Jak dokumentować naruszenia ochrony danych osobowych?

Posted on 2025-01-31

Administratorzy mają obowiązek gromadzić informacje o wszystkich naruszeniach ochrony danych osobowych – także tych, których nie trzeba zgłaszać Prezesowi UODO. Przedstawiamy rolę rejestru naruszeń ochrony danych osobowych oraz wskazówki dotyczące jego prowadzenia.

Dlaczego dokumentowanie naruszeń ochrony danych osobowych jest ważne?

Prowadzenie takiej dokumentacji jest nie tylko obowiązkiem prawnym. To narzędzie, które pomaga organizacjom lepiej zarządzać naruszeniami ochrony danych osobowych. Gromadzenie informacji na ten temat umożliwia pogłębioną analizę zagrożeń i ułatwia dobieranie skutecznych zabezpieczeń. Obowiązek prawny dokumentowania naruszeń ochrony danych osobowych wynika z 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. Dokumentacja zawierająca informacje o wykrytych naruszeniach ochrony danych osobowych jest podstawą do wykazania, że administrator działa zgodnie z przepisami. Ma to związek z zasadą rozliczalności (art. 5 ust. 2 RODO).

Kogo dotyczy obowiązek dokumentowania?

Dokumentowanie naruszeń ochrony danych osobowych jest wyłącznym obowiązkiem administratorów. Podmioty przetwarzające powinny jednak pomagać w jego realizacji, np. poprzez przekazywanie administratorom wszelkich niezbędnych informacji o naruszeniach ochrony danych osobowych (art. 28 ust. 3 lit. f RODO). Organizacje powinny też korzystać ze wsparcia inspektorów ochrony danych, polegającego na formułowaniu wskazówek i opinii dotyczących projektowania dokumentacji i zarządzania nią. Inspektorzy powinni także kontrolować, czy rejestry prowadzone są w sposób prawidłowy. Należy przy tym pamiętać, aby nie nakładać na inspektora zadań w zakresie obsługi naruszeń ochrony danych osobowych, które zagrażałyby jego niezależności, w szczególności powodowały konflikt interesów (art. 38 ust. 6 RODO) [1].

Jak prawidłowo

dokumentować naruszenia ochrony danych osobowych?

Administratorzy powinni na bieżąco aktualizować katalog wykrytych naruszeń ochrony danych osobowych, utrwalając informacje w odpowiednich rejestrach. Choć odrębna ewidencja nie jest formalnie wymagana, musi być wyraźnie oznaczona i dostępna do wglądu na żądanie Prezesa UODO. Obowiązek obejmuje wszystkie naruszenia ochrony danych osobowych, bez względu na to, czy wymagają one zgłoszenia organowi nadzorczemu. Rejestr naruszeń ochrony danych osobowych jest miejscem, w którym administrator powinien zamieścić m.in. uzasadnienie decyzji o niezgłaszaniu naruszenia ochrony danych osobowych, w przypadku zaistnienia ku temu stosownej przesłanki (art. 33 ust. 1 RODO). Ma to szczególne znaczenie, gdy z czasem ocena incydentu ulegnie zmianie i jego notyfikacja stanie się konieczna.

W RODO nie wskazano okresów przechowywania informacji o naruszeniach ochrony danych osobowych. Administratorzy powinni więc dysponować pełną dokumentacją tak długo i w takim zakresie, w jakim związani są zasadą rozliczalności. Innymi słowy, jak najdłużej. Z tego powodu umieszczanie w takim rejestrze jakichkolwiek danych osobowych nie jest zalecane. Jeżeli jednak tam się znajdą, należy pamiętać o ich prawidłowej ochronie, w tym o zasadzie ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO).

Jakie informacje powinny

znaleźć się w dokumentacji?

Rejestr naruszeń ochrony danych osobowych powinien uwzględniać m.in.:

- okoliczności naruszenia ochrony danych osobowych (takie jak data i czas wystąpienia, „stwierdzenia" i zakończenia naruszenia, sposób wykrycia naruszenia, przyczyny naruszenia, rodzaj naruszenia, przebieg naruszenia, rodzaj i zakres danych objętych naruszeniem, liczba i kategorie osób, których dane dotyczą);
- skutki (jeżeli wystąpiły) i/lub możliwe skutki naruszenia ochrony danych osobowych dla osób, których dane dotyczą;
- uzasadnienie oceny ryzyka;
- podjęte działania zaradcze (w celu powstrzymania i ograniczenia naruszenia ochrony danych osobowych oraz zminimalizowania jego skutków) i zapobiegawcze (w celu zminimalizowania wystąpienia podobnych naruszeń ochrony danych osobowych w przyszłości);
- szczegóły dotyczące zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO (takie jak data zgłoszenia, ewentualne przyczyny opóźnienia w zgłoszeniu, inne istotne informacje zawarte w zgłoszeniu; jeżeli administrator je zgłosił) lub uzasadnienie decyzji o niezgłoszeniu naruszenia ochrony danych osobowych Prezesowi UODO (art. 33 ust. 1 RODO);
- szczegóły dotyczące zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych (takie jak data zawiadomienia, treść zawiadomienia, metoda zawiadomienia, liczba zawiadomionych osób; jeżeli administrator je zawiadomił) lub – w stosownym przypadku – uzasadnienie decyzji o niezawiadomieniu osób, których dane dotyczą, o naruszeniu ochrony danych osobowych (art. 34 ust. 3 RODO).

Podsumowanie

Staranne dokumentowanie naruszeń ochrony danych osobowych to ważny element realizacji zasady rozliczalności i zapewnienia bezpieczeństwa przetwarzania. Dlatego też warto pamiętać o kilku dobrych praktykach:

1. Dokumentuj wszystkie naruszenia ochrony danych osobowych – Każdy przypadek naruszenia ochrony danych osobowych, niezależnie od tego, czy wymaga zgłoszenia Prezesowi UODO, musi zostać zarejestrowany.
2. Szczegółowo opisuj okoliczności zdarzenia – Uwzględnij takie informacje jak data i czas wystąpienia oraz wykrycia naruszenia ochrony danych osobowych, jego przyczyny, przebieg, liczba objętych nim osób oraz rodzaj i zakres naruszonych danych.
3. Rejestruj skutki – Wskaż faktyczne oraz potencjalne konsekwencje naruszenia ochrony danych osobowych dla osób, których dane dotyczą.
4. Dokumentuj działania zaradcze i zapobiegawcze – Opisz środki podjęte w celu ograniczenia skutków naruszenia ochrony danych osobowych oraz kroki mające zapobiec podobnym incydentom w przyszłości.
5. Aktualizuj rejestr na bieżąco – Utrwalaj informacje o naruszeniach ochrony danych osobowych niezwłocznie po ich wykryciu oraz uzupełniaj dane w miarę ich pozyskiwania.
6. Monitoruj proces dokumentowania – Regularnie weryfikuj prawidłowość i kompletność rejestru oraz procedur związanych z dokumentowaniem naruszeń ochrony danych osobowych, aby uniknąć ewentualnych braków.
7. Dbaj o przejrzystość i dostępność dokumentacji – Rejestr naruszeń ochrony danych osobowych powinien być kompletny, czytelny oraz dostępny dla organu nadzorczego na jego żądanie.

[1] Więcej na ten temat w artykule „Rola IOD przy naruszeniach ochrony danych osobowych” opublikowanym w „Biuletynie UODO” nr 10/10/24.