
LEX ARTIST

RODO - aktualności

17 stycznia 2022 r.

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 Plan kontroli sektorowych UODO na 2022 rok

02 Skarga kasacyjna od wyroku WSA ws. przetwarzania danych osobowych klienta banku

03 45 tys. zł kary dla Politechniki Warszawskiej

04 Korzystanie z Google Analytics narusza RODO

05 Nowe odpowiedzi na pytania IOD

01 Plan kontroli sektorowych UODO na 2022 rok

- jak wynika z zatwierdzonego przez Prezesa UODO rocznego planu kontroli jednym z punktów jest sprawdzenie procesów zabezpieczenia i udostępniania danych osobowych przetwarzanych przez podmioty przetwarzające w związku z użytkowaniem aplikacji mobilnych
- ponadto UODO przyjrzy się przetwarzaniu danych osobowych klientów i potencjalnych klientów banków w zakresie profilowania – sprawdzi też sposoby informowania osób ubiegających się o kredyt o dokonanej ocenie zdolności kredytowej w związku z art. 70a ustawy Prawo bankowe
- dodatkowo UODO zweryfikuje przetwarzanie danych osobowych przez organy przetwarzające w Systemie Informacyjnym Schengen i Wizowym Systemie Informacyjnym
- zaplanowane kontrole podyktowane są licznymi sygnałami (w tym skargami, pytaniami i zgłoszeniami naruszeń ochrony danych osobowych) wskazującymi na zagrożenia naruszenia przepisów o ochronie danych osobowych oraz duże społeczne zainteresowanie tego typu problemami – dlatego też Prezes Urzędu Ochrony Danych Osobowych uznał je za istotne z punktu widzenia zadań realizowanych przez organ nadzorczy

Źródło: https://uodo.gov.pl/pl/138/2250

02 Skarga kasacyjna od wyroku WSA ws. przetwarzania danych osobowych klienta banku (1)

- w jednej ze spraw prowadzonych w UODO, klient banku wystąpił do urzędu ze skargą o nakazanie usunięcia jego danych osobowych przetwarzanych przez bank i instytucję finansową utworzoną na podstawie Prawa bankowego, tj. Biuro Informacji Kredytowej w związku ze złożonymi przez niego zapytaniami kredytowymi
- klient banku wskazywał, że przetwarzanie jego danych jest nieuprawnione, gdyż nie doszło do zawarcia żadnej umowy z bankiem
- Prezes UODO po przeprowadzeniu postępowania administracyjnego, przyznał rację klientowi banku stwierdzając brak podstaw prawnych do przetwarzania jego danych osobowych przez ww. podmioty i wydał decyzję administracyjną nakazującą usunięcie danych
- tymczasem WSA w wyroku z dnia 28 września 2021 r., sygn. akt II SA/Wa 474/21, uchylając wskazaną decyzję uznał, że w sprawie zaniechano zwrócenia się do KNF jako organu właściwego w sprawach związanych m.in. z badaniem zdolności kredytowej i analizą ryzyka kredytowego, a także budową modeli scoringowych (metoda oceny wiarygodności kredytowej), co w jego ocenie było bezwzględnie konieczne

02 Skarga kasacyjna od wyroku WSA ws. przetwarzania danych osobowych klienta banku (2)

- UODO jest zaniepokojony niebezpiecznym kierunkiem w jakim zmierza dokonana przez sąd administracyjny ocena stosowania przepisów Kodeksu postępowania administracyjnego w kontekście rozstrzygania przez organ nadzorczy spraw z zakresu ochrony danych osobowych, niezgodna z treścią i celem przepisów prawa Unii Europejskiej, jakie stanowią przepisy RODO
- zdaniem UODO stanowisko zawarte w wyroku WSA w Warszawie w sprawie przetwarzania danych osobowych klienta banku godzi w niezależność i autonomię organu nadzorczego – dlatego też od tego wyroku złożona została skarga kasacyjna do Naczelnego Sądu Administracyjnego

Źródło: https://uodo.gov.pl/pl/138/2251

03 45 tys. zł kary dla Politechniki Warszawskiej

- PW otrzymała karę w wysokości 45 tys. zł m.in. za niezastosowanie odpowiednich środków technicznych i organizacyjnych mających zapewnić zdolność do ciągłego zapewnienia poufności usług przetwarzania, także za brak regularnego testowania, mierzenia i oceniania skuteczności środków – uczelnia nie uwzględniła również ryzyka związanego z przetwarzaniem danych w aplikacji
- postępowanie wszczęto po tym jak do UODO wpłynęło zgłoszenie naruszenia ochrony danych – nieuprawniona osoba dokonała pobrania z zasobów sieci informatycznej uczelni bazy danych, zawierającej dane osobowe studentów i wykładowców
- jak ustalono w czasie postępowania administracyjnego jednostka organizacyjna Politechniki wykorzystywała aplikację stworzoną przez pracowników uczelni, która służyła do zapisywania się na przedmioty oraz pozwalała mieć wgląd w historię nauczania, ocen czy rozliczania opłat – aplikacja ta była modyfikowana w zależności od potrzeb administratora
- na początku stycznia 2020 roku nieuprawniona osoba wykorzystała funkcjonalność umieszczania plików w aplikacji, dysponując danymi uwierzytelniającymi – z kolei z początkiem maja 2020 roku dokonano nieautoryzowanego pobrania danych osobowych
- w ocenie UODO, administrator nie przedstawił dowodów na spełnienie tych obowiązków, w tym nie dokonywał formalnej oceny ryzyka, a zagrożenia identyfikował poprzez zbieranie informacji od jednostek uczelni
- ponadto nie uzasadnił adekwatności stosowanych zabezpieczeń do ryzyka – PW skupiła się na zabezpieczeniu przed zagrożeniami infrastruktury informatycznej, nie wzięła jednak pod uwagę zagrożeń związanych z funkcjonowaniem stworzonej aplikacji

Źródło: https://uodo.gov.pl/pl/138/2248

04 Korzystanie z Google Analytics narusza RODO

- austriacki organ ochrony danych uznał, że korzystanie z Google Analytics narusza RODO – to kolejna odsłona w toczącej się od lat batalii prawnej o przekazywanie danych Europejczyków do USA, gdzie na rozstrzygnięcie czeka kolejnych 100 skarg skierowanych w 30 państwach EOG
- w każdej ze 101 spraw skarżących reprezentuje NOYB – organizacja non profit założona przez Maxa Schremsa, który doprowadził do unieważnienia programu „Safe Harbour" oraz jego następcy, czyli porozumienia „Privacy Shield"
- za każdym razem powód był ten sam - jak ujawnił Edward Snowden, amerykańskie firmy mają obowiązek udostępnienia na żądanie tamtejszych służb wszystkich danych, a to zaś nie odpowiada wymogom proporcjonalności, które przewiduje prawo unijne
- teraz NOYB znów dowodzi, że transfer danych do USA jest bezprawny – skupia się na dwóch firmach, Facebook i Google
- tyle że w rzeczywistości chodzi o tysiące europejskich przedsiębiorców korzystających z tych serwisów – także z Polski, bo skargi do UODO dotyczą TVN, TVP, Interii, PKO BP i Onet-RASP, wykorzystujących narzędzia Google i Facebooka
- w pierwszym przypadku chodzi o Google Analytics, który pozwala na mierzenie ruchu na stronach – problem w tym, że zebrane w ten sposób dane wędrują do USA, choć - jak uznał właśnie austriacki organ danych - dzieje się to bez podstawy prawnej

Źródło: https://www.gazetaprawna.pl/firma-i-prawo/artykuly/8334416,korzystanie-z-google-analytics-narusza-rodo.html

05 Nowe odpowiedzi na pytania IOD (1)

- na swojej stronie internetowej, UODO odpowiada na nowe pytania IOD

CZY NALEŻY PODPISAĆ UMOWĘ POWIERZENIA Z FIRMĄ SPRZĄTAJĄCĄ?

- same usługi sprzątania powierzchni danego obiektu (np. uczelni, biura) trudno zaliczyć do usług związanych z przetwarzaniem danych osobowych – należy zatem przyjąć, że co do zasady usługi takie nie wymagają powierzenia przetwarzania danych osobowych
- niemniej w przypadku korzystania przez administratora z takich usług (jak i innych usług wymagających dostępu do pomieszczeń administratora, w których przetwarzane są dane osobowe) – konieczne może się okazać zastosowanie odpowiednich środków technicznych i organizacyjnych, których celem będzie zapewnienie odpowiedniej ochrony danych osobowych, w tym przed nieuprawnionym ujawnieniem danych osobowych

Źródło: https://uodo.gov.pl/pl/225/2245

W JAKIM ZAKRESIE NALEŻY UJAWNIAĆ DANE PRZEDSIĘBIORCÓW PROWADZĄCYCH OŚRODKI SZKOLENIA KIEROWCÓW?

- dane osobowe osób fizycznych prowadzących jednoosobową działalność gospodarczą podlegają ochronie na mocy RODO, a podmioty, które chcą je przetwarzać, muszą spełnić wszystkie obowiązki wynikające z przepisów o ochronie danych osobowych, w tym legitymować się podstawą prawną do ich przetwarzania

05 Nowe odpowiedzi na pytania IOD (2)

- przedstawione w pytaniu wątpliwości dotyczą tego, czy w celu realizacji obowiązku określonego w art. 43 ust. 1 pkt 6 lit. a ustawy o kierujących pojazdami starosta może udostępnić informacje o firmie przedsiębiorcy zawierającej imię i nazwisko osoby prowadzącej jednoosobową działalność
- przywołany przepis nakłada na starostę obowiązek podania do publicznej wiadomości wyników analizy statystycznej dotyczących danego ośrodka szkolenia kierowców – zatem podstawę do przetwarzania danych osobowych w tym celu stanowi ww. przepis ustawy o kierujących pojazdami, nie zaś zgoda osoby, której dane dotyczą
- aby zrealizować powyższy obowiązek starosta może zatem podać do wiadomości publicznej takie informacje dotyczące ośrodka, które go jednoznacznie identyfikują, łącznie z oznaczeniem i adresem ośrodka szkolenia kierowców nawet w przypadku, gdy oznaczenie to obejmuje firmę przedsiębiorcy

Źródło: https://uodo.gov.pl/pl/225/2245

JAK POSTĘPOWAĆ W PRZYPADKU OTRZYMYWANIA TZW. NIECHCIANYCH DANYCH?

- RODO wymaga, aby pozyskiwane (przetwarzane) dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane - tzw. zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO)

05 Nowe odpowiedzi na pytania IOD (3)

- ponadto dane osobowe powinny być zbierane w wyraźnie określonym i prawnie uzasadnionym celu (art. 5 ust. 1 lit. c RODO)
- mając na uwadze wskazane zasady RODO oraz m.in. przepisy prawa regulujące realizację określonych zadań / obowiązków, administrator powinien dokonywać analizy, czy określony dokument zawierający dane osobowe istotnie został przesłany nadmiarowo lub pomyłkowo i w zależności od wyników takiej analizy np. pozostawić dokument, zwrócić lub przekazać do innego podmiotu / organu

Źródło: https://uodo.gov.pl/pl/225/2247