11.3.2025

Esencja z webinaru

Obowiązek dokumentowania naruszeń - jak przygotować organizację na kontrolę UODO

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
Koordynator Zespołu Merytorycznego

Linki do źródeł wiedzy, inspiracji i nie tylko

Linki
Nagranie webinaru • Obowiązek dokumentowania naruszeń - jak przygotować organizację na kontrolę UODO
Polecamy: • Poradnik UODO dotyczący naruszeń ochrony danych • Kalkulator wagi naruszeń • Wytyczne 9/2022 dotyczące zgłaszania naruszenia ochrony danych • Decyzja DKN.5131.53.2021 • Decyzja DKN.5131.44.2022 • Decyzja DKN.5131.1.2024
W czym możemy pomóc? • Outsourcing IOD • Kontrola UODO
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 rzeczywiście obsługa naruszeń i ich zgłaszanie przez IOD może mieć znamiona konfliktu interesu? To samo dot. działania jako pełnomocnik. To bardzo nieżyciowa interpretacja. W bardzo wielu organizacjach, szczególnie o mało rozbudowanej strukturze, IOD jest jedyną kompetentną osobą

Jak podnosi UODO w swoim najnowszym poradniku, inspektorzy ochrony danych to profesjonalni doradcy wspierający administratorów i podmioty przetwarzające w zapewnieniu zgodności z przepisami RODO i aby prawidłowo wykonywać swoje zadania, muszą być niezależni, a zakres ich odpowiedzialności powinien być wolny od konfliktu interesów. W ocenie UODO nie powinni oni dokumentować naruszeń ochrony danych osobowych w imieniu administratorów, w szczególności, jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określaniem działań zaradczych. Biorąc to pod uwagę można ostrożnie zakładać, że dokumentowanie pozbawione tych elementów, polegające jedynie na usystematyzowaniu i właściwym utrwaleniu wiedzy i okoliczności przekazanych przez administratora, nie rodziłoby konfliktu interesów, ale ze względu na obecne stanowisko UODO jest to interpretacja obarczona pewnym ryzykiem.

Czy w rejestrze naruszeń powinno się dokumentować także naruszenia przepisów o ochronie danych osobowych stwierdzone np. podczas audytu - brak klauzul informacyjnych, brak podstaw do udostępnienia danych osobowych? Czy osobny rejestr prowadzić na takie naruszenia?

Rejestr naruszeń gromadzi naruszenia ochrony danych w rozumieniu art. 4 pkt 12 RODO czyli naruszenia 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. Pojęcie to nie jest tożsame z naruszeniem przepisów RODO czyli np. niewywiązaniem się przez Administratora z obowiązków informacyjnych, czy przechowywaniem danych dłużej niż to konieczne. Innymi słowy w rejestrze gromadzimy naruszenia ochrony danych, a nie naruszenia przepisów RODO.

No tak, ale chyba były kary, za źle przeprowadzoną analizę ryzyka, zatem skuteczność, metodyka są ważne, chyba?

Właściwa ocena wagi naruszenia oczywiście ma bardzo duże znaczenie - Błędna ocena wagi naruszenia może doprowadzić do tego, że nie zostanie ono zgłoszone do PUODO i nie zostaną zawiadomione osoby, których dane dotyczą, pomimo że będzie to obligatoryjne. Takie braki oczywiście mogą być przedmiotem oceny i ewentualnie także kary ze strony Urzędu (jak chociażby w przypadku decyzji numer DKN.5131.53.2021, gdzie zakwestionowano niezgłoszenie naruszenia wynikające z jego niewłaściwej oceny).

Jeśli zaś chodzi o analizę ryzyka to ona oczywiście również bywa przedmiotem oceny Urzędu, który stoi na stanowisku, że bez analizy ryzyka właściwe nie ma ochrony danych osobowych. UODO w swoich decyzjach podkreśla, że brak analizy ryzyka sprawia, że działania administratora mające na celu ochronę danych osobowych, są mało skuteczne. Tylko kompleksowa analiza ryzyka daje świadomość zagrożeń i możliwość odpowiedniego przygotowania (tak chociażby decyzja numer DKN.5131.44.2022).

Kim jest ADO – czy jest to cały zarząd?

Administratorem danych osobowych przetwarzanych w spółce, np. z ograniczoną odpowiedzialnością jest sama spółka. Obowiązki administratora będzie realizować co do zasady zarząd spółki z o.o. jako podmiot ją reprezentujący, który to w swoich działaniach będzie korzystał z pomocy zatrudnionego personelu.

A co w sytuacji wycieku nr PESEL osoby, której dane są w KRS? Czy w tej sytuacji nie będzie ryzyka?

Fakt publicznej dostępności danych osobowych przed ich bezpodstawnym ujawnieniem rzeczywiście może obniżać ryzyko w ramach dokonywanej oceny naruszenia, ale automatycznie i każdorazowo sam w sobie nie świadczy o braku takiego ryzyka. Bezpodstawne ujawnienie numeru PESEL, nawet tego uprzednio dostępnego w rejestrze KRS może, w zależności od szczegółów sprawy, skutkować koniecznością zgłoszenia takiego naruszenia do UODO, a nawet zawiadomienia podmiotu danych.

Co należy zrobić w przypadku zagubienia dokumentu w obrębie organizacji, gdy mamy pewność (100%), że nie wydostał się on poza firmę, a jedynie został prawdopodobnie dołączony do innej dokumentacji?

Takie zdarzenie można zakwalifikować jako incydent bezpieczeństwa bowiem nie powstał skutek w postaci przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych zawartych na dokumencie (pod warunkiem, że na skutek wspomnianego podpięcia dokument nie trafił do osób wewnątrz organizacji nieuprawionych do przetwarzania danych osobowych zawartych w jego treści).

Czy upoważniony pracownik wysyłający maila z danymi osobowymi klientów na swojego prywatnego maila, to zaufany odbiorca?

Takie zdarzenie należy z pewnością traktować w kategoriach naruszenia wewnętrznych procedur czy naruszenia przepisów RODO, ale także rozważać w kontekście ewentualnego naruszenia ochrony danych osobowych, albowiem może ono prowadzić do udostępnienia danych osobowych nieuprawionemu odbiorcy w postaci dostawcy usługi poczty elektronicznej obsługującego prywatną pocztę wspomnianego pracownika. (Innymi słowy pracownik nadal jest podmiotem uprawnionym do dostępu do danych, ale przesłanie ich na prywatny adres może skutkować udzieleniem dostępu do tych danych nieuprawionemu odbiorcy tj. dostawcy usługi pocztowej).

Czy organy administracji publicznej, takie jak Policja, Zakład Ubezpieczeń Społecznych czy urzędy miejskie, można klasyfikować jako zaufanych odbiorców?

W poradniku najnowszym UODO, definiując zaufanego obiorcę, szczególny nacisk kładzie się na dwa następujące aspekty:

- pozostawanie z odbiorcą w stałych stosunkach (np. w bliskiej współpracy biznesowej lub wspólnej strukturze organizacyjnej);
- znajomość istotnych szczegółów dotyczących odbiorcy (np. procedury bezpieczeństwa i historia dotychczasowej, pozytywnej współpracy w podobnych sytuacjach).

Jeśli więc w realiach konkretnego naruszenia tych elementów zabraknie, nie ma podstaw by automatycznie takie organy uznawać za zaufanego odbiorcę. Poradnik wprost stanowi, że każdy przypadek wymaga indywidualnej analizy i żadnego podmiotu nie można z góry uznać za „zaufanego odbiorcę". Podobny wniosek płynie także z jednej z niedawnych decyzji PUODO (DKN.5131.1.2024) dotyczącej banku jako podmiotu zaufania publicznego będącego jednocześnie nieuprawnionym, przypadkowym odbiorcą danych osobowych. W decyzji tej kategorycznie stwierdzono, że: „aby uznać, że w określonej sytuacji mamy do czynienia z nieuprawnionym udostępnieniem danych osobowych na rzecz podmiotu zaufanego muszą wystąpić takie okoliczności, w których administrator danych będzie miał stałe relacje z odbiorcą i może znać jego procedury, historię i inne istotne szczegóły, dzięki którym odbiorca może być uznany za "zaufanego".

Ze zgromadzonego materiału dowodowego wynika, że z pakietem dokumentów zapoznali się pracownicy innego banku, nie wynika natomiast, aby administrator i podmiot trzeci posiadali zawarte porozumienia, bądź opracowane procedury na daną okoliczność, co byłoby kluczowe, aby faktycznie zminimalizować ryzyko wystąpienia konsekwencji związanych z naruszeniem ochrony danych osobowych i móc przyjąć, że nieuprawniony odbiorca jest odbiorcą zaufanym.", „Przyjęcie przeciwnego stanowiska, (…) prowadziłoby w konsekwencji do akceptacji pewnego rodzaju automatyzmu – bowiem w każdym przypadku, w którym nieuprawnionym odbiorcą byłby podmiot działający w ramach prawa, należałoby uznawać go za odbiorcę zaufanego. Takie podejście mogłoby jednak prowadzić do nieuzasadnionego odstępowania od realizacji obowiązku zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony jej danych osobowych w sytuacji wystąpienia wysokiego ryzyka naruszenia jej praw lub wolności. Z tego powodu, jak należy uznać, EROD w powołanych wyżej wytycznych nie przyjęła, że okoliczność działania nieuprawnionego odbiorcy w ramach prawa kwalifikuje go jako odbiorcę zaufanego, tylko wymaga pozostawania z takim odbiorcą w stałej relacji, dzięki czemu administrator zapewni sobie znajomość obowiązujących u tego odbiorcy procedur, historii i innych istotnych szczegółów go dotyczących."

Jeżeli obowiązki te mają być realizowane przez Administratora Danych Osobowych, to kto konkretnie powinien pełnić tę funkcję? Czy realistyczne jest założenie, że zarząd będzie wykonywał te zadania osobiście, czy raczej powinien delegować je wyznaczonym asystentom lub asystentkom?

Administratorem danych osobowych przetwarzanych w spółce, np. z ograniczoną odpowiedzialnością, jest sama spółka. Obowiązki administratora będzie realizować co do zasady zarząd spółki z o.o. jako podmiot ją reprezentujący, który to w swoich działaniach będzie korzystał z pomocy zatrudnionego personelu.

Czy przekazywanie rekomendacji oraz zaleceń dotyczących naruszeń należy klasyfikować jako działalność doradczą? Ponadto, kto powinien być odpowiedzialny za monitorowanie wdrażania tych zaleceń? Czy leży to w kompetencjach Administratora Danych Osobowych, czy też Inspektor Ochrony Danych może pełnić aktywną rolę w tym procesie?

Monitorowanie przestrzegania RODO (a co za tym idzie monitorowanie wykonywania obowiązków ADO zgodnie z wymogami RODO) należy do zadań IOD zgodnie z art. 39 RODO.

Jak długo się przechowuje te dowody naruszeń? Są jakieś terminy?

W przepisach RODO nie sprecyzowano okresu przechowywania dokumentacji naruszeń. Jak wynika z Wytycznych EROD, w przypadku, gdy taka dokumentacja zawiera dane osobowe, administrator musi określić właściwy okres przechowywania zgodnie z zasadami dotyczącymi przetwarzania danych osobowych oraz podstawą prawną przetwarzania. Musi on przechowywać dokumentację zgodnie z art. 33 ust. 5 RODO w zakresie, w jakim może zostać wezwany do przedstawienia organowi nadzorczemu dowodów na przestrzeganie przepisów tego artykułu lub, w ujęciu bardziej ogólnym, zasady rozliczalności. W tym zakresie ważną wskazówkę znajdziemy w krajowych przepisach o ochronie danych osobowych. Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r. odsyła do przepisów Kodeksu postępowania administracyjnego, który z kolei reguluje kwestię terminu przedawnienia możliwości nałożenia administracyjnej kary pieniężnej, a ta co do zasady nie może zostać nałożona, jeżeli upłynęło pięć lat od dnia naruszenia prawa albo wystąpienia skutków naruszenia prawa (tak art. 189g KPA). Jest to zatem pewien punkt odniesienia do określenia terminów retencji związanych z przechowywaniem danych osobowych w rejestrach RODO. Jeśli dokumentacja naruszeń nie zawiera danych osobowych UODO postuluje w swym najnowszym poradniku, by przechowywać ją jak najdłużej.

Kto prowadzi dalszą korespondencję z osobami których naruszenie dotyczyło i które w związku z tym zostały zawiadomione przez Administratora?

Jeśli zajdzie potrzeba dalszej korespondencji prowadzi ją Administrator, któremu w ramach wykonywania swojej funkcji i w granicach wyznaczonych przez RODO może oczywiście doradzać IOD.

W jaki sposób liczymy 72 godziny od stwierdzenia naruszenia, w sytuacji, kiedy ADO stwierdza naruszenie w piątek, po którym następują dni wolne (sobota, niedziela) lub świąteczne.

Naruszenie ochrony danych osobowych należy zgłosić niezwłocznie, nie później niż w ciągu 72 godzin od jego stwierdzenia i niezależnie od dni wolnych od pracy. Jak wynika z poradnika UODO, weekend nie tylko nie przedłuża ww. terminu, ale nie powinien być nawet traktowany jako okoliczność usprawiedliwiająca opóźnienie w dokonaniu zgłoszenia.

Co dokumentować jako naruszenie/incydent, który nie zgłaszamy do UODO?

W najnowszym poradniku UODO jako przykład naruszenia niewymagającego zgłoszenia z uwagi na znikome ryzyko podaje się zagubienie niezawodnie zabezpieczonego laptopa: „Laptop pracownika kliniki dentystycznej zawierający dane pacjentów został zgubiony. Urządzenie było zabezpieczone szyfrowaniem przy użyciu niezawodnej metody (przy ówczesnym stanie wiedzy technicznej), a klucz szyfrowania nie został utracony ani złamany. Ponadto klinika dysponowała kopią zapasową wszystkich informacji o pacjentach. W takim przypadku można było jednoznacznie stwierdzić brak ryzyka naruszenia praw lub wolności osób, których dane dotyczą."

Proszę o podanie przykładów naruszeń ochrony danych osobowych które wykazują niskie ryzyko i należy je tylko udokumentować w rejestrze.

W najnowszym poradniku UODO jako przykład naruszenia niewymagającego zgłoszenia z uwagi na znikome ryzyko podaje się zagubienie niezawodnie zabezpieczonego laptopa: „Laptop pracownika kliniki dentystycznej zawierający dane pacjentów został zgubiony. Urządzenie było zabezpieczone szyfrowaniem przy użyciu niezawodnej metody (przy ówczesnym stanie wiedzy technicznej), a klucz szyfrowania nie został utracony ani złamany. Ponadto klinika dysponowała kopią zapasową wszystkich informacji o pacjentach. W takim przypadku można było jednoznacznie stwierdzić brak ryzyka naruszenia praw lub wolności osób, których dane dotyczą."

W jaki sposób należy zharmonizować prowadzenie rejestru incydentów bezpieczeństwa wymaganego przez dyrektywę NIS2 oraz przepisy UKSC z rejestrem incydentów i naruszeń ochrony danych osobowych wynikającym z regulacji o ochronie danych osobowych? Czy rekomendowane jest utrzymywanie dwóch odrębnych rejestrów, czy też stworzenie jednego zintegrowanego systemu ewidencji? Pytanie to zadaję również w kontekście wcześniej omawianej kwestii alertów generowanych przez systemy wykrywania zdarzeń bezpieczeństwa oraz innych procesów z zakresu cyberbezpieczeństwa.

Zaleca się dokonywanie dwóch odrębnych analiz i prowadzenie dwóch odrębnych rejestrów. Oczywiście w jakimś zakresie mogą one czerpać z siebie nawzajem, ale konieczne jest też uwzględnienie specyfiki każdej z regulacji i przypisanych do niej wymagań.

Jakie ryzyko wiąże się z sytuacją, w której analiza logów systemowych wykazuje, że pracownik posiadający formalne upoważnienie do przetwarzania danych osobowych przeglądał znaczną liczbę kont klientów, przewyższającą liczbę klientów faktycznie przez niego obsługiwanych? Czy tego rodzaju zdarzenie należy klasyfikować jako naruszenie ochrony danych osobowych wymagające zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych?

Takie zdarzenie, w zależności od szczegółowych okoliczności (w tym rodzajów danych, ilości osób, których dotyczy) może zostać uznane za naruszenie ochrony danych skutkujące koniecznością jego zgłoszenia do UODO, a nawet zawiadomieniem osób, których dane dotyczą.

Czy w logach mogą być dane osobowe? Jak długo je przechowywać?

Logi mogą zawierać dane osobowe, np. numer IP, nick użytkownika, logi serwera pocztowego zawierające adres e-mail etc. W takim przypadku, jeśli stanowią one część dokumentacji dotyczącej naruszeń, przechowujemy je na zasadach opisanych w ramach odpowiedzi na pytanie:
Jak długo się przechowuje te dowody naruszeń? Są jakieś terminy?
Jest to z pewnością bezpieczniejszy sposób ich przechowywania, zwłaszcza jeśli zawierają one dane osobowe.
Czy w przypadku pracy zdalnej, stałej lub okazjonalnej można na podstawie logów ustalać miejsce przebywania pracownika, np. który wyjechał z kraju i pracuje np.
z jednego z krajów Azji lub Ameryki Południowej?
W zależności od konfiguracji jest to techniczne możliwe, by na podstawie logów ustalić miejsce logowania/pracy pracownika wykonującego pracę zdalnie, przy czym tego rodzaju informację wyczytać można także z używanego przez pracownika adresu IP.

Jaka jest odpowiedzialność IOD, gdy doradzi, aby nie zgłaszać do UODO? Może mieć jakieś konsekwencje za to?

Na gruncie samego RODO brak przepisów wskazujących na odpowiedzialność inspektora za działania związane z wykonywaniem jego obowiązków - IOD nie ponosi osobistej odpowiedzialności za naruszenia przepisów RODO. Natomiast możliwe jest pociągnięcie inspektora do odpowiedzialności jako pracownika (na zasadach dotyczących odpowiedzialności pracownika za wyrządzoną pracodawcy szkodę) lub, w razie innej formy współpracy, do odpowiedzialności cywilnej związanej z wyrządzoną szkodą.

Jak wygląda sytuacja, gdy nie jesteśmy jesteśmy ADO, tylkpo podmiotem przetwarzającym i doszło u nas do naruszenia?

Podmiot przetwarzający zobowiązany jest niezwłocznie zgłosić takie naruszenie Administratorowi i udzielić mu niezbędnego wsparcia przy wykonywaniu obowiązków, o których mowa w art. 33 i 34 RODO.

Co roku jest nowy rejestr, ale poprzednie przechowywane są przez 10 lat, czy to właściwe?

Czy logi musza być przechowywane w formie zaszyfrowanej?

Jest to z pewnością bezpieczniejszy sposób ich przechowywania, zwłaszcza jeśli zawierają one dane osobowe.

Czy w przypadku pracy zdalnej, stałej lub okazjonalnej można na podstawie logów ustalać miejsce przebywania pracownika, np. który wyjechał z kraju i pracuje np. z jednego z krajów Azji lub Ameryki Południowej?

W zależności od konfiguracji jest to techniczne możliwe, by na podstawie logów ustalić miejsce logowania/pracy pracownika wykonującego pracę zdalnie, przy czym tego rodzaju informację wyczytać można także z używanego przez pracownika adresu IP.

Jaka jest odpowiedzialność IOD, gdy doradzi, aby nie zgłaszać do UODO? Może mieć jakieś konsekwencje za to?

Na gruncie samego RODO brak przepisów wskazujących na odpowiedzialność inspektora za działania związane z wykonywaniem jego obowiązków - IOD nie ponosi osobistej odpowiedzialności za naruszenia przepisów RODO. Natomiast możliwe jest pociągnięcie inspektora do odpowiedzialności jako pracownika (na zasadach dotyczących odpowiedzialności pracownika za wyrządzoną pracodawcy szkodę) lub, w razie innej formy współpracy, do odpowiedzialności cywilnej związanej z wyrządzoną szkodą.

Jak wygląda sytuacja, gdy nie jesteśmy jesteśmy ADO, tylkpo podmiotem przetwarzającym i doszło u nas do naruszenia?

Podmiot przetwarzający zobowiązany jest niezwłocznie zgłosić takie naruszenie Administratorowi i udzielić mu niezbędnego wsparcia przy wykonywaniu obowiązków, o których mowa w art. 33 i 34 RODO.

Co roku jest nowy rejestr, ale poprzednie przechowywane są przez 10 lat, czy to właściwe?

Jeśli zachowana jest ciągłość i rejestry za poprzednie lata są przechowywane, to co do zasady nie widzę przeciwwskazań by taki rejestr prowadzić w ujęciu rocznym. Proszę natomiast pamiętać o dwóch istotnych kwestiach:

- Dokumentacja naruszeń jest narzędziem służącym także do analizy przyczyn i skutków incydentów oraz skuteczności działań organizacji. Z tych względów warto by poprzednie okresy również były dla Państwa na bieżąco dostępne i stanowiły całokształt z aktualną, tegoroczną częścią rejestru.
- Jeśli dokumentacja zawiera dane osobowe to przechowywanie ich w ramach tej dokumentacji przez okres aż 10 lat może być uznane za nadmiarowe. Z tych właśnie względów UODO postulując jak najdłuższe przechowywanie dokumentacji naruszeń, jednocześnie zaleca by w jej ramach nie przechowywać danych osobowych. W przypadku gdy dokumentacja jednak zawiera dane osobowe, administrator musi określić właściwy okres przechowywania dokumentacji zgodnie z zasadami dotyczącymi przetwarzania danych osobowych oraz podstawą prawną przetwarzania. Jak wynika z Wytycznych EROD musi on wówczas przechowywać dokumentację zgodnie z art. 33 ust. 5 RODO w zakresie, w jakim może zostać wezwany do przedstawienia organowi nadzorczemu dowodów na przestrzeganie przepisów tego artykułu lub, w ujęciu bardziej ogólnym, zasady rozliczalności. Właśnie ze względu na te zasady jako punkt odniesienia dla ustalenia czasu przechowywania dokumentacji zawierającej dane osobowe przyjąć można termin 5 – letni wynikający z art. 189 g KPA (szersze omówienie w tym zakresie w ramach odpowiedzi do pytania nr 13 powyżej.)

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