JOWITA SOBCZAK

Akademia Finansów i Biznesu Vistula

Obowiązek zgłaszania naruszeń ochrony danych osobowych w jednostkach organizacyjnych

Ostatnie zmiany legislacyjne w obszarze ochrony danych osobowych pokazały, że ochrona danych to dla wielu podmiotów priorytet w prowadzeniu działalności gospodarczej. Przepisy 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 („ogólne rozporządzenie o ochronie danych osobowych", „RODO") obligują wszystkie jednostki organizacyjne, które przetwarzają dane osobowe, do ochrony tych danych oraz ustanawiania odpowiednich zabezpieczeń określonych w powyższym rozporządzeniu.

Obowiązek zgłaszania naruszeń organowi nadzorczemu, czyli Prezesowi Urzędu Ochrony Danych Osobowych (PUODO), został wprowadzony na mocy przepisów ogólnego rozporządzenia o ochronie danych osobowych, które weszło w życie 25 maja 2018 r. Naruszenia ochrony danych osobowych przez wiele lat były skrupulatnie utrzymywane w tajemnicy przez jednostki organizacyjne, w których takie naruszenie wystąpiło (nie istniał obowiązek ich ujawniania). Wyjątek stanowili przedsiębiorcy usług telekomunikacyjnych, którzy w świetle przepisów prawa telekomunikacyjnego zobligowani byli, w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych, powiadomić o tym właściwy organ

do spraw ochrony danych osobowych[1], a także abonenta lub użytkownika końcowego, w przypadku którego tajemnica danych została naruszona.

Przepisy art. 33 ogólnego rozporządzenia o ochronie danych zobligowały wszystkie podmioty przetwarzające dane osobowe do zgłaszania przypadków naruszenia ochrony danych osobowych, w tym praw i wolności osób, których dane dotyczą, do organu nadzorczego (PUODO). Istotne jest, aby administratorzy danych[2] w procesie związanym ze zgłaszaniem naruszenia ochrony danych posiadali odpowiednie narzędzia umożliwiające im szybką reakcję na zdarzenie, zarówno wobec organu nadzorczego jak i osób, których dane dotyczą. W celu zapewnienia działania bez zbędnej zwłoki jednostki organizacyjne powinny opracować i wdrożyć procedury postępowania na wypadek wystąpienia naruszenia ochrony danych, które mogą znacznie usprawnić i przyspieszyć działania w przypadku wykrycia takiego naruszenia.

Pojęcie naruszenia ochrony danych osobowych

Przepisy ogólnego rozporządzenia o ochronie danych osobowych wprowadzają legalną definicję pojęcia „naruszenie ochrony danych osobowych". Termin ten zgodnie z art. 4 pkt 12 RODO oznacza „przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych". Oznacza to, że naruszenia mogą odnieść się do różnych czynności przetwarzania danych, a w szczególności ich przechowywania bądź przesyłania[3]. Naruszenie może być rodzajem incydentu bezpieczeństwa. Jednocześnie P. Fajgielski wyjaśnia, że naruszenie bezpieczeństwa można uznać

[1] Przed 25 maja 2018 r. organem do spraw ochrony danych osobowych był Generalny Inspektor Ochrony Danych Osobowych.

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

[3] P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Wyd. C.H.Beck, Warszawa 2018, s. 508.

za naruszenie danych osobowych[4]. Warto przypomnieć, że incydentem bezpieczeństwa, zgodnie z normą ISO/IEC 27001[5], będzie pojedyncze zdarzenie lub seria niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji. Przepisy ogólnego rozporządzenia o ochronie danych osobowych mają zastosowanie wyłącznie w sytuacji, gdy dochodzi do naruszenia ochrony danych osobowych. Wystąpienie takiego naruszenia prowadzi do sytuacji, w której podmiot nie jest w stanie zapewnić zgodności z zasadami dotyczącymi przetwarzania danych osobowych określonymi w art. 5 RODO. Pozwala to odróżnić incydent bezpieczeństwa od zdarzenia skutkującego naruszeniem ochrony danych osobowych[6]. Naruszenie ochrony danych musi spełniać łącznie trzy przesłanki:

1) dotyczyć danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych przez jednostkę organizacyjną, której dotyczy naruszenie;
2) skutkiem naruszenia może być zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych;
3) naruszenie jest skutkiem złamania zasad bezpieczeństwa danych osobowych.

Grupa Robocza Artykuł 29[7] w Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych[8] wyróżnia trzy typy naruszeń ochrony danych:

[4] P. Fajgielski, *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" 2016, nr 20, 2016.
[5] PN-EN ISO/IEC 27001:2017 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.
[6] Zob. także: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 6.
[7] Grupa robocza ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych powołana została na mocy art. 29 Dyrektywy 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych jako niezależny podmiot o charakterze doradczym. Grupa ta została rozwiązana 25 maja 2018 r., a w jej miejsce została powołana Europejska Rada Ochrony Danych.
[8] Tamże, s. 7.

1) Naruszenie poufności danych – występuje w przypadku nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Przykładowo naruszeniem takim będzie umożliwienie osobie nieuprawnionej wglądu do dokumentów zawierających dane osobowe.
2) Naruszenie integralności danych – dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych, np. pracownik zmienia imiona klientów w systemie informatycznym przetwarzającym.
3) Naruszenie dostępności danych – dochodzi do przypadkowej lub nieuprawnionej utraty dostępu do danych osobowych lub zniszczenia danych osobowych. Przykładem utraty dostępności będzie sytuacja, w której doszło do przypadkowego usunięcia danych albo ich usunięcia przez nieuprawnioną osobę, jeżeli doprowadziło ono do trwałej utraty lub zniszczenia tych danych. Do utraty dostępności może dojść również wskutek awarii systemu zasilania lub zainfekowania systemu informatycznego/oprogramowania „złośliwym" oprogramowaniem.

Warto 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.

Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu

Obowiązek zgłaszania naruszeń ochrony danych osobowych wynika z przepisów ogólnego rozporządzenie o ochronie danych, który w art. 33 określa, 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 […] chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych".

Stwierdzenie wystąpienia naruszenia bezpieczeństwa danych osobowych następuje w momencie, w którym administrator uzyskuje wystarczającą wiedzę potwierdzającą tego typu zdarzenie. Warto podkreślić, że administrator danych nie zawsze może zgłosić naruszenie w wyznaczonym terminie. Dokonanie zgłoszenia z opóźnieniem, czyli po upływie 72 godzin, może być w niektórych

przypadkach akceptowane przez organ nadzorczy (PUODO), ale podmiot zgłaszający naruszenie musi dołączyć stosowne wyjaśnienie przyczyn i okoliczności takiego opóźnienia.

Po stwierdzeniu naruszenia administrator danych powinien ocenić prawdopodobne ryzyko, na jakie narażone są osoby fizyczne, aby ustalić, czy w danym przypadku zastosowanie ma wymóg zgłoszenia takiego naruszenia, a także aby określić działania, które należy podjąć, aby zaradzić temu naruszeniu. Dlatego bardzo ważne jest, aby administrator danych posiadał odpowiednią dokumentację wewnętrzną, np. procedury dotyczące zgłaszania naruszeń. Zgodnie z zaleceniami Prezesa Urzędu Ochrony Danych Osobowych taka procedura powinna zawierać:

- cel, w jakim procedura została opracowana;
- zakres jej stosowania;
- katalog ewentualnych potencjalnych zagrożeń i naruszeń, które mogą się pojawić w danej jednostce organizacyjnej;
- opis etapów zarządzania naruszeniami;
- opis postępowania personelu administratora danych w przypadku wystąpienia naruszenia ochrony danych osobowych[9].

Administrator danych powinien zapoznać z tą procedurą personel oraz wszystkie inne osoby zaangażowane w przetwarzanie danych w jednostce organizacyjnej, np. podczas szkolenia z zakresu ochrony danych. Pracownicy powinni wiedzieć komu i w jakich okolicznościach należy zgłaszać zdarzenie naruszenia ochrony danych osobowych oraz jak mają postępować w takiej sytuacji. Dlatego też administrator danych powinien ustanowić wewnętrzne zasady wykrywania naruszenia i zaradzenia mu. Zgodnie z motywem 87 ogólnego rozporządzenia o ochronie danych administrator danych powinien upewnić się, czy zastosował wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by móc możliwie jak najszybciej stwierdzić naruszenie ochrony danych osobowych i w wyznaczonym terminie (72 godziny) poinformować organ nadzorczy (PUODO) oraz, jeśli zajdzie taka potrzeba, osobę, której dane dotyczą. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem

[9] Zob. także: Obowiązki administratorów związane z naruszeniami ochrony danych osobowych, Urząd Ochrony Danych Osobowych, wersja 1.0, czerwiec 2019, s. 5.

w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją Prezesa Urzędu Ochrony Danych Osobowych.

W sytuacji, kiedy administrator danych przeprowadził już stosowną analizę w celu ustalenia okoliczności naruszenia ochrony danych osobowych, dokonuje zgłoszenia na formularzu określonym przez PUODO, który dostępny jest na stronie internetowej tego organu. Tak jak wskazano wyżej, kluczowa dla każdego zgłoszenia naruszenia jest ochrona praw i wolności osób, których dane dotyczą, dlatego niezwykle ważny jest szybki czas reakcji administratora danych na zdarzenie. Warto podkreślić, że przepisy ogólnego rozporządzenia o ochronie danych osobowych przewidują dwa rodzaje obowiązków związanych ze zgłaszaniem naruszeń ochrony danych osobowych:

- zgłoszenie przez administratora danych organowi nadzorczemu;
- zgłoszenie przez podmiot przetwarzający[10] administratorowi danych.

Oznacza to, że podmiot, który przetwarza dane osobowe na zlecenie administratora danych (np. podmiot prowadzący obsługę księgową administratora, usługi archiwum czy usługi IT), po stwierdzeniu naruszenia bezpieczeństwa danych osobowych bez zbędnej zwłoki zobligowany jest zgłosić takie naruszenie administratorowi danych. Dotyczy to także dostawców usług chmurowych, którzy bardzo często korzystają z serwerów położonych w wielu krajach, w tym w państwach trzecich[11]. Ogólne rozporządzenie o ochronie danych zobowiązuje podmiot przetwarzający do wspierania administratora danych w realizacji obowiązku zgłoszenia naruszenia do Prezesa Urzędu Ochrony Danych Osobowych, np. poprzez udzielenie dostępnych mu w danej sprawie informacji. Dlatego bardzo ważnym elementem umowy z podmiotem przetwarzającym, który będzie wykonywał zadania związane z przetwarzaniem danych na rzecz administratora danych, są odpowiednio skonstruowane zabezpieczenia prawne w umowie dotyczące

[10] Zgodnie z art. 4 pkt 8 RODO przez podmiot przetwarzający należy rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

[11] Zob. także: J. Sobczak, *Realizacja usługi przetwarzania danych osobowych w chmurze obliczeniowej*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wyd. Nauk. UPH, Sieldce, 2019, s. 121.

zgłaszania naruszeń ochrony danych przez podmiot przetwarzający: tak, aby administrator danych mógł wywiązać się z obowiązku na nim spoczywającym w zakresie zgłoszenia naruszania do PUODO w terminie przewidzianym w ogólnym rozporządzeniu o ochronie danych, tj. 72 godzin po stwierdzeniu naruszenia. Najczęściej zastrzeżenia dotyczące terminu zgłaszania naruszeń ochrony danych osobowych przez podmiot przetwarzający wskazane są w umowie powierzenia, o której mowa w art. 28 RODO. Bowiem w przypadku, gdy administrator danych zdecyduje się na powierzenie przetwarzania danych osobowych, zobligowany jest podjąć odpowiednie zabezpieczenia, m.in. zawrzeć stosowna umowę powierzenia z podmiotem. Umowa powierzenia przetwarzania powinna zawierać w szczególności:

1) przedmiot przetwarzania – będzie on powiązany z realizacją przedmiotu umowy głównej zawartej pomiędzy administratorem danych a podmiotem przetwarzającym, np. outsourcing działań marketingowych, gdy dla ich wykonania konieczne jest przetwarzanie danych osobowych;
2) czas trwania przetwarzania – co do zasady powiązany z realizacją przedmiotu umowy;
3) charakter przetwarzania;
4) cel przetwarzania – określenie, dlaczego podmiot przetwarzający ma przetwarzać dane osobowe w imieniu administratora;
5) kategorię danych osobowych – wymienienie, jakie konkretnie dane osobowe będą podlegały powierzeniu przy uwzględnieniu podziału na dane zwykłe (przykładowo wymienione w art. 4 pkt 1 RODO) oraz dane szczególnych kategorii (katalog zawarty w art. 9 ust. 1 RODO);
6) kategorię osób, których dane dotyczą – sprecyzowanie grupy osób, których dane zostały powierzone do przetwarzania, np. dane klientów, dane pracowników.

Praktycznym rozwiązaniem w przypadku obowiązku zgłaszania naruszeń ochrony danych osobowych przez podmiot przetwarzający jest opracowanie przez administratora odpowiedniej procedury, która może stanowić załącznik do umowy. Przepisy dotyczące obowiązku zgłaszania naruszeń ochrony danych przez podmiot przetwarzający mogą być z praktycznego i prawnego punkt widzenia niewystarczające. Jeżeli podmiot przetwarzający świadczy usługi na rzecz kilku administratorów, a naruszenie wywiera wpływ na wszystkich z nich, podmiot

przetwarzający będzie zobowiązany do zgłoszenia wystąpienia wspomnianego naruszenia każdemu z tych administratorów. Warto podkreślić, że zasady zgłaszania naruszeń przez podmiot przetwarzający powinny być dostarczone i przekazane wszystkim osobom zaangażowanym w realizację umowy. Administratorzy danych oraz podmioty przetwarzające powinni propagować kulturę ochrony danych osobowych w organizacjach oraz przeprowadzać regularne szkolenia w tym zakresie.

Grupa Robocza Artykuł 29 w swoich Wytycznych dotyczących zgłaszania naruszeń ochrony danych osobowych przedstawiła propozycje postępowania w przypadku zaistnienia naruszenia ochrony danych osobowych. Według niej poniższe zasady powinny być uwzględniane we wszystkich przypadkach wystąpienia naruszeń:

1) Informacje na temat wszystkich zdarzeń powiązanych z ochroną danych powinny być przekazywane w szczególności osobom, którym powierzono zadanie reagowania na naruszenia.
2) Należy wyznaczyć w jednostce organizacyjnej osobę odpowiedzialną za ustalanie zaistnienia naruszenia i dokonania oceny poziomu ryzyka.
3) Ocena ryzyka dla osób fizycznych związana z danym naruszeniem powinna być przekazywana odpowiednim komórkom organizacyjnym w ramach danej organizacji.
4) W razie konieczności (po dokonaniu oceny) należy zgłosić dane naruszenie organowi nadzorczemu (podmiot przetwarzający zgłasza je do administratora danych) oraz w przypadku zaistnienia przesłanki należy poinformować o naruszeniu osoby fizyczne, których naruszenie dotyczy.
5) Administrator powinien podjąć działania mające na celu ograniczenie skali naruszenia i przywrócenie stanu sprzed wystąpienia naruszenia.
6) Informacje na temat naruszenia powinny być udokumentowane[12].

W przypadku konieczności zgłoszenia naruszenia ochrony danych do organu nadzorczego administrator danych powinien w szczególności zawrzeć w nim opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać:

[12] Zob. także: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 8.

- kategorię i przybliżoną liczbę osób, których dane dotyczą;
- kategorię i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- opis środków zastosowanych w procesie obsługi naruszenia ochrony danych osobowych, w tym środków, które – w stosownych przypadkach – mają służyć zminimalizowaniu jego ewentualnych, negatywnych skutków.

Według danych przekazanych przez Prezesa Urzędu Ochrony Danych Osobowych administratorzy bardzo często popełniają błędy w takim zgłoszeniu naruszenia, co utrudnia i wydłuża pracę tego organu. Najczęściej występującymi błędami podczas zgłaszania naruszeń ochrony danych osobowych są w szczególności:

- błędna liczba osób, których dane dotyczą;
- podanie niewłaściwej kategorii danych;
- wskazanie niewłaściwego poziomu ryzyka;
- podanie niewłaściwego czasu zaistnienia naruszenia.

Ponadto, zgodnie z art. 33 ust. 3 ogólnego rozporządzenia o ochronie danych, administrator powinien w zgłoszeniu podać tylko kategorie danych osobowych, których dotyczy naruszenie. Kategoriami danych będą np. imię, nazwisko, adres zamieszkania, adres e-mail, numer PESEL, dane dotyczące zdrowia, dane dotyczące wykształcenia itp. Niewłaściwą praktyką jest podawanie w takim zgłoszeniu konkretnych imion, nazwisk czy adresów zamieszkania osób, których dane dotyczą[13]. Wątpliwości pojawiają się także przy interpretacji terminu „kategoria osób". RODO nie określa definicji kategorii osób, których dane dotyczą. Grupa Robocza Artykuł 29 zaproponowała, aby kategorie osób, których dane dotyczą, obejmowały różnego rodzaju osoby fizyczne których dotyczy naruszenie danych osobowych, np. pracownicy, klienci, współpracownicy itp.

[13] Komunikat Prezesa Urzędu Ochrony Danych Osobowych, www.uodo.gov.pl [dostęp 12.02.2020].

Warto podkreślić, że brak dostępu do szczegółowych informacji nie może stanowić podstawy do niezgłoszenia naruszenia danych osobowych w terminie wymaganym przez ogólne rozporządzenie o ochronie danych osobowych. Jeżeli informacji o naruszeniu nie da się udzielić w tym samym czasie, można ich udzielać sukcesywnie PUODO, lecz bez zbędnej zwłoki. Różne kategorie naruszenia mogą bowiem wiązać się z koniecznością przekazania dodatkowych informacji, aby w pełni wyjaśnić okoliczności danej sprawy.

Grupa Robocza Artykuł 29 zaleca, aby w momencie, w którym administrator danych po raz pierwszy zgłasza naruszenie Prezesowi Urzędu Ochrony Danych Osobowych, poinformował również ten organ o tym, że nie dysponuje jeszcze wszystkimi wymaganymi informacjami, oraz że przekaże bardziej szczegółowe dane na późniejszym etapie, bez zbędnej zwłoki, po otrzymaniu takich informacji[14]. Organ nadzorczy powinien ustalić 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, które powinny zostać przekazane organowi nadzorczemu.

Warto zaznaczyć, że sam fakt wystąpienia naruszenia ochrony danych osobowych nie stanowi przesłanki do zgłoszenia takiego naruszenia do PUODO. Bowiem, tak jak zaznaczono w art. 33 ust. 1 RODO, dotyczy to naruszeń praw lub wolności osób fizycznych. Oznacza to, że natychmiast po stwierdzeniu naruszenia administrator danych musi nie tylko dążyć do ograniczenia negatywnych skutków zdarzenia (naruszenia), lecz również ocenić ryzyko, które może powstać w wyniku tego naruszenia dla osób, których dane dotyczą. Przykładowo naruszeniem, które nie będzie wymagało zgłoszenia organowi nadzorczemu, jest zagubienie przez pracownika bezpiecznie zaszyfrowanego komputera przenośnego (laptopa). Bowiem ryzyko zapoznania się przez osoby nieuprawnione z danymi zawartymi na tym dysku komputera przenośnego jest w tej sytuacji niskie.

Należy pamiętać, że bez względu na to, czy należy zgłosić dane naruszenie organowi nadzorczemu, czy też nie, administrator danych jest zobowiązany do dokumentowania wszystkich naruszeń danych osobowych. Dokumentacja

[14] Zob. także: Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 9.

powinna być prowadzona w taki sposób, by pozwalała organowi nadzorczemu na weryfikowanie przestrzegania obowiązków dotyczących zgłaszania naruszeń. Dokumentacja powinna zawierać co najmniej:

- informacje o okolicznościach naruszenia;
- skutki naruszenia;
- podjęte działania zaradcze.

Brak wypełnienia obowiązków w zakresie prowadzenia dokumentacji stanowi przesłankę do zastosowania wobec podmiotu administracyjnej kary pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa w wysokości do 2% jego całkowitego rocznego światowego obrotu (z poprzedniego roku obrotowego).

Zawiadamianie osoby o naruszeniu ochrony jej danych osobowych

W sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator danych – oprócz zgłoszenia do PUODO – zobligowany jest bez zbędnej zwłoki zawiadomić osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie ma na celu przede wszystkim dostarczenie szczegółowych informacji na temat działań zapobiegawczych, które osoby fizyczne powinny podjąć, aby uchronić się przed wszelkimi negatywnymi skutkami naruszenia. Administrator danych powinien dołożyć wszelkich starań, by zawiadomienie było zredagowane z użyciem przejrzystego i zrozumiałego języka dla osób, których dane dotyczą. Prezes Urzędu Ochrony Danych Osobowych, powołując się na wytyczne Grupy Roboczej Artykuł 29, zaleca, aby sformułowania kierowane do podmiotu danych były przekazem bezpośrednim. Należy wybrać taką formę zawiadomienia, by osoba fizyczna miała możliwość zapoznania się z jego treścią, np. wiadomość e-mail, SMS, korespondencja[15]. Zawiadomienie powinno zostać dostarczone osobie, której dane dotyczą, w możliwie najkrótszym czasie.

Zgodnie z RODO zawiadomienie osoby fizycznej nie jest wymagane w następujących przypadkach:

[15] Prezes Urzędu Ochrony Danych Osobowych, www.uodo.gov.pl [dostęp 15.02.2020].

1. Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, np. szyfrowanie uniemożliwiające odczyt osobom nieuprawnionym.
2. Administrator zastosował środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane zostały naruszone.
3. Zawiadomienie 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. W zakresie publicznego komunikatu należy przyjąć, iż powinien on zawierać takie elementy jak charakter naruszenia, opisany jasnym i prostym językiem oraz zawierać informacje o zastosowanych środkach zaradczych[16].

Kluczowe dla organizacji jest wdrożenie odpowiednich środków technicznych i organizacyjnych zapobiegających możliwym naruszeniom ochrony danych.

Zawiadomienie o naruszeniu ochrony danych osób fizycznych powinno zawierać w szczególności:

1) opis charakteru naruszenia (np. przedstawienie okoliczności wystąpienia naruszenia);
2) imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych (jeżeli został on wyznaczony) lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
3) opis możliwych konsekwencji naruszenia ochrony danych osobowych (np. możliwość zaciągnięcia zobowiązań finansowych);
4) opis środków zastosowanych i proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych lub zminimalizowania jego ewentualnych, negatywnych skutków.

Istotne jest, aby informacje przekazane osobie fizycznej, dotyczące naruszenia, były dla niej zrozumiałe w zakresie charakteru naruszenia oraz wiedzy na temat postępowania, aby się zabezpieczyć.

[16] Zob. także: P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Wyd. C.H.Beck, Warszawa 2018, s. 519.

Najczęściej występujące naruszenia danych osobowych

Zgodnie z danymi podanymi w sprawozdaniu z działalności Prezesa Urzędu Ochrony Danych Osobowych za 2018 rok[17] zakres przedmiotowy naruszeń ochrony danych osobowych zgłaszanych przez administratorów danych z sektora publicznego obejmował najczęściej nieprawidłowości w przetwarzaniu danych osobowych dotyczące:

1. Udostępnienia danych osobowych nieuprawnionym osobom w związku z wysyłaniem poczty elektronicznej. Naruszenie powstawało wskutek błędu pracowników. Administratorzy podejmowali działania mające na celu zdyscyplinowanie pracowników, przeprowadzali dodatkowe szkolenia, dokonywali przeglądu procedur, wykonywali audyty bezpieczeństwa. Warto zaznaczyć, że w takim przypadku, co do zasady, konieczne jest poinformowanie osób fizycznych o naruszeniu[18].
2. Udostępnienia danych w trybie dostępu do informacji publicznej, w wyniku nieprawidłowej anonimizacji danych, w tym w Biuletynie Informacji Publicznej. Naruszenia powstawały głównie wskutek niedopatrzenia pracowników zajmujących się anonimizacją danych. Administratorzy dokonywali przeglądu procedur oraz deklarowali wprowadzenie dodatkowych procedur (np. dodatkowe sprawdzanie dokumentów przez innego pracownika pod kątem anonimizacji dokumentów).
3. Zniszczenia/zagubienia/kradzieży dokumentacji bądź innych nośników (telefon, smartfon, komputer przenośny) zawierających dane osobowe. Administratorzy podejmowali działania mające na celu ustalenie przyczyn zagubienia korespondencji czy weryfikację umów zawartych z operatorem pocztowym. Sam fakt utraty danych osobowych w wyniku zagubienia czy kradzieży urządzeń lub nośników nie musi prowadzić do naruszenia praw lub wolności osób, których dane dotyczą, jeżeli administrator

[17] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r., www.uodo.gov.pl [dostęp 12.02.2020].

[18] Zob. Decyzja (ZWAD.405.154.2018) Prezesa Urzędu Ochrony Danych Osobowych z dnia 21 grudnia 2018 r. nakazująca ubezpieczycielowi ponowne zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych i wskazanie jej możliwych konsekwencji zdarzenia, a także powiadomienie jej o podjętych działaniach zaradczych i proponowanych środkach, które osoba ta może zastosować, by zminimalizować ewentualne negatywne skutki naruszenia.

zastosował skuteczne, adekwatne środki zabezpieczenia. Przykładowo, w celu eliminowania naruszeń, administrator danych powinien:

- ograniczyć ilość dokumentacji wynoszonej poza obszar obiektu administratora danych do niezbędnego minimum;
- tam, gdzie jest to możliwe, przewozić dokumentację w formie elektronicznej (na zaszyfrowanych urządzeniach informatycznych).

4. Naruszenia związane z udostępnieniem danych osobowych (np. zaświadczeń), które zawierały informacje o innych, osobom nieuprawnionym lub petentom urzędów. Najczęściej naruszenia wynikały z błędów pracowników urzędów. Administratorzy podejmowali działania podobne jak w poprzednich przypadkach, tj. mające na celu zdyscyplinowanie pracowników.
5. Naruszenia polegające na złamaniu zabezpieczeń systemu informatycznego, które skutkowało zablokowaniem dostępu do plików, całego komputera lub wewnętrznej sieci intranetowej przez złośliwe oprogramowanie typu ransomware. Administratorzy odzyskiwali dostęp do danych na podstawie kopii zapasowych baz danych wykonywanych automatycznie.

Z kolei informacje dotyczące najczęściej zgłaszanych naruszeń w sektorze prywatnym dotyczyły podobnych działań jak w sektorze publicznym, jednak dodatkowo można wyszczególnić:

1) lukę bezpieczeństwa w systemie informatycznym pozwalającą na uzyskanie nieuprawnionego dostępu do danych osobowych;
2) przesłanie newslettera z błędnie skonstruowanego skryptu z adresów e-mail do wszystkich odbiorców;
3) omyłkowe udostepnienie w trakcie rozmowy telefonicznej danych innego klienta przez pracownika call center;
4) ataki hackerskie, mające na celu uzyskanie nieuprawnionego dostępu do bazy danych klientów, sklepów internetowych w celu wysyłki phishingowych wiadomości SMS i wyłudzenia danych dostępowych do konta bankowego.

W przypadku naruszenia polegającego na udostępnieniu danych osobowych nieuprawnionym osobom w związku z wysyłką poczty elektronicznej, jeśli już doszło do takiego naruszenia, administrator danych powinien w szczególności:

- wprowadzić procedury kontroli poprawności adresu przy wysyłce dokumentów zawierających dane osobowe;
- przed wysyłką dokumentów weryfikować poprawność adresu z klientem.

Natomiast w przypadku niewłaściwej anonimizacji danych osobowych administrator danych powinien w szczególności:

- przeprowadzać regularne szkolenia dla personelu z zakresu ochrony danych;
- wprowadzić szczegółowe instrukcje postępowania z dokumentami zawierającymi dane osobowe, w tym – sposobów anonimizacji danych;
- wprowadzić wewnętrzne procedury regulujące przechowywanie archiwalnych dokumentów oraz ich późniejsze niszczenie.

Administratorzy powinni dokonywać szczegółowej analizy przypadków naruszeń ochrony danych osobowych, bowiem nie wszystkie będą wymagały zgłoszenia do organu nadzorczego. Jednocześnie istotne jest, by administratorzy danych potrafili prawidłowo i sprawnie reagować na już występujące naruszenia, aby możliwie ograniczyć negatywny wpływ na ochronę praw i wolności osób fizycznych.

Analiza występujących naruszeń ochrony danych

Według Prezesa Urzędu Ochrony Danych Osobowych brak przeprowadzenia prawidłowej oceny ryzyka naruszenia praw lub wolności osób fizycznych jest jednym z podstawowych błędów, które popełniają administratorzy danych. Zgodnie bowiem 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. Należy podkreślić, że podczas oceny ryzyka naruszenia praw i wolności osób fizycznych powstałego w wyniku wystąpienia naruszenia bardzo często administratorzy danych koncentrują się na innych (niż ochrona praw i wolności podmiotu danych) obszarach, np. zabezpieczaniu danych. Oceniając ryzyko dla osób fizycznych, będące wynikiem naruszenia, administrator powinien uwzględnić zatem konkretne okoliczności naruszenia, w tym wagę potencjalnego wpływu i prawdopodobieństwo jego wystąpienia. Grupa Robocza Artykuł 29 zaleca zatem, aby w trakcie oceny brano pod uwagę następujące kryteria[19]:

1) rodzaj naruszenia, np. konsekwencje naruszenia dla osoby fizycznej w przypadku naruszenia integralności;
2) charakter, wrażliwość i ilość danych osobowych;

[19] Wytyczne dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01), s. 28-30.

3) łatwość identyfikacji osób fizycznych;
4) wagę konsekwencji dla osób fizycznych, tj. możliwe szkody, których mogą doznać osoby fizyczne, np. w przypadku, gdy w wyniku naruszenia nastąpi kradzież lub sfałszowanie tożsamości, uszkodzenie ciała, cierpienie psychiczne, upokorzenie lub naruszenie dobrego imienia;
5) cechy szczególne danej osoby fizycznej;
6) cechy szczególne administratora danych;
7) liczbę osób fizycznych, na które wywiera wpływ dane naruszenie.

Mając na uwadze powyższe, administrator danych, dokonując oceny ryzyka, które może powstać w wyniku naruszenia, powinien łącznie uwzględnić wagę potencjalnego wpływu na prawa i 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. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) opracowała zalecenia dotyczące metod oceny wagi naruszenia[20], które mogą być przydatne administratorom i podmiotom przetwarzającym podczas opracowywania planów działania i zarzadzania w sytuacji wystąpienia naruszenia.

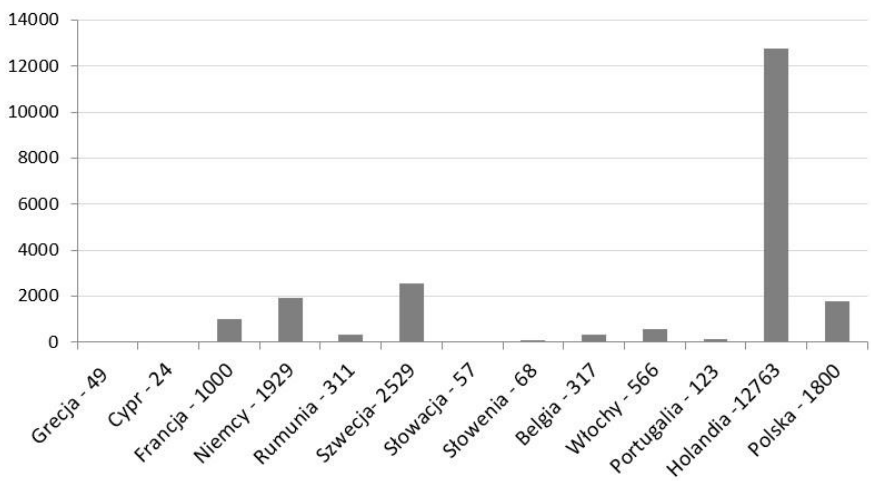
Statystyki zgłoszonych naruszeń ochrony danych

Zgodnie z danymi ze sprawozdania z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r. od 25 maja do 31 grudnia 2018 r. UODO dokonał analizy 2 446 zgłoszeń naruszeń pod kątem wystąpienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych, w tym – 1 882 naruszenia zostały zgłoszone przez podmioty sektora prywatnego, zaś 564 – przez podmioty sektora publicznego[21]. Dla porównania: do irlandzkiego organu nadzorczego wpłynęło w 2018 r. 3 687 zgłoszeń naruszeń ochrony danych osobowych[22], w tym – 2 429

[20] ENISA, Zalecenia dotyczące metod oceny wagi naruszeń ochrony danych osobowych, https://www.enisa.europa.eu/publications/dbn-severity [dostęp 12.02.2020].
[21] Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r., www.uodo.gov.pl [dostęp 12.02.2020].
[22] Annual Report 25 may – 31 december 2018, An Coimisium um Chosaint Sonrai, Data Protection Commission, s. 36-38.

z sektora prywatnego, a 1 258 – z sektora publicznego. Natomiast liczba powiadomień o naruszeniu danych otrzymanych przez holenderski organ nadzorczy wyniosła 20 881, w tym najbardziej dotknięte sektory to sektory zdrowia (29% zgłoszonych naruszeń), sektor finansowy (26% zgłoszonych naruszeń) oraz sektor publiczny (17% zgłoszonych naruszeń). 63% przypadków naruszeń, które wpłynęły do holenderskiego organu nadzorczego, dotyczyło danych osobowych wysłanych na niewłaściwy adres e-mail. Pozostałe 37% przypadków dotyczyło utraty danych osobowych (np. zagubienie laptopa lub pamięci USB), hackowania, phishingu lub złośliwego oprogramowania[23].

Według danych opublikowanych przez Komisję Europejską w UE w okresie od 25 maja 2018 r. do 28 stycznia 2019 r. zgłoszono w łącznie 41 502 powiadomień o naruszeniu ochrony danych osobowych. Z rysunku 1 wynika, że liczba zawiadomień o naruszeniach ochrony danych wpływających do poszczególnych organów nadzorczych w krajach Unii Europejskiej jest bardzo zróżnicowana, a najwięcej naruszeń zostało zgłoszonych w Holandii.



Rysunek 1. Całkowita liczba otrzymanych powiadomień o naruszeniu ochrony danych osobowych w okresie od 25 maja 2018 r. do 28 stycznia 2019 r.
Źródło: opracowanie własne na podstawie „GDPR Today", https://www.gdprtoday.org/gdpr-in-numbers-4/ [dostęp 10.02.2020].

[23] Autoriteit, Persoonsgegevens, Meldplicht dataleeken. Overzicht feiten en cijfers 2018, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2019/01/rapportage_datalekken_2018.pdf [dostęp 12.02.2020].

Zgodnie z informacją podaną przez Prezesa Urzędu Ochrony Danych Osobowych do maja 2019 r. administratorzy, realizując obowiązek wynikający z art. 33 ust. 1 ogólnego rozporządzenia o ochronie danych (RODO), zgłosili aż 4 539 naruszeń ochrony danych osobowych. Dwie trzecie notyfikacji pochodziło od administratorów z sektora prywatnego, a jedna trzecia – od administratorów z sektora publicznego. W przypadku sektora prywatnego najwięcej zgłoszeń napłynęło od firm telekomunikacyjnych, ubezpieczeniowych, finansowych, banków oraz służby zdrowia. W sektorze publicznym zawiadomienia o incydentach z danymi osobowymi najczęściej nadsyłały jednostki samorządu terytorialnego, szkoły, przedszkola, żłobki oraz placówki służby zdrowia[24].

Według Komisji Europejskiej w Unii Europejskiej do organów nadzorczych wpłynęło w okresie od 25 maja 2018 r. do maja 2019 r. aż 89 271 zgłoszeń o utracie danych, które mogły spowodować naruszenie praw lub wolności osób fizycznych[25], co pokazuje, że jednostki organizacyjne w Unii Europejskiej są świadome obowiązku związanego ze zgłaszaniem naruszeń ochrony danych.

Wnioski

Naruszenie bezpieczeństwa danych osobowych może potencjalnie spowodować szereg negatywnych skutków dla osób fizycznych, takich jak powstanie uszczerbku fizycznego, szkód majątkowych lub szkód niemajątkowych. Przykładowo mogą one obejmować utratę kontroli nad własnymi danymi osobowymi, ograniczenie praw, dyskryminację, kradzież lub sfałszowanie tożsamości, stratę finansową czy też naruszenie dobrego imienia. Mogą one również wiązać się z wszelkimi innymi znacznymi szkodami gospodarczymi lub społecznymi dla tych osób fizycznych.

Dlatego w art. 33 ogólnego rozporządzenia o ochronie danych osobowych zobligowano administratora danych do zgłoszenia naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, chyba że dane naruszenie nie wiąże się z ryzykiem wywołania takich negatywnych skutków.

[24] Prezes Urzędu Ochrony Danych Osobowych, https://uodo.gov.pl/pl/134/1029 [dostęp 12.02.2020].

[25] The European Data Protection Board, Rapport: "GDPR in numbers", edpb.europa.eu [dostęp 12.02.2020].

Warto podkreślić, że RODO przewiduje odpowiedzialność administracyjną za niezrealizowanie obowiązku zgłaszania naruszeń oraz innych postanowień zawartych w art. 33 RODO. W sytuacji, kiedy administrator danych nie zrealizuje obowiązku zgłoszenia naruszenia ochrony danych organowi nadzorczemu albo osobom, których dane dotyczą, albo zarówno organowi nadzorczemu, jak i osobom, których dane dotyczą, organ nadzorczy może skorzystać z możliwości zastosowania administracyjnej kary pieniężnej. Wartość tej kary może wynosić 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 albo nieadekwatności istniejących środków bezpieczeństwa. Ponadto wytyczne Grupy Roboczej Art. 29 w sprawie administracyjnych kar stanowią, że: „występowanie kilku różnych naruszeń popełnionych łącznie w konkretnym pojedynczym przypadku oznacza, że organ nadzorczy może nakładać administracyjne kary w sposób, który jest zarazem skuteczny, proporcjonalny i odstraszający na poziomie najpoważniejszego naruszenia". W takim przypadku organ nadzorczy będzie miał również możliwość nakładania kar za niewywiązanie się z obowiązku zgłoszenia naruszenia lub zawiadomienia o wystąpieniu naruszenia, określonego w art. 33 i 34 RODO z jednej strony, oraz za brak (odpowiednich) środków bezpieczeństwa, o których mowa w art. 32 RODO, z drugiej strony. Obydwie te sytuacje traktuje się jako dwa odrębne naruszenia.

Mając na uwadze powyższe przepisy podmioty, które przetwarzają dane osobowe, powinny zastosować odpowiednie środki organizacyjne i techniczne, w tym wdrożyć odpowiednie procedury, które pozwolą im sprawnie i szybko realizować proces ochrony danych osobowych w ich jednostce i w odpowiednim czasie (jeśli wymaga tego sytuacja) zgłosić takie naruszenie organowi nadzorczemu.

Bibliografia

Annual Report 25 may-31 december 2018, An Coimisium um Chosaint Sonrai, Data Protection Commission.

Autoriteit, Persoonsgegevens, Meldplicht dataleeken. Overzicht feiten en cijfers 2018, https://www.huntonprivacyblog.com/wp-content/uploads/sites/28/2019/01/rapportage_datalekken_2018.pdf.

Decyzja (ZWAD.405.154.2018) Prezesa Urzędu Ochrony Danych Osobowych z dnia 21 grudnia 2018 r. nakazująca ubezpieczycielowi ponowne zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych i wskazanie jej możliwych konsekwencji zdarzenia, a także powiadomienie jej o podjętych działaniach zaradczych i proponowanych środkach, które osoba ta może zastosować, by zminimalizować ewentualne negatywne skutki naruszenia.

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

Fajgielski P., *Informowanie o naruszeniu ochrony danych osobowych w świetle przepisów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" 2016, nr 20.

GDPR Today, GDPR in numbers, www.gdprtoday.org/gdpr-in-numbers.

Litwiński P., Barta P., Kawecki M., *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Komentarz*, Wyd. C.H.Beck, Warszawa 2018.

PN-EN ISO/IEC 27001:2017 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz.Urz. UE L z 2016 r. Nr 119/1).

Sobczak J., *Realizacja usługi przetwarzania danych osobowych w chmurze obliczeniowej*, [w:] *Informacje prawnie chronione – wybrane zagadnienia*, red. S. Topolewski, Wyd. Nauk. UPH, Siedlce 2019.

Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w 2018 r., www.uodo.gov.pl.

The European Data Protection Board, Rapport: "GDPR in numbers", edpb.europa.eu.

Wytyczne Grupy Roboczej Artykuł 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP 250 rev.01).

Obligation to report the breaches of personal data protection in organizational units

Summary: The article explains the process of notification of a personal data breach to the supervisory authority, in accordance with Article 33 of The General Data Protection Regulation (GDPR). The General Data Protection Regulation 2016/679 is a regulation in EU law on data protection and privacy for all individual citizens of the European Union and the European Economic Area. In case (preventive) security measures are breached and personal data is unlawfully processed, the controller must report such a breach to the supervisory authority within 72 hours, and possibly to affected data subjects as well. This is the case unless you can establish that the breach has caused no actual risks for the data subjects or other individuals. The article contains analysis of data breach notifications sent to data protection authorities by companies or other organizations.
Keywords: *GDPR, data protection, notification of a personal, data breach, personal data, supervisory authority*