
LEX ARTIST

RODO - aktualności

[11.12.2023]

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 WSA: Dane osobowe w prywatnym komputerze pracownika też trzeba chronić

02 TSUE: RODO sprzeciwia się dwóm praktykom przetwarzania danych przez biura informacji kredytowej

03 Pięć technologicznych kierunków, które będą wpływać na prawa osób do ochrony danych i prywatności

04 Sąd Apelacyjny zmniejsza zadośćuczynienie RODO z 20 000 na 10 000 zł

05 Prezes UODO zatwierdził Kodeks postępowania dla sektora ochrony zdrowia

01 WSA: Dane osobowe w prywatnym komputerze pracownika też trzeba chronić

- Wojewódzki Sąd Administracyjny podtrzymał decyzję prezesa UODO, w której nałożono karę upomnienia na Rzecznika Finansowego za brak odpowiednich środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych.
- Do naruszenia ochrony danych osobowych doszło w związku z kradzieżą prywatnego komputera byłego pracownika Rzecznika Finansowego. W komputerze tym przechowywane były dane osobowe przetwarzane podczas pracy zdalnej świadczonej dla administratora danych. Fakt nieprzeprowadzenia przez administratora analizy ryzyka sprawił, że dane te nie zostały odpowiednio zabezpieczone.
- Ponadto administrator nie upewnił się, czy pracownik po zakończeniu świadczenia pracy skutecznie i trwale usunął dane z komputera. Brak odpowiednich zabezpieczeń technicznych i organizacyjnych doprowadził do nałożenia przez prezesa UODO kary upomnienia na administratora.
- Skarżąc decyzję organu nadzorczego, Rzecznik Finansowy twierdził, iż skradziony komputer należał do byłego już pracownika, a Prezes UODO nie udowodnił, że na jego dysku twardym faktycznie znajdowały się dane osobowe.
- Żaden z powyższych argumentów nie został podzielony przez WSA w Warszawie. Wojewódzki Sąd Administracyjny nie miał wątpliwości, że administratorem danych w tym przypadku był Rzecznik Finansowy, a nie jego pracownik. Sąd, rozstrzygając tę kwestię, przywołał definicję administratora zawartą w RODO, zgodnie z którą jest nim ten, kto decyduje o celach i sposobach przetwarzania danych osobowych.
- WSA w Warszawie zgodził się z prezesem UODO, że administrator danych powinien przeprowadzić analizę ryzyka w związku z pracą zdalną pracowników i korzystaniem przez nich zarówno z prywatnych, jak i służbowych komputerów. Odpowiadając na zarzut skarżącego, że organ nadzorczy nie udowodnił w postępowaniu, iż komputer nie był odpowiednio chroniony, sąd wskazał, iż ciężar dowodowy w tym przypadku spoczywa po stronie administratora.
- W swoim orzeczeniu WSA zwrócił też uwagę, że administrator nie zweryfikował również, czy pracownik skutecznie usunął dane z komputera.

Źródło: Dane osobowe w prywatnym komputerze pracownika też pod ochroną. Wyrok WSA (prawo.pl)

02 TSUE: RODO sprzeciwia się dwóm praktykom przetwarzania danych przez biura informacji kredytowej

- Trybunał Sprawiedliwości Unii Europejskiej (dalej: Trybunał, TSUE) wydał wyrok w sprawie C-634/21 | SCHUFA Holding (Scoring) oraz w sprawach połączonych C-26/22 i C-64/22 | SCHUFA Holding (Zwolnienie z pozostałej części długu). Orzeczenie zapadło w czwartek, 7 grudnia 2023 r.
- Wiele osób zaskarżyło przed sądem administracyjnym w Wiesbaden (Niemcy) na odmowę podjęcia działań przez właściwego komisarza ds. ochrony danych przeciwko niektórym rodzajom działalności SCHUFA, będącego prywatnym biurem informacji kredytowej, którego klientami są w szczególności banki. Sprzeciwiają się scoringowi oraz przechowywaniu informacji dotyczących zwolnienia z pozostałej części długu przejętej z rejestrów publicznych.
- Scoring jest matematyczną metodą statystyczną umożliwiającą, oparte na prawdopodobieństwie, ustalenie przyszłego zachowania, takiego jak spłata kredytu. Informacje dotyczące zwolnienia z pozostałej części długu są przechowywane w niemieckim publicznym rejestrze upadłości przez sześć miesięcy, podczas gdy kodeks postępowania niemieckich biur informacji kredytowej przewiduje dla ich własnych baz danych okres przechowywania wynoszący trzy lata.
- W odniesieniu do scoringu Trybunał orzekł, że należy go uznać za „zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach", co do zasady zakazane przez RODO, o ile klienci SCHUFA, tacy jak banki, przypisują mu decydującą rolę przy udzielaniu kredytów. Według sądu administracyjnego w Wiesbaden sytuacja taka ma miejsce.
- Odnosząc się zaś do informacji dotyczących zwolnienia z pozostałej części długu Trybunał uznał za sprzeczne z RODO to, że prywatne biura przechowują takie dane dłużej niż publiczny rejestr upadłości. Zwolnienie z pozostałej części długu ma bowiem na celu umożliwienie zainteresowanej osobie ponownego uczestnictwa w życiu gospodarczym, a zatem ma dla niej egzystencjalne znaczenie. Tymczasem informacje te są zawsze wykorzystywane jako czynnik negatywny przy ocenie zdolności kredytowej danej osoby.
- W zakresie, w jakim przechowywanie danych jest niezgodne z prawem, jak ma to miejsce po upływie sześciu miesięcy, osoba, której dane dotyczą, ma prawo do usunięcia tych danych, a biuro jest zobowiązane do ich usunięcia bez zbędnej zwłoki.

Źródło: RODO a praktyki przetwarzania danych przez biura informacji kredytowej - wyrok TSUE (prawo.pl)

03 Pięć technologicznych kierunków, które będą wpływać na prawa osób do ochrony danych i prywatności

- EDPS - European Data Protection Supervisor opublikował kolejną edycję raportu TechSonar. W edycji 2023-2024 wskazano pięć technologicznych kierunków, które z dużym prawdopodobieństwem będą wpływać na prawa osób fizycznych do ochrony danych i prywatności. Są to: modele językowe (Large Language Models-LLM), wykrywanie deepfake (Deepfake detection), portfel tożsamości cyfrowej (Digital Identity Wallet-DIW), wirtualna rzeczywistość (Extended Reality-XR) oraz Internet of Behaviours (IoB).
- Jako rodzaj generatywnego systemu AI, LLM tworzy nowe treści w odpowiedzi na pytania użytkownika na podstawie danych z różnych źródeł, w tym ze źródeł publicznych. LLM mogłyby pomóc w wykrywaniu i lepszym zarządzaniu danymi osobowymi dotyczącymi informacji nieustrukturyzowanych (np. pola tekstowego zawierającego historię rodziny). LLM mogłyby również pomóc w identyfikacji, redagowaniu lub anonimizowaniu danych osobowych. Jeśli jednak nie są odpowiednio zabezpieczone, LLM mogą ujawnić poufne lub prywatne informacje zawarte w ich zbiorach danych, co prowadzi do potencjalnych lub rzeczywistych naruszeń danych.
- DIW to aplikacja, która umożliwia bezpieczne przechowywanie, zarządzanie i udostępnianie danych osobowych, danych uwierzytelniających i innych informacji, odnoszących się do właściciela tego wirtualnego portfela. DIW mają duży potencjał w celu umożliwienia profilowania osób fizycznych, jeśli cechy i sposób korzystania z DIW nie są spójne z podejściem uwzględniającym ochronę prywatności w fazie projektowania.
- Rozszerzona rzeczywistość (XR) to z kolei termin obejmujący wszystkie technologie immersyjne, w tym rzeczywistość wirtualną, rzeczywistość rozszerzoną i rzeczywistość mieszaną. Systemy VR mogą rejestrować zachowania, takie jak ruchy części różnych części ciała (np. głowa, dłoń, stopy, klatka piersiowa, łokieć lub kolana). Według niektórych autorów, pozycja głowy i ruch mogą być wykorzystywane do wnioskowania o schorzeniach, takich jak zespół nadpobudliwości psychoruchowej, autyzm lub demencja. Tak dużą ilość przetwarzanych danych jest trudno pogodzić z zasadami minimalizacji danych i ograniczenia celu.

Źródło: 23-12-04_techsonar_23-24_en.pdf (europa.eu)

04 Sąd Apelacyjny zmniejsza zadośćuczynienie RODO z 20 000 na 10 000 zł

- Sąd Okręgowy w Warszawie zasądził na rzecz pewnej Obywatelki kwotę 20 000 zł zadośćuczynienia za błąd popełniony przez Naczelny Sąd Administracyjny dotyczący braku anonimizacji danych osobowych.
- Sąd Apelacyjny zmienił to orzeczenie, zmniejszając kwotę 20 000 zł do 10 000 zł.
- Co istotne, Sąd Apelacyjny podzielił i przyjął jako własne ustalenia faktyczne Sądu Okręgowego z niewielkimi korektami, które nie dotyczą meritum postępowania.
- Sąd Apelacyjny dostrzega, że RODO ma zastosowanie dopiero od dnia 25 maja 2018 r. (art. 99 ust. 1 RODO), podczas gdy do opublikowania orzeczenia w wersji niezanonimizowanej doszło w 2016 roku.
- Niemniej jednak należy przyjąć, że stan nieuprawnionego przetwarzania danych osobowych powódki trwał do chwili ich usunięcia, co nastąpiło w 2021 roku, dlatego zasadne jest również dokonanie oceny prawnej na podstawie przepisów RODO;
- Ponadto nie można pomijać tego, że opublikowanie pełnych danych osobowych powódki w Centralnej Bazie Orzeczeń Sądów Administracyjnych było czynem bezprawnym również w roku 2016, gdyż pozostawało w sprzeczności z art. 23 ust. 1 ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922 ze zm.).

Źródło: Judykatura.pl; Opublikuj | LinkedIn

05 Prezes UODO zatwierdził Kodeks postępowania dla sektora ochrony zdrowia

- Prezes Urzędu Ochrony Danych Osobowych zatwierdził „Kodeks postępowania dla sektora ochrony zdrowia" przygotowany przez Polską Federację Szpitali. Podpisany dokument to pierwszy w Europie kodeks obejmujący podmioty publiczne i prywatne z sektora medycznego.
- Dokument przewiduje odrębne mechanizmy monitorowania przestrzegania jego postanowień dla publicznych placówek medycznych. Przystąpienie do kodeksu nie wiąże się z członkostwem w żadnej organizacji.
- W ocenie organu nadzorczego przedstawiony przez Polską Federację Szpitali kodeks postępowania jest zgodny z przepisami ogólnego rozporządzenia o ochronie danych (RODO) oraz stanowi odpowiednie zabezpieczenie w zakresie ochrony danych przewidzianych przepisami tego rozporządzenia. Ważnym aspektem było wypracowanie rozwiązań monitorowania podmiotów publicznych. Jest to pierwszy taki kodeks dla sektora medycznego umożliwiający szpitalom publicznym potwierdzanie zgodności procesu przetwarzania danych z RODO.
- Decyzja Prezesa UODO kończy okres pracy nad treścią kodeksu i daje placówkom medycznym możliwość rozpoczęcia przygotowań do jego wdrożenia.
- Przystąpienie do stosowania kodeksu postępowania wiąże się z licznymi korzyściami. Przede wszystkim podmioty, które będą go stosowały mogą mieć gwarancję prawidłowości używania określonych rozwiązań zatwierdzonych przez organ nadzoru. Mogą też liczyć na nadzór nad procesami przetwarzania danych osobowych w oparciu o mechanizmy monitorowania opisane w kodeksie. Nie bez znaczenia jest również fakt, iż zgodnie z RODO organ nadzorczy, gdy rozważa nałożenie kary na dany podmiot musi brać pod uwagę w każdym przypadku, czy podmiot ten prawidłowo stosuje zatwierdzony kodeks postępowania.
- Organ nadzorczy udzielił akredytacji KPMG Advisory sp. z o.o. sp. k., który będzie pełnił funkcję podmiotu monitorującego stosowanie kodeksu wśród jego członków z sektora prywatnego.

Źródło: Aktualności - UODO