma miejsce w kontekście przetwarzania transgranicznego i wymagane jest zgłoszenie go, administrator musi dokonać zgłoszenia naruszenia wiodącemu organowi nadzorczemu[29]. Dlatego też podczas przygotowywania planu reagowania na naruszenie administrator musi określić wiodący organ nadzorczy, któremu należy je zgłosić[30]. Pozwoli mu to szybko zareagować na naruszenie i wywiązać się z obowiązków wynikających z art. 33. W przypadku naruszenia mającego miejsce w związku z przetwarzaniem transgranicznym zawsze konieczne jest zgłoszenie go wiodącemu organowi nadzorczemu, który nie zawsze jest organem właściwym dla miejsca, gdzie znajdują się osoby, których dotyczy naruszenie lub dla miejsca naruszenia. W stosownych przypadkach administrator podczas zgłaszania naruszenia organowi nadzorczemu powinien wskazać, czy naruszenie dotyczy jednostek organizacyjnych znajdujących się w innych państwach członkowskich, oraz określić państwa członkowskie, w których naruszenie to prawdopodobnie będzie miało wpływ na osoby, których dane dotyczą. W przypadku jakichkolwiek wątpliwości co do tożsamości wiodącego organu nadzorczego administrator powinien co najmniej dokonać zgłoszenia lokalnemu organowi nadzorczemu w miejscu, w którym doszło do naruszenia.

2. Naruszenia w jednostkach organizacyjnych poza UE

Art. 3 dotyczy terytorialnego zakresu stosowania RODOD, w tym także sytuacji, gdy ma ono zastosowanie do przetwarzania danych osobowych przez administratora lub podmiot przetwarzający

---

[27] Patrz art. 4 ust. 23.
[28] Patrz także Motyw 122.
[29] Patrz Wytyczne GR Art. 29 dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora bądź przetwarzającego dostępne na stronie: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102
[30] Wykaz danych kontaktowych wszystkich europejskich krajowych organów ochrony danych można znaleźć na stronie: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

niemający jednostki organizacyjnej w UE. W szczególności art. 3 ust. 2 stanowi[31]:

> „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z::
>
> (a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
>
> (b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii."

Istotny jest także art. 3 ust. 3, który stanowi[32]:

> „Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego."

W przypadku gdy do administratora niemającego jednostki organizacyjnej w UE ma zastosowanie art. 3 ust. 2 lub art. 3 ust. 3 i doznaje on naruszenia, wówczas administrator ten podlega wciąż obowiązkowi zgłoszenia naruszenia na mocy art. 33 i 34. Art. 27 wymaga od administratora (i podmiotu przetwarzającego) wyznaczenia przedstawiciela w UE, jeżeli ma zastosowanie art. 3 ust. 2. W takich przypadkach GR Art. 29 zaleca zgłoszenie naruszenia organowi nadzorczemu w państwie członkowskim, w którym ma jednostkę organizacyjną przedstawiciel administratora w UE[33]. Podobnie w przypadku gdy do podmiotu przetwarzającego ma zastosowanie art. 3 ust. 2, podlega on obowiązkom nałożonym na podmioty przetwarzające, zwłaszcza obowiązkowi zgłoszenia naruszenia administratorowi na mocy art. 33 ust. 2.

D. Warunki, w których nie jest wymagane zgłoszenie

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 zgłaszania naruszenia organowi nadzorczemu. Przykładem może być sytuacja, w której dane osobowe są już ogólnie dostępne, a ich ujawnienie nie stanowi ryzyka dla osoby fizycznej. Jest to sprzeczne z obecnymi wymogami dotyczącymi zgłaszania naruszeń obowiązującymi 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 zgłaszania naruszeń[34] GR Art. 29 wyjaśnia, że naruszenie poufności danych osobowych zaszyfrowanych algorytmem zgodnym ze stanem wiedzy technicznej nadal stanowi naruszenie ochrony 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 odczyt danych jest co do zasady niemożliwy. W związku z tym istnieje więc niewielkie prawdopodobieństwo, ze naruszenie wpłynie negatywnie na osoby fizyczne, a zatem nie wymaga się zawiadamiania ich[35]. Jednak nawet w przypadku zaszyfrowanych danych ich utrata lub modyfikacja może mieć negatywne konsekwencje dla osób, których te dane dotyczą, jeżeli administrator nie ma odpowiednich kopii zapasowych. W takim przypadku wymagane jest zawiadomienie osób, których dane dotyczą, nawet jeśli same dane zostały odpowiednio zaszyfrowane.

---

[31] Patrz także Motywy 23 i 24.
[32] Patrz także Motyw 25.
[33] Patrz Motyw 80 i art. 27.
[34] Opinia GR Art. 29 03/2014 w sprawie zgłaszania naruszeń ochrony danych osobowych http://ec.europa.eu/justice/data-protection/article- 29/documentation/opinion-recommendation/files/2014/wp213_en.pdf
[35] Patrz także art. 4 ust.1 i 2 rozporządzenia 611/2013.

GR Art. 29 wyjaśniła również, że to samo dotyczy 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 wiedzy technicznej 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 niego.

Jeżeli więc odczyt danych osobowych jest co do zasady niemożliwy dla osób nieupoważnionych i jeśli istnieje kopia lub kopia zapasowa tych danych, wówczas nie ma obowiązku zgłaszania organowi nadzorczemu naruszenia poufności odpowiednio zaszyfrowanych danych osobowych. Wynika to z faktu, że prawdopodobieństwo, aby naruszenie takie stwarzało ryzyko dla praw i wolności osób fizycznych jest niskie. Oznacza to, że nie trzeba również zawiadamiać osoby fizycznej, ponieważ najprawdopodobniej nie występuje wysokie ryzyko. Należy mieć jednak na uwadze, że nawet jeśli zgłoszenie 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, zgłoszenie naruszenia może być konieczne.

Ponadto należy zauważyć, że w przypadku naruszenia w sytuacji braku kopii zapasowej szyfrowanych danych osobowych dochodzi do naruszenia dostępności, co może stanowić ryzyko dla osób fizycznych i w związku z tym wymagać zgłoszenia. Podobnie naruszenie obejmujące 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 dane 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 zgłoszenia organowi nadzorczemu jest utrata bezpiecznie zaszyfrowanego urządzenia mobilnego używanego przez administratora i jego personel. Pod warunkiem, że klucz użyty do zaszyfrowania pozostaje w posiadaniu administratora i jego personelu i nie jest to jedyna kopia danych osobowych, dane te pozostają niedostępne dla atakującego. Prawdopodobieństwo, by naruszenie stanowiło ryzyko dla praw lub wolności osób, których dotyczą naruszone dane, jest niskie. Jeżeli w późniejszym czasie stanie się jasne, że naruszono bezpieczeństwo klucza użytego do zaszyfrowania, lub że oprogramowanie lub algorytm są narażone na ataki, wówczas zmieni się ryzyko dla praw i wolności osób fizycznych, a w związku zgłoszenie może być wymagane.

Niespełnienie wymogów art. 33 ma miejsce, jeśli administrator nie dokonuje zgłoszenia naruszenia organowi nadzorczemu w sytuacji, gdy dane nie były bezpiecznie zaszyfrowane. Dlatego też przy wyborze oprogramowania szyfrującego administratorzy powinni dokładnie przyjrzeć się jakości i prawidłowemu wdrożeniu oferowanych rozwiązań szyfrujących, zrozumieć poziom zapewnianej ochrony i ocenić, czy jest on odpowiedni do istniejącego poziomu ryzyka. Administratorzy powinni również znać specyfikę działania produktów umożliwiających szyfrowanie. Na przykład urządzenie może ulegać szyfrowaniu po wyłączeniu, ale nie przy przejściu w tryb czuwania (stand-by). Niektóre produkty stosujące szyfrowanie mają „domyślny klucz”, który każdy klient musi zmienić, aby zapewnić skuteczność szyfrowania. Nawet jeśli specjaliści w dziedzinie bezpieczeństwa uznają szyfrowanie za odpowiednie, po kilku latach może się ono stać przestarzałe, co będzie rodzić wątpliwości co do tego, czy dany produkt nadal zapewnia wystarczające szyfrowanie i odpowiedni poziom ochrony.

III. Artykuł 34 - Zawiadamianie osoby, której dane dotyczą

A. Zawiadamianie osób fizycznych

W niektórych przypadkach poza zgłoszeniem naruszenia organowi nadzorczemu administrator zobowiązany jest również zawiadomić osoby fizyczne, których dane naruszono.

Art. 34 ust. 1 stanowi, że:

> „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 zgłaszanie naruszenia organowi nadzorczemu jest obowiązkowe, jeśli prawdopodobne jest narażenie na ryzyko praw i wolności osób fizycznych wskutek naruszenia. Ponadto w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych należy zawiadomić także te osoby. Próg, od którego zależy obowiązek zawiadomienia osób fizycznych o naruszeniu ich danych, jest zatem wyższy niż próg, od którego zależy obowiązek zgłoszenia naruszenia organom nadzorczym. Osób fizycznych nie trzeba zawiadamiać o wszystkich naruszeniach, co pozwala uchronić je przed zbędnym obciążeniem związanym z zawiadomieniami.

RODO stanowi, że osoby fizyczne należy zawiadamiać o naruszeniu ich danych „bez zbędnej zwłoki", czyli tak szybko, jak to możliwe. Głównym celem zawiadamiania osób fizycznych jest przekazanie im konkretnych informacji dotyczących kroków, jakie powinny podjąć, by zapewnić sobie bezpieczeństwo[36]. Jak zauważono powyżej, w zależności od charakteru naruszenia i stwarzanego przez nie ryzyka zawiadomienie na czas osób fizycznych może pomóc im ochronić się przed negatywnymi skutkami naruszenia.

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

B. Informacje, które należy przekazać

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

> „Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d)."

Administrator powinien zatem podać przynajmniej następujące informacje

- opis charakteru naruszenia;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego;
- opis prawdopodobnych konsekwencji naruszenia; oraz
- opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Przykładowo w ramach kroków podejmowanych w celu zaradzenia naruszeniu i złagodzenia jego potencjalnych negatywnych skutków administrator może oświadczyć, że po zgłoszeniu naruszenia właściwemu organowi nadzorczemu otrzymał radę w sprawie zarządzania skutkami naruszenia

[36] Patrz także Motyw 86.

i złagodzenia jego wpływu. W stosownych przypadkach administrator powinien również zapewnić odpowiednią radę osobom fizycznym, tak aby mogły się ochronić przed potencjalnymi negatywnymi skutkami naruszenia, np. zresetować hasła w przypadku naruszenia bezpieczeństwa ich danych dostępowych. Administrator może też postanowić przekazać więcej informacji niż jest to wymagane.

C. Kontaktowanie się z osobami fizycznymi

Co do zasady o naruszeniu ochrony danych osobowych osoby, których ono dotyczy, powinny być zawiadamiane bezpośrednio, chyba że wymagałoby to niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób (art.34 ust. 3 lit. c).

Do zawiadamiania o naruszeniu osób, których dane naruszono, należy stosować komunikaty dedykowane, których nie należy przesyłać razem z innymi informacjami, takimi jak aktualizacje, biuletyny czy standardowe komunikaty. Pomaga to w jasnym i przejrzystym zawiadomieniu o naruszeniu.

Przykładami przejrzystych metod komunikacji są: wiadomości bezpośrednie (np. e-mail, SMS, wiadomość bezpośrednia), widoczne banery lub zawiadomienia na stronach internetowych, przesyłki pocztowe i widoczne zawiadomienia w prasie. Zawiadomienia ograniczającego się do komunikatu prasowego czy firmowego bloga nie uznaje się za skuteczne zawiadomienie osoby fizycznej o naruszeniu. GR Art. 29 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 odpowiednich formatach alternatywnych i we właściwym języku, tak aby osoby fizyczne, których dane naruszono, mogły zrozumieć przekazywane informacje. Przykładowo w przypadku zawiadamiania o naruszeniu osoby fizycznej odpowiedni będzie język używany w normalnej codziennej komunikacji z takim odbiorcą. Jeżeli jednak naruszenie ma wpływ na osoby, których dane dotyczą, z którymi administrator nie miał uprzednio kontaktu, lub w szczególności osoby, które zamieszkują w innym państwie członkowskim lub w innym państwie poza UE niż to, gdzie znajduje się jednostka organizacyjna administratora, wówczas dopuszczalna jest komunikacja w języku lokalnym, z uwzględnieniem wymaganych zasobów. Kluczowe jest, aby pomóc osobie, której dane dotyczą, zrozumieć charakter naruszenia i kroki, które może podjąć, by zapewnić sobie ochronę.

Administratorzy mają największe możliwości określenia najbardziej odpowiedniego kanału komunikacji w celu zawiadomienia osób fizycznych o naruszeniu, zwłaszcza w przypadku częstych kontaktów z klientami. Administrator powinien jednak zachować ostrożność odnośnie kanału komunikacji, którego bezpieczeństwo zostało narażone wskutek naruszenia, ponieważ mogą z niego korzystać również osoby odpowiedzialne za naruszenie, podszywające się pod administratora.

Jednocześnie Motyw 86 wyjaśnia:

> „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 zawiadamiania o naruszeniu osób, których dane dotyczą, zgodnie z art. 34, ale również

odnośnie odpowiednich komunikatów i najodpowiedniejszego sposobu przekazania ich osobom fizycznym.

Wiąże się to z zaleceniem przedstawionym w Motywie 88, który stanowi, że w przypadku zawiadomienia „należy ponadto uwzględnić prawnie uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia ochrony danych osobowych." Może to oznaczać, że w określonych okolicznościach, gdy jest to uzasadnione, i za radą organów ścigania, administrator może opóźnić zawiadomienie o naruszeniu osób, których ono dotyczy, do momentu, gdy nie będzie to utrudniało postępowania w sprawie tego naruszenia. Osoby, których dane dotyczą, nadal będą jednak musiały zostać niezwłocznie zawiadomione po tym czasie.

Jeśli administrator nie jest w stanie zawiadomić osoby o naruszeniu, ponieważ nie ma wystarczających danych umożliwiających skontaktowanie się z nią, powinien poinformować tę osobę tak szybko, jak to jest rozsądnie możliwe (np. gdy taka osoba będzie wykonywać swoje prawo do dostępu do danych osobowych na mocy art. 15 i przekaże administratorowi niezbędne dodatkowe informacje, umożliwiające skontaktowanie się z nią).

D. Warunki, w których nie jest wymagane zawiadomienie

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

- Administrator wdrożył przed naruszeniem odpowiednie techniczne i organizacyjne środki ochrony danych osobowych, w szczególności środki uniemożliwiające ich odczyt osobom nieuprawnionym do dostępu do nich. Może to na przykład obejmować zabezpieczenie danych osobowych za pomocą szyfrowania zgodnego z aktualnym stanem wiedzy technicznej lub tokenizację.
- Niezwłocznie po naruszeniu administrator podjął kroki w celu zapewnienia, że nie ma prawdopodobieństwa wystąpienia wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej, której dane dotyczą. Przykładowo 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, z uwzględnieniem charakteru danych.
- Skontaktowanie się z osobami, których dane dotyczą, wymagałoby niewspółmiernie dużego wysiłku[37], na przykład w sytuacji, gdy ich dane kontaktowe zostały utracone w wyniku naruszenia lub nie były nigdy znane. Na przykład, gdy magazyn urzędu statystycznego uległ zalaniu, a dokumenty zawierające dane osobowe przechowywano jedynie w formie papierowej. Administrator musi w takim przypadku wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób. W przypadku niewspółmiernie dużego wysiłku można przewidzieć rozwiązania techniczne zapewniające dostępność informacji o naruszeniu na żądanie, co może okazać się przydatne dla osób, których dane zostały naruszone, 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 spełniają jeden lub kilka z tych warunków[38]. Należy mieć na uwadze, że nawet jeśli zgłoszenie 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.

Jeżeli administrator postanowi nie zawiadamiać osoby, której naruszenie dotyczy, zgodnie z art. 34 ust.

[37] Patrz Wytyczne GR Art. 29 w sprawie przejrzystości, które uwzględniają kwestię niewspółmiernie dużego wysiłku, dostępne na stronie http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850
[38] Patrz art. 5 ust. 2.

4 organ nadzorczy może od niego tego zażądać w przypadku uznania, że naruszenie może stanowić wysokie ryzyko dla osób fizycznych. Ewentualnie może uznać, że zostały spełnione warunki określone w art. 34 ust. 3, a zatem zawiadomienie osób fizycznych nie jest wymagane. Jeżeli organ nadzorczy uzna decyzję o niezawiadamianiu osób, których dane dotyczą, 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 RODO wprowadza obowiązek zgłoszenia naruszenia, nie jest ono wymagane we wszystkich okolicznościach:

- Zgłoszenie naruszenia właściwemu organowi nadzorczemu jest wymagane, chyba że jest mało prawdopodobne, by naruszenie naraziło na ryzyko prawa i wolności osób fizycznych.
- Zawiadomienie osoby fizycznej o naruszeniu jest wymagane tylko, jeśli jest prawdopodobne, że naruszenie spowoduje wysokie ryzyko naruszenia praw lub wolności tej osoby.

Niezwykle ważne jest zatem, by natychmiast po stwierdzeniu naruszenia administrator nie tylko starał się mu zaradzić, ale także ocenił ryzyko, jakie może ono stworzyć. Są ku temu dwie ważne przesłanki: po pierwsze określenie prawdopodobieństwa i wagi potencjalnych skutków dla osoby fizycznej, której dane dotyczą, pomoże administratorowi podjąć skuteczne działania w celu zaradzenia naruszeniu; po drugie, pomoże mu to ustalić, czy konieczne jest zgłoszenie naruszenia organowi nadzorczemu i, jeśli to wymagane, zawiadomienie o nim osób fizycznych, których ono dotyczy.

Jak wyjaśniono powyżej zgłoszenie naruszenia jest wymagane, chyba że jest mało prawdopodobne, by naruszenie naraziło na ryzyko prawa i wolności osób fizycznych, a kluczowym warunkiem rodzącym wymóg zawiadomienia osób fizycznych o naruszeniu jest *wysokie* ryzyko dla ich praw i wolności. Takie ryzyko istnieje, gdy 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 rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych lub obejmuje dane genetyczne, dane dotyczące zdrowia lub życia seksualnego, wyroków skazujących i wykroczeń lub związanych z nimi środków bezpieczeństwa, należy uznać, że występuje duże prawdopodobieństwo takiej szkody[39].

B. Czynniki, jakie należy uwzględnić przy ocenie ryzyka

Zgodnie z Motywami 75 i 76 RODO przy ocenie ryzyka należy uwzględnić zarówno prawdopodobieństwo, jak i potencjalną powagę ryzyka naruszenia praw i wolności osób, których dane dotyczą. Ponadto stanowią one, że ryzyko należy oszacować na podstawie obiektywnej oceny.

[39] Patrz Motyw 75 i Motyw 85.

Należy zauważyć, że ocena ryzyka dla praw i wolności osób w wyniku naruszenia skupia się na innych zagadnieniach niż ocena skutków dla ochrony danych[40]. Ocena skutków dla ochrony danych uwzględnia zarówno ryzyko związane z przetwarzaniem danych zgodnie z planem, jak i ryzyko w przypadku naruszenia. Rozważając możliwe naruszenie administrator dokonuje ogólnej oceny prawdopodobieństwa jego wystąpienia oraz szkody, jaką może ponieść osoba, której dane dotyczą, innymi słowy – oceny hipotetycznego zdarzenia. W przypadku rzeczywistego naruszenia, zdarzenie miało już miejsce, więc cała uwaga powinna skupiać się na ryzyku wynikającym z naruszenia dla osób fizycznych.

Przykład

Zgodnie z oceną skutków dla ochrony danych konkretne oprogramowanie zapewniające bezpieczeństwo w celu ochrony danych osobowych jest odpowiednim środkiem zapewniającym poziom ochrony adekwatny do ryzyka, na jakie przetwarzanie danych narażałoby w przeciwnym razie osoby fizyczne. Jeśli jednak w późniejszym czasie odkryta zostanie podatność, 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.

Podatność produktu zostaje później wykorzystana i ma miejsce naruszenie. Administrator powinien ocenić konkretne okoliczności naruszenia, naruszone dane i poziom potencjalnych skutków dla osób fizycznych, a także prawdopodobieństwo zaistnienia takiego ryzyka.

Podobnie przy ocenie ryzyka dla osób fizycznych w następstwie naruszenia administrator powinien wziąć pod uwagę konkretne okoliczności naruszenia, w tym powagę potencjalnych skutków i prawdopodobieństwo ich wystąpienia. GR Art. 29 zaleca zatem, by przy ocenie uwzględnić następujące kryteria[41]:

- Rodzaj naruszenia

Rodzaj naruszenia może mieć wpływ na poziom ryzyka dla osób fizycznych. Przykładowo naruszenie poufności, wskutek którego osobom nieupoważnionym ujawnione zostały informacje medyczne może mieć inne konsekwencje dla osoby fizycznej niż naruszenie, wskutek którego dane medyczne osoby fizycznej zostają utracone i nie są już dostępne.

- Charakter, wrażliwość i ilość danych osobowych

Kluczowym czynnikiem przy ocenie ryzyka jest rodzaj i wrażliwość danych osobowych, których ochrona została naruszona. Z reguły im wrażliwsze dane, tym wyższe ryzyko szkód dla osób, na które naruszenie ma wpływ, jednakże należy również wziąć pod uwagę inne dane osobowe, które dotyczą tych osób i mogą być już dostępne. Na przykład ujawnienie nazwiska i adresu osoby fizycznej w zwyczajnych okolicznościach najprawdopodobniej nie doprowadzi do istotnej szkody. Natomiast ujawnienie nazwiska i adresu rodzica przysposabiającego rodzicowi biologicznemu może mieć bardzo poważne konsekwencje zarówno dla rodzica przysposabiającego, jak i dla dziecka.

Naruszenia dotyczące danych na temat stanu zdrowia, dokumentów tożsamości lub danych finansowych takich jak szczegóły kart kredytowych mogą z osobna powodować szkody, ale w połączeniu mogą zostać wykorzystane do kradzieży tożsamości. Większa ilość powiązanych danych osobowych jest zazwyczaj bardziej wrażliwa niż pojedyncza dana osobowa.

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

[41] Art. 3 ust. 2 rozporządzenia 611/2013 dostarcza wskazówek, jakie czynniki należy wziąć pod uwagę w związku z powiadomieniem o naruszeniach w sektorze usług komunikacji elektronicznej, co może być przydatne w kontekście zgłaszania na mocy RODO. Patrz http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:P DF

Niektóre rodzaje danych osobowych mogą początkowo wydawać się względnie nieszkodliwe, jednakże należy dokładnie rozważyć, 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 urlopu, mogą okazać się użyteczne dla przestępców.

Niewielka ilość bardzo wrażliwych danych osobowych może mieć duży wpływ na osobę fizyczną, a duży zakres danych może ujawnić więcej informacji na jej temat. Naruszenie wpływające na dużą ilość danych osobowych na temat wielu osób, których dane dotyczą, może mieć wpływ na odpowiednio dużą liczbę osób.

- Łatwość identyfikacji osób fizycznych

Ważnym czynnikiem do uwzględnienia jest to, z jaką łatwością osoba trzecia, która uzyskała dostęp do danych w wyniku naruszenia, może wykorzystać je w celu zidentyfikowania poszczególnych osób fizycznych lub dopasować te dane do innych informacji w celu zidentyfikowania osób fizycznych. W zależności od okoliczności identyfikacja może być możliwa bezpośrednio w oparciu o dane osobowe, których dotyczyło naruszenie, bez konieczności zbierania dodatkowych informacji, lub dopasowanie danych osobowych do konkretnej osoby fizycznej może okazać się bardzo trudne, ale wciąż możliwe w konkretnych okolicznościach. Identyfikacja może być możliwa bezpośrednio lub pośrednio w oparciu o naruszone dane, ale może również zależeć od konkretnego kontekstu naruszenia i publicznej dostępności powiązanych danych osobowych. Może być to bardziej istotne w przypadku naruszeń poufności i dostępności.

Jak opisano powyżej odczyt danych osobowych chronionych odpowiednim poziomem zaszyfrowania jest niemożliwy dla nieupoważnionych osób bez klucza do deszyfrowania. Ponadto odpowiednio wdrożona pseudonimizacja (zdefiniowana w art. 4 ust. 5 jako „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej") może również zmniejszyć prawdopodobieństwo zidentyfikowania osób w przypadku naruszenia. Jednak same techniki pseudonimizacji nie mogą być uważane za uniemożliwiające odczytanie danych.

- Powaga konsekwencji dla osób fizycznych.

W zależności od charakteru danych osobowych, których dotyczy naruszenie (np. specjalne kategorie danych) możliwa szkoda dla osób fizycznych może okazać się nadzwyczaj poważna, zwłaszcza w przypadku naruszeń, które mogą skutkować kradzieżą lub sfałszowaniem tożsamości, obrażeniami fizycznymi, cierpieniem psychicznym, upokorzeniem lub naruszeniem dobrego imienia. Jeżeli naruszenie dotyczy danych osobowych osób wymagających szczególnej opieki, ryzyko szkody może być jeszcze wyższe.

Wpływ na poziom potencjalnego ryzyka może mieć również to, czy administrator jest świadomy tego, że dane osobowe znajdują się w rękach osób o nieznanych lub wrogich zamiarach. Może dojść do naruszenia poufności polegającego na przypadkowym ujawnieniu danych osobowych osobie trzeciej w rozumieniu art. 4 ust. 10 lub innemu błędnemu odbiorcy. Może mieć to miejsce na przykład w sytuacji przypadkowego przesłania danych osobowych do niewłaściwego działu organizacji lub do powszechnie stosowanego dostawcy. Administrator może zażądać od odbiorcy zwrotu lub bezpiecznego zniszczenia danych, które uzyskał. W obydwu przypadkach jeżeli relacje pomiędzy administratorem a takim odbiorcą są długotrwałe i administrator może znać procedury, historię oraz inne istotne szczegóły dotyczące odbiorcy, wówczas odbiorcę takiego można uznać za „zaufanego". Innymi słowy administrator może mieć określony poziom pewności co do odbiorcy, co pozwala mu rozsądnie oczekiwać, że odbiorca nie będzie starał się odczytać lub uzyskać dostępu do błędnie wysłanych danych, oraz że zwróci je na żądanie administratora. Nawet jeśli nastąpił dostęp do danych, administrator może potencjalnie ufać odbiorcy, że ten nie podejmie żadnych dalszych działań i niezwłocznie zwróci dane

administratorowi oraz będzie współpracować przy ich odzyskiwaniu. W takich przypadkach można to uwzględni w ocenie ryzyka przeprowadzanej przez administratora po naruszeniu - fakt, że odbiorca jest zaufany może zmniejszyć powagę konsekwencji naruszenia, ale nie oznacza, że nie nastąpiło naruszenie Może jednak skutkować wyeliminowaniem prawdopodobieństwa ryzyka dla osób fizycznych, w związku z czym nie wymaga się już zgłaszania naruszenia organowi nadzorczemu ani zawiadamiania osób, których dane naruszono. Jest to każdorazowo zależne od konkretnego przypadku. Niemniej jednak administrator musi zachować informacje dotyczące naruszenia w ramach ogólnego obowiązku prowadzenia rejestrów naruszeń (patrz pkt. V poniżej).

Należy także wziąć pod uwagę czas trwania konsekwencji dla osób fizycznych, jako że wpływ może być postrzegany jako bardziej znaczący, jeśli skutki są długofalowe.

- 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 niebezpieczeństwa. Również inne cechy osoby fizycznej mogą wpływać na to, jak duży jest wpływ naruszenia na nią.

- Cechy szczególne administratora danych

Rodzaj i rola administratora oraz jego działań mogą mieć wpływ na poziom ryzyka wynikającego z naruszenia dla osób fizycznych. Przykładowo organizacja medyczna przetwarza specjalne kategorie danych osobowych, co oznacza, że naruszenie takich danych będzie stanowić większe zagrożenie dla osób fizycznych niż ujawnienie listy dystrybucyjnej czasopisma.

- Liczba osób fizycznych, których dane naruszono

Naruszenie może dotyczyć zaledwie jednej czy kilku lub kilku tysięcy, a nawet większej liczby osób fizycznych. Im większa liczba osób fizycznych, których dane naruszono, tym większy wpływ naruszenia. Naruszenie może mieć poważne skutki dla tylko jednej osoby w zależności od rodzaju danych osobowych, które naruszono, i kontekstu naruszenia. Kluczowe jest uwzględnienie prawdopodobieństwa i powagi skutków dla osób fizycznych, których dane naruszono.

- Uwagi ogólne

Przy ocenie ryzyka, które może być skutkiem naruszenia, administrator powinien uwzględnić zarówno powagę możliwego wpływu naruszenia na prawa i wolności osób fizycznych jak i prawdopodobieństwo jego wystąpienia. Jeśli konsekwencje naruszenia są poważniejsze, ryzyko jest wyższe i analogicznie podwyższone prawdopodobieństwo ich wystąpienia oznacza podwyższone ryzyko. 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 wagi naruszenia, które administratorzy i podmioty przetwarzające dane mogą uznać za przydatne podczas tworzenia planu reagowania na naruszenie[42].

V. Rozliczalność i prowadzenie rejestrów

A. Dokumentowanie naruszeń

Niezależnie od tego, czy naruszenie wymaga zgłoszenia organowi nadzorczemu, administrator musi

[42] ENISA, Zalecenia dotyczące metodologii oceny wagi naruszenia ochrony danych osobowych, https://www.enisa.europa.eu/publications/dbn-severity

dokumentować wszystkie naruszenia 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."

Jest to powiązane z zasadą rozliczalności ustanowioną w art. 5 ust. 2 RODO. Cel rejestrowania naruszeń niepodlegających obowiązkowi zgłaszania oraz naruszeń podlegających obowiązkowi zgłaszania jest związany z obowiązkami administratora wynikającymi z art. 24, a organ nadzorczy może zażądać dostępu do takiego rejestru. Zachęca się zatem administratorów do tworzenia wewnętrznych rejestrów naruszeń niezależnie od tego, czy są oni zobowiązani do zgłaszania ich czy też nie[43].

Administrator określa sposób i strukturę dokumentowania naruszeń, niemniej jednak istnieją pewne kluczowe elementy odnośnie rejestrowanych informacji, które muszą zostać zawarte w każdym przypadku. Jak stanowi art. 33 ust. 5 administrator jest zobowiązany dokumentować informacje o naruszeniu obejmujące jego przyczyny, przebieg i s i dane osobowe, których ono dotyczyło. Powinny one również zawierać skutki i konsekwencje naruszenia oraz działania naprawcze podjęte przez administratora.

RODO nie określa czasu przechowywania takiej dokumentacji. W przypadku, gdy rejestr zawiera dane osobowe, obowiązkiem administratora będzie określenie odpowiedniego okresu przechowywania zgodnie z zasadami dotyczącymi przetwarzania danych osobowych[44] oraz spełnienie wymogów odnośnie podstawy prawnej przetwarzania[45]. Administrator musi przechowywać dokumentację zgodnie z art. 33 ust. 5 na wypadek, gdyby został wezwany do udowodnienia przed organem nadzorczym spełnienia wymogów zapisanych w tym artykule lub zgodności z zasadą rozliczalności. Jeżeli takie rejestry nie zawierają danych osobowych, wówczas zasada ograniczenia przechowywania[46] zawarta w RODO nie ma zastosowania.

Oprócz tego GR Art. 29 zaleca również dokumentowanie uzasadnienia decyzji podjętej w odpowiedzi na naruszenie. W szczególności należy udokumentować powody decyzji o niezgłoszeniu naruszenia. Należy także podać przyczyny, dla których administrator uważa, że jest mało prawdopodobne, by naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych[47]. Ewentualnie, jeżeli administrator uzna, że spełniony jest któryś z warunków opisanych w art. 34 ust. 3, powinien być w stanie przedstawić odnośne dowody.

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 opóźnienie było uzasadnione i nienadmierne.

Przy zawiadamianiu osób fizycznych o naruszeniu ochrony ich danych administrator powinien przedstawić naruszenie w przejrzysty sposób i poinformować o nim skutecznie i na czas. Zachowanie dowodów zawiadomienia pomoże mu wykazać rozliczalność i zgodność z przepisami.

Dla zgodności z art. 33 i 34 korzystne jest, by zarówno administratorzy, jak i podmioty przetwarzające wdrożyły udokumentowaną procedurę zgłaszania naruszeń określającą zasady postępowania na wypadek wykrycia naruszenia, w tym sposoby ograniczania skutków, zarządzania i zaradzania mu, jak również obejmującą ocenę ryzyka, i zgłaszania naruszenia. W celu wykazania zgodności z RODO przydatne może być także wykazanie, że pracownicy zostali poinformowani o istnieniu tego rodzaju procedur i mechanizmów oraz wiedzą, jak powinni reagować na naruszenia.

[43] Administrator może postanowić o dokumentowaniu naruszeń we własnym rejestrze czynności przetwarzania prowadzonym zgodnie z art. 30. Nie wymaga się prowadzenia osobnego rejestru, jeżeli informacje dotyczące naruszenia można łatwo zidentyfikować i przedłożyć na żądanie.
[44] Patrz art. 5.
[45] Patrz art. 6 i art. 9.
[46] Patrz art. 5 ust. 1 lit. e.
[47] Patrz Motyw 85.

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 posiadać inspektora ochrony danych (IOD)[48] zgodnie z wymogami art. 37 lub dobrowolnie w ramach dobrych praktyk. Art. 39 RODO określa szereg obowiązkowych zadań IOD, ale nie zabrania przydzielania mu kolejnych zadań przez administratora, jeśli to konieczne.

Do najistotniejszych obowiązkowych zadań IOD w zakresie zgłaszania naruszeń należą między innymi: udzielanie administratorowi lub podmiotowi przetwarzającemu porad dotyczących ochrony danych oraz monitorowanie zgodności z RODO, a także udzielanie porad dotyczących oceny skutków dla ochrony danych. IOD musi także współpracować z organem nadzorczym i stanowić punkt kontaktowy dla organu nadzorczego i osób, których dane dotyczą. Należy również zauważyć, że w przypadku zgłoszenia naruszenia organowi nadzorczemu zgodnie z art. 33 ust. 3 lit. b administrator zobowiązany jest podać nazwisko i dane kontaktowe swojego IOD lub innego punktu kontaktowego.

W zakresie dokumentowania naruszeń administrator lub podmiot przetwarzający może chcieć uzyskać opinię IOD w zakresie struktury, tworzenia i administrowania taką dokumentacją. IOD można również dodatkowo powierzyć zadanie prowadzenia takich rejestrów.

Oznacza to, że IOD powinien odgrywać kluczową rolę w zapobieganiu lub przygotowywaniu się na naruszenia, udzielając porad i monitorując przestrzeganie przepisów, a także gdy dojdzie do naruszenia (tj. przy zgłaszaniu go organowi nadzorczemu) oraz podczas wszelkich dalszych postępowań prowadzonych przez organ nadzorczy. Dlatego też GR Art. 29 zaleca, aby IOD był niezwłocznie informowany o zaistnieniu naruszenia i był zaangażowany w cały proces zarządzania naruszeniem i zgłaszania go.

VI. Obowiązki zgłaszania naruszeń na mocy innych instrumentów prawnych

Oprócz i poza obowiązkiem zgłaszania naruszeń organowi nadzorczemu i zawiadamiania o naruszeniach osób, których dane dotyczą wynikającym z RODO administratorzy powinni również być świadomi wymogów odnośnie zgłaszania zdarzeń naruszających bezpieczeństwo na mocy innych obowiązujących aktów prawnych, które mogą mieć do nich zastosowanie, oraz czy może to również wymagać od nich jednoczesnego zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu. Wymogi takie mogą się różnić w poszczególnych państwach członkowskich. Poniżej podano przykłady wymogów zgłaszania i powiadamiania o naruszeniach na mocy innych instrumentów prawnych oraz ich związek z RODO:

- Rozporządzenie (EU) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS)[49].

Art. 19 ust. 2 rozporządzenia eIDAS wymaga od dostawców usług zaufania zawiadomienia organu nadzoru o przypadkach naruszenia bezpieczeństwa lub utraty integralności, które mają znaczący wpływ na świadczoną usługę zaufania lub przetwarzane w jej ramach dane osobowe. W stosownych przypadkach, tj. jeśli takie naruszenie bezpieczeństwa lub utrata integralności stanowi także naruszenie ochrony danych osobowych na mocy RODO, dostawca usług zaufania powinien także zgłosić je organowi nadzorczemu.

- Dyrektywa (UE) 2016/1148 dotycząca środków zapewniających wysoki wspólny poziom

[48] Patrz wytyczne GR Art. 29 dotyczące inspektorów ochrony danych na stronie http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[49] Patrz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

bezpieczeństwa sieci i systemów informatycznych w całej Unii (dyrektywa NIS)[50].

Art. 14 i 16 dyrektywy NIS zobowiązują podmioty świadczące usługi podstawowe i dostawców usług cyfrowych do zgłaszania właściwemu organowi nadzorczemu zdarzeń naruszających bezpieczeństwo. Motyw 63 dyrektywy NIS[51] stanowi, że w wielu przypadkach w wyniku incydentów istnieje niebezpieczeństwo naruszenia danych osobowych. O ile dyrektywa NIS wymaga od właściwych organów i organów nadzorczych współpracy i wymiany informacji w tym kontekście, to jednak w przypadku, gdy takie incydenty są lub staną się naruszeniami ochrony danych osobowych na mocy RODO, tacy operatorzy i/lub dostawcy będą musieli zgłosić naruszenie organowi nadzorczemu osobno od wynikających z dyrektywy NIS obowiązków dotyczących powiadamiania o incydentach.

Przykład

Dostawca usług w chmurze obliczeniowej zgłaszający naruszenie na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji może również stanąć przed koniecznością zgłoszenia go administratorowi, jeżeli naruszenie dotyczy ochrony danych osobowych. Podobnie od dostawcy usług zaufania zgłaszającego naruszenie zgodnie z rozporządzeniem eIDAS może być wymagane zgłoszenie go właściwemu organowi ochrony danych.

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

Dostawcy ogólnie dostępnych usług łączności elektronicznej w rozumieniu dyrektywy 2002/58/WE[52] muszą zgłaszać naruszenia właściwym organom krajowym.

Administratorzy powinni również być świadomi jakichkolwiek dodatkowych obowiązków zgłaszania o charakterze prawnym, medycznym lub zawodowym wynikających z obowiązujących przepisów prawa.

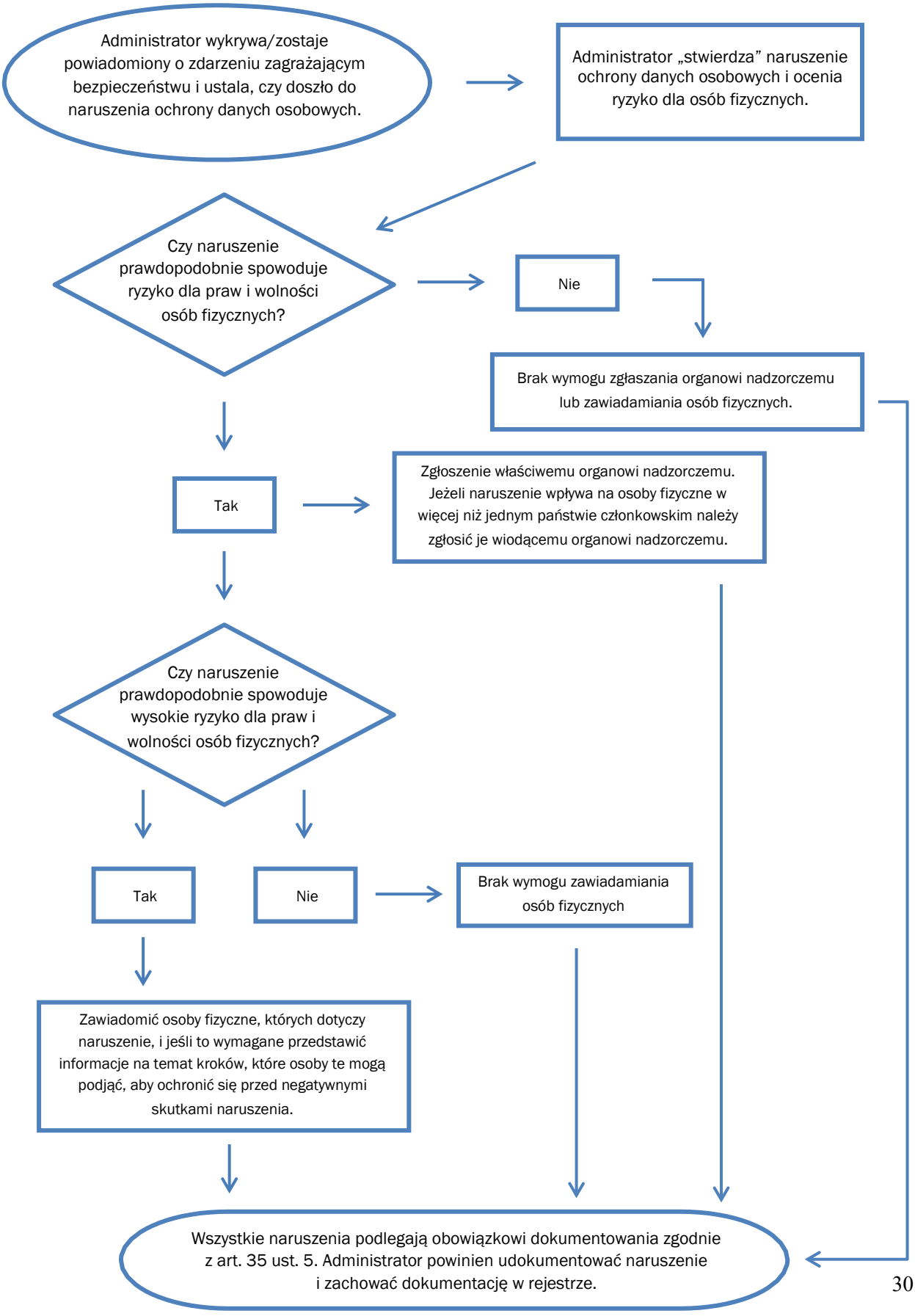
[50] Patrz http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

[51] Motyw 63: *„W wielu przypadkach istnieje niebezpieczeństwo naruszenia danych osobowych w wyniku incydentów. W tym kontekście właściwe organy oraz organy ochrony danych powinny ze sobą współpracować oraz wymieniać się informacjami dotyczącymi wszystkich istotnych kwestii w celu rozwiązywania problemów związanych z wszelkimi przypadkami naruszeń danych osobowych w wyniku incydentów."*

[52] 10 stycznia 2017 r. Komisja Europejska przedstawiła projekt rozporządzenia o prywatności i łączności elektronicznej, które zastąpi dyrektywę 2009/136/WE i zniesie wymogi dotyczące powiadamiania. Jednakże do czasu przyjęcia projektu przez Parlament Europejski w mocy pozostają obecne wymogi dotyczące powiadamiania – patrz https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic- communications

VII. Załącznik

A. Schemat przedstawiający wymogi dotyczące zgłaszania naruszeń



B. Przykłady naruszeń ochrony danych osobowych i wymogów odnośnie zgłaszania

Poniższa niewyczerpująca lista przykładów pomoże administratorom określić, czy muszą zgłosić naruszenie ochrony danych osobowych i zawiadomić osoby fizyczne w zależności od przypadku. Przykłady te mogą również być pomocne przy odróżnianiu ryzyka od wysokiego ryzyka dla praw i wolności osób fizycznych.

Przykład	**Czy należy zgłosić naruszenie organowi nadzorczemu?**	**Czy należy zawiadomić osobę, której dane dotyczą?**	**Uwagi/rekomendacje**
i. Administrator przechowywał kopię zapasową archiwum danych osobowych zaszyfrowaną na nośniku danych USB. Klucz skradziono podczas włamania.	Nie.	Nie.	Jeżeli dane są zaszyfrowane za pomocą algorytmu zgodnego ze stanem wiedzy technicznej, istnieją kopie zapasowe danych, a dane mogą zostać odzyskane we właściwym czasie, może to być naruszenie niepodlegające obowiązkowi zgłoszenia. Jeżeli jednak w późniejszym czasie coś zagrozi temu bezpieczeństwu, zgłoszenie będzie wymagane.
ii. Administrator prowadzi serwis internetowy. Dane osobowe osób fizycznych wyprowadzono w wyniku cyberataku. Administrator ma klientów w jednym kraju członkowskim.	Tak, należy zgłosić naruszenie organowi nadzorczemu, jeżeli istnieje prawdopodobieństwo konsekwencji dla osób fizycznych.	Tak, należy zawiadomić osoby fizyczne w zależności od rodzaju danych osobowych oraz , jeżeli prawdopodobne konsekwencje dla tych osób są poważne.	
iii. Z powodu krótkotrwałej przerwy w dostawie prądu w centrum obsługi telefonicznej administratora klienci nie mogli się dodzwonić i uzyskać dostępu do swoich danych.	Nie.	Nie.	To nie jest naruszenie ochrony danych osobowych podlegające obowiązkowi zgłoszenia; niemniej, zdarzenie należy zarejestrować zgodnie z art. 33 ust. 5. Administrator 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 postępowania staje się jasne, że oprogramowanie jedynie szyfruje dane, a w systemie nie wykryto żadnego innego złośliwego oprogramowania.	Tak, należy zgłosić naruszenie organowi nadzorczemu, jeżeli istnieje możliwość konsekwencji dla osób fizycznych, ponieważ doszło do utraty dostępności.	Tak, należy zawiadomić 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 zgłaszać naruszenia organowi nadzorczemu ani zawiadamiać osób fizycznych, ponieważ nie doszło do trwałej utraty dostępności lub poufności. Niemniej jeśli organ nadzorczy stwierdzi naruszenie innymi sposobami, może rozważyć przeprowadzenie postępowania w celu oceny zgodności z szerszymi wymogami bezpieczeństwa wynikającymi z art. 32.
v. Osoba fizyczna dzwoni na infolinię banku, by zgłosić naruszenie ochrony danych. Osoba ta otrzymała miesięczny wyciąg z rachunku przeznaczony dla kogoś innego. Administrator przeprowadza krótkie postępowanie (tj. zakończone w ciągu 24 godzin) i stwierdza z należytą pewnością, że doszło do naruszenia ochrony danych osobowych i może istnieć błąd w systemie, w związku z którym mogło ucierpieć więcej osób.	Tak.	Należy zawiadomić tylko poszkodowane osoby – jeżeli występuje wysokie ryzyko i jasne jest, że nie naruszono danych pozostałych osób.	Jeżeli w toku dalszego postępowania okaże się, że ucierpiało więcej osób, należy dostarczyć organowi nadzorczemu aktualne informacje, a administrator musi dodatkowo zawiadomić także inne osoby, jeżeli są narażone na wysokie ryzyko.
vi. Administrator prowadzi targ internetowy i ma klientów w wielu państwach członkowskich. Na targ przeprowadzono cyberatak, w wyniku którego w Internecie opublikowano nazwy użytkownika, hasła i historię zakupów.	Tak, należy zgłosić naruszenie wiodącemu organowi nadzorczemu, 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 zmniejszenie ryzyka. Administrator musi rozważyć inne obowiązki odnośnie zgłaszania, np. na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji, jeśli jest dostawcą usług cyfrowych.

vii. Firma hostingowa jako 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 zgłosić naruszenie swoim klientom, na których ma ono wpływ (oraz administratorom) bez zbędnej zwłoki. Zakładając, że firma hostingowa przeprowadziła własne postępowanie, 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 zgłoszenia od firmy hostingowej (podmiotu przetwarzającego). Administrator musi zgłosić naruszenie organowi nadzorczemu.	Jeśli prawdopodobnie nie ma wysokiego ryzyka dla osób fizycznych, nie trzeba ich zawiadamiać.	Firma hostingowa (podmiot przetwarzający) musi rozważyć inne obowiązki odnośnie zgłaszania (np. na mocy dyrektywy w sprawie bezpieczeństwa sieci i informacji jako dostawca usług cyfrowych). Jeżeli nie ma dowodów na wykorzystanie podatności u tego konkretnego administratora, mogło nie dojść do naruszenia podlegającego obowiązkowi zgłoszenia, ale prawdopodobnie miało miejsce zdarzenie wymagające zarejestrowania lub przypadek niezgodności z zapisami 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 zawiadomić osoby fizyczne, których dane naruszono.	
ix. W wyniku pomyłki rozesłano dane osobowe dużej liczby studentów do ponad tysiąca odbiorców za pomocą niewłaściwej listy dystrybucyjnej.	Tak, należy zgłosić naruszenie organowi nadzorczemu.	Tak, należy zawiadomić osoby fizyczne w zależności od zakresu i rodzaju naruszonych danych osobowych oraz powagi możliwych konsekwencji.	
x. W ramach marketingu bezpośredniego rozesłano pocztą elektroniczną wiadomości do odbiorców wpisanych w polu „do", a nie w polu „do wiadomości" („DW"), dając tym samym każdemu odbiorcy wgląd w adresy e-mail pozostałych odbiorców.	Tak, zgłoszenie naruszenia organowi nadzorczemu może być obowiązkowe, jeżeli ucierpiała duża liczba osób fizycznych, ujawniono dano wrażliwe (np. lista dystrybucyjna psychoterapeuty) lub wystąpiły inne czynniki wysokiego ryzyka (np. wiadomość zawierała wstępne hasła).	Tak, należy zawiadomić osoby fizyczne w zależności od zakresu i rodzaju naruszonych danych osobowych oraz powagi możliwych konsekwencji.	Zgłoszenie nie musi być konieczne, jeżeli nie ujawniono żadnych danych wrażliwych i ujawniono jedynie niewielką liczbę adresów e-mail.