Wytyczne

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

Wersja 2.0

Przyjęte 28 marca 2023 r.

Historia wersji

Wersja 1.0	10 października 2022 r.	Przyjęcie wytycznych (zaktualizowana wersja wytycznych WP250 rev.01 przyjętych przez Grupę Roboczą Art. 29 i zatwierdzonych przez EROD 25 maja 2018 r.) na potrzeby przeprowadzenia ukierunkowanych konsultacji publicznych
Wersja 2.0	28 marca 2023 r.	Przyjęcie wytycznych po ukierunkowanych konsultacjach publicznych na temat zgłaszania naruszenia ochrony danych w przypadków administratorów danych spoza EOG.

SPIS TREŚCI

0 PRZEDMOWA 5

WPROWADZENIE 5

I. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ZGODNIE Z RODO 7

A. Podstawowe kwestie dotyczące bezpieczeństwa 7

B. Czym jest naruszenie ochrony danych osobowych? 8

1. Definicja 8

2. Rodzaje naruszeń ochrony danych osobowych 8

3. Potencjalne konsekwencje naruszenia ochrony danych osobowych 10

II. ART. 33 – ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU 12

A. Kiedy należy zgłosić naruszenie? 12

1. Wymogi przewidziane w art. 33 12

2. Kiedy administrator „stwierdza" wystąpienie naruszenia? 12

3. Współadministratorzy 15

4. Obowiązki podmiotu przetwarzającego 15

B. Udzielanie informacji organowi nadzorczemu 16

1. Informacje, których należy udzielić 16

2. Sukcesywne dokonywanie zgłoszenia 18

3. Zgłoszenia dokonane z opóźnieniem 19

C. Naruszenia o charakterze transgranicznym i naruszenia w jednostkach organizacyjnych spoza UE 20

1. Naruszenia o charakterze transgranicznym 20

2. Naruszenia w jednostkach organizacyjnych spoza UE 20

D. Sytuacje, w których zgłaszanie nie jest konieczne 21

III. ART. 34 – ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ 23

A. Zawiadamianie osób fizycznych 23

B. Informacje, które należy podać 24

C. Kontakt z osobami fizycznymi 24

D. Sytuacje, w których zawiadomienie nie jest konieczne 25

IV. OCENA RYZYKA I WYSOKIEGO RYZYKA 26

A. Ryzyko a obowiązek zgłoszenia 26

B. Czynniki, które należy uwzględnić podczas oceny ryzyka 27

V. ROZLICZALNOŚĆ I PROWADZENIE DOKUMENTACJI 30

A. Dokumentowanie naruszeń 30

B. Rola inspektora ochrony danych 32

VI. OBOWIĄZKI ZGŁASZANIA OKREŚLONE W INNYCH INSTRUMENTACH PRAWNYCH 32

VII. ZAŁĄCZNIK 34

A. Schemat ilustrujący wymogi zgłaszania naruszeń 34

B. Przykłady naruszeń ochrony danych osobowych i podmiotów, które należy poinformować 35

uwzględniając art. 70 ust. 1 lit. e) i l) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (zwanego dalej „RODO"),

uwzględniając Porozumienie EOG, w szczególności załącznik XI i protokół 37 do tego Porozumienia, zmienione decyzją Wspólnego Komitetu EOG nr 154/2018 z dnia 6 lipca 2018 r.[1],

uwzględniając art. 12 i 22 swojego regulaminu wewnętrznego,

uwzględniając wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679, WP250 rev.01,

PRZYJMUJE NASTĘPUJĄCE WYTYCZNE:

0 PRZEDMOWA

1. 3 października 2017 r. Grupa Robocza Art. 29 (zwana dalej „WP29") przyjęła wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP250 rev.01)[2], które zostały zatwierdzone przez Europejską Radę Ochrony Danych (dalej „EROD") na jej pierwszym posiedzeniu plenarnym[3]. Niniejszy dokument stanowi wersję tych wytycznych, do której wprowadzono niewielkie zmiany służące ich aktualizacji. Wszelkie odniesienia do wytycznych Grupy Roboczej Art. 29 dotyczących zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP250 rev.01) należy odtąd interpretować jako odniesienie do niniejszych wytycznych EROD 9/2022.
2. EROD zwróciła uwagę na potrzebę objaśnienia wymogów dotyczących zgłaszania naruszeń ochrony danych osobowych w jednostkach organizacyjnych spoza UE. Punkt dotyczący tej kwestii poprawiono i zaktualizowano, natomiast do reszty dokumentu wprowadzono wyłącznie zmiany redakcyjne. Zmiana dotyczy konkretnie pkt 73 w sekcji II.C.2 niniejszego dokumentu.

WPROWADZENIE

3. W RODO wprowadzono wymóg zgłaszania naruszeń ochrony danych osobowych (zwanych dalej „naruszeniami") właściwemu krajowemu organowi nadzorczemu [4] (lub – w przypadku naruszeń o charakterze transgranicznym – wiodącemu organowi nadzorczemu) oraz, w określonych przypadkach, przekazywania informacji o naruszeniach osobom fizycznym, na których dane osobowe wywarły one wpływ.

[1] Odniesienia do „państw członkowskich" zawarte w niniejszym dokumencie należy rozumieć jako odniesienia do „państw członkowskich EOG".
[2] Wytyczne Grupy Roboczej Art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP250 rev.01) (ostatnio zmienione i zaktualizowane 6 lutego 2018 r.), dostępne pod adresem https://ec.europa.eu/newsroom/article29/items/612052.
[3] Zob. https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en.
[4] Zob. art. 4 ust. 21 RODO.

4. Obowiązek zgłaszania przypadków naruszeń spoczywa obecnie na określonych rodzajach organizacji, np. na dostawcach publicznie dostępnych usług łączności elektronicznej (zgodnie z dyrektywą 2009/136/WE i rozporządzeniem (UE) nr 611/2013) [5]. Niektóre państwa członkowskie również ustanowiły już wymóg zgłaszania naruszeń w swoich własnych przepisach krajowych. Wymóg ten może wiązać się z koniecznością zgłaszania naruszeń powiązanych z określonymi kategoriami administratorów i dostawców publicznie dostępnych usług łączności elektronicznej (na przykład w Niemczech i we Włoszech) lub z koniecznością powiadamiania o wszystkich naruszeniach związanych z danymi osobowymi (na przykład w Niderlandach). Inne państwa członkowskie mogą mieć stosowne kodeksy praktyk w tym zakresie (na przykład Irlandia [6]). Choć szereg organów ochrony danych zachęca administratorów do zgłaszania naruszeń, w dyrektywie 95/46/WE o ochronie danych[7], którą RODO zastąpiło, nie ustanowiono żadnego konkretnego obowiązku zgłaszania naruszeń, dlatego też wprowadzenie takiego wymogu sprawiło, że wiele organizacji musiało dostosować się do nowej sytuacji. Zgodnie z przepisami RODO wszyscy administratorzy są zobowiązani do zgłaszania naruszeń, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw lub wolności osób fizycznych [8]. Podmioty przetwarzające również mają do odegrania ważną rolę i muszą zgłaszać wszelkie naruszenia swojemu administratorowi[9].

5. EROD uważa, że wymóg powiadomienia daje szereg korzyści. Zgłaszając naruszenie organowi nadzorczemu, administratorzy mogą zasięgnąć opinii tego organu w kwestii tego, czy w danym przypadku należy przekazać stosowne informacje osobom fizycznym, na które naruszenie wywiera wpływ. Organ nadzorczy może nakazać administratorowi, aby poinformował odpowiednie osoby fizyczne o naruszeniu [10]. Zawiadomienie osób fizycznych o naruszeniu zapewnia administratorowi możliwość przekazania tym osobom informacji na temat ryzyka związanego z naruszeniem oraz wskazania działań, jakie osoby te mogą podjąć, aby uchronić się przed potencjalnymi skutkami naruszenia. Każdy plan reagowania na naruszenia powinien koncentrować się przede wszystkim na zapewnieniu ochrony osobom fizycznym i ich danym osobowym. Dlatego też mechanizm zgłaszania naruszeń powinien być postrzegany jako narzędzie przyczyniające się do poprawy przestrzegania przepisów w zakresie ochrony danych osobowych. Jednocześnie należy podkreślić, że niewywiązanie się z obowiązku zgłoszenia naruszenia osobie fizycznej albo organowi nadzorczemu może potencjalnie skutkować nałożeniem na administratora kary zgodnie z art. 83 RODO.

6. Z tego względu administratorów i podmioty przetwarzające zachęca się do opracowywania stosownych planów z wyprzedzeniem i wdrażania procedur umożliwiających wykrywanie naruszeń i szybkie ograniczanie ich negatywnych skutków, ocenianie ryzyka dla osób fizycznych[11], a następnie podejmowanie decyzji w kwestii tego, czy w danym przypadku zachodzi konieczność zgłoszenia naruszenia właściwemu organowi nadzorczemu, jak również – w stosownych przypadkach – zawiadomienia zainteresowanych osób fizycznych o naruszeniu. Zgłoszenie naruszenia organowi nadzorczemu powinno stanowić jeden z elementów takiego planu reagowania na incydenty.

---

[5] Zob. http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32009L0136 oraz http://eur-lex.europa.eu/legalcontent/PL/TXT/?uri=CELEX%3A32013R0611

[6] Zob. https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[7] Zob. http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:31995L0046

[8] Prawa zapisane w Karcie praw podstawowych UE dostępnej pod adresem: http://eurlex.europa.eu/legal-content/PL/TXT/?uri=CELEX:12012P/TXT

[9] Zob. art. 33 ust. 2 RODO. Przepis ten jest koncepcyjnie zbliżony do art. 5 rozporządzenia (UE) nr 611/2013, który stanowi, że dostawca, z którym zawarto umowę, który będzie świadczyć część usług łączności elektronicznej i który nie jest związany z abonentami bezpośrednim stosunkiem umownym, jest zobowiązany do niezwłocznego powiadomienia dostawcy zamówienia o przypadku naruszenia ochrony danych osobowych.

[10] Zob. art. 34 pkt 4 oraz art. 58 ust. 2 lit. e) RODO.

[11] Można to zagwarantować w ramach wymogu dotyczącego monitorowania i przeglądu ustanowionego w ocenie skutków dla ochrony danych, której przeprowadzenie jest konieczne w przypadku operacji przetwarzania mogących powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 i 11).

7. RODO zawiera przepisy określające, kiedy i komu należy zgłosić naruszenie, a także jakie informacje powinny znaleźć się w zgłoszeniu. Choć informacje, które muszą znaleźć się w zgłoszeniu, można przekazywać stopniowo, administratorzy powinni każdorazowo reagować na wszelkie naruszenia w odpowiednim czasie.

8. W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych[12] Grupa Robocza Art. 29 przedstawiła wytyczne dla administratorów, aby ułatwić im podjęcie decyzji w kwestii tego, czy w danym przypadku osoby, których dane dotyczą, powinny zostać zawiadomione o naruszeniu. W opinii wzięto pod uwagę obowiązki spoczywające na dostawcach usług łączności elektronicznej zgodnie z dyrektywą 2002/58/WE, zaprezentowano przykłady zaczerpnięte z wielu sektorów w kontekście RODO, które wówczas znajdowało się na etapie projektu, i przedstawiono dobre praktyki dla wszystkich administratorów.

9. W niniejszych wytycznych objaśniono ustanowione w RODO wymogi w zakresie obowiązkowego zgłaszania naruszeń i zawiadamiania o naruszeniach oraz omówiono niektóre działania, jakie administratorzy i podmioty przetwarzające mogą podjąć, aby należycie wywiązać się z tych zobowiązań. Przedstawiono w nich również przykłady różnych rodzajów naruszeń oraz wskazano podmioty, którym w poszczególnych scenariuszach należałoby zgłosić naruszenie.

I. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ZGODNIE Z RODO

A. Podstawowe kwestie dotyczące bezpieczeństwa

10. Zgodnie z jednym z wymogów ustanowionych w RODO dane osobowe muszą być przetwarzane za pomocą odpowiednich środków technicznych i organizacyjnych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem[13].

11. Tym samym przepisy RODO zobowiązują zarówno administratorów, jak i podmioty przetwarzające do przyjęcia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku związanemu z przetwarzaniem danych osobowych. Administratorzy i podmioty przetwarzające powinni uwzględnić stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze[14]. Ponadto w RODO ustanowiono wymóg przyjęcia wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych, co z kolei ma decydujące znaczenie dla ustalenia, czy w danym przypadku obowiązek zgłoszenia naruszenia ma zastosowanie[15].

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

---

[12] Zob. Opinia WP29 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[13] Zob. art. 5 ust. 1 lit. f) i art. 32 RODO.

[14] Art. 32; zob. również motyw 83 RODO.

[15] Zob. motyw 87 RODO.

B. Czym jest naruszenie ochrony danych osobowych?

1. Definicja

13. Podejmując jakiekolwiek działania mające na celu zaradzenie naruszeniu, administrator powinien w pierwszej kolejności potwierdzić jego wystąpienie. Termin „naruszenie ochrony danych osobowych" został zdefiniowany w art. 4 pkt 12 RODO 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".

14. To, co należy rozumieć pod pojęciem „zniszczenia" danych osobowych, powinno być stosunkowo jasne: pojęcie to odnosi się do sytuacji, w której dane już nie istnieją lub przestały istnieć w postaci, w której administrator mógłby je w jakikolwiek sposób wykorzystać. Znaczenie pojęcia „uszkodzenie" również powinno być stosunkowo oczywiste: odnosi się ono do sytuacji, w której dane osobowe zostały zmodyfikowane, zniekształcone lub przestały być kompletne. Jeżeli chodzi o pojęcie „utraty" danych osobowych, należy interpretować je jako odnoszące się do sytuacji, w której dane mogą nadal istnieć, ale administrator utracił nad nimi kontrolę, nie posiada już do nich dostępu lub nie znajdują się one już w jego posiadaniu. Nieuprawnione lub niezgodne z prawem przetwarzanie może oznaczać ujawnienie (lub udostępnienie) danych osobowych odbiorcom, którzy nie są upoważnieni do ich otrzymania (lub do uzyskania do nich dostępu), lub jakąkolwiek inną formę przetwarzania skutkującą naruszeniem przepisów RODO.

> **Przykład**
>
> Przykładem utraty danych osobowych może być sytuacja, w której dochodzi do zgubienia lub kradzieży urządzenia, na którym przechowywana jest kopia bazy danych klientów administratora. Kolejnym przykładem zdarzenia skutkującego utratą danych może być również sytuacja, w której jedyna kopia zbioru danych osobowych została zaszyfrowana wskutek zastosowania oprogramowania typu ransomware, lub sytuacja, w której administrator zaszyfrował dane za pomocą klucza, który nie znajduje się już w jego posiadaniu.

15. W tym kontekście należy podkreślić, że naruszenie jest rodzajem incydentu bezpieczeństwa. Jak jednak wskazano w art. 4 pkt 12, przepisy RODO mają zastosowanie wyłącznie w przypadku, gdy dochodzi do naruszenia ochrony danych osobowych. Wystąpienie takiego naruszenia prowadzi do sytuacji, w której administrator nie jest w stanie zapewnić zgodności z zasadami dotyczącymi przetwarzania danych osobowych ustanowionymi w art. 5 RODO. Stanowi to element pozwalający odróżnić incydent bezpieczeństwa od zdarzenia skutkującego naruszeniem ochrony danych osobowych – co do zasady, choć wszystkie przypadki naruszenia ochrony danych osobowych są incydentami bezpieczeństwa, nie wszystkie incydenty bezpieczeństwa muszą wiązać się z naruszeniem ochrony danych osobowych[16].

16. Poniżej omówiono potencjalne negatywne skutki naruszenia ochrony danych osobowych dla osób fizycznych.

2. Rodzaje naruszeń ochrony danych osobowych

17. W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia Grupa Robocza Art. 29 wyjaśniła, że zgodnie z trzema powszechnie uznawanymi zasadami bezpieczeństwa informacji[17] naruszenia można podzielić na następujące kategorie:

---

[16] Należy podkreślić, że zakres pojęcia „incydent bezpieczeństwa" nie ogranicza się wyłącznie do modeli zagrożeń, w których źródło ataku na organizację znajduje się poza organizacją, ale obejmuje również incydenty związane z przetwarzaniem danych wewnątrz organizacji w sposób naruszający zasady bezpieczeństwa.

[17] Zob. opinia WP29 03/2014.

- „**naruszenie dotyczące poufności danych**” – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

- „**naruszenie dotyczące integralności danych**” – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych.

- „**naruszenie dotyczące dostępności danych**” – naruszenie, w rezultacie którego dochodzi do przypadkowej lub nieuprawnionej utraty dostępu [18] do danych osobowych lub zniszczenia danych osobowych.

18. Należy również podkreślić, że – w zależności od okoliczności – naruszenie może dotyczyć jednocześnie poufności, integralności i dostępności danych, a także dowolnego połączenia dwóch spośród tych trzech kategorii naruszeń.

19. Choć ustalenie, czy w danym przypadku doszło do naruszenia dotyczącego poufności lub integralności danych, jest stosunkowo łatwe, stwierdzenie wystąpienia naruszenia dotyczącego dostępności danych może okazać się trudniejsze. Naruszenie zostanie każdorazowo uznane za naruszenie dotyczące dostępności danych, jeżeli doprowadziło ono do trwałej utraty lub zniszczenia danych osobowych.

Przykład

Przykłady utraty dostępności obejmują sytuacje, w których doszło do przypadkowego usunięcia danych albo ich usunięcia przez nieuprawnioną osobę, lub – w przypadku bezpiecznie zaszyfrowanych danych – sytuacje, w których utracono klucz deszyfrujący. Sytuację, w której administrator nie jest w stanie przywrócić dostępu do danych, na przykład korzystając z kopii bezpieczeństwa, uznaje się za sytuację, w której doszło do trwałej utraty dostępności.

Do utraty dostępności może dojść również w przypadku poważnego zakłócenia normalnego sposobu funkcjonowania organizacji, np. wskutek awarii systemu zasilania lub ataku typu „odmowa usługi”, skutkującego utratą dostępu do danych osobowych.

20. W tym kontekście warto zastanowić się nad tym, czy tymczasowa utrata dostępności danych osobowych powinna zostać uznana za sytuację, w której doszło do wystąpienia naruszenia, a jeżeli tak – czy naruszenie to należy zgłosić. W art. 32 RODO zatytułowanym „Bezpieczeństwo przetwarzania” wyjaśniono, że przy wdrażaniu środków technicznych i organizacyjnych pozwalających zapewnić stopień bezpieczeństwa odpowiadający ryzyku, należy wziąć pod uwagę m.in. „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”.

21. Dlatego też incydent bezpieczeństwa skutkujący utratą dostępu do danych osobowych przez określony czas również stanowi rodzaj naruszenia, ponieważ brak dostępu do danych może wywrzeć istotny wpływ na prawa lub wolności osób fizycznych. Gwoli wyjaśnienia, jeżeli dane osobowe są niedostępne

[18] Powszechnie przyjmuje się, że pojęcie „dostępu” stanowi zasadniczo element pojęcia „dostępności”. Zob. na przykład dokument NIST SP80053rev4, w którym przedstawiono następującą definicję terminu „dostępność”: „zapewnienie możliwości uzyskania terminowego i niezawodnego dostępu do informacji oraz możliwości terminowego i niezawodnego korzystania z informacji”; dokument jest dostępny pod adresem http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. W dokumencie CNSSI-4009 wspomina się również o: „terminowym i niezawodnym dostępie do usług w zakresie danych i informacji dla upoważnionych użytkowników”. Zob. https://rmf.org/wpcontent/uploads/2017/10/CNSSI-4009.pdf. Również w normie ISO/IEC 27000:2016 „dostępność” zdefiniowano jako „właściwość polegającą na tym, że cechujący się nią obiekt jest dostępny i gotowy do wykorzystania na żądanie uprawnionego podmiotu”: https://www.iso.org/obp/ui/#iso:std:isoiec:27000:ed-4:v1:en

z uwagi na fakt, że system jest poddawany wcześniej zaplanowanym pracom konserwacyjnym, taka sytuacja nie stanowi przypadku „naruszenia bezpieczeństwa", o którym mowa w definicji ustanowionej w art. 4 pkt 12 RODO.

22. Naruszenie skutkujące tymczasową utratą dostępności danych powinno zostać udokumentowane zgodnie z art. 33 ust. 5 RODO, podobnie jak naruszenie skutkujące trwałą utratą lub zniszczeniem danych osobowych (lub dowolny inny rodzaj naruszenia). Ułatwi to administratorowi wykazanie rozliczalności przed organem nadzorczym, który może zwrócić się o udostępnienie mu rejestrów do wglądu[19]. W zależności od specyfiki danego naruszenia konieczne może jednak okazać się zgłoszenie go organowi nadzorczemu lub zawiadomienie o jego wystąpieniu osób fizycznych, na które wywiera ono wpływ. Administrator będzie musiał ocenić prawdopodobieństwo wystąpienia i wagę wpływu na prawa lub wolności osób fizycznych w związku z brakiem dostępności danych osobowych. Zgodnie z art. 33 RODO administrator jest zobowiązany do zgłoszenia naruszenia, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw lub wolności osób fizycznych. Kwestię tę trzeba będzie oczywiście ocenić w poszczególnych przypadkach.

Przykład

Utrata dostępu do kluczowych danych medycznych w szpitalu – nawet jeżeli ma wyłącznie tymczasowy charakter – może wiązać się z ryzykiem naruszenia praw lub wolności osób fizycznych; wystąpienie takiej sytuacji może np. wiązać się z koniecznością odwołania operacji, co stwarza zagrożenie dla życia pacjentów.

Z kolei jeżeli przedsiębiorstwo medialne nie mogło przesłać swoim subskrybentom biuletynów informacyjnych z uwagi na kilkugodzinną utratę dostępu do swoich systemów (np. z powodu awarii systemu zasilania), prawdopodobieństwo, że taka sytuacja będzie wiązała się z ryzykiem naruszenia praw lub wolności osób fizycznych, nie istnieje.

23. Należy podkreślić, że choć utrata dostępu do systemów administratora może mieć wyłącznie tymczasowy charakter i może nie wywierać wpływu na osoby fizyczne, administrator powinien wziąć pod uwagę wszystkie potencjalne konsekwencje naruszenia, ponieważ może ono nadal wymagać zgłoszenia z innych względów.

Przykład

Zainfekowanie oprogramowaniem typu ransomware (złośliwym oprogramowaniem, które szyfruje dane administratora do momentu zapłacenia okupu) mogłoby doprowadzić do tymczasowej utraty dostępności, jeżeli w danym przypadku możliwe byłoby przywrócenie danych z kopii bezpieczeństwa. Nie zmienia to jednak faktu, że włamanie do sieci miało miejsce i może podlegać obowiązkowi zgłoszenia, jeżeli dany incydent zostanie uznany za naruszenie dotyczące poufności danych (tj. jeżeli hakerowi udało się uzyskać dostęp do danych osobowych) i wiąże się z ryzykiem naruszenia praw lub wolności osób fizycznych.

3. Potencjalne konsekwencje naruszenia ochrony danych osobowych

24. Naruszenie może potencjalnie wywrzeć szereg negatywnych skutków dla osób fizycznych, które mogą skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub szkód niemajątkowych. W RODO wyjaśniono, że takie skutki mogą obejmować utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, dyskryminację, kradzież lub sfałszowanie tożsamości, stratę finansową, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia oraz naruszenie poufności

[19]Zob. art. 33 ust. 5 RODO.

danych osobowych chronionych tajemnicą zawodową. Mogą one również wiązać się z wszelkimi innymi znacznymi szkodami gospodarczymi lub społecznymi dla tych osób fizycznych[20].

25. Dlatego też w RODO ustanowiono wymóg zobowiązujący administratora do zgłoszenia naruszenia właściwemu organowi nadzorczemu, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem wywołania takich negatywnych skutków. Jeżeli w danym przypadku istnieje wysokie ryzyko wystąpienia negatywnych skutków, przepisy RODO zobowiązują administratora do poinformowania o naruszeniu osób fizycznych, na które wywiera ono wpływ, tak szybko, jak będzie to rozsądnie możliwe[21].

26. Znaczenie zdolności do określenia, czy w danym przypadku doszło do naruszenia, ocenienia ryzyka dla osób fizycznych oraz późniejszego zgłoszenia naruszenia w przypadkach, w których będzie to konieczne, podkreślono w motywie 87 RODO:

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

27. Dalsze wytyczne dotyczące oceny ryzyka negatywnych skutków dla osób fizycznych przedstawiono w sekcji IV.

28. Jeżeli administratorzy nie wywiążą się z obowiązku zgłoszenia naruszenia ochrony danych organowi nadzorczemu albo osobom, których dane dotyczą, albo zarówno organowi nadzorczemu, jak i osobom, których dane dotyczą, pomimo spełnienia wymogów ustanowionych w art. 33 lub 34 RODO, organ nadzorczy może skorzystać z możliwości, która obejmowałaby wzięcie pod uwagę wszystkich środków naprawczych znajdujących się do jego dyspozycji, co wiązałoby się z możliwością zastosowania administracyjnej kary pieniężnej[22] w połączeniu ze środkiem naprawczym przewidzianym w art. 58 ust. 2 RODO albo bez takiego środka. Jeżeli zdecydowano się zastosować administracyjną karę pieniężną, wartość tej kary może opiewać na kwotę do 10 000 000 EUR lub do 2 % całkowitego rocznego światowego obrotu przedsiębiorstwa zgodnie z art. 83 ust. 4 lit. a) RODO. Należy również pamiętać o tym, że w niektórych przypadkach niewywiązanie się z obowiązku zgłoszenia naruszenia mogłoby doprowadzić do ujawnienia braku istniejących środków bezpieczeństwa albo nieadekwatności istniejących środków bezpieczeństwa. Wytyczne Grupy Roboczej Art. 29 w sprawie administracyjnych kar pieniężnych stanowią, że: „występowanie kilku różnych naruszeń [przepisów RODO – *przypis tłum.*] 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 [przepisów RODO – *przypis tłum.*]". W takim przypadku organ nadzorczy będzie miał również możliwość nakładania kar za niewywiązanie się z obowiązku zgłoszenia naruszenia lub zawiadomienia o wystąpieniu naruszenia (art. 33 i 34 RODO), z jednej strony, oraz za brak (odpowiednich) środków bezpieczeństwa (art. 32 RODO), z drugiej strony, ponieważ obydwie te sytuacje traktuje się jako dwa odrębne naruszenia [przepisów RODO – *przypis tłum*.].

---

[20] Zob. również motywy 85 i 75 RODO.

[21] Zob. również motyw 86 RODO.

[22] Aby uzyskać dalsze szczegółowe informacje, zob. wytyczne Grupy Roboczej Art. 29 w sprawie stosowania i ustalania administracyjnych kar pieniężnych dostępne pod adresem: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

II. ART. 33 – ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

A. Kiedy należy zgłosić naruszenie?

1. Wymogi przewidziane w art. 33

29. Art. 33 ust. 1 RODO 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*.

30. Motyw 87 RODO stanowi, że[23]:

> *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" wystąpienie naruszenia?

31. Jak wyszczególniono powyżej, w RODO ustanowiono wymóg, zgodnie z którym 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. Stosowanie tego wymogu może wiązać się z koniecznością ustalenia momentu, w którym można uznać, że administrator „stwierdził" wystąpienie naruszenia. W opinii EROD należy uznać, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym uzyskał dostateczną pewność co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do narażenia danych osobowych.

32. Jak jednak wspomniano wcześniej, w RODO ustanowiono wymóg zobowiązujący administratora do wdrożenia wszelkich odpowiednich technicznych środków ochrony i wszelkich odpowiednich środków organizacyjnych, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osoby, których dane dotyczą. W RODO stwierdzono również, że 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[24]. Wiąże się to z nałożeniem na administratora obowiązku utrzymania zdolności do terminowego „stwierdzania" wystąpienia wszelkich naruszeń, aby zapewnić możliwość podjęcia stosownych działań.

33. To, kiedy dokładnie można uznać, że administrator „stwierdził" wystąpienie określonego naruszenia, będzie zależało od okoliczności, w jakich doszło do tego naruszenia. W niektórych przypadkach wystąpienie naruszenia można stosunkowo łatwo stwierdzić już na początku, natomiast w innych ustalenie, czy doszło do narażenia danych osobowych, może wymagać czasu. W tym kontekście

[23] W tym kontekście istotne znaczenie ma również motyw 85 RODO.

[24] Zob. motyw 87 RODO.

powinno się jednak położyć nacisk na szybkie zbadanie danego incydentu w celu ustalenia, czy faktycznie doszło do naruszenia ochrony danych osobowych, a jeżeli tak – podjąć działania zaradcze i, w razie konieczności, zgłosić naruszenie.

Przykłady

1. W przypadku utraty pamięci USB zawierającej niezaszyfrowane dane osobowe ustalenie, czy nieuprawnione osoby uzyskały dostęp do tych danych, okazuje się często niemożliwe. Niemniej jednak, mimo że administrator może nie być w stanie ustalić, czy w danym przypadku doszło do naruszenia dotyczącego poufności danych, taki przypadek musi zostać zgłoszony, ponieważ można z dostateczną pewnością stwierdzić, że doszło do naruszenia dotyczącego dostępności danych; w tym kontekście przyjmuje się, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym zdał sobie sprawę z utraty pamięci USB.

2. Osoba trzecia informuje administratora, że przypadkowo otrzymała dane osobowe jednego z jego klientów, i przedstawia dowody potwierdzające, że doszło do nieuprawnionego ujawnienia tych danych. Ponieważ administrator otrzymał dowody jednoznacznie świadczące o wystąpieniu naruszenia dotyczącego poufności danych, nie można mieć żadnych wątpliwości co do tego, że „stwierdził" wystąpienie takiego naruszenia.

3. Administrator wykrywa potencjalne włamanie do swojej sieci. Administrator sprawdza systemy w celu ustalenia, czy bezpieczeństwo danych osobowych przechowywanych w tym systemie zostało narażone na szwank, po czym potwierdza, że faktycznie tak się stało. Ponownie, ponieważ administrator uzyskał dowody jednoznacznie świadczące o wystąpieniu naruszenia, nie można mieć żadnych wątpliwości co do tego, że „stwierdził" wystąpienie takiego naruszenia.

4. Cyberprzestępca kontaktuje się z administratorem po włamaniu się do jego systemu, aby zażądać okupu. W takim przypadku – po sprawdzeniu swojego systemu i potwierdzeniu, że faktycznie został on zaatakowany – administrator dysponuje dowodem jednoznacznie świadczącym o wystąpieniu naruszenia, dlatego też nie można mieć żadnych wątpliwości co do tego, że stwierdził wystąpienie takiego naruszenia.

34. Po otrzymaniu pierwszej informacji o potencjalnym naruszeniu ochrony danych osobowych od osoby fizycznej, organizacji medialnej lub z innego źródła lub po samodzielnym wykryciu incydentu bezpieczeństwa administrator może przeprowadzić krótkotrwałe postępowanie, aby ustalić, czy faktycznie doszło do danego naruszenia. W trakcie prowadzenia tego postępowania nie można uznać, że administrator „stwierdził" wystąpienie naruszenia. Oczekuje się jednak, że wstępne postępowanie powinno rozpocząć się możliwie jak najszybciej i doprowadzić do ustalenia z dostateczną pewnością, czy w danym przypadku faktycznie doszło do wystąpienia naruszenia; następnie można przeprowadzić bardziej szczegółowe postępowanie.

35. Po stwierdzeniu wystąpienia naruszenia przez administratora podlegające zgłoszeniu naruszenie musi zostać zgłoszone bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. W tym okresie administrator powinien ocenić prawdopodobne ryzyko, na jakie narażone są osoby fizyczne, aby ustalić, czy w danym przypadku zastosowanie ma wymóg zgłoszenia naruszenia, a także aby określić działanie lub działania, które należy podjąć, aby zaradzić naruszeniu. Administrator mógł już jednak przeprowadzić wstępną ocenę potencjalnego ryzyka, z jakim może wiązać się naruszenie, w ramach oceny skutków dla ochrony danych[25] dokonanej przed przeprowadzeniem danej operacji przetwarzania. Ocena skutków dla ochrony danych może mieć jednak bardziej ogólnikowy charakter niż ocena konkretnych okoliczności, w których doszło do dowolnego faktycznego naruszenia, dlatego też należy również każdorazowo przeprowadzić

[25] Zob. wytyczne Grupy Roboczej Art. 29 WP248 dotyczące oceny skutków dla ochrony danych: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

dodatkową ocenę uwzględniającą te okoliczności. Aby uzyskać bardziej szczegółowe informacje na temat oceny ryzyka, zob. sekcja IV.

36. W większości przypadków takie wstępne działania powinny zostać zakończone wkrótce po otrzymaniu początkowego ostrzeżenia (tj. w momencie powzięcia przez administratora lub podmiot przetwarzający podejrzenia o możliwości wystąpienia incydentu bezpieczeństwa mogącego wywrzeć wpływ na dane osobowe) – działania te mogą zostać zakończone w późniejszym terminie wyłącznie w wyjątkowych przypadkach.

Przykład

Osoba fizyczna informuje administratora, że otrzymała wiadomość e-mail, której nadawca podszywa się pod administratora i która zawiera dane osobowe dotyczące (faktycznego) korzystania z usług administratora przez tę osobę, i sugeruje, że doszło do złamania środków bezpieczeństwa stosowanych przez administratora. Administrator przeprowadza krótkie postępowanie, w toku którego uzyskuje potwierdzenie, że doszło do włamania do jego sieci, i gromadzi dowody świadczące o nieuprawnionym dostępie do danych osobowych. Od tego momentu przyjmuje się, że administrator „stwierdził" wystąpienie naruszenia, a zgłoszenie naruszenia organowi nadzorczemu staje się obowiązkowe, chyba że prawdopodobieństwo, iż będzie wiązało się ono z ryzykiem naruszenia praw lub wolności osób fizycznych, nie istnieje. Administrator będzie musiał podjąć odpowiednie działania zaradcze, aby zaradzić naruszeniu.

37. Dlatego też administrator powinien ustanowić wewnętrzne procedury zapewniające mu możliwość wykrycia naruszenia i zaradzenia mu. Na przykład, aby wykryć pewne nieprawidłowości w procesie przetwarzania danych, administrator lub podmiot przetwarzający mogą korzystać z określonych środków technicznych, takich jak analizatory przepływu danych i analizatory dziennika umożliwiające zidentyfikowanie zdarzeń i ostrzeżeń poprzez ich zestawienie z dowolnymi danymi dziennika[26]. Po wykryciu naruszenia należy powiadomić o jego wystąpieniu organ zarządzający wyższego szczebla, aby można było mu zaradzić i – w razie potrzeby – zgłosić je zgodnie z art. 33 oraz, w stosownych przypadkach, art. 34. Takie środki i mechanizmy zgłaszania powinny zostać szczegółowo opisane w sporządzonych przez administratora planach reagowania na incydenty lub w przyjętych przez niego zasadach zarządzania. Ułatwi to administratorowi efektywne planowanie działań i ustalenie podmiotów w organizacji, na których spoczywa odpowiedzialność operacyjna za zarządzanie naruszeniem, a także określenie – w stosownych przypadkach – czy lub w jaki sposób powiadomić organ zarządzający wyższego szczebla o wystąpieniu danego incydentu.

38. Administrator powinien również zawrzeć porozumienia ze wszystkimi podmiotami przetwarzającymi, z których usług korzysta – podmioty te są z kolei zobowiązane do zgłaszania administratorowi przypadków wystąpienia naruszenia (zob. poniżej).

39. Choć odpowiedzialność za ustanawianie odpowiednich środków umożliwiających przeciwdziałanie naruszeniom, reagowanie na naruszenia i zaradzanie im spoczywa na administratorach i podmiotach przetwarzających, istnieją pewne praktyczne działania, które powinny być podejmowane we wszystkich przypadkach:

    - informacje na temat wszystkich zdarzeń powiązanych z bezpieczeństwem powinny być przekazywane osobie lub osobom, którym powierzono zadanie reagowania na incydenty, ustalania istnienia naruszenia i oceniania poziomu ryzyka;
    - następnie należy ocenić ryzyko dla osób fizycznych związane z danym naruszeniem (prawdopodobieństwo braku ryzyka, istnienie ryzyka lub wysoki poziom ryzyka) oraz

[26] Należy podkreślić, że dane dziennika ułatwiające audytowanie, np. dane dotyczące przechowywania, modyfikowania lub usuwania danych, mogą być również zaklasyfikowane jako dane osobowe dotyczące osoby, która wszczęła daną operację przetwarzania.

przekazać stosowne informacje w tym zakresie odpowiednim działom w ramach danej organizacji;

- w razie konieczności należy zgłosić dane naruszenie organowi nadzorczemu oraz, potencjalnie, zawiadomić o naruszeniu osoby fizyczne, na które wywarło ono wpływ;
- jednocześnie administrator powinien podjąć działania mające na celu ograniczenie skali naruszenia i przywrócenie stanu sprzed wystąpienia naruszenia; informacje na temat naruszenia powinny być dokumentowane w miarę rozwoju sytuacji.

40. Tym samym na administratorze spoczywa wyraźny obowiązek podejmowania działań w związku z wszelkimi ostrzeżeniami otrzymanymi na początkowym etapie oraz obowiązek ustalenia, czy w danym przypadku faktycznie doszło do naruszenia, czy też nie. W tym krótkim okresie administrator może przeprowadzić pewne postępowania oraz zgromadzić dowody i inne istotne szczegółowe informacje. Jednak po tym, gdy administrator z dostateczną pewnością stwierdzi, że w danym przypadku doszło do naruszenia – i jeżeli spełnione zostały warunki ustanowione w art. 33 ust. 1 RODO – musi zgłosić dane naruszenie organowi nadzorczemu bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin[27]. Jeżeli administrator nie wywiąże się z obowiązku podjęcia działań w odpowiednim terminie, a okoliczności danej sprawy będą jednoznacznie wskazywały na to, że doszło do naruszenia, taka sytuacja może zostać uznana za przypadek niewywiązania się z obowiązku zgłoszenia naruszenia zgodnie z art. 33 RODO.

41. Z art. 32 RODO jednoznacznie wynika, że administrator i podmiot przetwarzający powinni dysponować odpowiednimi środkami technicznymi i organizacyjnymi, aby zapewnić odpowiedni stopień bezpieczeństwa danych osobowych: zdolność do wykrywania naruszeń, zaradzania im oraz ich terminowego zgłaszania powinna być postrzegana jako kluczowy element tych środków.

3. Współadministratorzy

42. Art. 26 RODO dotyczy współadministratorów i stanowi, że współadministratorzy określają zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO[28]. Wiąże się to z koniecznością ustalenia, która strona będzie odpowiedzialna za wywiązywanie się z zobowiązań ustanowionych w art. 33 i 34 RODO. EROD zaleca, aby uzgodnienia umowne między współadministratorami uwzględniały postanowienia wskazujące administratora, który będzie zajmował się dbaniem o wypełnianie ustanowionych w RODO obowiązków w zakresie zgłaszania naruszeń lub który będzie odpowiedzialny za wypełnianie tych obowiązków.

4. Obowiązki podmiotu przetwarzającego

43. Choć ogólna odpowiedzialność za dbanie o ochronę danych osobowych spoczywa na administratorze, podmiot przetwarzający odgrywa istotną rolę w zapewnianiu administratorowi możliwości wywiązania się ze spoczywających na nim obowiązków; obejmuje to również zgłaszanie naruszeń. W art. 28 ust. 3 RODO stwierdzono, że przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego. Zgodnie z art. 28 ust. 3 lit. f) umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający: „uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36".

44. W art. 33 ust. 2 RODO wskazano wyraźnie, że w przypadku, gdy administrator korzysta z usług podmiotu przetwarzającego, a podmiot przetwarzający stwierdzi wystąpienie naruszenia ochrony danych osobowych, które przetwarza w imieniu administratora, musi zgłosić to naruszenie administratorowi „bez zbędnej zwłoki". Należy przy tym podkreślić, że podmiot przetwarzający nie

[27] Zob. rozporządzenie nr 1182/71 określające zasady mające zastosowanie do okresów, dat i terminów dostępne pod adresem: http://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:31971R1182&from=PL

[28] Zob. również motyw 79 RODO.

musi ocenić prawdopodobieństwa wystąpienia ryzyka wynikającego z naruszenia przed jego zgłoszeniem administratorowi; odpowiedzialność za przeprowadzenie takiej oceny w momencie stwierdzenia wystąpienia naruszenia spoczywa na administratorze. Podmiot przetwarzający musi jedynie ustalić, czy doszło do naruszenia, a następnie zgłosić to naruszenie administratorowi. Administrator korzysta z usług podmiotu przetwarzającego, aby realizować wyznaczone cele; dlatego też zasadniczo należy przyjąć, że administrator „stwierdził" wystąpienie naruszenia w momencie, w którym podmiot przetwarzający poinformował go o jego wystąpieniu. Nałożenie na podmiot przetwarzający obowiązku zgłoszenia naruszenia administratorowi, na rzecz którego podmiot ten świadczy usługi, zapewnia temu administratorowi możliwość zaradzenia naruszeniu i ustalenia, czy w danym przypadku należy zgłosić to naruszenie organowi nadzorczemu zgodnie z art. 33 ust. 1 oraz zawiadomić o jego wystąpieniu osoby fizyczne, na które naruszenie wywiera wpływ, zgodnie z art. 34 ust. 1. Administrator może również zdecydować się na przeprowadzenie postępowania w sprawie naruszenia, ponieważ podmiot przetwarzający może nie dysponować wiedzą na temat wszystkich istotnych okoliczności faktycznych danej sprawy – na przykład tego, czy w posiadaniu administratora znajduje się kopia lub kopia bezpieczeństwa danych osobowych zniszczonych lub utraconych przez podmiot przetwarzający. Może to decydować o tym, czy administrator musiałby następnie zgłosić naruszenie.

45. W RODO nie ustanowiono precyzyjnie określonego terminu, w którym podmiot przetwarzający musi zgłosić naruszenie administratorowi – stwierdzono jedynie, że musi to nastąpić „bez zbędnej zwłoki". Dlatego też EROD zaleca, aby podmiot przetwarzający szybko zgłaszał naruszenia administratorowi i następnie stopniowo przekazywał dalsze informacje na temat naruszenia, w miarę uzyskiwania dostępu do bardziej szczegółowych danych. Ma to istotne znaczenie dla ułatwienia administratorowi spełnienia wymogu zgłoszenia naruszenia organowi nadzorczemu w terminie 72 godzin.

46. Jak wyjaśniono powyżej, w umowie między administratorem a podmiotem przetwarzającym należy określić, w jaki sposób planuje się zagwarantować spełnienie wymogów ustanowionych w art. 33 ust. 2 oraz zapewnić zgodność z innymi przepisami RODO. Może wiązać się to z ustanowieniem obowiązku wczesnego zgłaszania naruszeń przez podmiot przetwarzający, co z kolei ułatwia administratorowi wywiązanie się ze spoczywających na nim obowiązków w zakresie zgłaszania naruszeń organowi nadzorczemu w terminie 72 godzin.

47. Jeżeli podmiot przetwarzający świadczy usługi na rzecz szeregu administratorów, a dany incydent wywiera wpływ na wszystkich z nich, podmiot przetwarzający będzie zobowiązany do zgłoszenia wystąpienia wspomnianego incydentu każdemu z tych administratorów.

48. Podmiot przetwarzający mógłby dokonać zgłoszenia w imieniu administratora, jeżeli administrator udzieliłby takiemu podmiotowi przetwarzającemu stosownego zezwolenia, a kwestia ta zostałaby uregulowana w uzgodnieniach umownych między administratorem a podmiotem przetwarzającym. Takiego zgłoszenia należy dokonać zgodnie z art. 33 i 34 RODO. W tym kontekście należy jednak pamiętać, że zgodnie z obowiązującymi przepisami odpowiedzialność za dokonanie zgłoszenia spoczywa na administratorze.

B. Udzielanie informacji organowi nadzorczemu

1. Informacje, których należy udzielić

49. Art. 33 ust. 3 RODO stanowi, że w przypadku, gdy administrator zgłasza naruszenie organowi nadzorczemu, zgłoszenie to powinno 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.

50. W RODO nie zawarto definicji kategorii osób, których dane dotyczą, ani kategorii wpisów danych osobowych. EROD proponuje jednak kategorie osób, których dane dotyczą, obejmujące różnego rodzaju osoby fizyczne, na których dane osobowe naruszenie wywarło wpływ: w zależności od zastosowanych wskaźników kategorie te mogą obejmować m.in. dzieci i przedstawicieli innych grup szczególnie wrażliwych, osoby niepełnosprawne, pracowników lub klientów. Podobnie kategorie wpisów danych osobowych mogą odnosić się do poszczególnych rodzajów wpisów, które administrator może przetwarzać, takich jak dane dotyczące zdrowia, dane dotyczące wykształcenia, informacje z dziedziny opieki społecznej, szczegółowe informacje finansowe, numery rachunków bankowych, numery paszportów itp.

51. W motywie 85 RODO wyraźnie stwierdzono, że jednym z powodów, dla których zgłasza się naruszenie, jest ograniczenie związanych z nim szkód dla osób fizycznych. Dlatego też jeżeli rodzaje osób, których dane dotyczą, lub rodzaje danych osobowych wskazują na istnienie ryzyka wyrządzenia określonych szkód w rezultacie naruszenia (np. kradzież tożsamości, oszustwo, strata finansowa, ryzyko naruszenia poufności danych chronionych tajemnicą zawodową), należy wskazać stosowne kategorie w zgłoszeniu. Pozwoli to spełnić wymóg opisania możliwych konsekwencji naruszenia.

52. Brak dostępu do szczegółowych informacji (np. informacji o dokładnej liczbie osób, których dane dotyczą, na które naruszenie wywarło wpływ) nie powinien stanowić przeszkody dla terminowego zgłoszenia naruszenia. Przepisy RODO dopuszczają możliwość wskazywania przybliżonej liczby osób fizycznych, na które dane naruszenie wywarło wpływ, oraz przybliżonej liczby wpisów danych osobowych, których dotyczy to naruszenie. W tym kontekście należy skoncentrować się na dążeniu do zaradzenia negatywnym skutkom naruszenia, a nie na przedstawieniu precyzyjnych danych liczbowych.

53. Dlatego też w przypadku, w którym fakt wystąpienia naruszenia nie wzbudza żadnych wątpliwości, ale jego skala nie jest jeszcze znana, sukcesywne dokonywanie zgłoszenia (zob. poniżej) stanowi bezpieczną metodę wywiązania się z zobowiązań w zakresie zgłaszania naruszeń.

54. Art. 33 ust. 3 RODO stanowi, że administrator „musi co najmniej" przekazać tego rodzaju informacje w zgłoszeniu, aby – w stosownych przypadkach – mieć możliwość przekazania dodatkowych szczegółowych informacji na późniejszym etapie. Różne rodzaje naruszeń (dotyczące poufności, integralności lub dostępności) mogą wiązać się z koniecznością przekazania dodatkowych informacji, aby w pełni wyjaśnić okoliczności danej sprawy.

Przykład

W zgłoszeniu skierowanym do organu nadzorczego administrator może podać nazwę swojego podmiotu przetwarzającego, jeżeli do danego naruszenia doszło na poziomie takiego podmiotu, a w szczególności jeżeli naruszenie doprowadziło do incydentu wywierającego wpływ na wpisy danych osobowych wielu innych administratorów, którzy korzystają z usług tego samego podmiotu przetwarzającego.

55. Niezależnie od danego przypadku organ nadzorczy może zwrócić się o udzielenie mu dalszych szczegółowych informacji w ramach prowadzonego przez siebie postępowania w przedmiocie naruszenia.

2. Sukcesywne dokonywanie zgłoszenia

56. W zależności od charakteru danego naruszenia ustalenie wszystkich istotnych okoliczności faktycznych związanych z incydentem może wiązać się z koniecznością przeprowadzenia bardziej szczegółowego postępowania przez administratora. Dlatego też art. 33 ust. 4 RODO stanowi:

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

57. Oznacza to, że w RODO uznaje się, iż administratorzy nie zawsze są w stanie uzyskać dostęp do wszystkich niezbędnych informacji na temat naruszenia w ciągu 72 godzin od stwierdzenia wystąpienia naruszenia, ponieważ pełne i wyczerpujące szczegółowe informacje na temat danego incydentu nie zawsze są dostępne w tym początkowym okresie. Z tego względu w RODO przewidziano możliwość sukcesywnego dokonywania zgłoszenia. Możliwość ta będzie prawdopodobnie wykorzystywana w przypadku bardziej złożonych naruszeń, takich jak niektóre rodzaje cyberincydentów, w przypadku których pełne ustalenie charakteru naruszenia oraz skali naruszenia ochrony danych osobowych może wiązać się np. z koniecznością przeprowadzenia dogłębnego dochodzenia kryminalistycznego. Z tego względu w wielu przypadkach administrator będzie zobowiązany do przeprowadzenia szerzej zakrojonych postępowań i podjęcia działań następczych w momencie uzyskania dodatkowych informacji na późniejszym etapie. Taką sytuację uznaje się za dopuszczalną, o ile administrator wyjaśni przyczyny opóźnienia zgodnie z art. 33 ust. 1 RODO. EROD zaleca, aby w momencie, w którym administrator po raz pierwszy zgłasza dane naruszenie organowi nadzorczemu, poinformował również ten organ o tym, że nie dysponuje jeszcze wszystkimi wymaganymi danymi i że przekaże bardziej szczegółowe informacji na późniejszym etapie. Organ nadzorczy powinien uzgodnić z administratorem sposób i termin przekazania tych dodatkowych informacji. Nie uniemożliwia to administratorowi udzielania dodatkowych informacji na dowolnym innym etapie w przypadku, gdy uzyska wiedzę o dalszych istotnych okolicznościach faktycznych związanych z naruszeniem, która powinna zostać przekazana organowi nadzorczemu.

58. Wymóg zgłaszania naruszeń ustanowiono przede wszystkim, aby zachęcić administratorów do szybkiego reagowania na naruszenia, ograniczania ich wpływu oraz – w miarę możliwości – przywrócenia bezpieczeństwa danych osobowych, których bezpieczeństwo zostało naruszone, a także zasięgania opinii organu nadzorczego w tym zakresie. Zgłoszenie naruszenia organowi nadzorczemu w ciągu pierwszych 72 godzin od jego wystąpienia może umożliwić administratorowi zagwarantowanie podjęcia prawidłowych decyzji w kwestii tego, czy w danym przypadku należy zawiadomić osoby fizyczne o wystąpieniu naruszenia.

59. Celem zgłoszenia naruszenia organowi nadzorczemu nie jest jednak wyłącznie uzyskanie wskazówek w kwestii tego, czy o jego wystąpieniu należy zawiadomić osoby fizyczne, na które wywiera ono wpływ. W niektórych przypadkach administrator – opierając się na charakterze naruszenia i powadze związanego z nim ryzyka – będzie mógł jednoznacznie stwierdzić, że osoby fizyczne, na które dane naruszenie wywiera wpływ, muszą zostać niezwłocznie zawiadomione o jego wystąpieniu. Na przykład w sytuacji bezpośredniego zagrożenia kradzieżą tożsamości lub w przypadku ujawnienia szczególnych kategorii danych osobowych [29] w internecie administrator powinien bez zbędnej zwłoki podjąć działania mające na celu ograniczenie skali naruszenia i zawiadomienie osób fizycznych, na które wywiera ono wpływ, o jego wystąpieniu (zob. sekcja III). W wyjątkowych okolicznościach administrator może zawiadomić osoby fizyczne o wystąpieniu naruszenia przed zgłoszeniem naruszenia organowi nadzorczemu. Ogólniej rzecz biorąc, zgłoszenie naruszenia organowi nadzorczemu nie może stanowić usprawiedliwienia dla niewywiązania się z obowiązku zawiadomienia osoby, której dane dotyczą, o wystąpieniu naruszenia w przypadkach, w których jest to konieczne.

[29] Zob. art. 9 RODO.

60. Należy również podkreślić, że po dokonaniu początkowego zgłoszenia administrator może przekazywać organowi nadzorczemu bardziej aktualne informacje, jeżeli w toku postępowania przeprowadzonego po stwierdzeniu naruszenia ujawnione zostaną dowody świadczące o tym, że incydent bezpieczeństwa został zneutralizowany i że w rzeczywistości nie doszło do żadnego naruszenia. Takie informacje mogą następnie zostać wykorzystane jako uzupełnienie informacji, które zostały już przekazane organowi nadzorczemu, a sam incydent powinien zostać zarejestrowany jako niewiążący się z naruszeniem. Nie przewidziano żadnych sankcji z tytułu zgłaszania incydentów, co do których w ostatecznym rozrachunku okazało się, że nie wiązały się z naruszeniem.

Przykład

Administrator zgłasza organowi nadzorczemu utratę pamięci USB zawierającej kopię danych osobowych niektórych z jego klientów w terminie 72 godzin od wykrycia wystąpienia naruszenia. Pamięć USB zostaje następnie odnaleziona wśród innych dokumentów przechowywanych w pomieszczeniach administratora i odzyskana. Administrator przekazuje stosowne informacje w tym zakresie organowi nadzorczemu i występuje o zmianę treści zgłoszenia.

61. Należy przy tym podkreślić, że podejście bazujące na sukcesywnym zgłaszaniu naruszeń jest już stosowane w kontekście zobowiązań ustanowionych w dyrektywie 2002/58/WE i rozporządzeniu nr 611/2013 oraz w kontekście innych samodzielnie zgłaszanych incydentów.

3. Zgłoszenia dokonane z opóźnieniem

62. W art. 33 ust. 1 RODO wyraźnie stwierdzono, że do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Na mocy tego przepisu – w połączeniu z koncepcją sukcesywnego dokonywania zgłoszenia – uznaje się, że administrator może nie zawsze być w stanie zgłosić naruszenie w wyznaczonym terminie oraz że dokonanie zgłoszenia z opóźnieniem może być w niektórych przypadkach dopuszczalne.

63. Taka sytuacja może wystąpić np. wówczas, gdy administrator będzie musiał w krótkim czasie stawić czoła szeregowi podobnych naruszeń dotyczących poufności danych wywierających taki sam wpływ na dużą liczbę osób, których dane dotyczą. Administrator może stwierdzić wystąpienie naruszenia i – na początkowym etapie postępowania, przed jego zgłoszeniem – wykryć kolejne podobne naruszenia wynikające z różnych przyczyn. W zależności od okoliczności danej sprawy ustalenie skali naruszeń może zająć administratorowi pewną ilość czasu, dlatego też zamiast zgłaszać poszczególne naruszenia indywidualnie, administrator może zgromadzić je w ramach jednego większego zgłoszenia uwzględniającego szereg bardzo podobnych naruszeń, które potencjalnie mogą wynikać z różnych przyczyn. W rezultacie naruszenia mogą zostać zgłoszone organowi nadzorczemu z opóźnieniem większym niż 72 godziny od momentu, w którym administrator po raz pierwszy stwierdził ich wystąpienie.

64. Ściśle rzecz biorąc, każde pojedyncze naruszenie stanowi incydent, który należy zgłosić. Aby jednak uniknąć nadmiernego obciążania administratorów, zapewniono im możliwość „zbiorczego" zgłoszenia wszystkich takich naruszeń, o ile dotyczą one tego samego rodzaju danych osobowych, których ochrona została naruszona w taki sam sposób, i o ile doszło do nich w stosunkowo krótkim odstępie czasu. Jeżeli w danym przypadku doszło do szeregu naruszeń dotyczących różnych rodzajów danych osobowych, których ochrona została naruszona w różny sposób, zgłoszenia należy dokonać w standardowym trybie, zgłaszając każde naruszenie zgodnie z przepisami art. 33.

65. Choć w niektórych przypadkach w RODO dopuszcza się możliwość dokonywania zgłoszeń z opóźnieniem, takie sytuacje należy traktować jako sytuacje nadzwyczajne. W tym względzie warto podkreślić, że zgłoszeń zbiorczych można również dokonywać w celu zgłoszenia szeregu podobnych naruszeń w wyznaczonym terminie 72 godzin.

C. Naruszenia o charakterze transgranicznym i naruszenia w jednostkach organizacyjnych spoza UE

1. Naruszenia o charakterze transgranicznym

66. W przypadku, w którym dochodzi do transgranicznego przetwarzania[30] danych osobowych, naruszenie może wywierać wpływ na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim. W art. 33 ust. 1 RODO wyraźnie stwierdzono, że w przypadku wystąpienia naruszenia, administrator powinien zgłosić je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO[31]. Art. 55 ust. 1 RODO stanowi, że:

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

67. Art. 56 ust. 1 RODO stanowi jednak, że:

> „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".

68. Ponadto art. 56 ust. 6 RODO stanowi, że:

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

69. Oznacza to, że administrator będzie zobowiązany do zgłoszenia naruszenia wiodącemu organowi nadzorczemu za każdym razem, gdy w kontekście transgranicznego przetwarzania dojdzie do naruszenia wymagającego zgłoszenia[32]. Dlatego też przy sporządzaniu swojego planu reagowania na naruszenia administrator musi ustalić, który organ nadzorczy jest wiodącym organem nadzorczym, któremu należy zgłosić naruszenie[33]. Dzięki temu administrator będzie mógł szybko reagować na pojawiające się naruszenia i wywiązywać się z zobowiązań spoczywających na nim zgodnie z art. 33. W tym kontekście należy wyjaśnić, że naruszenie wiążące się z transgranicznym przetwarzaniem należy zgłosić wiodącemu organowi nadzorczemu, którego siedziba niekoniecznie musi znajdować się w tym samym miejscu co miejsce, w którym znajdują się osoby, których dane dotyczą, lub co miejsce, w którym doszło do naruszenia. Zgłaszając naruszenie wiodącemu organowi nadzorczemu, administrator powinien – w stosownych przypadkach – określić, czy naruszenie dotyczy jednostek organizacyjnych znajdujących się w innych państwach członkowskich, oraz wskazać państwa członkowskie, w których dane naruszenie może potencjalnie wywrzeć wpływ na osoby, których dane dotyczą. Jeżeli administrator ma jakiekolwiek wątpliwości co do tożsamości wiodącego organu nadzorczego, powinien przynajmniej zgłosić naruszenie lokalnemu organowi nadzorczemu w miejscu, w którym doszło do naruszenia.

2. Naruszenia w jednostkach organizacyjnych spoza UE

70. Art. 3 RODO dotyczy terytorialnego zakresu stosowania RODO, uwzględniając przypadki, w których przepisy RODO mają zastosowanie do przetwarzania danych osobowych przez administratora lub

---

[30] Zob. art. 4 ust. 23 RODO.

[31] Zob. również motyw 122 RODO.

[32] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego dostępne pod adresem: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[33] Z wykazem danych kontaktowych wszystkich krajowych organów ochrony danych w Europie można zapoznać się pod adresem: https://edpb.europa.eu/about-edpb/about-edpb/members_pl

podmiot przetwarzający niemających jednostek organizacyjnych w UE. W szczególności art. 3 ust. 2 RODO stanowi, że[34]:

> *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*.

71. W tym kontekście za istotne należy również uznać przepisy art. 3 ust. 3 RODO, który stanowi, że[35]:

> „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".

72. A zatem w przypadku, gdy naruszenie odnotuje administrator niemający jednostki organizacyjnej w UE, który podlega przepisom art. 3 ust. 2 lub 3 RODO, na administratorze tym wciąż spoczywają obowiązki zgłaszania określone w art. 33 i 34 RODO. W art. 27 RODO ustanowiono wymóg zobowiązujący administratora (i podmiot przetwarzający) do wyznaczenia przedstawiciela w UE w przypadku, gdy zastosowanie ma art. 3 ust. 2 RODO.

73. Sama obecność przedstawiciela w państwie członkowskim nie powoduje uruchomienia systemu kompleksowej współpracy.[36] W związku z tym naruszenie będzie musiało zostać zgłoszone każdemu organowi nadzorczemu, w którego państwie członkowskim mieszkają osoby, których dane dotyczą i których dotyczy naruszenie. Za takie zgłoszenia odpowiada administrator.[37]

74. Podobnie w przypadku gdy podmiot przetwarzający podlega przepisom art. 3 ust. 2 RODO, spoczywają na nim obowiązki dotyczące podmiotów przetwarzających, a w szczególności obowiązek zgłaszania naruszenia administratorowi na podstawie art. 33 ust. 2 RODO.

D. Sytuacje, w których zgłaszanie nie jest konieczne

75. W art. 33 ust. 1 RODO wyraźnie stwierdzono, że nie ma obowiązku zgłaszania organowi nadzorczemu naruszeń, co do których „jest mało prawdopodobne, by [...] skutkował[y] ryzykiem naruszenia praw lub wolności osób fizycznych". Przykładem może być sytuacja, w której dane osobowe już są publicznie dostępne i ujawnienie takich danych nie wiąże się z prawdopodobnym ryzykiem dla danej osoby fizycznej. Jest to sprzeczne z istniejącymi wymogami powiadamiania o naruszeniu określonymi

[34] Zob. również motywy 23 i 24 RODO.
[35] Zob. również motyw 25 RODO.
[36] Zob. wytyczne Grupy Roboczej Art. 29 dotyczące ustalania wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego dostępne pod adresem: http://ec.europa.eu/newsroom/document.cfm?doc_id=44102
[37] Zgodnie z wytycznymi 3/2018 dotyczącymi terytorialnego zakresu stosowania RODO (art. 3), dostępnym pod adresem https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en, EROD uznaje funkcję przedstawiciela w Unii za niezgodną z rolą zewnętrznego inspektora ochrony danych („DPO"), a zatem odpowiedzialność za zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu jest nadal odpowiedzialnością administratora zgodnie z art. 27 ust. 5 RODO. Przedstawiciel może jednak uczestniczyć w procedurze zgłaszania, jeżeli zostało to wyraźnie określone w pisemnym upoważnieniu.

w dyrektywie 2009/136/WE, które spoczywają na dostawcach publicznie dostępnych usług łączności elektronicznej, zgodnie z którymi wszelkie istotne naruszenia należy zgłaszać właściwemu organowi.

76. W swojej opinii 03/2014 na temat powiadamiania o przypadkach naruszenia[38] Grupa Robocza Art. 29 wyjaśniła, że naruszenie dotyczące poufności danych osobowych, które zaszyfrowano przy użyciu najnowocześniejszego algorytmu, nadal stanowi naruszenie danych osobowych i musi zostać zgłoszone. Jeżeli jednak nie dojdzie do naruszenia poufności klucza – tj. jeżeli klucz nie został złamany w wyniku naruszenia bezpieczeństwa oraz został wygenerowany w sposób, który uniemożliwia osobie nieupoważnionej poznanie go za pomocą dostępnych technologicznie środków – to dane zasadniczo pozostają nieczytelne. Nie jest więc prawdopodobne, aby takie naruszenie wywarło niekorzystny wpływ na osoby, których dane dotyczą, a zatem nie zachodzi konieczność powiadomienia o nim takich osób[39]. Nawet jeżeli dane są zaszyfrowane, ich utrata lub zmiana może jednak wywrzeć niekorzystny wpływ na osoby, których dane dotyczą, jeżeli administrator danych nie posiada odpowiednich kopii zapasowych. W takim przypadku należy zawiadomić osoby, których dane dotyczą, nawet jeżeli same dane odpowiednio zaszyfrowano.

77. Grupa Robocza Art. 29 wyjaśniła również, że taka sama sytuacja miałaby miejsce, gdyby w stosunku do danych osobowych, takich jak hasła, zastosowano bezpieczną funkcję skrótu i ciągu zaburzającego, dane zostały zastąpione wartością klucza haszującego, obliczoną za pomocą najnowocześniejszej kryptograficznej funkcji haszującej z kluczem tajnym, klucz użyty do haszowania tych danych nie został złamany w wyniku naruszenia bezpieczeństwa, oraz został wygenerowany w sposób, który uniemożliwia osobie nieupoważnionej poznanie go za pomocą dostępnych technologicznie środków.

78. A zatem, jeżeli zapewniono, aby dane osobowe były zasadniczo nieczytelne dla osób nieupoważnionych, oraz jeżeli dane są kopią lub istnieje kopia bezpieczeństwa, nie ma potrzeby zgłaszania organowi nadzorczemu naruszenia dotyczącego poufności danych związanego z odpowiednio zaszyfrowanymi danymi osobowymi. Wynika to z braku prawdopodobieństwa, że takie naruszenie stworzy ryzyko naruszenia praw lub wolności osób fizycznych. Oznacza to oczywiście, że nie ma również konieczności powiadamiania danej osoby fizycznej, ponieważ ryzyko prawdopodobnie nie jest wysokie. Warto jednak pamiętać, że choć początkowo zgłoszenie może nie być wymagane ze względu na fakt, iż prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych nie istnieje, z czasem sytuacja może się zmienić i może wystąpić konieczność przeprowadzenia kolejnej oceny ryzyka. Przykładowo konieczność zgłoszenia może występować także w sytuacji, gdy w późniejszym czasie stwierdzono, że klucz został złamany, lub wykryto lukę w oprogramowaniu szyfrującym.

79. Należy również podkreślić, że wystąpienie naruszenia w sytuacji, w której nie istnieje kopia bezpieczeństwa zaszyfrowanych danych osobowych, oznacza, iż miało miejsce naruszenie dotyczące dostępności danych, które może stwarzać ryzyko dla osób fizycznych i w związku z tym może wymagać zgłoszenia. Sytuacja jest podobna w przypadku wystąpienia naruszenia związanego z utratą zaszyfrowanych danych – nawet jeżeli istnieje kopia bezpieczeństwa danych osobowych – takie naruszenie może również wymagać zgłoszenia w zależności od tego, ile czasu zajęło przywracanie danych z kopii zapasowej, oraz od tego, jak brak dostępności wpłynął na osoby fizyczne. Zgodnie z art. 32 ust. 1 lit. c) RODO istotnym czynnikiem gwarantującym bezpieczeństwo jest „zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego”.

Przykład

[38] Opinia WP29 03/2014 na temat powiadamiania o przypadkach naruszenia danych osobowych, http://ec.europa.eu/justice/data-protection/article29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[39] Zob. również art. 4 ust. 1 i 2 rozporządzenia nr 611/2013.

Przykładem naruszenia, które nie wymagałoby zgłoszenia organowi nadzorczemu, byłaby utrata bezpiecznie zaszyfrowanego urządzenia mobilnego, z którego korzystają administrator i jego pracownicy. Zakładając, że klucz kryptograficzny jest bezpiecznie przechowywany przez administratora i nie jest to jedyna kopia danych osobowych, dane osobowe będą niedostępne dla atakującego. Oznacza to, że przedmiotowe naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw lub wolności osób, których te dane dotyczą. Jeżeli później okaże się, że klucz kryptograficzny został złamany lub oprogramowanie lub algorytm szyfrujący ma słabe punkty, poziom ryzyka naruszenia praw lub wolności osób fizycznych zmieni się i wówczas zgłoszenie może stać się konieczne.

80. Jeżeli jednak administrator nie zgłosi naruszenia do organu nadzorczego w sytuacji, w której dane w rzeczywistości nie zostały bezpiecznie zaszyfrowane, wówczas ma miejsce niewywiązanie się z zobowiązań wynikających z art. 33 RODO. Dokonując wyboru oprogramowania szyfrującego, administratorzy powinni zatem dokładnie zastanowić się nad jakością i odpowiednim wdrożeniem oferowanej metody szyfrowania, dowiedzieć się, jaki poziom ochrony faktycznie ona zapewnia, oraz czy jest adekwatna do poziomu istniejącego ryzyka. Administratorzy powinni również być zaznajomieni ze szczegółami funkcjonowania wykorzystywanego przez nich produktu szyfrującego. Na przykład urządzenie może być szyfrowane po wyłączeniu, ale nie wtedy, gdy znajduje się w trybie uśpienia. Niektóre produkty wykorzystujące szyfrowanie mogą posiadać „domyślne klucze", które każdy klient musi zmienić, aby szyfrowanie było skuteczne. Chociaż eksperci ds. bezpieczeństwa mogą obecnie uznawać daną metodę szyfrowania za odpowiednią, może ona się za kilka lat stać przestarzała, co stworzy wątpliwości, czy szyfrowanie danych zapewniane przez ten produkt będzie wystarczające i czy będzie zapewniało właściwy poziom ochrony.

III. ART. 34 – ZAWIADAMIANIE OSOBY, KTÓREJ DANE DOTYCZĄ

A. Zawiadamianie osób fizycznych

81. W niektórych przypadkach administrator musi nie tylko zgłosić naruszenie organowi nadzorczemu, ale również zawiadomić o nim osoby fizyczne, na które to naruszenie wywiera wpływ.

Art. 34 ust. 1 RODO 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".

82. Administratorzy powinni pamiętać, że zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu jest obowiązkowe, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw lub wolności osób fizycznych. Ponadto jeżeli istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych spowoduje wysokie ryzyko naruszenia praw lub wolności osób fizycznych, należy poinformować o nim również osoby fizyczne. A zatem poziom zagrożenia skutkujący powstaniem obowiązku przekazania osobom fizycznym informacji o naruszeniu jest wyższy niż w przypadku zgłaszania naruszenia organom nadzorczym, dzięki czemu nie ma obowiązku zgłaszania osobom fizycznym wszystkich naruszeń, co pozwala ochronić je przed nadmiarem niepotrzebnych powiadomień.

83. RODO stanowi, że osoby fizyczne należy poinformować o naruszeniu „bez zbędnej zwłoki" – tj. najszybciej, jak to możliwe. Zawiadomienie osób fizycznych ma na celu przede wszystkim dostarczenie im szczegółowych informacji na temat działań zapobiegawczych, które powinny podjąć [40]. Jak wspomniano powyżej, w zależności od charakteru naruszenia i powstałego ryzyka, szybkie

[40] Zob. również motyw 86 RODO.

zawiadomienie pozwoli osobom fizycznym podjąć działania, aby uchronić się przed wszelkimi negatywnymi skutkami naruszenia.

84. W załączniku B do niniejszych wytycznych przedstawiono niewyczerpujący wykaz przykładowych sytuacji, w których istnieje prawdopodobieństwo, że naruszenie stworzy wysokie ryzyko dla osób fizycznych, a co za tym idzie przypadków, w których administrator musi zgłosić wystąpienie naruszenia osobom, na które ma ono wpływ.

B. Informacje, które należy podać

85. W odniesieniu do zawiadamiania osób fizycznych art. 34 ust. 2 RODO 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)".

86. Zgodnie z tym przepisem administrator musi udzielić co najmniej następujących informacji:

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

87. Jednym z przykładów środków zastosowanych w celu zaradzenia naruszeniu i zminimalizowania jego ewentualnych negatywnych skutków może być deklaracja administratora, że po zgłoszeniu naruszenia właściwemu organowi nadzorczemu administrator uzyskał zalecenie dotyczące zarządzania naruszeniem i ograniczenia jego wpływu. Administrator powinien również – w stosownych przypadkach – przekazać osobom fizycznym szczegółowe zalecenia na temat sposobów ochrony przed potencjalnymi niekorzystnymi skutkami naruszenia – takich jak zmiana haseł – jeżeli ich dane uwierzytelniające zostały ujawnione. Również w tym wypadku administrator może podjąć decyzję o przekazaniu większej ilości informacji, niż jest to wymagane.

C. Kontakt z osobami fizycznymi

88. Co do zasady osoby, których dane dotyczą, należy zawiadomić o naruszeniu bezpośrednio, chyba że takie działanie wymagałoby 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) RODO).

89. Osoby, których dane dotyczą, należy zawiadamiać o naruszeniu za pomocą specjalnie do tego przeznaczonych wiadomości i nie należy tych wiadomości przesyłać wraz z innymi informacjami, takimi jak regularne aktualizacje, biuletyny lub standardowe wiadomości. Dzięki temu zawiadomienie o naruszeniu będzie jasne i przejrzyste.

90. Do przykładów przejrzystych metod zawiadamiania należą komunikacja bezpośrednia (np. wiadomości e-mail, SMS, wiadomości bezpośrednie), rzucające się w oczy bannery lub powiadomienia na stronach internetowych, komunikacja pocztowa oraz rzucające się w oczy reklamy w mediach drukowanych. Powiadomienie, które jest tylko częścią komunikatu prasowego lub zostało zamieszczone na blogu przedsiębiorstwa, nie byłoby skuteczną metodą zawiadomienia osób fizycznych o naruszeniu. EROD zaleca, aby administratorzy wybierali metody pozwalające zapewnić jak największą szansę właściwego przekazania informacji wszystkim osobom fizycznym, na które to naruszenie wywiera wpływ. W niektórych okolicznościach może to oznaczać, że administrator wykorzysta szereg metod komunikacji, a nie tylko jeden kanał kontaktowy.

91. Może zdarzyć się, że administratorzy będą również musieli zapewnić dostępność zawiadomienia w odpowiednich formatach alternatywnych i stosownych językach, aby zapewnić osobom fizycznym możliwość zrozumienia przedstawionych im informacji. Na przykład do zawiadomienia osoby fizycznej o naruszeniu właściwy będzie zazwyczaj język wykorzystywany we wcześniejszych zwykłych relacjach gospodarczych z odbiorcą. Jednak jeżeli naruszenie ma wpływ na osoby, z którymi administrator nie miał wcześniej kontaktu, lub w szczególności na osoby zamieszkujące w państwie członkowskim lub państwie trzecim innym niż państwo, w którym administrator posiada jednostkę organizacyjną, dopuszczalne może być użycie w zawiadomieniu miejscowego języka urzędowego, uwzględniając przy tym potrzebne zasoby. Najważniejsze, aby osoby, których dane dotyczą, zrozumiały charakter naruszenia i wiedziały, co muszą zrobić, aby się zabezpieczyć.

92. Administratorzy mają największe kompetencje do określenia kanału kontaktowego, który byłby najwłaściwszy do zawiadomienia osób fizycznych o naruszeniu, w szczególności jeżeli regularnie wchodzą w interakcję ze swoimi klientami. Jest jednak oczywiste, że administrator powinien uważać, aby nie wykorzystywać kanału kontaktowego, który w wyniku naruszenia przestał być bezpieczny, ponieważ kanał ten mogą wykorzystać również atakujący podszywający się pod administratora.

93. Jednocześnie w motywie 86 RODO wyjaśniono, że:

> „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".

94. Kontakt i konsultacje z organem nadzorczym pozwolą administratorom uzyskać nie tylko zalecenia na temat powiadamiania osób, których dane dotyczą, o naruszeniu zgodnie z art. 34, ale również na temat stosownych wiadomości, które należy wysłać do osób fizycznych, oraz najwłaściwszego sposobu skontaktowania się z nimi.

95. Kwestii tej dotyczy zalecenie zawarte w motywie 88 RODO, które stanowi, że w zawiadomieniu o naruszeniu „należy [...] uwzględnić prawnie uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia ochrony danych osobowych". Może to oznaczać, że w pewnych okolicznościach, gdy jest to uzasadnione, oraz zgodnie z zaleceniami organów ścigania administrator może opóźnić wysłanie zawiadomienia o naruszeniu do osób fizycznych, na które wywiera ono wpływ, do momentu, w którym takie zawiadomienie nie zaszkodzi takim postępowaniom. Osoby, których dane dotyczą, należy jednak wciąż natychmiast poinformować po upływie tego okresu.

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

D. Sytuacje, w których zawiadomienie nie jest konieczne

97. W art. 34 ust. 3 RODO określono trzy sytuacje, w których nie ma konieczności zawiadomienia osób fizycznych w przypadku wystąpienia naruszenia. Sytuacje te są następujące:

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

Może to na przykład obejmować zabezpieczenie danych osobowych za pomocą najnowocześniejszego szyfrowania lub tokenizacji;

- natychmiast po wystąpieniu naruszenia administrator podjął działania w celu wyeliminowania prawdopodobieństwa powstania wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej. Na przykład w niektórych sytuacjach administrator mógł natychmiast zidentyfikować osobę fizyczną, która uzyskała dostęp do danych osobowych, i podjąć wobec niej działania, zanim mogła ona w jakikolwiek sposób wykorzystać te dane. Mimo to należy odpowiednio uwzględnić możliwe skutki każdego naruszenia poufności, również w tym wypadku biorąc pod uwagę charakter przedmiotowych danych;
- skontaktowanie się z danymi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku[41], na przykład ponieważ w wyniku naruszenia utracono ich dane kontaktowe albo dane te nigdy nie były znane. Na przykład archiwum urzędu statystycznego uległo zalaniu, a dokumenty zawierające dane osobowe przechowywano tylko w formie papierowej. W takim przypadku administrator musi wydać publiczny komunikat lub zastosować podobny środek, za pomocą którego osoby fizyczne zostaną poinformowane w równie skuteczny sposób. Jeżeli wykonanie tego działania wymagałoby niewspółmiernie dużego wysiłku, można również przewidzieć uzgodnienia techniczne, dzięki którym informacje na temat naruszenia będą dostępne na żądanie, co może okazać się przydatne dla osób, na które naruszenie mogło wywrzeć wpływ, lecz z którymi administrator nie mógł się w inny sposób skontaktować.

98. Zgodnie z zasadą rozliczalności administratorzy powinni być w stanie wykazać przed organem nadzorczym, że spełniają co najmniej jeden z tych warunków[42]. Warto pamiętać, że choć początkowo zgłoszenie może nie być wymagane ze względu na fakt, iż prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych nie istnieje, z czasem sytuacja może się zmienić i może wystąpić konieczność przeprowadzenia kolejnej oceny ryzyka.

99. Jeżeli administrator zdecyduje się nie zawiadamiać osoby fizycznej o naruszeniu, w art. 34 ust. 4 RODO wyjaśniono, że organ nadzorczy może od niego tego zażądać, jeżeli jego zdaniem naruszenie może powodować wysokie ryzyko dla osób fizycznych. Ewentualnie może stwierdzić, że spełnione zostały warunki, o których mowa w art. 34 ust. 3 RODO, i w takim przypadku zawiadomienie osób fizycznych nie jest konieczne. Jeżeli organ nadzorczy stwierdzi, że decyzja o niezawiadamianiu osób, których dane dotyczą, nie jest odpowiednio uzasadniona, może rozważyć wykorzystanie swoich uprawnień i nałożenie sankcji.

IV. OCENA RYZYKA I WYSOKIEGO RYZYKA

A. Ryzyko a obowiązek zgłoszenia

100. Mimo że w RODO wprowadzono obowiązek zgłaszania naruszenia, nie jest ono wymagane we wszystkich sytuacjach:

- zgłoszenie naruszenia właściwemu organowi nadzorczemu jest obowiązkowe, chyba że dane naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw lub wolności osób fizycznych;
- osobę fizyczną zawiadamia się o naruszeniu jedynie wówczas, gdy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności tych osób.

101. Oznacza to, że natychmiast po stwierdzeniu naruszenia administrator musi nie tylko dążyć do ograniczenia negatywnych skutków incydentu, lecz również ocenić ryzyko, które może powstać w wyniku tego naruszenia. Wynika to z dwóch ważnych przyczyn: po pierwsze, znajomość

[41] Zob. wytyczne Grupy Roboczej Art. 29 w sprawie przejrzystości, w których zajęto się kwestią niewspółmiernie dużego wysiłku, dostępne pod adresem: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[42] Zob. art. 5 ust. 2 RODO.

prawdopodobieństwa i potencjalnej dotkliwości wpływu na osoby fizyczne pomoże administratorowi w podjęciu skutecznych działań pozwalających zapanować nad skutkami naruszenia i je zminimalizować; po drugie, pomoże administratorowi stwierdzić, czy zgłoszenie naruszenia organowi nadzorczemu oraz – w stosownych przypadkach – osobom, których dotyczy naruszenie, jest konieczne.

102. Jak wyjaśniono powyżej, zgłoszenie naruszenia jest obowiązkowe, chyba że jest mało prawdopodobne, by skutkowało ono ryzykiem naruszenia praw lub wolności osób fizycznych, a to, czy o naruszeniu należy zawiadomić osoby, których dane dotyczą, zależy przede wszystkim od tego, czy naruszenie może powodować *wysokie* ryzyko naruszenia praw lub wolności osób fizycznych. Ryzyko to istnieje w przypadku, gdy naruszenie może prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych dla osób, których dane zostały naruszone. Przykłady takich szkód obejmują dyskryminację, kradzież lub sfałszowanie tożsamości, straty finansowe i naruszenie dobrego imienia. Jeżeli naruszenie obejmuje dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub seksualności lub dane dotyczące wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa – należy uznać, że taka szkoda prawdopodobnie nastąpi[43].

B. Czynniki, które należy uwzględnić podczas oceny ryzyka

103. Zgodnie z zaleceniami zawartymi w motywach 75 i 76 RODO podczas oceny ryzyka zasadniczo należy wziąć pod uwagę zarówno prawdopodobieństwo, jak i powagę ryzyka naruszenia praw lub wolności osób, których dane dotyczą. Stwierdzono również, że ryzyko naruszenia należy oszacować na podstawie obiektywnej oceny.

104. Należy podkreślić, że podczas oceny ryzyka naruszenia praw lub wolności osób fizycznych powstałego w wyniku wystąpienia naruszenia kładzie się nacisk na inne kwestie, niż kwestie dotyczące ryzyka uwzględniane w ocenie skutków dla ochrony danych[44]. W ocenie skutków dla ochrony danych bierze się pod uwagę zarówno ryzyko dla planowego przetwarzania danych, jak i ryzyko powstałe w przypadku wystąpienia naruszenia. Badając możliwe naruszenie, rozpatruje się w ujęciu ogólnym prawdopodobieństwo jego wystąpienia oraz szkody dla osób, których dane dotyczą, jakie mogą z niego wyniknąć; innymi słowy, jest to ocena wydarzenia hipotetycznego. W przypadku faktycznego naruszenia wydarzenie już nastąpiło, więc nacisk kładzie się w całości na powstałe ryzyko, że naruszenie będzie skutkowało wpływem na osoby fizyczne.

Przykład

Z oceny skutków dla ochrony danych wynika, że rozważane wykorzystanie określonego oprogramowania zabezpieczającego do ochrony danych osobowych stanowi właściwy środek służący zapewnieniu stopnia bezpieczeństwa, który jest odpowiedni względem ryzyka dla osób fizycznych, jakie w innym przypadku wynikałoby z przetwarzania danych. Gdyby jednak w późniejszym czasie wykryto lukę w zabezpieczeniach, sytuacja ta wpłynęłaby na przydatność oprogramowania do ograniczenia ryzyka dla chronionych danych osobowych, a zatem oprogramowanie należałoby poddać ponownej ocenie w ramach trwającej oceny skutków dla ochrony danych. Luka w oprogramowaniu zostaje później wykorzystana i następuje naruszenie. Administrator powinien przeprowadzić ocenę konkretnych okoliczności naruszenia, sprawdzić, których danych dotyczy naruszenie, a także oszacować potencjalny poziom wpływu na osoby fizyczne i prawdopodobieństwo wystąpienia tego ryzyka.

[43] Zob. motywy 75 i 85 RODO.

[44] Zob. wytyczne Grupy Roboczej dotyczące oceny skutków dla ochrony danych dostępne pod adresem: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

105. Oceniając ryzyko dla osób fizycznych będące wynikiem naruszenia, administrator powinien uwzględnić zatem konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia. EROD zaleca zatem, aby w trakcie oceny brano pod uwagę następujące kryteria[45]:

- **Rodzaj naruszenia**

106. Rodzaj stwierdzonego naruszenia może wpłynąć na poziom ryzyka dla osób fizycznych. Na przykład konsekwencje dla osoby fizycznej w przypadku naruszenia dotyczącego poufności danych, którego istotą jest ujawnienie informacji medycznych osobom nieupoważnionym, mogą być inne niż konsekwencje naruszenia polegającego na utracie informacji medycznych danej osoby, do których nie ma już dostępu.

- **Charakter, wrażliwość i ilość danych osobowych**

107. Kluczowym czynnikiem podczas oceniania ryzyka jest oczywiście rodzaj i wrażliwość danych osobowych, które zostały narażone w wyniku naruszenia. Zazwyczaj ryzyko powstania szkody dla osób, których dotyczy naruszenie, wzrasta wraz z wrażliwością danych, lecz należy wziąć pod uwagę również inne dane osobowe dotyczące tych osób, które mogą już być dostępne. Na przykład ujawnienie imienia i nazwiska oraz adresu danej osoby prawdopodobnie nie wyrządzi jej znaczącej szkody w normalnej sytuacji. Jednak jeżeli imię i nazwisko oraz adres rodzica adopcyjnego zostaną ujawnione rodzicowi biologicznemu, może mieć to bardzo poważne konsekwencje zarówno dla rodzica adopcyjnego, jak i dziecka.

108. Naruszenia powiązane z danymi dotyczącymi zdrowia, dokumentami tożsamości lub danymi finansowymi, takimi jak dane kart kredytowych, mogą spowodować szkody, jeżeli występują pojedynczo, lecz jeżeli wystąpią łącznie, mogą zostać wykorzystane do kradzieży tożsamości. Zbiór różnych danych osobowych ma zazwyczaj bardziej wrażliwy charakter niż pojedynczy element danych osobowych.

109. Niektóre rodzaje danych osobowych mogą się na pierwszy rzut oka wydawać nieszkodliwe, ale należy dokładnie rozważyć, jakie informacje takie dane mogą ujawnić na temat osoby fizycznej, na którą naruszenie wywiera wpływ. Wykaz klientów regularnie odbierających dostawy może nie stanowić szczególnie wrażliwych danych, ale takie same dane na temat klientów, którzy poprosili o wstrzymanie dostaw na czas urlopu, byłyby dla przestępców przydatne.

110. Ponadto niewielka ilość bardzo wrażliwych danych osobowych może mieć znaczny wpływ na daną osobę fizyczną, a wiele różnych szczegółów może ujawnić szerszy zakres informacji na temat tej osoby. Podobnie naruszenie, które ma wpływ na duże ilości danych osobowych dotyczące wielu osób, może wywołać skutki dla odpowiednio dużej liczby osób fizycznych.

- **Łatwość identyfikacji osób fizycznych**

111. Istotnym czynnikiem, który należy wziąć pod uwagę, jest łatwość, z jaką strona, która ma dostęp do ujawnionych danych osobowych, będzie w stanie zidentyfikować konkretne osoby fizyczne lub dopasować dane do innych informacji służących identyfikacji osób fizycznych. W zależności od okoliczności identyfikacja może być możliwa bezpośrednio w oparciu o dane osobowe, których dotyczy naruszenie, bez potrzeby gromadzenia dodatkowych informacji pozwalających określić tożsamość danej osoby lub dopasowanie danych osobowych do konkretnej osoby może być bardzo trudne, lecz wciąż wykonalne pod pewnymi warunkami. Identyfikacja może być pośrednio lub bezpośrednio możliwa w oparciu o ujawnione dane, ale może również zależeć od konkretnego kontekstu naruszenia

[45] W art. 3 ust. 2 rozporządzenia nr 611/2013 przedstawiono wytyczne dotyczące czynników, które należy wziąć pod uwagę w związku ze zgłaszaniem naruszeń w sektorze usług łączności elektronicznej – mogą one okazać się przydatne w kontekście dokonywania zgłoszeń zgodnie z RODO. Zob. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:pl:PDF

i publicznej dostępności powiązanych danych osobowych. Może to mieć większe znaczenie w przypadku naruszeń dotyczących poufności i dostępności danych.

112. Jak stwierdzono powyżej, dane osobowe chronione za pomocą odpowiedniego poziomu szyfrowania będą nieczytelne dla osób nieupoważnionych, które nie posiadają klucza deszyfrującego. Ponadto odpowiednio wdrożona pseudonimizacja (zdefiniowana w art. 4 pkt 5 RODO 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") również może zmniejszyć prawdopodobieństwo zidentyfikowania osób fizycznych w przypadku naruszenia. Jednak aby dane były nieczytelne, nie można polegać jedynie na technikach pseudonimizacji.

- **Waga konsekwencji dla osób fizycznych**

113. W zależności od charakteru danych osobowych, których dotyczy naruszenie – na przykład szczególnych kategorii danych osobowych – możliwe szkody, których mogą doznać osoby fizyczne, mogą być szczególnie poważne, zwłaszcza w przypadku gdy w wyniku naruszenia może nastąpić kradzież lub sfałszowanie tożsamości, uszkodzenie ciała, cierpienie psychiczne, upokorzenie lub naruszenie dobrego imienia. Jeżeli naruszenie jest związane z danymi osobowymi dotyczącymi osób szczególnie narażonych, może to dla nich stwarzać większe ryzyko szkody.

114. To, czy administrator wie, że dane osobowe znajdują się w rękach osób, których zamiary są nieznane lub które mogą mieć złe intencje, może mieć znaczenie dla poziomu potencjalnego ryzyka. Może nastąpić naruszenie dotyczące poufności danych polegające na omyłkowym ujawnieniu danych osobowych stronie trzeciej, zgodnie z definicją w art. 4 pkt 10, lub innemu odbiorcy. Może to nastąpić na przykład w sytuacji, gdy dane osobowe zostaną przypadkowo wysłane do niewłaściwego działu organizacji lub do organizacji dostawców, z której usług powszechnie się korzysta. Administrator może wezwać odbiorcę do zwrotu albo bezpiecznego zniszczenia otrzymanych danych. W obu przypadkach – z uwagi na fakt, że administrator pozostaje z tymi podmiotami w stałych stosunkach i może znać stosowane przez nie procedury, ich historię i inne istotne szczegóły ich dotyczące – odbiorcę można uznać za „zaufanego". Innymi słowy, administrator może ufać odbiorcy na tyle, aby móc racjonalnie oczekiwać, że strona ta nie odczyta omyłkowo wysłanych danych lub nie uzyska do nich wglądu oraz że wypełni polecenie ich odesłania. Nawet jeżeli do danych uzyskano wgląd, administrator nadal może mieć zaufanie do odbiorcy, że nie podejmie on żadnych dalszych działań w kwestii tych danych oraz że niezwłocznie zwróci dane do administratora i będzie współpracować przy ich odzyskaniu. W takich przypadkach administrator może uwzględnić tę kwestię w ocenie ryzyka przeprowadzanej w następstwie naruszenia – fakt, że odbiorca jest zaufany może spowodować, że skutki naruszenia nie będą poważne, ale nie znaczy to, że naruszenie nie miało miejsca. To z kolei może jednak wyeliminować prawdopodobieństwo wystąpienia ryzyka dla osób fizycznych, w wyniku czego nie będzie już potrzeby powiadomienia organu nadzorczego lub osób fizycznych, na które to naruszenie wywiera wpływ Również w tym wypadku wszystko będzie zależało od konkretnej sytuacji. Administrator wciąż jednak musi przechowywać informacje dotyczące naruszenia w ramach ogólnego obowiązku prowadzenia dokumentacji na temat naruszeń (zob. sekcja V poniżej).

115. Należy również zwrócić uwagę na to, jak trwałe są konsekwencje wobec osób fizycznych, gdyż wpływ może być postrzegany jako poważniejszy, jeżeli dotyczy długiego okresu.

- **Cechy szczególne danej osoby fizycznej**

116. Naruszenie może mieć wpływ na dane osobowe dotyczące dzieci lub innych osób szczególnie narażonych, w przypadku których w takiej sytuacji może występować większe ryzyko, że znajdą się w niebezpieczeństwie. Z daną osobą fizyczną mogą wiązać się również inne czynniki wpływające na wagę konsekwencji naruszenia, jakie mogą dla niej wyniknąć.

- **Cechy szczególne administratora danych**

117. Charakter i rola administratora oraz prowadzone przez niego działania mogą mieć wpływ na poziom ryzyka dla osób fizycznych wynikającego z naruszenia. Przykładowo w organizacji medycznej przetwarzane są szczególne kategorie danych osobowych, co oznacza, że w przypadku naruszenia tych danych osobowych osoby fizyczne są narażone na większe zagrożenie niż w przypadku, gdy naruszenie dotyczy listy adresowej czasopisma.

- **Liczba osób fizycznych, na które naruszenie wywiera wpływ**

118. Naruszenie może dotyczyć tylko jednej osoby, kilku osób lub kilku tysięcy osób – albo dużo większej ich liczby. Zazwyczaj potencjalny wpływ naruszenia wzrasta wraz z liczbą osób, których ono dotyczy. Jednak w zależności od charakteru danych osobowych oraz kontekstu, w którym zostały one narażone, naruszenie może mieć poważne konsekwencje nawet dla jednej osoby. Również w tym wypadku najważniejsze jest przeanalizowanie prawdopodobieństwa wystąpienia konsekwencji dla osób, na które naruszenie na wpływ, oraz tego, jak poważne będą te konsekwencje.

- **Uwagi ogólne**

119. W związku z tym podczas oceny ryzyka, które może powstać w wyniku naruszenia, administrator powinien łącznie uwzględnić wagę potencjalnego wpływu na prawa lub wolności osób fizycznych i prawdopodobieństwo jego wystąpienia. Oczywiście ryzyko wzrasta, gdy konsekwencje naruszenia są poważniejsze, jak również wtedy, gdy wzrasta prawdopodobieństwo ich wystąpienia. W przypadku jakichkolwiek wątpliwości administrator powinien zgłosić naruszenie, nawet jeśli taka ostrożność mogłaby się okazać nadmierna. W załączniku B przedstawiono użyteczne przykłady różnych rodzajów naruszeń skutkujących ryzykiem lub wysokim ryzykiem dla osób fizycznych.

120. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) opracowała zalecenia dotyczące metod oceny wagi naruszenia, które mogą się przydać administratorom i podmiotom przetwarzającym podczas opracowywania planów działania i zarządzania w sytuacji wystąpienia naruszenia[46].

V. ROZLICZALNOŚĆ I PROWADZENIE DOKUMENTACJI

A. Dokumentowanie naruszeń

121. Bez względu na to, czy należy zgłosić dane naruszenie organowi nadzorczemu, czy też nie, administrator jest zobowiązany do dokumentowania wszystkich naruszeń, jak wyjaśniono w art. 33 ust. 5 RODO:

> „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 na weryfikowanie przestrzegania niniejszego artykułu".

122. Jest to powiązane z zasadą rozliczalności zawartą w art. 5 ust. 2. RODO. Wymóg dokumentowania zarówno naruszeń, których nie trzeba zgłaszać, jak i naruszeń, które zgłaszać trzeba, jest również związany z obowiązkami administratora określonymi w art. 24 RODO, a organ nadzorczy może zażądać wglądu do tej dokumentacji. Administratorzy powinni zatem stworzyć wewnętrzny rejestr naruszeń bez względu na to, czy muszą je zgłaszać, czy też nie[47].

---

[46] ENISA, Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych, https://www.enisa.europa.eu/publications/dbn-severity

[47] Administrator może podjąć decyzję o dokumentowaniu naruszeń w prowadzonym na podstawie art. 30 RODO rejestrze czynności przetwarzania. Nie ma konieczności prowadzenia odrębnego rejestru pod warunkiem, że informacje dotyczące naruszenia są wyraźnie oznaczone i można je pobrać na żądanie.

123. Chociaż administrator określa metody i strukturę dokumentowania naruszeń, we wszystkich przypadkach należy uwzględnić określone kluczowe elementy zapisywanych informacji. Zgodnie z art. 33 ust. 5 RODO administrator jest zobowiązany do rejestrowania szczegółowych informacji na temat naruszenia, które obejmują jego przyczyny, przebieg wydarzeń oraz zakres danych osobowych, których dotyczyło naruszenie. Powinny one obejmować również skutki i konsekwencje naruszenia, uwzględniając działania zaradcze podjęte przez administratora.

124. W przepisach RODO nie sprecyzowano okresu przechowywania takiej dokumentacji. W przypadku gdy takie zapisy zawierają dane osobowe, administrator musi określić właściwy okres przechowywania zgodnie z zasadami dotyczącymi przetwarzania danych osobowych[48] oraz podstawą prawną przetwarzania[49]. Musi on przechowywać dokumentację zgodnie z art. 33 ust. 5 RODO w zakresie, w jakim może zostać wezwany do przedstawienia organowi nadzorczemu dowodów na przestrzeganie przepisów tego artykułu lub, w ujęciu bardziej ogólnym, zasady rozliczalności. W przypadku gdy dokumentacja nie zawiera żadnych danych osobowych, ustanowiona w RODO zasada ograniczenia przechowywania oczywiście nie ma zastosowania[50].

125. EROD zaleca, aby poza tymi informacjami szczegółowymi administrator dokumentował również uzasadnienia decyzji podjętych w odpowiedzi na naruszenie. Uzasadnienie decyzji należy udokumentować w szczególności w przypadku niezgłoszenia naruszenia. Uzasadnienie powinno obejmować powody, dla których administrator uznał, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych[51]. Jeżeli natomiast administrator uznał, że spełnione zostały którekolwiek warunki określone w art. 34 ust. 3 RODO, powinien być w stanie przedstawić wystarczające dowody potwierdzające.

126. W przypadku gdy administrator zgłasza naruszenie organowi nadzorczemu, lecz robi to z opóźnieniem, administrator musi przedstawić przyczyny takiego opóźnienia; stosowna dokumentacja może pomóc w wykazaniu, że opóźnienie w zgłoszeniu naruszenia jest uzasadnione i nie jest nadmierne.

127. Zawiadamiając o naruszeniu osoby fizyczne, na które wywiera ono wpływ, administrator powinien zachować w tej kwestii przejrzystość i przekazać informacje w sposób sprawny i terminowy. Przechowywanie dowodów takiego zawiadamiania ułatwi również administratorowi wykazanie swojej rozliczalności i zgodności z przepisami.

128. Zarówno administratorom, jak i podmiotom przetwarzającym łatwiej będzie przestrzegać przepisów art. 33 i 34 RODO, jeżeli wdrożą udokumentowaną procedurę powiadamiania, w której określone zostaną procesy postępowania po wykryciu naruszenia, jak również metody ograniczenia skutków incydentu, zarządzania nim i przywrócenia stanu sprzed jego wystąpienia, a także metody oceny ryzyka i zgłaszania naruszenia. W tym kontekście w wykazaniu zgodności z RODO pomocne może być również wykazanie, że pracownicy zostali poinformowani o istnieniu takich procedur i mechanizmów oraz że wiedzą, jak reagować na naruszenia.

129. Należy przy tym również podkreślić, że niewywiązanie się z obowiązku właściwego udokumentowania naruszenia może spowodować, że organ nadzorczy wykorzysta swoje uprawnienia na mocy art. 58 RODO lub nałoży administracyjną karę pieniężną zgodnie z art. 83 RODO.

[48] Zob. art. 5 RODO.

[49] Zob. art. 6, a także art. 9 RODO.

[50] Zob. art. 5 ust. 1 lit. e) RODO.

[51] Zob. motyw 85 RODO.

B. Rola inspektora ochrony danych

130. Administrator lub podmiot przetwarzający może wyznaczyć inspektora ochrony danych[52] – zgodnie z wymogami art. 37 RODO albo dobrowolnie w ramach dobrej praktyki. W art. 39 RODO określono szereg zadań wchodzących w zakres obowiązków inspektora ochrony danych, co jednak nie uniemożliwia przydzielenia mu – w stosownych przypadkach – dodatkowych zadań przez administratora.

131. Do zadań wchodzących w zakres obowiązków inspektora ochrony danych, które są szczególnie istotne z punktu widzenia zgłaszania naruszenia – obok innych obowiązków – należą: przekazywanie administratorowi lub podmiotowi przetwarzającemu zaleceń oraz informacji dotyczących ochrony danych, monitorowanie przestrzegania przepisów RODO oraz przekazywanie zaleceń w zakresie ocen skutków dla ochrony danych. Inspektor ochrony danych musi również współpracować z organem nadzorczym i służyć jako punkt kontaktowy dla organu nadzorczego i osób, których dane dotyczą. Należy również podkreślić, że zgodnie z art. 33 ust. 3 lit. b) RODO podczas zgłaszania naruszenia organowi nadzorczemu administrator musi przekazać imię i nazwisko oraz dane kontaktowe swojego inspektora ochrony danych lub innego punktu kontaktowego.

132. W kwestii dokumentowania naruszeń administrator lub podmiot przetwarzający mogą rozważyć zasięgnięcie opinii swojego inspektora ochrony danych na temat struktury i przygotowania dokumentacji oraz zarządzania nią. Inspektor ochrony danych może również otrzymać dodatkowe zadanie polegające na przechowywaniu takich rejestrów.

133. Z powyższych czynników wynika, że inspektor ochrony danych powinien odgrywać kluczową rolę we wspieraniu zapobiegania naruszeniom lub przygotowaniu na wypadek ich wystąpienia poprzez wydawanie zaleceń i monitorowanie przestrzegania przepisów, jak również w sytuacji naruszenia (tj. podczas zgłaszania naruszenia organowi nadzorczemu) oraz podczas wszelkich dalszych postępowań prowadzonych przez organ nadzorczy. W tym kontekście EROD zaleca niezwłoczne informowanie inspektora ochrony danych o wystąpieniu naruszenia oraz angażowanie go na wszystkich etapach procesu zarządzania w sytuacji wystąpienia naruszenia oraz procesu zgłaszania naruszenia.

VI. OBOWIĄZKI ZGŁASZANIA OKREŚLONE W INNYCH INSTRUMENTACH PRAWNYCH

134. Poza zgłaszaniem naruszeń i zawiadamianiem o nich na podstawie RODO i niezależnie od tych działań administratorzy powinni również posiadać wiedzę na temat wszelkich wymogów w zakresie zgłaszania incydentów bezpieczeństwa na podstawie innego powiązanego prawodawstwa, które może w ich przypadku mieć zastosowanie, a także wiedzę na temat tego, czy są na tej podstawie również zobowiązani do jednoczesnego zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu. Poszczególne państwa członkowskie mogą nakładać takie wymogi w różnych postaciach, lecz jako przykładowe wymogi zgłaszania naruszeń zawarte w innych instrumentach prawnych oraz ich współzależności z RODO można wymienić:

- *rozporządzenie (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (rozporządzenie eIDAS)*[53]

135. W art. 19 ust. 2 rozporządzenia eIDAS nałożono na dostawców usług zaufania wymóg zawiadamiania organu nadzoru o wszelkich 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. gdy tego rodzaju naruszenie lub utrata

[52] Zob. wytyczne Grupy Roboczej dotyczące inspektorów ochrony danych dostępne pod adresem: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

[53] Zob. http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.POL

stanowią również naruszenie ochrony danych osobowych zgodnie z RODO – dostawca usług zaufania powinien również zgłosić naruszenie organowi nadzorczemu.

- *dyrektywę (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dyrektywa dotycząca cyberbezpieczeństwa)*[54].

136. W art. 14 i 16 dyrektywy dotyczącej cyberbezpieczeństwa nałożono na operatorów usług kluczowych oraz na dostawców usług cyfrowych obowiązek zgłaszania incydentów bezpieczeństwa właściwemu organowi. Zgodnie z motywem 63 dyrektywy dotyczącej cyberbezpieczeństwa [55] incydenty bezpieczeństwa często wiążą się z niebezpieczeństwem naruszenia danych osobowych. Chociaż w dyrektywie dotyczącej cyberbezpieczeństwa nałożono na właściwe organy i organy nadzorcze wymóg współpracy i wymiany informacji w tym kontekście, pozostaje faktem, że w przypadku gdy takie incydenty stanowią naruszenie ochrony danych osobowych zgodnie z RODO lub w momencie gdy się nim stają, wspomniani operatorzy lub dostawcy musieliby zawiadomić organ nadzorczy niezależnie od wymogów dotyczących zgłoszenia incydentu zawartych w dyrektywie dotyczącej cyberbezpieczeństwa.

Przykład

Dostawca usługi przetwarzania w chmurze, który zgłasza naruszenie na podstawie dyrektywy dotyczącej cyberbezpieczeństwa, może również mieć obowiązek powiadomienia administratora, jeżeli naruszenie to obejmuje naruszenie ochrony danych osobowych. Podobnie dostawca usług zaufania, który zgłasza naruszenie na podstawie rozporządzenia eIDAS, może być również zobowiązany do powiadomienia odpowiedniego organu ochrony danych, jeżeli doszło do naruszenia.

- *dyrektywę 2009/136/WE (dyrektywa w sprawie praw obywateli) oraz rozporządzenie nr 611/2013 (rozporządzenie w sprawie powiadamiania o przypadkach naruszenia danych osobowych).*

137. W kontekście dyrektywy 2002/58/WE [56] dostawcy publicznie dostępnych usług łączności elektronicznej są zobowiązani do zgłaszania naruszeń właściwym organom krajowym.

138. Administratorzy powinni mieć również świadomość wszelkich dodatkowych spoczywających na nich obowiązków zgłaszania naruszeń o charakterze prawnym, medycznym lub zawodowym przewidzianych w ramach pozostałych mających zastosowanie systemów.

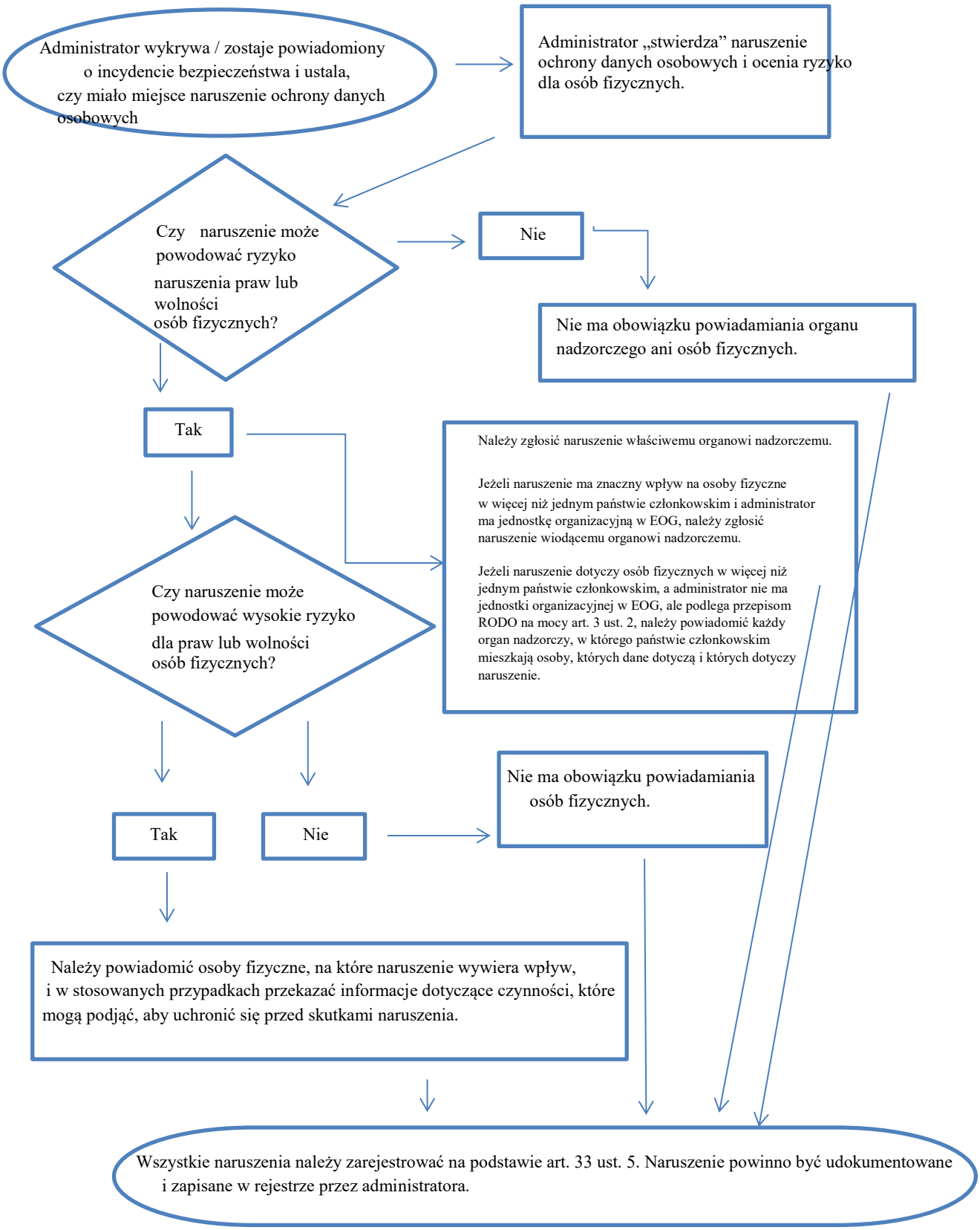
[54] Zob. http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.POL

[55] 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”.*

[56] W dniu 10 stycznia 2017 r. Komisja Europejska przedstawiła wniosek dotyczący rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej, które zastąpi dyrektywę 2009/136/WE i zlikwiduje wymogi zgłaszania naruszeń. Jednakże do czasu zatwierdzenia tego wniosku przez Parlament Europejski obowiązuje dotychczasowy wymóg zgłoszenia, zob. https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electroniccommunications

VII. ZAŁĄCZNIK

A. Schemat ilustrujący wymogi zgłaszania naruszeń



B. Przykłady naruszeń ochrony danych osobowych i podmiotów, które należy poinformować

Poniższy niewyczerpujący wykaz przykładowych sytuacji pomoże administratorom określić, czy w poszczególnych scenariuszach naruszenia ochrony danych osobowych należy dokonać zgłoszenia. Przykłady te mogą również pomóc odróżnić „ryzyko" od „wysokiego ryzyka" naruszenia praw lub wolności osób fizycznych.

	Przykład	Czy należy zgłosić organowi nadzorczemu?	Czy należy zgłosić osobie, której dane dotyczą?	Uwagi/zalecenia
i	Administrator przechowywał zaszyfrowaną kopię bezpieczeństwa archiwum danych osobowych na pamięci USB. Pamięć ukradziono podczas włamania.	Nie.	Nie.	Jeżeli dane zostały zaszyfrowane za pomocą najnowocześniejszego algorytmu, utworzono kopie bezpieczeństwa danych, unikalny klucz nie został złamany, a dane można przywrócić w odpowiednim czasie – być może naruszenie to nie podlega zgłoszeniu. Jeżeli jednak w późniejszym czasie klucz zostanie złamany, sytuacja ta będzie wymagała zgłoszenia.
ii	Administrator prowadzi usługę internetową. W wyniku cyberataku na tę usługę nastąpił wyciek danych osobowych osób fizycznych. Klienci administratora znajdują się w jednym państwie członkowskim.	Tak, naruszenie należy zgłosić organowi nadzorczemu, jeżeli możliwe są konsekwencje dla osób fizycznych.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od charakteru danych osobowych, których dotyczy naruszenie, oraz gdy możliwe konsekwencje dla osób fizycznych są poważne.	
iii	Krótkotrwała, kilkuminutowa awaria systemu zasilania w centrum obsługi telefonicznej administratora, w wyniku której klienci nie mogą skontaktować się z administratorem i uzyskać dostępu do swoich danych.	Nie.	Nie.	Naruszenie to nie podlega zgłoszeniu, lecz mimo to należy ten incydent zarejestrować na podstawie art. 33 ust. 5. Administrator musi prowadzić odpowiednie rejestry.

iv	Administrator pada ofiarą ataku za pomocą oprogramowania typu ransomware, w wyniku którego wszystkie dane zostały zaszyfrowane. Nie są dostępne żadne kopie bezpieczeństwa, a danych nie można przywrócić. W trakcie postępowania okazuje się, że oprogramowanie typu ransomware wykorzystano jedynie do zaszyfrowania danych, a w systemie nie stwierdzono obecności żadnego innego złośliwego oprogramowania.	Tak, naruszenie należy zgłosić organowi nadzorczemu, jeżeli możliwe są konsekwencje dla osób fizycznych, ponieważ sytuacja ta jest równoznaczna z utratą dostępności.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od charakteru danych osobowych, których dotyczy naruszenie, potencjalnych skutków braku dostępności danych oraz innych możliwych konsekwencji.	Jeżeli istniałaby kopia bezpieczeństwa i możliwe byłoby przywrócenie danych w odpowiednim czasie, zgłaszanie naruszenia organowi nadzorczemu lub osobom fizycznym nie byłoby konieczne, ponieważ nie miałyby miejsca trwała utrata dostępności lub naruszenie poufności danych. Jeżeli jednak organ nadzorczy dowiedziałby się o tym incydencie z innych źródeł, mógłby rozważyć wszczęcie postępowania do celów oceny zgodności z szerszymi wymogami dotyczącymi bezpieczeństwa określonymi w art. 32.

v	Pewna osoba dzwoni do centrum obsługi telefonicznej banku, by zgłosić naruszenie ochrony danych. Osoba ta otrzymała miesięczny wyciąg bankowy przeznaczony dla kogoś innego. Administrator przeprowadza krótkie postępowanie (tj. trwające do 24 godzin) i ustala z uzasadnioną pewnością, że miało miejsce naruszenie ochrony danych osobowych, i stwierdza, czy w jego systemie występuje wada, która może oznaczać, że naruszenie	Tak.	Naruszenie zgłasza się wyłącznie osobom fizycznym, na które naruszenie wywarło wpływ, jeżeli istnieje wysokie ryzyko i jest jasne, że naruszenie nie dotyczy nikogo innego.	Jeżeli w wyniku dalszego postępowania stwierdzono, że naruszenie ma wpływ na większą liczbę osób fizycznych, należy przekazać organowi nadzorczemu aktualne informacje, a administrator wykonuje dodatkową czynność polegającą na zawiadomieniu o naruszeniu innych osób fizycznych, jeżeli sytuacja ta może powodować dla nich wysokie ryzyko.

	wpłynęło lub mogło wpłynąć na inne osoby fizyczne.			
vi	Administrator prowadzi internetową platformę handlową, a jego klienci znajdują się w wielu państwach członkowskich. Platforma pada ofiarą cyberataku i atakujący publikuje w internecie identyfikatory użytkownika, hasła i historię zakupów.	Tak, naruszenie należy zgłosić wiodącemu organowi nadzorczemu, jeżeli ma miejsce transgraniczne przetwarzanie.	Tak, ponieważ może to doprowadzić do powstania wysokiego ryzyka.	Administrator powinien zareagować, np. wymusić zmianę haseł kont, których dotyczy naruszenie, jak również poczynić inne kroki w celu zminimalizowania ryzyka. Administrator powinien również wziąć pod uwagę wszelkie inne wymogi zgłaszania naruszeń, np. wynikające z dyrektywy dotyczącej cyberbezpieczeństwa, które mają do niego zastosowanie z uwagi na fakt, że jest dostawcą usług cyfrowych.
vii	Przedsiębiorstwo zajmujące się web hostingiem, które pełni rolę podmiotu przetwarzającego, znajduje błąd w kodzie, który kontroluje autoryzację użytkowników. W wyniku tej wady każdy użytkownik może uzyskać wgląd w szczegółowe informacje na temat	Jako podmiot przetwarzający przedsiębiorstwo zajmujące się web hostingiem musi niezwłocznie zgłosić naruszenie swoim klientom, na których wywarło ono wpływ (administratorom). Zakładając, że przedsiębiorstwo zajmujące się web hostingiem	Jeżeli prawdopodobieństwo istnienia wysokiego ryzyka dla osób fizycznych jest niewielkie, nie ma potrzeby ich powiadomienia.	Przedsiębiorstwo zajmujące się web hostingiem (podmiot przetwarzający) musi również uwzględnić wszelkie inne obowiązki zgłaszania naruszeń (np. wynikające z dyrektywy dotyczącej cyberbezpieczeństwa – z uwagi na fakt, że jest dostawcą usług cyfrowych). Jeżeli nic nie wskazuje na to, że tę lukę w zabezpieczeniach wykorzystano przeciwko

	konta dowolnego innego użytkownika.	przeprowadziło swoje własne postępowanie, administratorzy, na których naruszenie wywarło wpływ, powinni mieć wystarczającą pewność co do tego, czy padli ofiarą naruszenia, a tym samym tego, czy można uznać, że „stwierdzili naruszenie" po zgłoszeniu naruszenia przez przedsiębiorstwo zajmujące się web hostingiem (podmiot przetwarzający). Administrator musi następnie zgłosić naruszenie organowi nadzorczemu.		jakiemukolwiek administratorowi, naruszenie mogło nie podlegać zgłoszeniu, lecz prawdopodobnie należy je udokumentować lub jest związane z nieprzestrzeganiem art. 32.
viii	Szpitalna dokumentacja medyczna jest niedostępna przez 30 godzin w wyniku cyberataku.	Tak, szpital ma obowiązek zgłoszenia naruszenia, ponieważ może powstać wysokie ryzyko dla dobrostanu i prywatności pacjentów.	Tak, naruszenie należy zgłosić osobom fizycznym, na które wywiera ono wpływ.	
ix	Dane osobowe znacznej liczby studentów omyłkowo wysłano do niewłaściwej listy adresowej, na której znajduje się ponad 1000 odbiorców.	Tak, naruszenie należy zgłosić organowi nadzorczemu.	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju ujawnionych danych osobowych i wagi możliwych konsekwencji.	
x	E-mail marketingu bezpośredniego zostaje wysłany do odbiorców wymienionych w polach „do:" lub „dw:", co umożliwia każdemu odbiorcy wgląd w adresy innych odbiorców.	Tak, zgłoszenie naruszenia organowi nadzorczemu może być obowiązkowe, jeżeli naruszenie dotyczy dużej liczby osób, jeżeli ujawniono dane wrażliwe (takie jak np. lista adresowa psychoterapeuty) lub jeżeli inne czynniki stwarzają wysokie ryzyko (np. wiadomość e-mail zawiera hasła startowe).	Tak, naruszenie należy zgłosić osobom fizycznym w zależności od zakresu i rodzaju ujawnionych danych osobowych i wagi możliwych konsekwencji.	Zgłoszenie może nie być konieczne, jeżeli nie ujawniono żadnych danych wrażliwych i jeżeli ujawniono tylko niewielką liczbę adresów e-mail.