



A large, faint fingerprint pattern is visible in the background of the slide, rendered in a dark blue color that matches the overall theme. The fingerprint is centered and occupies most of the frame.

RODO - aktualności

[18.03.2024]

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

TSUE: Organ nadzorczy może nakazać z urzędu usunięcie danych przetwarzanych niezgodnie z prawem

02

Komisja Europejska na celowniku EIOD. Przez produkt Microsoft

03

PUODO: Propozycje zmiany przepisów o sygnalistach wymagają poprawek

04

Sprzedaż odcisków palców, skanów tęczówki. Wyrok ws. firmy obracającej danymi (Hiszpania)

05

Wyciek danych klientów The North Face

01 TSUE: Organ nadzorczy może nakazać z urzędu usunięcie danych przetwarzanych niezgodnie z prawem

- W 2020 r. urząd dzielnicy Újpest w Budapeszcie podjął decyzję o udzieleniu pomocy finansowej osobom szczególnie narażonym na skutki pandemii COVID-19. W tym celu zwrócił się do węgierskiego skarbu państwa i do urzędu miasta Budapeszt o przekazanie danych osobowych niezbędnych do sprawdzenia warunków kwalifikowalności do uzyskania wsparcia. O wniosku urzędu dzielnicowego ktoś zawiadomił węgierski organ nadzorczy odpowiedzialny za ochronę danych osobowych (odpowiednik polskiego Prezesa Urzędu Ochrony Danych Osobowych). Ten stwierdził, że zarówno urząd dzielnicy Újpest, skarb państwa jak i organ municypalny naruszyły przepisy RODO. I wymierzył im kary pieniężne.
- Jak ustalono, administracja Újpestu, wbrew obowiązkowi wynikającemu z RODO, nie poinformowała (w terminie jednego miesiąca) osób, których dane dotyczą, ani o celach wykorzystywania ich danych, ani o ich prawach w zakresie ochrony danych. W związku z tym urząd dzielnicy dostał nakaz usunięcia danych tych osób kwalifikujących się do pomocy, które o taką pomoc nie wystąpiły.
- Administracja Újpestu zakwestionowała tę decyzję przed budapesztańskim sądem twierdząc, że organ nadzorczy nie ma prawa nakazywać usunięcia danych osobowych bez uprzedniego żądania osoby, której dane dotyczą.
- Organ nadzorczy państwa członkowskiego UE może nakazać z urzędu – tj. nawet bez uprzednio wyrażonego w tym celu żądania osoby, której dane dotyczą – usunięcie danych przetwarzanych niezgodnie z prawem, jeżeli taki środek jest konieczny dla wywiązania się z powierzonego mu zadania polegającego na egzekwowaniu pełnego przestrzegania RODO. Jeżeli organ ten stwierdzi, że przetwarzanie danych nie jest zgodne z RODO, ma wręcz obowiązek usunąć stwierdzone naruszenie, nawet bez uprzedniego żądania osoby, której dane dotyczą. Takie usunięcie może dotyczyć zarówno danych uzyskanych od tej osoby, jak i danych pochodzących z innego źródła - zaznaczył TSUE.

Źródło: [Ważny wyrok TSUE ws. RODO. Chodzi o dane przetwarzane przez urzędy - rp.pl](#)

02 Komisja Europejska na celowniku EIOD. Przez produkt Microsoft

- Europejski Inspektor Ochrony Danych udzielił reprimendy Komisji Europejskiej w związku z naruszeniem przepisów o ochronie danych osobowych. Do złamania obowiązujących zasad miało dojść podczas użytkowania pakietu Microsoft 365.
- Portal The Register przypomina, że śledztwo Europejskiego Inspektora Ochrony Danych (EDPS) rozpoczęło się w maju 2021 roku i trwało trzy lata. Jego efektem jest decyzja dotycząca udzielenia reprimendy na KE.
- Ze stanowiska EDPS wynika, że umowa między Komisją i Microsoftem nie precyzowała, jakie dokładnie rodzaje danych osobowych i w jakim celu będą zbierane podczas używania pakietu Microsoft 365.
- Poza tym, Komisja Europejska zaniedbała kwestię zabezpieczenia danych poza terytorium Unii Europejskiej. Chodzi dokładnie o to, by dane osobowe poza Europą miały zapewniony taki sam poziom ochrony, jak na terytorium Wspólnoty.
- Europejski Inspektor Ochrony Danych wydał również KE dwa nakazy w związku z wykrytymi naruszeniami. Pierwszy z nich dotyczy całkowitego zaprzestania używania pakietu Microsoft 365, a tym samym wstrzymania przepływu danych do amerykańskiego giganta i podległych mu podmiotów spoza UE. Drugi nakaz EIOD zobowiązuje Komisję do poprawienia wszystkich nieścisłości w przetwarzaniu danych podczas korzystania z Microsoft 365 w ten sposób, aby zgadzały się one z przepisami o ochronie danych. Jako termin ten wskazano 9 grudnia 2024 roku.
- Microsoft zapewnia, że europejscy klienci mogą korzystać z pakietu bez obaw o naruszenie przepisów RODO. Zdaniem giganta, problem leży w regulacjach obowiązujących europejskie organy, które są znacznie bardziej restrykcyjne od RODO.

Źródło: [Komisja Europejska na celowniku EIOD. Przez produkt Microsoft | CyberDefence24](#)

03 PUODO: Propozycje zmiany przepisów o sygnalistach wymagają poprawek

- Prezes UODO ma zastrzeżenia do projektu ustawy o ochronie osób zgłaszających naruszenia prawa z dnia 8 stycznia br. wznowiającego proces legislacyjny, który przygotował Minister Rodziny, Pracy i Polityki Społecznej. Swoje uwagi PUODO przekazał Maciejowi Berkowi, Przewodniczącemu Stałego Komitetu Rady Ministrów, jako wskazówki do dalszych prac rządu nad tymi regulacjami.
- Mirosław Wróblewski zwraca uwagę, że projektodawca nie zdecydował się na dopuszczenie anonimowego zgłaszania naruszeń prawa, gdyż zgłoszenie wymaga podania danych, to jednak w innym miejscu projektowanych rozwiązań przewidział ochronę osób, które anonimowo zgłoszą naruszenie. Zdaniem Prezesa UODO to niekonsekwencja i należy skonstruować przepisy jednolicie kształtujące prawa i obowiązki osób, które zgłaszają informacje o naruszeniach prawa.
- Kolejnym brakiem projektowanych rozwiązań jest to, że projektodawca nie określił zakresu danych, które mają służyć do identyfikacji osób zgłaszających naruszenia prawa, jak i osób, których dotyczy takie zgłoszenie. Zdaniem Prezesa UODO określenie w ustawie zakresu danych ujednoliciłoby poszczególne rejestry, do których trafią te dane. Ponadto sam dobór danych do identyfikacji powinien zostać określony z uwzględnieniem zasady minimalizacji danych, określonej w RODO.
- Prezes UODO zwraca też uwagę, że przetwarzanie danych w związku z realizacją celów projektowanej ustawy o ochronie osób zgłaszających naruszenia prawa powinny być uregulowane w jej przepisach, a nie w treści aktów wewnątrzorganizacyjnych. Dotyczy to także określenia w ustawie, a nie w regulaminach czy zarządzeniach, zasad ochrony osób, których dotyczy zgłoszenie oraz innych osób. Określenie w przepisach rangi ustawowy wprowadziłoby jednakowy standard ochrony tożsamości tych osób.

Źródło: [Aktualności - UODO](#)

04 Sprzedaż odcisków palców, skanów tęczówki. Wyrok ws. firmy obracającej danymi (Hiszpania)

- Hiszpański sąd wydał orzeczenie zakazujące sprzedaży danych biometrycznych obywateli. Wyrok dotyczy niemieckiej firmy Worldcoin, która pozyskiwała za kryptowalutę dane biometryczne.
- Decyzja sądu jest werdyktem w sprawie firmy Worldcoin, która wytoczyła proces Hiszpańskiej Agencji Danych Osobowych (AEPD), kiedy ta zakazała spółce nabywania za kryptowalutę danych biometrycznych obywateli.
- W trakcie rozprawy potwierdzono, że spółka Worldcoin pozyskiwała dane dotyczące tęczówki oka, a także twarzy. Nie zawsze, jak ustalono, osoby przekazujące swoje dane w zamian za kryptowalutę wyrażały zgodę na obrót swoimi danymi.
- Hiszpański sąd potwierdził też, że doszło do przypadków pozyskiwania danych biometrycznych od nieletnich, a także od osób nieświadomych tego, że ich dane będą w przyszłości przekazywane innym podmiotom.
- Sąd orzekł, że istnieje konieczność "ochrony danych ogółu ludności", w tym prawa ochrony danych osobowych, przed partykularnym interesem finansowym firmy pozyskującej dane biometryczne.
- Tymczasem według szefostwa Worldcoin skanowanie tęczówek i twarzy osób służy stworzeniu tzw. paszportu ludzkości, który ma pozwolić odróżnić ludzi od sztucznej inteligencji w Internecie, zaś opłaty w kryptowalutach były jedynie formą wynagradzania wolontariuszy.

Źródło: [Sprzedaż odcisków palców, skanów tęczówki. Wyrok ws. firmy obracającej danymi - RMF 24](#)

05 Wyciek danych klientów The North Face

- Firma VF Corp. w styczniu 2024 r. poinformowała o incydencie dotyczącym bezpieczeństwa danych swoich klientów. W tym czasie odnotowano problemy z systemami informatycznymi, które objawiały się utrudnieniami z realizacją zamówień, a nawet anulowaniem części z nich.
- Mimo komunikatu o usunięciu skutków ataku, nie została wówczas udostępniona informacja, jakie dane użytkowników zostały ujawnione. Firma uspokajała potencjalnych poszkodowanych informując, że nie przechowują danych wrażliwych, ani dotyczących płatności. Do cyberataku na VF Corp. przyznała się grupa hakerska ALPHV (lub BlackCat).
- Jak wykazało wewnętrzne śledztwo, cyberprzestępcy mogli dostać się do niektórych danych osobowych klientów takich jak e-mail, imię i nazwisko, numer telefonu, adres rozliczeniowy oraz adres do wysyłki. W niektórych przypadkach mogli oni zyskać także dostęp do historii zamówień, całkowitej wartości zamówienia, a także informacji o wybranej przez użytkownika metodzie płatności. Firma twierdzi jednak, że nie przechowuje żadnych szczegółowych danych, takich jak numer konta czy numer karty płatniczej.
- Firma zapewniła, że zakończono proces usuwania podmiotów atakujących i obecnie wszelkie systemy działają poprawnie.
- Klienci sklepu internetowego The North Face powinni być uczuleni na różnego rodzaju maile i SMS-y wysyłane rzekomo przez firmę. Dane pozyskane przez cyberprzestępców mogą zostać teraz wykorzystane w działaniach phishingowych.

Źródło: [Wyciek danych klientów The North Face – aktualizacja – SATinfo24.pl](#); [Wyciek danych w znanym sklepie internetowym. Ostrzeżenie dla klientów \(radiozet.pl\)](#)

*Niniejszy dokument bez zezwolenia nie może być w żaden sposób wykorzystywany,
w szczególności rozpowszechniany i kopiowany.*