





RODO - aktualności

[20.05.2024]

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

UODO: 240 tys. zł kary dla firmy, której pracownik zgubił pendrive z danymi osobowymi

02

Nasze dane medyczne trafią do chmury. Kluczowy będzie ich operator

03

Stellantis przegrał ze studentką prawa. Za błahy błąd zapłaci 9 mln dolarów odszkodowania

04

Istniejące organy nie wystarczą - Polska potrzebuje urzędu ds. sztucznej inteligencji

05

W jakim przypadku naruszenie DSA będzie równocześnie naruszeniem RODO?

01 UODO: 240 tys. zł kary dla firmy gastronomicznej, której pracownik zgubił pendrive z danymi osobowymi

- Pracownik firmy Res-Gastro zgubił pendrive'a, na którym znajdowały się niezasyfrowane pliki zawierające dane osobowe innego pracownika, a mianowicie imię i nazwisko, adres, obywatelstwo, płeć, data urodzenia, numer PESEL, seria i numer paszportu, numer telefonu, adres e-mail, zdjęcia oraz dane dotyczące wysokości zarobków. Na pendrive'ie znajdowały się też zasyfrowane pliki z danymi finansowymi.
- W toku postępowania firma wykazała, że posiadała dokumenty takie jak rejestr ryzyka czy potwierdzenia przeprowadzania monitorowania procedur RODO. Problemem okazały się jednak zasady korzystania z zewnętrznych nośników danych, w tym ich szyfrowanie. O tym, jak szyfrować pliki, firma informowała pracowników na filmie instruktażowym. A to, jak zauważył UODO, przerzucało na nich odpowiedzialność za sposób przetwarzania danych.
- Prezes UODO ustalił, że firma źle oceniła ryzyko dla danych. Założono, że nośniki danych mogą być skradzione albo zniszczone – nie wzięto jednak pod uwagę tego, że nośnik można po prostu zgubić bez złych intencji.
- Do tego, pomimo zakładania wystąpienia różnych zdarzeń, nie wdrożono rozwiązań kryptograficznych dla ochrony danych osobowych na zewnętrznych nośnikach. Film instruktażowy „w jaki sposób szyfrować pliki na pendrive oraz jakiego programu do tego celu użyć” to za mało wobec zakresu danych przetwarzanych na takich nośnikach.
- Kolejny problem polegał na tym, że firma nie dopełniła obowiązku regularnego mierzenia, testowania i oceniania skuteczności zastosowanych środków bezpieczeństwa.
- Prezes UODO nałożył na Res-Gastro karę finansową w wysokości 238 345 zł.

Źródło: [UODO: 240 tys. zł kary dla firmy, której pracownik zgubił pendrive z danymi osobowymi \(prawo.pl\)](#); [Aktualności - UODO](#)

02 Nasze dane medyczne trafią do chmury. Kluczowy będzie ich operator

- Parlament Europejski 24 kwietnia opowiedział się za przyjęciem rozporządzenia w sprawie europejskiej przestrzeni danych dotyczących zdrowia (European Health Data Space, czyli EHDS). To kolejna po niedawno przegłosowanym AI Act duża reforma, która kształtować będzie ramy systemu e-zdrowia w całej Europie.
- Dane medyczne trafią automatycznie do chmury, a jej operator będzie decydował o tym, komu te informacje - na potrzeby badań czy budowy modelu sztucznej inteligencji - udostępnić. To od kraju członkowskiego Unii Europejskiej będzie zależało, czy będzie nim podmiot publiczny czy prywatny. Każdy kraj ustali także opłaty za dostęp do tych danych, a także to, ile z tych pieniędzy trafi do szpitali i innych podmiotów, które je udostępnią.
- EHDS tworzy ramy prawne dla transgranicznego dostępu personelu medycznego do danych pacjentów przetwarzanych w postaci elektronicznej. Dzięki temu lekarz powinien mieć możliwość uzyskania dokumentacji medycznej przetwarzanej w podmiotach leczniczych w innych państwach UE. Będzie to zatem ułatwienie przy leczeniu zarówno obcokrajowców, jak i Polaków, którzy leczyli się wcześniej za granicą. Podstawowym dokumentem w tym zakresie będzie skrócona karta zdrowia pacjenta (Patient Summary), zawierające kluczowe informacje o stanie zdrowia pacjenta.
- Barię w polskim systemie ochrony zdrowia będzie jednak poziom cyfryzacji podmiotów leczniczych i cyberbezpieczeństwo. Z ostatniego badania stopnia informatyzacji podmiotów wykonujących działalność leczniczą prowadzonego przez Centrum e-Zdrowia we współpracy z Ministerstwem Zdrowia wynika, że wymianę EDM z innymi podmiotami z uwzględnieniem Systemu e-Zdrowie (P1) wdrożyło zaledwie 18 proc. badanych placówek. W konsekwencji dane medyczne gromadzone w systemie ochrony zdrowia są niepełne.

Źródło: [EHDS, czyli dane medyczne w chmurze \(prawo.pl\)](#)

03 Stellantis przegrał ze studentką prawa. Za błahy błąd zapłaci ok. 9 mln dolarów odszkodowania

- W wyniku pozwu zbiorowego koncern Stellantis zgodził się zapłacić 8,95 miliona dolarów odszkodowania za naruszenie ustawy o ochronie konsumentów przed niechcianymi połączeniami telefonicznymi (Telephone Consumer Protection Act - TCPA).
- Sprawa dotyczyła tzw. "cichych" wiadomości głosowych, które w 2018 roku zostały wysłane przez FCA U.S., obecnie część koncernu Stellantis. Wiadomości wysłane do 89 tys. osób zawierały ofertę dotyczącą modelu Chrysler Pacifica Hybrid, co Grigorian (powódka) uznała za naruszenie TCPA. Studentka prawa twierdziła, że wiadomości te nie mogły być zablokowane ani odrzucone przez odbiorców, co było podstawą jej pozwu.
- Początkowo sprawa została odrzucona przez sąd, jednak później apelacja zakończyła się na korzyść Grigorian. Główna argumentacja studentki opierała się na fakcie, że wiadomości te były naruszeniem TCPA, ponieważ odbiorcy nie wyrazili zgody na ich otrzymanie.
- Sąd nie był pewny, jakie szkody te połączenia wyrządziły odbiorcom, jednak Grigorian argumentowała, że czas spędzony na słuchaniu tych wiadomości zamiast na nauce do egzaminu adwokackiego na Florydzie, stanowił dla niej znaczne obciążenie.
- FCA U.S. zgodziło się na ugodę, aby zakończyć spór i zobowiązało się dostarczyć sądowi listę wszystkich potencjalnych członków grupy, którzy zostaną powiadomieni listownie o możliwości otrzymania odszkodowania oraz o sposobie jego uzyskania.
- Mimo że FCA U.S. utrzymywało, że nie zrobiło nic złego, zgodziło się zapłacić osobom, które otrzymały te wiadomości - około 60 dolarów każdej (lub 25 dolarów, jeśli były częścią innego pozwu zbiorowego dotyczącego pojazdów Ram, który również został rozstrzygnięty w ramach tego porozumienia). Łączna kwota odszkodowań, jakie będzie musiał wypłacić koncern, oscyluje w granicach 8,95 miliona dolarów.

Źródło: [Studentka pozwała Stellantis. Koncern zapłaci 9 mln dol. odszkodowania \(moto.pl\)](#)

04 Istniejące organy nie wystarczą - Polska potrzebuje urzędu ds. sztucznej inteligencji

- Akt o sztucznej inteligencji (AI Act) najprawdopodobniej zacznie obowiązywać w połowie czerwca. W Polsce zakończyły się właśnie prekonsultacje koncepcji projektu ustawy. Jednym z istotniejszych postulatów, który zgłoszono w ich trakcie, jest stworzenie nowego urzędu.
- Włochy nie czekając nawet na unijnego prawodawcę, jako pierwsze w Europie przyjęły projekt ustawy w sprawie sztucznej inteligencji. Przewidziano w nim również surowe kary, zwłaszcza za wykorzystywanie wizerunku fałszywie zmienionego przez sztuczną inteligencję. Włoski projekt przewiduje również stworzenie osobnego urzędu, który będzie kompleksowo zajmował się wszelkimi sprawami dotyczącymi sztucznej inteligencji.
- Jak przekazał PAP, włoski minister sprawiedliwości Carlo Nordio, przedstawiając projekt przepisów wyjaśnił, że więzieniem karane będzie tworzenie i rozpowszechnianie (bez uzyskania zgody) filmów i wizerunków zmienionych przy użyciu systemów sztucznej inteligencji i wywołujących szkody (np. deepfake). Jak wskazał, takie posługiwanie się tą technologią może mieć „niszczące” konsekwencje, doprowadzając do stworzenia realistycznego, choć wirtualnego, wizerunku osoby.
- Do wdrożenia AI Actu przygotowuje się również Polska. W ubiegłym tygodniu zakończyły się prekonsultacje, w ramach których do resortu trafiły uwagi 50 podmiotów. Jedną z kwestii, o którą pytano, było to, czy potrzebny jest nowy organ nadzoru rynku, który zająłby się sprawami dotyczącymi sztucznej inteligencji. Zdecydowana większość wypowiedziała się za takim samym rozwiązaniem, jakie będzie wdrażane we Włoszech, a więc za stworzeniem całkowicie nowego urzędu.
- Jak wskazuje resort, organ ten ma m.in: być pojedynczym punktem kontaktowym dla ogółu społeczeństwa, rozpatrywać wnioski dot. zezwolenia na wprowadzenie do obrotu lub oddanie do użytku systemów AI wysokiego ryzyka oraz skargi osób poddanych działaniom systemów AI, przyjmować zgłoszenia dot. poważnych incydentów oraz współpracować z Komisją, forum doradczym oraz Radą ds. AI.

05 W jakim przypadku naruszenie DSA będzie równocześnie naruszeniem RODO?

- Digital Services Act (DSA) to akt o usługach cyfrowych obowiązujący w Unii Europejskiej od 16 listopada 2022 roku. Przedsiębiorcy otrzymali czas na dostosowanie się do nowych wymogów do 17 lutego 2024 roku.
- Nowe wymogi oznaczają, że od platform technologicznych wymaga się usuwania nielegalnych i szkodliwych treści. W przypadku niezastosowania się tzw. dostawców usług pośrednich (np. usługi hostingu) do DSA będzie nakładana grzywna.
- Przepisy DSA odnoszą się m.in. do nielegalnych treści – a te mogą być powiązane z danymi osobowymi. Może to być np. czyjś wizerunek – będący daną osobową w rozumieniu RODO – opublikowany bez zgody tej osoby, a zatem stanowiący nielegalną treść w rozumieniu DSA.
- Teoretycznie jest możliwe, by wobec jednej firmy toczyły się 2 postępowania – przed UKE i przed RODO, natomiast można się spodziewać, że postępowanie na gruncie DSA będzie dla obywatela łatwiejsze. Jeśli zgłosi pani nielegalną treść platformie, na której została ona umieszczona, to platforma – chcąc skorzystać z wyłączenia swojej odpowiedzialności – tę treść od razu usunie. A na tym przede wszystkim zależy osobie, której wizerunek bezprawnie wykorzystano.
- Natomiast firma, która opublikowała zdjęcie, może ponieść odpowiedzialność dopiero na gruncie RODO. W uproszczeniu: DSA pozwala karać i dyscyplinować platformy (niestosujące się do wymogów rozporządzenia), natomiast w odniesieniu do przedsiębiorców korzystających z tych platform nadal będziemy stosować RODO.

Źródło: [Dochodzenie swoich praw będzie łatwiejsze na podstawie DSA niż RODO \[WYWIAD\] - GazetaPrawna.pl](#); [DSA – akt o usługach cyfrowych. O co chodzi i kogo dotyczy? - Tu Dział Prawny \(tudzialprawny.pl\)](#)

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