
LEX ARTIST

RODO - aktualności

[27.08.2024]

UWAGA!

Tezy przedstawione w artykułach, zamieszczone w niniejszym materiale i niebędące wytycznymi organu nadzorczego albo orzeczeniami sądów lub organów administracji publicznej, stanowią wyłącznie opinię ich autorów i nie są oficjalnym stanowiskiem Lex Artist Sp. z o.o.

01 NSA wskazuje, że decyzja Prezesa UODO nakładająca karę na Prezesa Sądu jest prawidłowa

02 Podsumowanie – na co organizacja musi zwrócić uwagę, wdrażając przepisy ustawy o sygnalistach

03 Jak stosować „ustawę Kamilka” w zgodzie ze standardami ochrony danych osobowych

04 Holandia: 290 mln euro kary dla Ubera

05 Administracyjna kara pieniężna 40 tys. zł po utracie danych osób w wyniku ataku hackerskiego

01 NSA wskazuje, że decyzja Prezesa UODO nakładająca karę na Prezesa Sądu jest prawidłowa

- W tym orzeczeniu NSA nie pozostawił żadnej wątpliwości, że w przypadku przetwarzania danych osobowych przez Kuratora Sądowego administratorem danych osobowych jest Prezes Sądu Rejonowego przy którym działa ten kurator, a nie Sąd.
- Tę różnicę podnosił w skardze kasacyjnej Prezes Sądu Rejonowego wskazując, że „rażące naruszenie 102 ust. 1. pkt. 1 ustawy o ochronie danych osobowych w związku z art 175db ustawa z dnia 27 lipca 2001 r. Prawo o ustroju sądów powszechnych poprzez nałożenie przez Prezesa Urzędu Ochrony Danych Osobowych kary pieniężnej na Prezesa Sądu Rejonowego […] będącego organem jednostki sektora finansów publicznych w sytuacji, gdy administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej są sądy, a nie ich organy.
- W orzeczeniu WSA w Warszawie wiele miejsce poświęcono temu zagadnieniu i wskazano m. in., że Prezes UODO nie nałożył przecież kary pieniężnej na konkretną osobę fizyczną pełniącą funkcję Prezesa Sądu. Kara została prawidłowo skierowana do organu danej jednostki organizacyjnej, bo tylko jej organ uprawniony jest do jej reprezentowania i działania za nią.
- NSA podzielił to stanowisko i podniósł, że w sprawie nie ma sporu, że PUODO nałożył karę administracyjną na Prezesa Sądu […], jako administratora danych osobowych. Karę nałożono z uwagi na naruszenie zasad przetwarzania danych osobowych przez kuratora sądowego. Zgodnie z art. 9b ustawy z dnia 27 lipca 2001 r. o kuratorach sądowych (Dz. U. 2020 r. poz. 167 ze zm.; dalej: “u.k.s.”) “Administratorem danych przetwarzanych w celu wykonania zadań lub obowiązków przez kuratora sądowego jest prezes sądu, w którym kurator sądowy pełni obowiązki służbowe.

Źródło: Judykatura.pl

02 Podsumowanie – na co organizacja musi zwrócić uwagę, wdrażając przepisy ustawy o sygnalistach

- Przed przystąpieniem do wdrożenia ustawy, organizacja musi ustalić jakimi kanałami będzie przyjmować zgłoszenia (elektronicznie, telefonicznie, czy dopuszczalne są anonimowe zgłoszenia i czym to będzie skutkowało w ocenie ryzyka formularza). Organizacja powinna podjąć decyzję, kto będzie przyjmował zgłoszenia i prowadził działania następcze. Mogą to robić wyłącznie osoby bezstronne. W tym kontekście pojawił się również temat outsourcingu – zakres dopuszczalnego outsourcingu wynika z art. 28 ust.1 ustawy o ochronie sygnalistów w powiązaniu w zakresie przetwarzania danych osobowych z RODO.
- Organizacja musi przeprowadzić ocenę ryzyka naruszenia praw lub wolności osób fizycznych (z art. 25 RODO i 32 RODO) już w fazie projektowania procesu przyjmowania zgłoszeń sygnalistów uwzględniając także wymagania dotyczące oceny skutków (art. 35 RODO).
- Organizacja powinna również zastanowić się, jak będzie spełniać obowiązki informacyjne - należy je wypełniać warstwowo .Jeśli chodzi o informowanie o procedurze kandydatów do pracy, kontrahentów – tu istnieje możliwość spełnienia wprost obowiązku informacyjnego, jak i przekierowania do właściwych dokumentów. Klauzule informacyjne muszą być dostosowane w szczególności w zakresie informowania o obowiązku lub też dobrowolności podania danych przez sygnalistę. Ustawa o ochronie sygnalistów nie wymaga podania danych do kontaktu przez sygnalistę. Należy to zsynchronizować z kwestią zakresu tych danych, w zależności od tego, czy organizacja dopuści anonimowe zgłoszenia czy też nie.
- Bardzo ważne jest uwzględnienie kwestii powierzenia przekazania danych oraz weryfikacji nadawanych upoważnień. Organizacja musi też ustalić jak zarządzać usuwaniem danych i dokonać aktualizacji rejestru czynności, w zależności od typu i zakresu pozyskiwanych danych. Niezbędne jest, by wskazała podstawę do przetwarzania danych. Musi również uwzględnić konieczność aktualizacji rejestru czynności o nowy proces przetwarzania danych (w tym kontekście warto wspomnieć o tym, że w procesie szeroko pojętej obsługi zgłoszeń sygnalistów pojawiają się różne kategorie osób, których dane są przetwarzane m.in. sygnalista, osoba, której dotyczy zgłoszenie, świadek, osoba powiązana z sygnalistą).

Źródło: BIULETYN UODO Nr 07_08 /07_08 /24, str. 66; www.uodo.gov.pl

03 Jak stosować „ustawę Kamilka” w zgodzie ze standardami ochrony danych osobowych

- Prezes UODO w związku z ostatnio napływającymi do niego sygnałami, pytaniami w zakresie przetwarzania danych osobowych dla przyjęcia i realizacji standardów ochrony małoletnich (dzieci), wskazuje – wraz ze Społecznym Zespołem Ekspertów przy Prezesie UODO – na co zwrócić uwagę przy przetwarzaniu ich danych osobowych.
- Po śmierci Kamilka z Częstochowy prawo zostało zmienione tak, by wprowadzić standardy ochrony małoletnich we wszystkich placówkach, gdzie przebywają dzieci. Nowe obowiązki dotyczą organów zarządzających jednostkami systemu oświaty (przedszkoli, szkół i schronisk młodzieżowych) oraz innych placówek oświatowych, opiekuńczych wychowawczych, resocjalizacyjnych, religijnych, artystycznych, medycznych, rekreacyjnych, sportowych lub związanymi z rozwijaniem zainteresowań, do których uczęszczają albo w której przebywają małoletni, a także organizatorzy tychże działalności oraz podmioty świadczące usługi hotelarskie, turystyczne czy prowadzące inne miejsca zakwaterowania zbiorowego.
- Placówki te miały do 15 sierpnia 2024 r. czas na wprowadzenie standardów pracy i postępowania z dziećmi. Chodzi m.in. o to, by lepiej rejestrować i analizować sygnały o problemach zgłaszanych przez dzieci. Nowe wymogi dotyczą też opiekunów. Osoba, z którą ma być nawiązany stosunek pracy lub która ma być dopuszczona do działalności, musi przedstawić informacje o swojej karalności.
- Prezes UODO zwraca uwagę, że zarówno dane o pracownikach i kandydatach do pracy, jak i informacje przekazywane przez dzieci trzeba przetwarzać z poszanowaniem prawa ochrony danych osobowych.
- W kontekście nowych przepisów należy zweryfikować i zaktualizować m.in.: Kategorie osób, których dane są przetwarzane oraz zakres zbieranych i przetwarzanych danych osobowych – ograniczyć je do danych niezbędnych dla realizacji obowiązków nałożonych przepisami prawa; Klauzule obowiązków informacyjnych – zweryfikować w szczególności: cele, podstawę prawną przetwarzania, informacje o odbiorcach lub kategoriach odbiorców danych, retencję danych, źródła pochodzenia danych; dbać o przejrzystość informacji i komunikacji.

Źródło: Aktualności - UODO

04 Holandia: 290 mln euro kary dla Ubera

- Karę w wysokości 290 mln euro ma zapłacić w Holandii amerykańskie przedsiębiorstwo Uber, twórca internetowej platformy kojarzącej kierowców samochodów i pasażerów – poinformował w poniedziałek (26.08.2024) holenderski urząd ds. ochrony danych osobowych.
- Według urzędu Uber dopuścił się ciężkiego naruszenia przepisów UE, ponieważ gromadził i przekazywał wrażliwe dane swoich kierowców w Europie do centrali firmy w USA, nie gwarantując wymaganej ochrony. Były to dane dotyczące lokalizacji, fotografie, dokumenty dotyczące wynagrodzenia, dowody osobiste, a „w niektórych przypadkach" nawet dane o popełnionych czynach karalnych albo stanie zdrowia.
- Przez dwa lata dane te były przekazywane do USA. Powodem wszczęcia dochodzenia przeciwko Uberowi były skargi ponad 170 kierowców Ubera we Francji.
- Amerykańska firma odrzuca te oskarżenia i zapowiedziała odwołanie się od decyzji. Oświadczyła ona, że decyzja holenderskiego urzędu jest „błędna", a „nadzwyczajna grzywna" całkowicie nieuzasadniona. Tłumaczy, że transgraniczne przekazywanie danych odbywało się „w czasie trzyletniego okresu dużej niepewności pomiędzy UE i USA" i zgodnie z obowiązującym rozporządzeniem o ochronie danych osobowych (RODO).
- Według holenderskiego organu ochrony danych Uber zakończył teraz naruszanie RODO. Szef urzędu Aleid Wolfsen podkreślił, że w Europie RODO wymaga od firm i rządów „ostrożnego obchodzenia się z danymi osobowymi". Niestety nie jest to oczywiste poza Europą. „Pamiętajmy, że niektóre rządy mogą uzyskać dostęp do danych na dużą skalę. Dlatego firmy są zobowiązane do podjęcia dodatkowych środków, gdy przechowują dane Europejczyków poza Europą" – dodał.

Źródło: Holandia. 290 mln euro kary dla Ubera – DW – 26.08.2024

05 Administracyjna kara pieniężna 40 tys. zł po utracie danych osób w wyniku ataku hackerskiego

- Prezes UODO nałożył na Samodzielny Publiczny ZOZ w Pajęcznie karę 40 tys. złotych. W wyniku ataku hakerskiego placówka straciła dostęp do danych pacjentów i pracowników. Działania naprawcze podjęła dopiero po fakcie.
- Do ataku hakerskiego doszło w lutym 2022 r. Złośliwe oprogramowanie typu „ransomware" zaszyfrowało dane osobowe 30 tys. pacjentów i ponad tysiąca pracowników. ZOZ zawiadomił o tym UODO i Policję. Uznał jednak, że atak nie był poważny, bo dane nie wyciekły – stały się tylko niedostępne (zewnętrzny ekspert wskazał, że danych nie da się odszyfrować – atakujący uzależnili odszyfrowanie danych od zapłacenia okupu w kryptowalucie).
- Na zagrożenie dla danych osobowych ZOZ zareagował dopiero po ataku. Wtedy wezwał ekspertów, którzy wskazali luki w zabezpieczeniach i zarekomendowali zmiany. Odbyły się też szkolenia dla pracowników dotyczące bezpieczeństwa systemów informatycznych i danych.
- ZOZ nie miał jednak – co jest kluczowe – dokumentów potwierdzających sporządzenie i aktualizowanie analizy ryzyka dla danych osobowych. Bezpieczeństwo danych powierzono informatykowi, który na bieżąco analizował m.in. podatności, zagrożenia, możliwe skutki naruszenia oraz środki bezpieczeństwa mające na celu zapewnienie poufności, integralności i dostępności przetwarzanych danych osobowych. To w żaden sposób nie mogło zapewnić należytej kontroli nad bezpieczeństwem danych.
- W efekcie, przyjęte w ZOZ procedury nie były adekwatne do ryzyk dla danych osobowych. Wykazał to przeprowadzony już po ataku audyt. Nie mając analizy ryzyka ZOZ popełnił błędy także po incydencie – zgłosił swój problem UODO i Policji, ale nie zauważył problemu osób, których dane dotyczyły. Nie powiadomił ich, że stracił kontrolę nad danymi takimi jak: imię i nazwisko, imiona rodziców, datę urodzenia, numer rachunku bankowego, adres zamieszkania lub pobytu, nr PESEL, nazwę użytkownika i/lub hasło, dane dotyczące zarobków lub posiadanego majątku, nazwisko rodowe matki, serię i numer dowodu osobistego, numer telefonu oraz dane dotyczące zdrowia.

Źródło: Aktualności - UODO