6.5.2025

Esencja z webinaru

Co mówią kary UODO o bezpieczeństwie IT? Kluczowe wnioski i lekcje.

Dziękuję za udział w webinarze

Jeśli uważasz, że przekazałem wiedzę w sposób rzetelny
to dodaj proszę swoją opinię na wizytówce ODO 24 w Google.

Z góry dziękuję 😊

Jeśli potrzebujesz dodatkowego wsparcia merytorycznego – zachęcam do skorzystania z bezpłatnych porad prawnych i IT.

Tomasz Ochocki
Wiceprezes Zarządu, Koordynator Zespołu Merytorycznego

Linki do źródeł wiedzy, inspiracji i nie tylko

Linki
Nagranie webinaru • Co mówią kary UODO o bezpieczeństwie IT? Kluczowe wnioski i lekcje.
Polecamy: • Zestawienie kar finansowych RODO. • Digital Identity Guidelines. • Top 10 Web Application Security Risks. • Practice guide for the security of personal data : 2024 edition. • The National Cyber Security Centre.
W czym możemy pomóc? • Usługi RODO – w Twojej branży. • Szkolenie z cyberbezpieczeństwa dla Twoich pracowników. • Jak bezpiecznie korzystać z AI w pracy – szkolenie dla pracowników.
Bezpłatne konsultacje • Porozmawiaj z naszymi doradcami:  Marcin Kuźniak umów spotkanie  Cezary Lutyński umów spotkanie

Pytania i odpowiedzi

Szanowni Państwo,
dziękuję za udział w webinarium i przesyłam odpowiedzi na zadane za pomocą czatu pytania. Jednocześnie uczulam, że odpowiedzi tych nie należy traktować jako „prawdy objawionej", gdyż – z uwagi na formę zadawania pytań – są to raczej wskazówki, sformułowane w oparciu o skromne informacje na temat stanu faktycznego.

Czy planują Państwo aktualizację kalkulatora wagi naruszeń, tak aby uwzględniał informacje o poziomie ryzyka wskazane w Poradniku UODO?

Już dokonaliśmy stosownych zmian. Wprowadzone modyfikacje obejmują:

- Obniżenie progu ryzyka, od którego wymagane jest zgłoszenie naruszenia do UODO – z 2 punktów do 1,5.
- Dodanie przykładu naruszenia polegającego na ujawnieniu serii i numeru dowodu osobistego – jako przypadku dotyczącego danych osobowych zwykłych, który ze względu na swoją specyfikę wiąże się z podwyższonym poziomem ryzyka.
- Uzupełnienie opisu kryterium „Szeroki zakres danych", aby precyzyjniej odzwierciedlało wpływ skali danych na ocenę ryzyka.
- Rozszerzenie opisu kryterium „Specyfika osób, których dane dotyczą", z uwzględnieniem szczególnie wrażliwych grup.
- Doprecyzowanie kryterium „Zaufany odbiorca", w celu lepszego rozróżnienia sytuacji, w których odbiorca faktycznie minimalizuje ryzyko dla osób, których dane dotyczą.

Jak długo należy przechowywać logi systemowe?

Francuski organ ochrony danych (CNIL) zaleca przechowywanie logów systemowych przez okres od 6 miesięcy do 1 roku. Rekomendacja ta stanowi część szerszych wytycznych dotyczących narzędzi do rejestrowania danych, które obejmują również zalecenia w zakresie wdrażania mechanizmów analizy tych danych oraz środków zapobiegających ich niewłaściwemu wykorzystaniu (https://www.cnil.fr/en/practice-guide-security-personal-data-2024-edition).

Czy wszystkie aspekty bezpieczeństwa wdrożone w organizacji – np. tworzenie kopii zapasowych – powinny być udokumentowane na wypadek kontroli UODO?

Tak, wszystkie środki bezpieczeństwa wdrożone w organizacji – w tym np. tworzenie kopii zapasowych – powinny być odpowiednio udokumentowane.

Zgodnie z zasadą rozliczalności wynikającą z RODO (art. 5 ust. 2), administrator danych musi być w stanie wykazać zgodność z przepisami, w tym także z art. 32 RODO dotyczącym bezpieczeństwa przetwarzania danych. Dokumentacja stosowanych środków technicznych i organizacyjnych, takich jak backupy, szyfrowanie, kontrola dostępu czy monitorowanie systemów, jest kluczowa podczas kontroli organu nadzorczego.

Brak dokumentacji może zostać uznany za brak wdrożenia odpowiednich środków, nawet jeśli faktycznie funkcjonują one w praktyce.

Jakie konsekwencje grożą za brak przeprowadzenia audytu zgodnie z wymaganiami KRI?

Brak przeprowadzenia audytu zgodnie z wymaganiami KRI (Krajowych Ram Interoperacyjności) stanowi naruszenie § 20 ust. 2 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie KRI (Dz.U. z 2016 r. poz. 1130), który stanowi: „Audyt bezpieczeństwa informacji przeprowadza się nie rzadziej niż raz na dwa lata."

KRI wydano na podstawie art. 18 ust. 1 pkt 1 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz.U. z 2023 r. poz. 57). Podmioty zobowiązane do stosowania KRI, a więc m.in. jednostki sektora finansów publicznych, uczelnie publiczne, szpitale, JST, mają prawny obowiązek przeprowadzania audytu zgodnie z § 20. Jego brak oznacza naruszenie przepisów prawa powszechnie obowiązującego.

Sam KRI nie przewiduje kar finansowych, jednak:

1. UODO może nałożyć administracyjną karę pieniężną za brak odpowiednich środków bezpieczeństwa (art. 32 RODO), jeśli brak audytu skutkował brakiem wykrycia ryzyk lub niewdrożeniem odpowiednich środków.
2. Audyt KRI jest często dokumentem referencyjnym przy ocenie zgodności z RODO, ISO 27001 czy NIS2. Jego brak utrudnia wykazanie zgodności.

W sektorze publicznym konsekwencje mogą objąć również kierownika jednostki (jako podmiotu odpowiedzialnego za zgodność z przepisami).

Jak długo należy przechowywać dowody realizacji procedur na wypadek kontroli UODO? Czy obowiązują w tym zakresie minimalne lub maksymalne okresy przechowywania?

Uważam, że odpowiedź w tym przypadku powinna być analogiczna do tej, jakiej udzieliliśmy w kontekście przechowywania dokumentacji dotyczącej naruszeń ochrony danych.

RODO nie określa wprost, przez jaki okres należy przechowywać dokumentację naruszeń. Zgodnie jednak z Wytycznymi Europejskiej Rady Ochrony Danych (EROD), jeżeli dokumentacja ta zawiera dane osobowe, administrator jest zobowiązany do ustalenia odpowiedniego okresu przechowywania na podstawie ogólnych zasad przetwarzania danych – w szczególności celowości, minimalizacji i ograniczenia przechowywania – oraz przy uwzględnieniu podstawy prawnej przetwarzania.

Zgodnie z art. 33 ust. 5 RODO administrator musi dokumentować wszelkie naruszenia ochrony danych osobowych i być w stanie, na żądanie organu nadzorczego, przedstawić dowody na przestrzeganie tego przepisu. Obowiązek ten wpisuje się również w szerszą zasadę rozliczalności (art. 5 ust. 2 RODO).

W kontekście ustalania okresu przechowywania warto również odnieść się do przepisów krajowych. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. odsyła w zakresie postępowania administracyjnego do Kodeksu postępowania administracyjnego. Ten zaś (art. 189g KPA) przewiduje, że administracyjna kara pieniężna nie może zostać nałożona po upływie pięciu lat od dnia naruszenia prawa lub wystąpienia jego skutków. Może to stanowić racjonalny punkt odniesienia przy ustalaniu okresów retencji dokumentacji związanej z naruszeniami, które zawierają dane osobowe.

W przypadku natomiast, gdy dokumentacja nie zawiera danych osobowych, UODO – zgodnie z najnowszymi zaleceniami zawartymi w swoim poradniku – postuluje jej przechowywanie możliwie jak najdłużej, ze względu na jej znaczenie dowodowe i analityczne.

W jakich organizacjach wymagane jest stosowanie przepisów dyrektywy NIS2?

Kwestia, w jakich konkretnie organizacjach stosowanie przepisów dyrektywy NIS2 będzie wymagane w Polsce, zostanie ostatecznie rozstrzygnięta w ustawie o krajowym systemie cyberbezpieczeństwa (KSC), której projekt jest obecnie w trakcie prac legislacyjnych. Poniższe informacje opierają się wyłącznie na założeniach wynikających bezpośrednio z dyrektywy NIS2 (UE) 2022/2555 i mogą ulec doprecyzowaniu na poziomie krajowym.

Zgodnie z dyrektywą NIS2, obowiązki w zakresie cyberbezpieczeństwa będą miały zastosowanie do:

1. Podmiotów kluczowych (essential entities), czyli m.in.:
   - dostawców usług energetycznych (elektroenergetyka, gazownictwo, ciepłownictwo),
   - podmiotów z sektora transportu (kolej, lotnictwo, żegluga, drogowy),
   - dostawców usług zdrowotnych (w tym szpitale, laboratoria, dostawcy e-zdrowia),
   - dostawców usług wodnych (zaopatrzenie w wodę i oczyszczanie ścieków),
   - dostawców usług cyfrowych (np. DNS, rejestry domen, chmura),
   - administracji publicznej (wybrane podmioty administracji centralnej i samorządowej).
2. Podmiotów ważnych (important entities), czyli m.in.:
   - dostawców usług pocztowych i kurierskich,
   - producentów urządzeń elektronicznych, komputerowych, optycznych, medycznych,
   - podmiotów z sektora żywności i chemikaliów,
   - usług doradczych i badawczych istotnych dla infrastruktury krytycznej,
   - dostawców niektórych usług ICT na rzecz podmiotów kluczowych.

Zasadniczo dyrektywa stosuje się do organizacji zatrudniających powyżej 50 pracowników lub osiągających roczny obrót/przychód powyżej 10 mln euro. Wyjątkiem są organizacje działające w sektorach szczególnie wrażliwych – w ich przypadku obowiązki mogą mieć zastosowanie niezależnie od wielkości.

Czy administrator danych osobowych (ADO) powinien przeprowadzić analizę ryzyka w podmiocie przetwarzającym, czy też to podmiot przetwarzający powinien przedstawić administratorowi gotową analizę ryzyka dotyczącą przetwarzania danych po swojej stronie? Na jakim etapie powinna zostać przeprowadzona analiza ryzyka — czy powinno to nastąpić już na etapie zawierania umowy powierzenia przetwarzania danych lub ich udostępnienia, czy raczej wcześniej, np. podczas oceny podmiotu przetwarzającego przed podpisaniem umowy?

Analiza ryzyka powinna być przeprowadzona zarówno przez administratora danych, jak i podmiot przetwarzający – każdy w zakresie swojej odpowiedzialności. Administrator nie wykonuje analizy za procesora, ale powinien ocenić ryzyka związane z powierzeniem danych i zweryfikować, czy procesor wdrożył odpowiednie środki bezpieczeństwa. Procesor z kolei powinien mieć własną analizę ryzyka i na żądanie administratora udostępnić jej wyniki. Analiza ryzyka (z perspektywy podmiotu przetwarzającego) powinna być gotowa przed podpisaniem umowy powierzenia, najlepiej już na etapie oceny procesora danych.

Czy w przypadku korzystania z narzędzi, w ramach których dochodzi do transferu danych osobowych poza Europejski Obszar Gospodarczy (EOG), należy przeprowadzić analizę ryzyka?

Tak, choć będzie to specyficzna analiza ryzyka. W przypadku korzystania z narzędzi, które wiążą się z transferem danych osobowych poza Europejski Obszar Gospodarczy, należy przeprowadzić ocenę skutków transferu danych (Transfer Impact Assessment, TIA). TIA pozwala ocenić, czy w państwie trzecim istnieją odpowiednie gwarancje ochrony danych osobowych, zgodne z wymogami RODO oraz orzecznictwem Trybunału Sprawiedliwości UE, w szczególności wyrokiem w sprawie Schrems II.

Zachęcamy do skorzystania do przygotowanego przez nas narzędzia do analizy TIA: https://odo24.pl/kalkulator-tia

Wartość ODO 24 tkwi w merytoryce zespołu ekspertów

Ochrona danych osobowych

Bezpieczeństwo informacji

Szkolenia RODO

Sprawdź nas

Tomasz Ochocki
Koordynator
zespołu merytorycznego

ZAPYTAJ O OFERTĘ