
LEX ARTIST

RODO - aktualności

16 listopada 2020 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 EROD przyjęła zalecenia w sprawie środków uzupełniających wz. z Schrems II (I)

- Europejska Rada Ochrony Danych przyjęła zalecenia w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności ze stopniem ochrony danych osobowych UE, jak również zalecenia w sprawie niezbędnych gwarancji europejskich dla środków nadzoru
- oba dokumenty, przyjęte przez EROD 10 listopada 2020 r. podczas 41. posiedzenia plenarnego, powstały w konsekwencji wyroku TSUE w sprawie Schrems II
- zalecenia mają pomóc administratorom i podmiotom przetwarzającym dane, działającym jako podmioty przekazujące dane, w ich obowiązku określenia i wdrożenia odpowiednich środków uzupełniających, jeżeli są one niezbędne do zapewnienia merytorycznie równoważnego stopnia ochrony danych przekazywanych do państw trzecich
- zalecenia zawierają plan działań, jakie muszą podjąć podmioty przekazujące dane, aby ustalić, czy muszą wdrożyć środki uzupełniające, żeby móc przesyłać dane poza EOG zgodnie z prawem UE, oraz pomóc im określić te, które mogłyby być skuteczne

01 EROD przyjęła zalecenia w sprawie środków uzupełniających wz. z Schrems II (II)

- zalecenia w sprawie środków uzupełniających zostaną przedłożone do konsultacji publicznych – będą one stosowane niezwłocznie po ich opublikowaniu.
- ponadto EROD przyjęła zalecenia w sprawie niezbędnych gwarancji europejskich dla środków nadzoru, które uzupełniają zalecenia w sprawie środków uzupełniających
- zapewniają one podmiotom przekazującym dane elementy pozwalające ustalić, czy ramy prawne regulujące dostęp organów publicznych do danych w celach nadzoru w państwach trzecich, można uznać za uzasadnioną ingerencję w prawa do prywatności i ochrony danych osobowych
- zalecenia w sprawie środków uzupełniających dostępne są pod linkiem: https://edpb.europa.eu/sites/edpb/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf#xd_co_f=MmVkMmQwNTYtZWEzOC00YzBiLTk4MmMtMGU0YjY5ZjZmZWMz~
- zalecenia w sprawie niezbędnych gwarancji dostępne są pod linkiem: https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_recommendations_202002_europeanessentialguaranteessurveillance_en.pdf

Źródło: https://uodo.gov.pl/pl/138/1768 https://edpb.europa.eu/news/news/2020/european-data-protection-board-41st-plenary-session-edpb-adopts-recommendations_en https://www.prawo.pl/biznes/wytyczne-erod-w-sprawie-przekazywania-danych-do-panstw-trzecich,504456.html

02 Pierwsza decyzja EROD na podstawie art. 65 RODO

- podczas 41. posiedzenia plenarnego EROD większością 2/3 głosów swoich członków przyjęła pierwszą decyzję rozstrzygającą spór na podstawie art. 65 RODO, dotyczącą spółki Twitter International Company
- wiążąca decyzja ma na celu rozwiązanie sporu powstałego w następstwie projektu decyzji irlandzkiego organu nadzorczego, będącego wiodącym organem nadzorczym w sprawie, dotyczącego spółki Twitter International Company, a następnie mających znaczenie dla sprawy i uzasadnionych sprzeciwów zgłoszonych przez szereg organów, których sprawa dotyczy
- irlandzki organ nadzorczy sporządził projekt decyzji w następstwie przeprowadzonego z własnej inicjatywy postępowania w sprawie Twitter International Company, po tym jak spółka zgłosiła mu naruszenie ochrony danych osobowych
- organy nadzorcze, których sprawa dotyczy, zgłosiły sprzeciwy, między innymi, co do naruszeń RODO zidentyfikowanych przez wiodący organ nadzorczy, roli spółki Twitter International Company jako administratora danych oraz kwantyfikacji kary
- w związku z tym, że wiodący organ nadzorczy odrzucił sprzeciwy i/lub uznał je za niemające znaczenia dla sprawy lub nieuzasadnione, zgodnie z art. 60 ust. 4 RODO przekazał sprawę EROD, inicjując tym samym procedurę rozstrzygania sporów
- w dniu 9 listopada 2020 r. EROD przyjęła wiążącą decyzję i wkrótce notyfikuje ją irlandzkiemu organowi nadzorczemu - irlandzki organ nadzorczy przyjmie ostateczną decyzję na podstawie decyzji EROD

Źródło: https://uodo.gov.pl/pl/138/1762 https://edpb.europa.eu/news/news/2020/edpb-adopts-first-art-65-decision_en

03 ICO nakłada na Ticketmaster UK Limited karę w wysokości 1,25 mln funtów (I)

- Biuro Komisarza ds. Informacji (ICO) nałożyło na Ticketmaster UK Limited grzywnę w wysokości 1,25 miliona funtów za niezachowanie bezpieczeństwa danych osobowych klientów
- ICO stwierdziło, że firma nie wdrożyła odpowiednich środków bezpieczeństwa, aby zapobiec cyberatakowi na chatbota zainstalowanego na stronie płatności online
- naruszenie danych, które obejmowało nazwiska, numery kart płatniczych, daty ważności i numery CVV, potencjalnie dotknęło 9,4 miliona klientów Ticketmaster w całej Europie, w tym 1,5 miliona w Wielkiej Brytanii
- śledczy ustalili, że w wyniku naruszenia 60 000 kart płatniczych należących do klientów Barclays Bank padło ofiarą oszustwa, a kolejne 6 000 kart zostało zablokowanych przez Monzo Bank po podejrzeniu nieuczciwego użycia
- ICO stwierdziło, że Ticketmaster nie:
  - ✓ nie ocenił ryzyka związane z używaniem chatbota na jego stronie płatności
  - ✓ nie zidentyfikował i zastosował odpowiednich środków bezpieczeństwa, aby wyeliminować ryzyko
  - ✓ nie zidentyfikował źródła sugerowanych nieuczciwych działań

03 ICO nakłada na Ticketmaster UK Limited karę w wysokości 1,25 mln funtów (II)

- naruszenie zaczęło się w lutym 2018 roku, kiedy klienci Monzo Bank zgłosili podejrzane transakcje
- w sumie Ticketmaster potrzebował dziewięciu tygodni od powiadomienia o możliwym oszustwie do monitorowania ruchu sieciowego za pośrednictwem strony płatności online
- dochodzenie ICO wykazało, że decyzja Ticketmaster o umieszczeniu bota czatowego, hostowanego przez stronę trzecią, na swojej stronie płatności online umożliwiła atakującemu dostęp do danych finansowych klientów
- chociaż naruszenie rozpoczęło się w lutym 2018 r. kara dotyczy tylko naruszenia od 25 maja 2018 r. kiedy rozpoczęto stosowanie przepisów RODO
- chat-bot został całkowicie usunięty ze strony internetowej Ticketmaster UK Limited w dniu 23 czerwca 2018 r.
- naruszenie miało miejsce, zanim Wielka Brytania opuściła UE, dlatego ICO przeprowadziło dochodzenie w imieniu wszystkich organów UE jako wiodący organ nadzorczy na mocy RODO

Źródło: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/11/ico-fines-ticketmaster-uk-limited-125million-for-failing-to-protect-customers-payment-details/ /

04 Uprzednie konsultacje? Nie w Polsce

- żaden przedsiębiorca nie przeprowadził dotąd w Polsce obowiązkowych konsultacji przed wdrożeniem produktów czy usług, które mogą zagrażać ochronie danych
- obowiązek przeprowadzania uprzednich konsultacji został wprowadzony przez RODO – są one powiązane z oceną skutków dla ochrony danych osobowych (DPIA)
- *Wpływają do nas nieliczne pisma zatytułowane jako „wniosek o uprzednie konsultacje", jednak po ich analizie okazuje się, że dotyczą one wątpliwości związanych z przetwarzaniem danych osobowych w konkretnych opisanych sytuacjach* – mówi Adam Sanocki, rzecznik prasowy UODO
- portal GDPR.pl zapytał europejskie organy ochrony danych o uprzednie konsultacje i choć nie uzyskał odpowiedzi od wszystkich, to już te, które zebrał, pokazują olbrzymie dysproporcje pomiędzy poszczególnymi państwami
- np. w mającej 5,5 mln mieszkańców Finlandii złożono 90 wniosków o uprzednie konsultacje, a w 60-milionowej Wielkiej Brytanii już tylko 10, w Chorwacji było 35 takich wniosków, w Szwecji 30, Norwegii i Słowacji po siedem, a na Łotwie i Islandii po pięć
- dane te nie do końca muszą być miarodajne, bo liczba wniosków nie zawsze przekłada się na rzeczywiste konsultacje, gdyż podobnie jak to jest w Polsce, sam tytuł może być mylący - w Finlandii na 90 wniosków tylko 20 zakończyło się zaleceniami

Źródło: https://biznes.gazetaprawna.pl/artykuly/1495932,ochrona-danych-konsultacje-przed-wdrozeniem-produktow-czy-uslug.html

05 TSUE: To klient, a nie sprzedawca zaznacza okienko ze zgodą na przetwarzanie danych

- firma nie może zaznaczać za klientów zgody na przechowywanie kopii ich dokumentów i wymagać, aby ewentualny sprzeciw wyrażali w dodatkowym oświadczeniu – uznał Trybunał Sprawiedliwości Unii Europejskiej
- sprawa dotyczyła rumuńskiego operatora telekomunikacyjnego Orange România
- zawierając umowy z klientami, prosił on o wyrażenie zgody na przechowywanie kopii dokumentu tożsamości - stosowna klauzula widniała w treści umowy
- jednocześnie okienko wyboru było zaznaczane już przez sprzedawcę – co więcej, jeśli klient nie wyrażał zgody na przetwarzanie swych danych, to musiał to odnotować odręcznie na umowie
- istotne jest przy tym również to, że bez wyrażenia zgody na zeskanowanie dokumentu i przechowywanie jego kopii umowa mogła być zawarta, a więc przetwarzanie danych nie było niezbędne do jej realizacji

Źródło: https://biznes.gazetaprawna.pl/artykuly/1496237,tsue-rodo-dane-osobowe-zgoda.html
http://curia.europa.eu/juris/document/document.jsf?text=&docid=233544&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=12687107

06 EROD, RPO i UODO o ujawnieniu danych osobowych zakażonego pracownika (I)

- przewodnicząca Europejskiej Rady Ochrony Danych (EROD) wydała oświadczenie odnoszące się do pandemii COVID-19 i jak wskazała, że pracodawcy powinni informować pracowników o przypadkach COVID-19 i podejmować środki ochronne, ale nie powinni przekazywać więcej informacji niż jest to konieczne
- w przypadkach, w których konieczne jest ujawnienie nazwiska pracownika, który zarażony jest wirusem (np. w kontekście profilaktyki), a prawo krajowe na to zezwala, pracownicy, których sprawa dotyczy, powinni zostać poinformowani z wyprzedzeniem
- kwestia ujawniania zakażeń przez pracodawcę budzi wiele pytań, dlatego na stronie RPO ten temat kilkukrotnie spotykał się z komentarzem
- w informacji opublikowanej na stronie w październiku podkreślono, że wiadomość, o dodatnim wyniku przekazywana jest do powiatowej stacji sanitarno-epidemiologicznej - wówczas rozpoczyna się procedura dochodzeniowa i przeprowadzany jest wywiad, a zakażony wskazuje między innymi, z kim ostatnio miał kontakt, by takie osoby można było objąć kwarantanną lub nadzorem epidemiologicznym
- to sprawia, że już na tym etapie wielu pracowników może się dowiedzieć o zakażeniu, otrzymując tę informację od pracownika sanepidu

06 EROD, RPO i UODO o ujawnieniu danych osobowych zakażonego pracownika (II)

- jeśli zaś chodzi o samego pracodawcę, to zdaniem RPO ujawnienie danych osobowych zakażonego pracownika jest możliwe zgodnie z art. 209(2) Kodeksu pracy – w przypadku wystąpienia zagrożenia dla zdrowia lub życia pracodawca ma bowiem obowiązek między innymi poinformować pracowników o tym zagrożeniu
- UODO w odpowiedzi na pytanie zadane przez Prawo.pl wskazał z kolei, że Kodeks pracy dopuszcza przetwarzanie danych pracowników, natomiast nie reguluje kwestii ich przetwarzania (w tym ujawnienia danych zakażonego pracownika) w celu zwalczania epidemii
- zdaniem UODO to służby sanitarne powinny wskazywać kierunki podejmowanych działań, nie pracodawcy
- zdaniem UODO pracodawca powinien przedstawić kluczowe informacje służbom sanitarnym, a te na podstawie informacji i wiedzy epidemiologicznej podjąć właściwe decyzje i wprowadzić odpowiednie rozwiązania

Źródło: https://bezprawnik.pl/ujawnienie-danych-osobowych-zakazonego-pracownika/ https://www.prawo.pl/kadry/czy-pracodawca-moze-ujawnic-informacje-o-chorobie-covid-19,504414.html

07 Newsletter UODO

- w najnowszym, październikowym numerze newslettera Urzędu Ochrony Danych Osobowych dla inspektorów ochrony danych znajdziemy między innymi:

1. MIASTO NIE MOŻE MIEĆ STAŁEGO DOSTĘPU DO BAZY DANYCH MPWIK

- obowiązujące przepisy prawa nie dają podstaw do tego, by organy podatkowe miały stały dostęp do danych o zużyciu wody przez wszystkich klientów firmy wodociągowej

2. DO ORGANIZACJI PANELU OBYWATELSKIEGO NIE MOŻNA WYKORZYSTYWAĆ DANYCH Z REJESTRU WYBORCÓW

- w opinii Prezesa UODO, gmina na potrzeby organizacji panelu obywatelskiego nie może wykorzystywać danych osobowych swoich mieszkańców, które są zawarte w rejestrze wyborców

3. UDZIELANIE INFORMACJI PRZEZ OŚRODEK POMOCY SPOŁECZNEJ INNYM PODMIOTOM PUBLICZNYM

- podstawa prawna do przetwarzania, w tym udostępniania, danych osobowych przez podmioty publiczne powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami

Źródło: Newsletter UODO dla IOD, archiwum Newslettera https://uodo.gov.pl/p/archiwum-newslettera-dla-iod

08 Czy praca IOD może być kontrolowana?

- UODO odpowiedział na pytanie czy działania podejmowane przez IOD w związku z wykonywaniem przez niego jego zadań mogą podlegać kontroli przeprowadzanej przez administratora
- UODO wskazuje, że niezależność IOD jest jedną z najważniejszych gwarancji skutecznego i prawidłowego wykonywania jego zadań, a tym samym realnego zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa
- jednocześnie to administrator ponosi pełną odpowiedzialność za zgodne z przepisami ochrony danych osobowych przetwarzanie danych
- inspektor ochrony danych podlega bezpośrednio administratorowi i w związku z tym sposób wykonywania funkcji przez IOD musi podlegać jego kontroli, przy czym może to być kontrola wewnętrzna lub zlecona przez administratora podmiotowi zewnętrznemu - w jednym i drugim przypadku taka kontrola (audyt) musi uwzględniać niezależne funkcjonowanie (gwarancje niezależności) IOD, tak wyraźnie podkreślane w RODO
- dotyczy to również wdrożonych w danej organizacji systemów wewnętrznej kontroli (systemy oceny zgodności) – systemy te nie mogą w jakikolwiek sposób ograniczać możliwości wykonywania przez IOD jego zadań, w tym dokonywania kompleksowej, bieżącej oceny zgodności przetwarzania danych osobowych z przepisami prawa

Źródło: https://uodo.gov.pl/pl/223/1765