Jak dokumentować naruszenia ochrony danych osobowych

zgodnie z RODO

experto24.pl

Spis treści

Zgłaszanie naruszeń ochrony danych osobowych organowi nadzorczemu i ich dokumentowanie to kolejny nowy obowiązek administratora danych wynikający z ogólnego rozporządzenia o ochronie danych osobowych (RODO). Wyjaśniamy jaki sposób trzeba będzie go realizować i jakie informacje zawrzeć w rejestrze naruszeń ochrony danych osobowych. Administrator powinien też już teraz zacząć przygotowywać się do realizowania obowiązku zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu. Może to zrobić np., opracowując wewnętrzną procedurę postępowania w przypadku naruszenia ochrony danych.

Jedną z zasadniczych zmian, jaką wprowadza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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, RODO), które zacznie być stosowane w całej Unii Europejskiej od 25 maja 208 r., jest kwestia związana z bezpieczeństwem danych osobowych. Ustawodawca europejski przewidział bowiem w art. 33 i 34 RODO różnego rodzaju obowiązki administratora i podmiotu przetwarzającego (tj. procesora) związane z wystąpieniem naruszenia ochrony danych osobowych.

Dokumentowanie naruszeń – nowy obowiązek

Administrator, zgodnie z art. 33 ust. 5 RODO, powinien dokumentować wszelkie naruszenia ochrony danych osobowych. W tym celu będzie mógł prowadzić rejestr naruszeń ochrony danych osobowych. Ważne, aby organ nadzorczy mógł zweryfikować, czy administrator realizuje ten obowiązek.

Pojęcie „naruszenie ochrony danych osobowych" zostało zdefiniowane 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" (art. 4 pkt 12 RODO). Pojęcie naruszenia ochrony danych osobowych (incydent) obejmuje bardzo szeroki katalog zdarzeń, które można podzielić na:

- zdarzenia losowe zewnętrzne (np. pożar prowadzący do utraty dokumentów papierowych zawierających dane osobowe),
- zdarzenia losowe wewnętrzne (takie jak np. zgubienie nośnika pendrive, na którym zapisane były pliki zawierające dane osobowe) oraz
- zdarzenia o charakterze umyślnym (np. atak hakerski, którego skutkiem jest nieuprawniony dostęp do systemów informatycznych, w których przetwarzane są dane osobowe).

Do czego może doprowadzić naruszenie

Ogólne rozporządzenie o ochronie danych kładzie duży nacisk na zapobieganie skutkom wystąpienia incydentu, który może doprowadzić do naruszenia ochrony danych osobowych. W motywie 85 RODO wskazuje, że „brak odpowiedniej i szybkiej reakcji na wystąpienie incydentu może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne".

WAŻNE

Administrator będzie musiał zgłosić naruszenie ochrony danych organowi nadzorczemu. W niektórych przypadkach będzie też zobowiązany poinformować o naruszeniu ochrony danych osobowych osobę, której danych dotyczyło naruszenie.

Czy informować o wszytskich naruszeniach

Naruszenia ochrony danych osobowych, które będą powodowały wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zgodnie z ogólnym rozporządzeniem o ochronie danych, trzeba będzie zgłaszać zarówno organowi nadzorczemu, jak i osobom, których danych dotyczyło naruszenie. Ze względu na ryzyko naruszenia praw lub wolności osób fizycznych i związane z tym dalsze konsekwencje, na gruncie ogólnego rozporządzenia o ochronie danych, można wyodrębnić trzy rodzaje incydentów:

- naruszenie ochrony danych osobowych, które nie podlega zgłoszeniu organowi nadzorczemu (czyli takie, które z małym prawdopodobieństwem skutkować będzie ryzykiem naruszenia praw i wolności osób fizycznych – art. 33 ust. 1 zdanie 1 *in fine* ogólnego rozporządzenia o ochronie danych),
- incydent, o którym trzeba zawiadomić zarówno organ nadzorczy, jak i osobę, której dane dotyczą (naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych – art. 34 ust. 1 ogólnego rozporządzenia o ochronie danych),
- naruszenie podlegające zgłoszeniu jedynie organowi nadzorczemu.

Jakie naruszenie zgłasza się tylko organowi nadzorczemu

Z naruszeniem ochrony danych osobowych, które trzeba zgłosić jedynie organowi nadzorczemu, mamy do czynienia w dwóch przypadkach. Po pierwsze, naruszenie ochrony danych zgłasza się tylko organowi nadzorczemu, w sytuacji gdy nie jest mało prawdopodobne, aby naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 ust. 1 zdanie 1 *in principio* ogólnego rozporządzenia o ochronie danych). Po drugie, naruszenie ochrony danych zgłasza się tylko organowi nadzorczemu także, gdy naruszenie ma charakter naruszenia drugiego rodzaju (tj. może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych), ale jednak zawiadomienie osoby, której dane dotyczą, nie jest konieczne ze względu na wypełnienie przesłanek z art. 34 ust. 3 RODO – tj. np. dane są szyfrowane.

Zgodnie z art. 34 ust. 3 RODO nie trzeba będzie zawiadamiać osoby, której dane dotyczą, że doszło do naruszenia ochrony danych osobowych w poniższych przypadkach:

- administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki

takie, jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,

- administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
- wymagałoby to niewspółmirnie 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.

Obowiązek oceny ryzyka naruszenia praw i wolności osób fizycznych spoczywa na administratorze. Niektórzy uważają, że aby nie narazić się na administracyjne kary pieniężne, administratorzy będą z ostrożności zgłaszać wszystkie incydenty.

Trzeba będzie dokumentować naruszenia ochrony danych

Zgodnie z art. 33 ust. 5 zdanie 1 *in principio* RODO administrator dokumentuje wszelkie naruszenia ochrony danych osobowych. Najlepiej w celu dokumentowania tego rodzaju naruszeń prowadzić rejestr incydentów, w którym powinny znaleźć się wszystkie trzy wskazane powyżej rodzaje incydentów. Zgodnie z art. 33 ust. 5 zdanie 1 RODO rejestr naruszeń ochrony danych osobowych powinien wskazywać:

- okoliczności naruszenia ochrony danych osobowych,
- jego skutki oraz
- podjęte działania zaradcze.

Poziom szczegółowości prowadzonego rejestru naruszeń ochrony danych osobowych będzie na pewno określony w praktyce kontrolnej organu nadzorczego. Stosownie do art. 33 ust. 5 zdanie 2 RODO prowadzony rejestr naruszeń ochrony danych osobowych musi pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania tego przepisu. Jest to odniesienie do wyrażonej w art. 5 ust. 2 RODO zasady rozliczalności. Zgodnie z nią administrator musi być w stanie wykazać przestrzeganie zasad przetwarzania danych osobowych (m.in. zasadę integralności i poufności).

W jakim czasie trzeba będzie zgłosić naruszenia

Przede wszystkim należy zwrócić uwagę na bardzo krótki czas pozostawiony na dokonanie zgłoszenia naruszenia ochrony danych do organu nadzorczego. Zgodnie z RODO administrator powinien zgłosić naruszenie organowi nadzorczemu „bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia".

WAŻNE

Jeśli administrator nie zgłosi naruszenia ochrony danych osobowych w terminie 72 godzin, do zgłoszenia naruszenia będzie musiał dołączyć wyjaśnienia dotyczące przyczyny opóźnienia.

Obowiązek zgłoszenia naruszenia ochrony danych osobowych będzie ciążył również na podmiocie przetwarzającym, przy czym nie będzie on zgłaszał naruszenia bezpośrednio organowi nadzorczemu, a tylko administratorowi, który następnie zgłosi naruszenie do organu nadzorczego. Podmiot przetwarzający zobowiązany będzie do zgłoszenia naruszenia administratorowi bez zbędnej zwłoki.

Jakie informacje zgłosić organowi nadzorczemu

Przepisy ogólnego rozporządzenia o ochronie danych określają minimum informacji, które powinny znaleźć się w zgłoszeniu naruszenia ochrony danych osobowych organowi nadzorczemu. Zgodnie z nimi zgłoszenie musi:

- 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,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- 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.

UWAGA

Ogólne rozporządzenie o ochronie danych nie określa formy, w jakiej należy zgłosić naruszenie ochrony danych osobowych (papierowa czy elektroniczna) oraz nie wprowadza wzoru zgłoszenia.

UWAGA

Za niezgłoszenie naruszenia organowi nadzorczemu i brak powiadomienia o nim osoby, której dane dotyczą będzie groziła ogromna kara pieniężna. Taryfikator z RODO określa ją na kwotę w wysokości do 10 mln euro lub do 2% całkowitego rocznego światowego obrotu przedsiębiorstwa z poprzedniego roku obrotowego (zastosowanie będzie miała wyższa kara).

Przygotuj procedurę postępowania w przypadku naruszenia

Jeśli administrator nie będzie miał zatwierdzonego kodeksu postępowania, warto, by wprowadził wewnętrzne procedury postępowania w przypadku naruszenia ochrony danych. Jest to istotne również z tego powodu, że ogólne rozporządzenie o ochronie danych nakłada na administratora obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym ich okoliczności, skutków oraz podjętych działań zaradczych.

7 elementów, jakie trzeba uregulować w wewnętrznej procedurze postępowania w przypadku naruszenia ochrony danych osobowych

1. Określenie, jakie zdarzenia mogą stanowić naruszenia ochrony danych osobowych, przy uwzględnieniu specyfiki danego administratora (na podstawie definicji naruszenia ochrony danych).

2. Sposób reagowania na naruszenia przez pracowników, którzy je ujawnili. Powinien się tu znaleźć:

- obowiązek niezwłocznego poinformowania o zdarzeniu osoby nadzorującej (powinien to być inspektor ochrony danych, a w przypadku gdy nie został wyznaczony – inna osoba upoważniona przez administratora lub sam administrator),

- obowiązek pozostawienia miejsca zdarzenia w stanie nienaruszonym do czasu przybycia inspektora ochrony danych lub innej osoby nadzorującej.

3. Obowiązki inspektora ochrony danych lub innej osoby odpowiedzialnej związane z dokumentowaniem okoliczności naruszenia, tj.:

- sporządzenie notatki z przeprowadzonych oględzin miejsca zdarzenia,
- sporządzenie kopii obrazu wyświetlonego na ekranie monitora komputera związanego z naruszeniem,
- sporządzenie kopii zapisów rejestrów systemu informatycznego służącego do przetwarzania danych lub zapisów konfiguracji technicznych środków zabezpieczeń systemu,
- odebranie pisemnych wyjaśnień od osoby, która ujawniła naruszenie.

4. Obowiązek niezwłocznego przedstawienia zebranych materiałów administratorowi, który z pomocą inspektora ochrony danych, w terminie i na podstawie przesłanek określonych w ogólnym rozporządzeniu o ochronie danych powinien ocenić, czy zaistniałe naruszenie podlega obowiązkowi zgłoszenia organowi nadzorczemu oraz powiadomieniu osoby, której dane dotyczą.

5. Obowiązek przedstawienia administratorowi przez inspektora ochrony danych skutków naruszenia oraz środków i działań mających zaradzić naruszeniu, a także, jeżeli to konieczne, mających zminimalizować negatywne skutki naruszenia.

6. Jeżeli istnieje taki obowiązek – sporządzenie zgłoszenia do organu nadzorczego oraz zawiadomienia do osoby, której dane dotyczą.

7. Udokumentowanie skutków oraz podjętych środków i działań, o których mowa w pkt 5.

Podstawa prawna:

- rozporządzenie Parlamentu Europejskiego i Rady 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).

Autorzy:
Jan Tyski,
specjalista ds. ochrony danych osobowych,
Piotr Janiszewski,
radca prawny, prezes zarządu spółki zajmującej się ochroną danych osobowych, audytem w obszarze ochrony danych osobowych zajmuje się od 8 lat

Stopka redakcyjna

Redaktor:	Wioleta Szczygielska
ISBN:	978-83-269-7052-8
E-book nr:	2HH0663
Wydawnictwo:	Wiedza i Praktyka sp. z o.o.
Adres:	03-918 Warszawa, ul. Łotewska 9a
Kontakt:	Telefon 22 518 29 29, faks 22 617 60 10, e-mail: *cok@wip.pl*
NIP:	526-19-92-256
Numer KRS:	0000098264 – Sąd Rejonowy dla m.st. Warszawy, Sąd Gospodarczy XIII Wydział Gospodarczy Rejestrowy. Wysokość kapitału zakładowego: 200.000 zł