Naruszenia ochrony danych osobowych w świetle ustawy o KSC

Posted on 2026-03-28

Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, wdrażająca dyrektywę NIS 2, wprowadza mechanizm, na podstawie którego organy właściwe ds. cyberbezpieczeństwa będą informować Prezesa UODO o podejrzeniach naruszeń ochrony danych osobowych stwierdzanych w toku nadzoru. Kształtuje to nowy kanał pozyskiwania przez Prezesa UODO informacji o potencjalnych naruszeniach, niezależny od zgłoszeń dokonywanych przez samych administratorów w trybie art. 33 RODO. Co to oznacza w praktyce?

Nowy punkt styku ochrony danych osobowych i

cyberbezpieczeństwa

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (ustawa o KSC), której nowelizacja wejdzie w życie 3 kwietnia br., reguluje przede wszystkim kwestie związane z bezpieczeństwem systemów informacyjnych. Jej adresatami są tzw. podmioty kluczowe i ważne, działające w sektorach takich jak energetyka, transport, ochrona zdrowia, infrastruktura cyfrowa czy sektor publiczny. Choć ustawa o KSC i RODO stanowią odrębne reżimy prawne, służące odmiennym celom, ich zakresy w praktyce częściowo się pokrywają – incydent zagrażający bezpieczeństwu systemu informacyjnego często wiąże się z naruszeniem ochrony przetwarzanych w tym systemie danych osobowych.

Przykładem krzyżowania się tych systemów jest art. 59a znowelizowanej ustawy o KSC, zgodnie z którym, w przypadku stwierdzenia podczas sprawowania nadzoru podejrzenia naruszenia ochrony danych osobowych organ właściwy ds. cyberbezpieczeństwa w terminie 7 dni informuje o tym Prezesa UODO (lub ewentualnie inny właściwy organ nadzorczy – np. odpowiedni organ prokuratury).

Nadzór na gruncie ustawy o KSC

Rozdział 11 ustawy o KSC reguluje nadzór nad podmiotami kluczowymi i ważnymi, sprawowany przez organy właściwe ds. cyberbezpieczeństwa, którego celem jest weryfikacja, czy podmioty te prawidłowo wykonują obowiązki wynikające z ustawy. Przewiduje ona szeroki wachlarz narzędzi nadzorczych: organ może prowadzić kontrole w

siedzibie podmiotu lub zdalnie, nakazać przeprowadzenie audytu bezpieczeństwa, zlecić odpowiedniemu CSIRT-owi ocenę bezpieczeństwa systemu informacyjnego, żądać przekazania dokumentów i informacji, a nawet okresowo wyznaczyć urzędnika monitorującego (art. 53 ust. 2 i 5 ustawy o KSC). Osoba prowadząca czynności kontrolne ma przy tym prawo wglądu do dokumentów, przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli, żądania wyjaśnień oraz przeprowadzania oględzin urządzeń, nośników i systemów informacyjnych (art. 55 ustawy o KSC).

Dlaczego to istotne? Zakres tych uprawnień sprawia, że organy ds. cyberbezpieczeństwa, badając np. konfigurację zabezpieczeń baz danych, logi systemu czy rejestr incydentów lub analizując składane wyjaśnienia, mogą natrafić na okoliczności wskazujące na naruszenie ochrony danych osobowych, takie jak np. przypadkowa utrata lub nieuprawniony dostęp do danych osobowych. Oznacza to, że źródłem informacji o naruszeniach może być potencjalnie kilkanaście różnych organów, takich jak np. KNF, Prezes UKE czy właściwi ministrowie wskazani w ustawie – każdy w ramach nadzorowanego przez siebie sektora (art. 41 i 41a ustawy o KSC).

Latest

RODO ma nadal pierwszoplanową rolę – mówi prof. Arwid Mednis

2026-05-31

Ochrona wizerunku uczniów w placówkach oświatowych – dobre praktyki w cyfrowej

rzeczywistości

2026-05-31

Podsumowanie miesiąca – maj 2026 r.

2026-05-30

Naruszenia ochrony danych osobowych w świetle ustawy o KSC

10 lat od uchwalenia RODO – świadomość Polek i Polaków wzrasta. Podobnie jak liczba skarg

2026-05-29

Informowanie o podejrzeniu naruszenia ochrony danych osobowych

Warto zwrócić uwagę, że art. 59a ustawy o KSC kreuje obowiązek, a nie uprawnienie. Sformułowanie „organ właściwy do spraw cyberbezpieczeństwa informuje” nie pozostawia pola do uznaniowości. Jeżeli taki organ stwierdzi podejrzenie naruszenia ochrony danych osobowych, co do zasady powinien przekazać informację Prezesowi UODO.

Próg aktualizacji obowiązku jest zaś stosunkowo niski. Przepis posługuje się określeniem „stwierdzenie podejrzenia naruszenia", a nie „stwierdzenie naruszenia", znane z art. 33 ust. 1 RODO. Organ ds. cyberbezpieczeństwa nie musi zatem mieć pewności, że doszło do naruszenia w rozumieniu art. 4 pkt 12 RODO ani dokonywać jego kwalifikacji prawnej. Wystarczy, że okoliczności stwierdzone w toku czynności nadzorczych wskażą na samo podejrzenie jego wystąpienia.

Co ciekawe, mechanizm ten będzie funkcjonować niezależnie od obowiązku zgłoszenia naruszenia przez samego administratora w trybie art. 33 RODO. Terminy będą biec odrębnie i rozpoczynać się w innym momencie: w przypadku administratora – w ciągu 72 godzin od stwierdzenia naruszenia; w przypadku organu ds. cyberbezpieczeństwa – w ciągu 7 dni od stwierdzenia jego podejrzenia. Prezes UODO może więc otrzymywać informacje o tych samych zdarzeniach z co najmniej dwóch niezależnych źródeł, w różnym czasie i o różnym stopniu szczegółowości.

Praktyczne znaczenie dla ochrony danych osobowych

Art. 59a ustawy o KSC stworzy więc nowy, nieistniejący dotychczas kanał pozyskiwania przez Prezesa UODO (i inne właściwe organy) informacji o potencjalnych naruszeniach ochrony danych osobowych. Do tej pory głównym źródłem wiedzy na ten temat były zgłoszenia dokonywane przez samych administratorów na podstawie art. 33 RODO.

Nadchodzące wejście w życie nowelizacji wdrażającej NIS 2 spowoduje, że obowiązek notyfikacyjny – choć o innym charakterze – będzie spoczywał także na organach prowadzących nadzór w zakresie cyberbezpieczeństwa.

Z perspektywy podmiotów, które będą podlegać jednocześnie ustawie o KSC, jako podmioty kluczowe lub ważne, oraz RODO, jako administratorzy danych, oznacza to, że wzrośnie prawdopodobieństwo wykrycia w ich organizacjach ewentualnych zaniedbań, w tym np. niezgłoszonych naruszeń ochrony danych osobowych. Nadzór nad cyberbezpieczeństwem, prowadzony na podstawie ustawy o KSC, będzie mógł więc ujawnić nie tylko uchybienia w zakresie zarządzania bezpieczeństwem systemów informacyjnych, ale także okoliczności istotne w świetle potencjalnego naruszenia przepisów RODO.

Praktyczne stosowanie art. 59a ustawy o KSC będzie wymagało wypracowania standardów współpracy pomiędzy organami właściwymi ds. cyberbezpieczeństwa a organami nadzorczymi na gruncie RODO. Zagospodarowanie informacji napływających z wielu różnych organów sektorowych będzie stanowić wyzwanie operacyjne, ale jednocześnie szansę na pełniejszy obraz stanu ochrony danych osobowych w podmiotach objętych ustawą o KSC.