Jedno zdarzenie, dwa reżimy prawne, czyli naruszenia i incydenty na styku RODO i uKSC

Posted on 2026-05-26

To samo zdarzenie można zakwalifikować jako naruszenie ochrony danych osobowych w rozumieniu RODO, jako incydent w rozumieniu ustawy o Krajowym Systemie Cyberbezpieczeństwa (uKSC), a także… jako jedno i drugie jednocześnie. Każdy scenariusz uruchamia odrębny zestaw obowiązków, w tym notyfikacyjnych. Dla wielu administratorów oznacza to konieczność równoległego stosowania dwóch reżimów prawnych w reakcji na tę samą sytuację. Jak prawidłowo kwalifikować takie zdarzenia i o czym warto przy tym pamiętać?

Jedno zdarzenie, dwa reżimy prawne, czyli naruszenia i incydenty na styku RODO i uKSC

Developers, robot work at laptop with magnifier. Industrial cybersecurity, industrial robotics malware, safeguarding of industrial robotics concept. Pinkish coral bluevector isolated illustration

Choć pojęcia „naruszenia ochrony danych osobowych” (RODO) oraz „incydentu” (uKSC) są do siebie zbliżone, a potocznie mogą występować jako synonimy, ich definicje legalne zawierają istotne różnice. Zgodnie z art. 4 pkt 12 RODO naruszeniem ochrony danych osobowych jest „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”. Przedmiotem ochrony są więc dane osobowe, a podstawowym celem regulacji – ochrona osób fizycznych przed zagrożeniami związanymi z ich przetwarzaniem.

Z kolei art. 2 pkt 5 uKSC definiuje incydent jako „zdarzenie, które ma lub może mieć niekorzystny wpływ na bezpieczeństwo systemów informacyjnych”. W tym przypadku ustawodawca koncentruje się na ochronie infrastruktury, w której dane (niekoniecznie osobowe) są przetwarzane. Regulacja służy w konsekwencji zapewnieniu ciągłości świadczenia usług za pomocą systemów informacyjnych przez podmioty kluczowe i ważne. Chroni przy tym zarówno odbiorców tych usług, jak i interesy samych podmiotów.

Dwie perspektywy

Warto pamiętać, że katalog incydentów na gruncie uKSC jest zniuansowany. W tym kontekście szczególne znaczenie ma kategoria incydentu poważnego, z którego wystąpieniem ustawa wiąże obowiązki notyfikacyjne wobec właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT). Zgodnie z art. 2 pkt 7 uKSC jest to „incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi przez podmiot kluczowy lub podmiot ważny, straty finansowe dla tego podmiotu lub wpływa na inne osoby fizyczne, osoby prawne, jednostki organizacyjne nieposiadające osobowości prawnej przez wywołanie poważnej szkody materialnej lub niematerialnej”.

Pomimo wyraźnych różnic ścisłe rozgraniczenie naruszeń ochrony danych osobowych i incydentów w rozumieniu uKSC nie zawsze jest możliwe. Choć te pojęcia osadzone są w odrębnych reżimach prawnych, w praktyce często się krzyżują. Jak ta zależność wygląda w konkretnych sytuacjach, najlepiej pokazują poniższe przykłady.

Trzy scenariusze

Przyjrzyjmy się trzem scenariuszom, które mogą wystąpić w organizacji objętej zarówno RODO, jak i uKSC. Wystąpienie każdego z nich uruchamia inny zestaw obowiązków.

1. Naruszenie niebędące incydentem

Pierwszą kategorię tworzą zdarzenia, które stanowią naruszenie ochrony danych osobowych, ale pozostają poza zakresem przedmiotowym uKSC. Dotyczą one sytuacji, w których dochodzi do naruszenia poufności, integralności lub dostępności przetwarzanych danych osobowych, które nie ma jednak bezpośredniego wpływu na funkcjonowanie systemu informacyjnego.

Klasycznym przykładem jest pomyłkowe wysłanie e-maila z danymi osobowymi do niewłaściwego odbiorcy w wyniku błędu ludzkiego, podczas gdy system pocztowy działa prawidłowo, a jego bezpieczeństwo nie zostało zakłócone. Podobnie wygląda sytuacja zgubienia lub przypadkowego zniszczenia papierowej dokumentacji zawierającej dane osobowe. Choć dochodzi tu do naruszenia poufności w rozumieniu RODO, dokumenty papierowe nie wchodzą w zakres pojęcia „systemu informacyjnego”, którym posługuje się uKSC.

2. Incydent niebędący naruszeniem

Drugą kategorię stanowią zdarzenia, które wpływają na bezpieczeństwo systemu informacyjnego, lecz nie dotyczą danych osobowych. W praktyce ta kategoria bywa węższa, niż mogłoby się wydawać – znaczna część systemów informacyjnych przetwarza dane osobowe niejako przy okazji, nawet jeśli ich główne przeznaczenie jest zupełnie inne. Można jednak wskazać sytuacje, w których system takich danych nie przetwarza lub – mimo że to robi – nie wywiera na nie żadnego wpływu.

Przykładem może być awaria systemu sterowania procesem przemysłowym (np. SCADA w sektorze energetycznym czy wodociągowym), obejmująca wyłącznie dane techniczne i procesowe. Zakłócenie pracy takiego systemu może naruszyć ciągłość świadczenia usługi i zostać zakwalifikowane jako incydent, a w określonych okolicznościach – jako incydent poważny.

3. Scenariusz hybrydowy

Osobną kategorię tworzą zdarzenia, które wpływają zarówno na bezpieczeństwo systemu informacyjnego, jak i na bezpieczeństwo danych osobowych.

Wyrazistym przykładem takiej sytuacji może być atak ransomware na bazę danych pacjentów w podmiocie kluczowym z sektora ochrony zdrowia. Zaszyfrowanie danych narusza ich dostępność, modyfikacja – integralność, a w przypadku eksfiltracji – również poufność. Taki scenariusz stwarza podstawy do stwierdzenia naruszenia ochrony danych

osobowych. Jednocześnie zdarzenie wpływa na ciągłość świadczenia usług medycznych, co kwalifikuje je jako incydent w rozumieniu uKSC.

To właśnie ta grupa może wymagać od organizacji zachowania największej czujności. Każde tego rodzaju zdarzenie powinno zostać równolegle przeanalizowane z perspektywy obu reżimów, a pozytywna kwalifikacja w ramach jednego z nich nie zwalnia z przeprowadzenia oceny pod kątem drugiego.

Równoległe obowiązki notyfikacyjne

Prawidłowe zakwalifikowanie zdarzenia to jednak dopiero początek. W przypadku scenariusza hybrydowego organizacja staje przed koniecznością równoległej realizacji obowiązków wynikających z obu aktów prawnych. Choć dotyczą one tego samego zdarzenia, ich kształt jest na tyle odmienny, że w praktyce trudno mówić o jednym, zintegrowanym procesie. Przyjrzyjmy się obowiązkom notyfikacyjnym.

W tym przypadku inny jest przede wszystkim adresat zgłoszenia. RODO przewiduje obowiązek zgłoszenia naruszenia organowi nadzorczemu (art. 33 ust. 1), a gdy może ono powodować wysokie ryzyko dla praw lub wolności osób fizycznych – także zawiadomienia tych osób (art. 34 ust. 1). uKSC wymaga natomiast zgłoszenia incydentu poważnego do właściwego CSIRT sektorowego (art. 11 ust. 1 pkt 4 i 4a uKSC), zaś w określonych sytuacjach – poinformowania użytkowników usługi (art. 11 ust. 2a i 2b uKSC).

Również terminy biegną odrębnie. Administrator powinien zgłosić naruszenie ochrony danych osobowych bez zbędnej zwłoki, nie później niż w ciągu 72 godzin od jego

stwierdzenia. Natomiast uKSC przewiduje tryb wieloetapowy (częściowo zresztą obecny też w RODO, za sprawą art. 33 ust. 4). Wczesne ostrzeżenie należy przekazać w ciągu 24 godzin od wykrycia incydentu poważnego, właściwe zgłoszenie w ciągu 72 godzin, a sprawozdanie końcowe – w terminie miesiąca od dokonania zgłoszenia. Nawet 72-godzinny termin, wspólny obu reżimom, biegnie niezależnie i może się rozpocząć w innym momencie – w jednym przypadku liczy się go od stwierdzenia naruszenia, w drugim od wykrycia incydentu.

Odmiennie określono też próg aktualizujący obowiązek. Na gruncie RODO jest on ściśle związany z ryzykiem naruszenia praw lub wolności osób fizycznych. uKSC posługuje się natomiast kategorią incydentu poważnego, której progi określa (co do zasady) Rada Ministrów w drodze rozporządzenia, według rodzajów zdarzeń charakterystycznych dla poszczególnych sektorów i podsektorów (art. 11 ust. 4 uKSC).

Wreszcie różny jest także cel zgłoszenia, a co za tym idzie – jego treść. Zgłoszenie naruszenia ochrony danych osobowych ma przede wszystkim umożliwić ocenę ryzyka w celu zapewnienia ochrony objętych nim osób. Koncentruje się zatem na kategoriach i liczbie tych osób, charakterze naruszonych danych, opisie możliwych konsekwencji oraz środkach zaradczych (art. 33 ust. 3 RODO). Zgłoszenie incydentu poważnego ma natomiast pozwolić na ocenę wpływu zdarzenia na świadczenie usługi – wymaga więc m.in. opisu tego wpływu, liczby dotkniętych użytkowników, zasięgu geograficznego oraz informacji o przyczynach i przebiegu zdarzenia (art. 12 ust. 3 uKSC).

W rezultacie podmiot dotknięty scenariuszem hybrydowym musi prowadzić w istocie dwa równoległe procesy notyfikacyjne – z dwoma różnymi adresatami, dwoma odrębnie biegnącymi terminami i dwoma zestawami wymaganych informacji. To istotne wyzwanie organizacyjne, zwłaszcza w pierwszych godzinach po wykryciu zdarzenia, charakteryzujących się niepewnością i presją czasu.

Potrzeba harmonizacji

Rosnąca liczba podmiotów objętych jednocześnie RODO i uKSC sprawia, że ustawodawca dostrzega potrzebę wprowadzenia mechanizmów łączących oba reżimy prawne. Niektóre z nich już funkcjonują, inne dopiero zaczynają budować swoją rolę w praktyce.

Jednym z przykładów jest art. 59a uKSC, o którym niedawno pisaliśmy w Biuletynie UODO. Zgodnie z tym przepisem organ właściwy ds. cyberbezpieczeństwa, który w toku sprawowanego nadzoru stwierdzi podejrzenie naruszenia ochrony danych osobowych, jest zobowiązany w terminie 7 dni przekazać tę informację Prezesowi UODO. Mechanizm ten zapewnia przepływ informacji między organami nadzoru, niezależny od zgłoszeń dokonywanych przez samych administratorów.

Innym przykładem jest system teleinformatyczny prowadzony przez ministra właściwego do spraw informatyzacji, funkcjonujący pod nazwą S46 (art. 46 ust. 1 uKSC). Wspiera on współpracę podmiotów krajowego systemu cyberbezpieczeństwa, w tym zgłaszanie i obsługę incydentów, ale również – co istotne z perspektywy niniejszych rozważań – zgłaszanie naruszeń ochrony danych osobowych w trybie art. 33 RODO i art. 44 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (art. 46 ust. 1 pkt 7 uKSC). Co więcej, Prezes UODO jest jednym z organów korzystających z S46 w celu realizacji swoich ustawowych zadań (art. 46 ust. 2 uKSC), co czyni ten system realnym punktem instytucjonalnego styku obszaru cyberbezpieczeństwa i ochrony danych osobowych. W dłuższej perspektywie może on się stać wspólnym kanałem dla obu rodzajów zgłoszeń, usprawniającym funkcjonowanie zarówno organów nadzorczych, jak i samych organizacji.

Mechanizmy te stanowią fundament, na którym może być budowana coraz bardziej spójna praktyka. Wiele istotnych pytań pozostaje jednak otwartych. Czy organizacje powinny

projektować jeden, zintegrowany proces reagowania na zdarzenia z zakresu bezpieczeństwa informacyjnego, czy też co najmniej dwa odrębne? Jak rozkładać akcenty pomiędzy perspektywą RODO a perspektywą uKSC, szczególnie w pierwszych godzinach po wykryciu zdarzenia? Jak budować spójną dokumentację między równoległymi zgłoszeniami dotyczącymi tego samego zdarzenia? Odpowiedzi na te i wiele innych pytań będą się stopniowo wyłaniać w praktyce stosowania omawianych tu przepisów.

Wyzwanie na przyszłość

Choć RODO i uKSC stanowią odrębne reżimy prawne, w praktyce coraz częściej będą stosowane równolegle wobec tego samego zdarzenia. Krajobraz regulacyjny w obszarze bezpieczeństwa informacji jest zresztą znacznie bogatszy. Obejmuje również akty szczególne, takie jak rozporządzenie DORA dla sektora finansowego czy Prawo komunikacji elektronicznej. Każdy z nich może wprowadzać (i wprowadza) własne zasady realizacji obowiązków notyfikacyjnych i krzyżować się z RODO lub uKSC w sposób wymagający odrębnej analizy. Tym istotniejsza staje się prawidłowa kwalifikacja zaistniałego zdarzenia – jako punkt wyjścia do wykonania ciążących na organizacji obowiązków oraz warunek prawidłowej reakcji.

Przenikanie się wszystkich tych regulacji stwarza konieczność równoległego patrzenia na to samo zdarzenie z różnych perspektyw – ochrony praw i wolności osób fizycznych, bezpieczeństwa systemów informacyjnych, ciągłości świadczonych usług i innych chronionych dóbr. Łączenie ich w codziennej pracy jest wyzwaniem, które będzie wymagać stopniowego wypracowywania spójnych standardów dzięki współpracy organów

Jedno zdarzenie, dwa reżimy prawne, czyli naruszenia i incydenty na styku RODO i uKSC

nadzorczych i samych organizacji.