
LEX ARTIST

RODO - aktualności

[05.02.2024]

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 Krajowi regulatorzy chcą opinii EROD w sprawie modelu „pay or okay”

- Model „pay or okay” polega on na tym, że aby uzyskać dostęp do danej platformy, użytkownik musi albo zgodzić się na przetwarzanie jego danych osobowych na potrzeby reklamowe, albo uiścić opłatę pieniężną.
- Przepisy RODO wymagają, aby zgoda na wykorzystanie danych osobowych była wyrażona dobrowolnie. W stosunku do systemu „pay or okay” są podnoszone jednak wątpliwości co do spełnienia tego wymogu. Dobrowolność oznacza bowiem, że nie należy wywierać nacisku na użytkowników, aby wyrazili zgodę, i nie powinni oni ponieść szkody w przypadku odmowy na zbieranie ich danych. Innymi słowy obie możliwości – śledzenie internauty i opłata pieniężna – powinny być równoważne.
- Najsłynniejszym przypadkiem zastosowania „pay or okay” są serwisy społecznościowe Facebook i Instagram, które w listopadzie ub.r. wprowadziły ten model korzystania z usług dla internautów w Europejskim Obszarze Gospodarczym (EOG). Obecna metoda obejmuje wprawdzie zgodę, ale według organizacji obrońców prywatności NOYB przy tak wygórowanym wynagrodzeniu jako opcji alternatywnej – nie jest to zgoda dobrowolna. Dlatego NOYB złożyła do austriackiego organu ochrony danych skargę przeciwko właścicielowi Facebooka i Instagrama. W odniesieniu do modelu subskrypcyjnego Mety organy w Niemczech i Norwegii pod koniec ub.r. same podjęły się zbadania zgodności z przepisami.
- Kontrowersje wobec zmian wprowadzonych przez Metę i brak zharmonizowanego na poziomie europejskim podejścia do tej kwestii sprawiły, że trzy organy ochrony danych (Norwegia, Holandia i Niemcy) zwróciły się do EROD o wydanie opinii w sprawie zgodności „pay or okay” z RODO. Opinia rady będzie podstawą do egzekwowania przepisów RODO w całym EOG.
- EROD powinna wydać opinię w ciągu ośmiu tygodni.

Źródło: Krajowi regulatorzy chcą opinii EROD w sprawie modelu „pay or okay” - GazetaPrawna.pl

02 IOD nie powinien być pełnomocnikiem administratora

- W najnowszym numerze biuletynu UODO, organ nadzorczy zasygnalizował, że IOD nie powinien być pełnomocnikiem administratora.
- Pełnienie roli pełnomocnika przez IOD w sprawach z zakresu ochrony danych osobowych u administratora, u którego IOD pełni swoją funkcję, stoi ponadto w kolizji z nakazem nienakładania na IOD zadań powodujących konflikt interesów. IOD działając jako pełnomocnik administratora (czyli zgodnie z wolą i interesem mocodawcy), mógłby być zmuszony do pomijania i własnych spostrzeżeń i rekomendacji, które wypracował jako IOD.
- Występowanie w roli pełnomocnika administratora, w zakresie obowiązków nałożonych na administratora, może istotnie utrudniać lub uniemożliwiać inspektorowi niezależną ocenę, czy obowiązki administratora są wykonywane i czy są wykonywane prawidłowo. Z analogicznych powodów ocenić należy, że konflikt interesów powodowałoby dokonywanie przez IOD na podstawie pełnomocnictwa administratora również innych czynności, np. podpisywanie formularza zgłoszenia naruszenia czy pism, w których w imieniu administratora miałby zobowiązywać się do realizacji pewnych działań, w tym doskonalących, np. wdrożenie nowych rozwiązań informatycznych związanych z podniesieniem bezpieczeństwa danych.
- Inspektor ochrony danych powinien, zdaniem UODO, odpowiednio wcześnie identyfikować i sygnalizować administratorowi ryzyko wystąpienia konfliktu interesów, by możliwe było odpowiednio wczesne zapobieganie mu. W przypadku wystąpienia takiego konfliktu inspektor ochrony danych powinien powstrzymać się od dokonywania czynności w imieniu administratora lub wypowiedzieć udzielone mu pełnomocnictwo.
- Stanowisko UODO jest pokłosiem sprawozdania EROD podsumowującego badanie dotyczące wyznaczania i pozycji inspektorów ochrony danych oraz zawierającego rekomendacje, które mogą być pomocne we właściwym kształtowaniu zadań, roli i pozycji inspektora ochrony danych (IOD) w powołującej go organizacji.

Źródło: **Biuletyn UODO 01/24**; DLA IOD – UODO; Aktualności - UODO

03 Ubywa skarg, rośnie zaś szybko liczba powiadomień o incydentach

- Liczba skarg kierowanych do Urzędu Ochrony Danych Osobowych, choć nieznacznie, to jednak od trzech lat spada. Odmienną tendencję można zaś zaobserwować, jeśli chodzi o zgłaszanie incydentów związanych z danymi osobowymi. W 2023 r. liczba takich zgłoszeń przekroczyła już 14 tys. Dla porównania w 2019 r. do UODO zgłoszono nieco ponad 6 tys. takich naruszeń.
- Zgłoszenia dotyczą różnych kwestii – od włamań hakerów i wykradzenia czy zaszyfrowania danych, poprzez zgubienie laptopa czy pamięci przenośnej, do omyłkowego wysłania korespondencji elektronicznej pod niewłaściwy adres. W zasadzie każda z takich sytuacji może prowadzić do jakiegoś zagrożenia. Sądząc natomiast po spadku liczby skarg, sami zainteresowani w mniejszym stopniu dostrzegają ryzyko. Dlatego też część ekspertów uważa, że działania administratorów, zwłaszcza przedsiębiorców, często są podejmowane nieco na wyrost, tylko po to, by uniknąć ewentualnej kary.
- Brak zgłoszenia (lub zgłoszenie z opóźnieniem) stosunkowo często jest podstawą do wymierzenia samoistnej kary finansowej. Przykładów na to nie trzeba daleko szukać – w ubiegłym tygodniu UODO poinformował o nałożeniu 10 tys. zł kary z tego właśnie powodu na Sąd Okręgowy w Krakowie, który nie poinformował o tym, że wysłana korespondencja doszła do adresata w rozerwanej kopercie, co oznacza, że ktoś mógł się z nią zapoznać.
- – Administratorzy dla świętego spokoju wolą zgłosić naruszenie. To ostrożnościowe podejście wynika z dotychczasowej praktyki prezesa UODO, który uznawał, że już niskie ryzyko powoduje konieczność zgłoszenia naruszenia. Bezpieczniej jest więc zgłosić nawet mało istotny incydent, by uniknąć kary – komentuje Sławomir Kowalski, partner w kancelarii JustLAW.
- W przygotowanym przez kancelarię DLA Piper raporcie o naruszeniach RODO i karach („GDPR Fines and Data Breach Survey") Polska pod względem liczby zgłoszonych w ostatnim roku incydentów zajęła trzecie miejsce, za Niemcami i Holandią. Te dwa kraje przodują również w zestawieniu obejmującym cały okres obowiązywania RODO (tj. od 25 maja 2018 r. do 27 stycznia 2024 r.).

Źródło: Ubywa skarg, rośnie zaś szybko liczba powiadomień o incydentach - GazetaPrawna.pl

04 WSA dwa razy potwierdza nakaz usunięcia danych przez Bank i BIK

- Obydwa wyroki dotyczą zagadnienia skupiającego się na możliwości przetwarzania danych osobowych osób, które zgłosiły się do Banku z chęcią zawarcia umowy kredytu, ale z jakiś powodów nie dochodzi do zawarcia takiej umowy.
- W obydwu sprawach Prezes UODO nakazał usunięcie danych osobowych w zakresie zapytania kredytowego i w obydwu sprawach WSA w Warszawie wskazał wiele bardzo istotnych argumentów za oddaleniem skargi na powyższe decyzje.
- Sąd wskazał, że:
    - Nie ma wątpliwości i nie było kwestionowane przez Prezesa UODO, że Bank oraz BIK, na podstawie art. 105a ust. 1 Prawa bankowego w zw. z art. 70 ust. 1 tej ustawy, były uprawnione do przetwarzania danych osobowych G. K. w celu oceny zdolności kredytowej i analizy ryzyka kredytowego. Pogląd ten podziela Sąd rozpoznający niniejszą sprawę
    - Podkreślenia jednak wymaga, że w sprawie tej nie doszło do zawarcia umowy kredytowej pomiędzy wymienioną a Bankiem. Osoba po 2 tygodniach od złożenia wniosku o kredyt wniosła o zaprzestanie przetwarzania jej danych i ich usunięcie.
- W drugiej sprawie BIK próbował wykazać, że przetwarzanie danych osobowych Uczestniczki postępowania umożliwia udokumentowanie tego, że są one przetwarzane z poszanowaniem podstawowych zasad jakości danych osobowych, o których mowa w art. 5 RODO. Innymi słowy, że przetwarza dane osobowe po to, aby móc wykazać, że są one przetwarzane zgodnie z prawem.
- W ocenie Sądu nie jest w takiej sytuacji spełniona przesłanka określona w art. 6 ust. 1 lit f RODO. Przetwarzanie danych w celu udokumentowania prawidłowości ich przetwarzania nie stanowi celu, który wynika z prawnie uzasadnionego interesu.

Źródło: https://www.linkedin.com/posts/piotr-liwszic_orzecznictwo-rodo-w-jednym-miejscu-activity-7158379698215956480-P_Cs?utm_source=share&utm_medium=member_desktop

05 Węgry: kara dla linii lotniczej za brak zawiadomienia osoby o realizacji żądania usunięcia danych osobowych

- W przedmiotowej sprawie mimo wyraźnego żądania usunięcia danych osobowych, które dodatkowo było uzasadnione, Administrator nie udzielił żadnej odpowiedzi. Osoba, której dane dotyczą wniosła więc skargę do organu nadzorczego.
- Węgierski urząd ochrony danych osobowych wszczął postępowanie wyjaśniające, podczas którego ustalił, że administrator już po miesiącu usunął całe konto użytkownika, nie dzieląc się jednak tą informacją z podmiotem danych. Zdaniem Administratora żądanie zostało zatem zrealizowane.
- Organ w swojej decyzji stwierdził naruszenie przez linię lotniczą art. 12 ust. 3 RODO poprzez niepoinformowanie osoby, która złożyła żądanie o usunięcie danych osobowych o przychyleniu się do żądania i podjęciu działań w jej sprawie. Organ stwierdził ponadto naruszenie artykułu 5 ust. 1 lit. a RODO ze względu na brak przejrzystości przetwarzania. Osoba skarżąca nie miała bowiem dostępu do informacji o tym jakie dane, na jakiej podstawie prawnej i w jakim celu są przetwarzane przez administratora po usunięciu jej konta z serwisu podmiotu.
- Decyzją administracyjną linia lotnicza otrzymała karę 5 milionów forintów - ponad 13 000 Euro.

Źródło: https://www.linkedin.com/posts/tomasz-osiej_hungarian-sa-deletion-request-in-concerning-activity-7158011811198382081-ljEF?utm_source=share&utm_medium=member_desktop

06 Kary finansowe za naruszenia RODO – podsumowanie roku 2023

- W ubiegłym roku polski organ nadzorczy nałożył rekordową liczbę 20 kar pieniężnych, których łączna suma wyniosła 656 089 zł.
- Najwyższa administracyjna kara pieniężna nałożona przez Prezesa UODO w 2023 r. wynosiła 103 752 zł i została nałożona z powodu niezgłoszenia naruszenia ochrony danych osobowych do organu nadzorczego. Natomiast najniższa – to kara o wysokości 472 zł. (najniższa jak dotąd) nałożona z powodu niewdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych przez podmiot przetwarzający, co w konsekwencji doprowadziło do naruszenia ochrony danych osobowych u administratora.
- Z 20 decyzji UODO o ukaraniu administratorów danych osobowych:
    - 6 dotyczyło podmiotów publicznych;
    - 14 dotyczyło sektora prywatnego;
    - 12 wydanych zostało wskutek wpłynięcia skarg;
    - 7 wydanych zostało w związku ze zgłoszeniem naruszenia;
    - 1 wydana została na skutek niewykonania obowiązku wynikającego z wcześniejszej decyzji Prezesa UODO;
    - aż 7 nałożonych kar było rezultatem braku współpracy z organem nadzorczym.

Źródło: Kary finansowe za naruszenia RODO - podsumowanie roku 2023 - Soczko & Partnerzy