
LEX ARTIST

RODO - aktualności

[05.12.2023]

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 Największy wyciek danych medycznych w Polsce (ALAB)

02 Czy PUODO może zajmować się Chatem GPT, czyli RODO a AI

03 Organizacja NOYB złożyła do austriackiego organu ochrony danych skargę przeciwko właścicielowi Facebooka i Instagrama

04 Data Act – nowe zasady dostępu do danych

05 Irlandia: nowe wytyczne dla administratorów danych w sprawie prowadzenia monitoringu wizyjnego

06 TSUE: Jedynie zawinione naruszenie RODO może skutkować nałożeniem administracyjnej kary pieniężnej

01 Największy wyciek danych medycznych w Polsce (ALAB)

- Do Internetu trafiły wyniki badań medycznych wykonanych przez ostatnie kilka lat w jednej z największych ogólnopolskich sieci laboratoriów medycznych, firmy ALAB. Wyciek jest skutkiem ataku grupy ransomware.
- W sieci znalazły się dane co najmniej kilkudziesięciu tysięcy Polek i Polaków, którzy od roku 2017 do 2023 wykonywali badania medyczne w sieci ALAB laboratoria. Według serwisu, szerzej nieznana grupa ransomware RA World opublikowała na swoim blogu nie tylko informację o skutecznym włamaniu do firmy ALAB, ale także próbkę wykradzionych danych, a w niej między innymi wyniki ponad 50 tysięcy badań medycznych.
- Wstępna analiza incydentu wykazała, że osoby trzecie w sposób bezprawny mogły uzyskać dostęp do następujących danych osobowych: imię i nazwisko, numer PESEL, data urodzenia, miejsce zamieszkania oraz wynik badania laboratoryjnego.
- Hakerzy domagają się okupu od firmy za to, że nie ujawnią wszystkich przejętych danych. Grożą przy tym, że jeśli nie dostaną pieniędzy, do 31 grudnia opublikują wszystkie wykradzione dane. Jak nieoficjalnie ustaliła PAP, szantażyści zażądali od firmy kilkuset tysięcy dolarów.
- Skutkiem ataku hakerskiego było utrudnienie dostępu do danych informatycznych oraz uniemożliwienie ich automatycznego przetwarzania, gromadzenia i przekazywania.
- Spółka zgłosiła naruszenie do Prezesa Urzędu Ochrony Danych Osobowych oraz poinformowała CERT Polska, Ministerstwo Zdrowia i Centrum E-Zdrowia. Złożyła także zawiadomienie o podejrzeniu popełnienia przestępstwa do Centralnego Biura Zwalczania Cyberprzestępczości.
- Po wycieku danych pacjentów ALAB Laboratoria, zespół CERT Polska wspólnie z Centralnym Ośrodkiem Informatyki zasilił stronę bezpiecznedane.gov.pl numerami PESEL upublicznionymi przez hakerów z grupy "RA World". Każdy może więc łatwo sprawdzić, czy jego dane osobowe są objęte wyciekiem z ALAB.

Źródło: Wyciek danych z ALAB Laboratoria. Hakerzy zażądali kilkuset tysięcy dolarów - RMF 24; Wyciek danych pacjentów ALAB - jak sprawdzić swoje dane? (prawo.pl)

02 Czy PUODO może zajmować się Chatem GPT, czyli RODO a AI

- Już na 6 grudnia b.r. zaplanowana jest następna sesja trilogu, czyli trójstronnych negocjacji między Parlamentem, Komisją a Radą UE, w toku których powstaje ostateczna wersja unijnego rozporządzenia w sprawie sztucznej inteligencji („AI Act").
- Zgodnie z projektem AI Act, w każdym państwie członkowskim UE powinien zostać ustanowiony właściwy, bezstronny organ, którego zadaniem będzie zapewnienie stosowania i wykonania AI Act. Pojawiają się sygnały, że regulatorem stojącym na straży zgodności z AI Act może stać się w Polsce Prezes Urzędu Ochrony Danych Osobowych. Mimo tego, RODO pozostanie w pełni niezależną od AI Act regulacją w zakresie ochrony danych osobowych. Oznacza to, że firmy budujące lub wdrażające systemy oparte na AI będą musiały przestrzegać nakazów i zakazów wynikających zarówno z AI Act, jak i RODO.
- Przetwarzanie danych przez system AI musi być zgodne z ogólnymi zasadami przetwarzania danych zapisanymi w RODO, w szczególności zasadami zgodności z prawem, rzetelności i przejrzystości, zaś dane powinny być zbierane w konkretnych celach i ograniczone do tego, co niezbędne do realizacji tych celów (tzw. minimalizacja danych).
- Ponadto, przetwarzanie danych osobowych przez system oparty na AI musi opierać się na jednej z podstaw określonych w art. 6 RODO – w szczególności taką podstawą może być zgoda, umowa lub uzasadniony interes. Przykładowo, włoski organ ochrony danych dopuścił dalsze przetwarzanie danych osobowych użytkowników systemu Chat GPT dla celów szkolenia algorytmu pod warunkiem, że oparte będzie ono na zgodzie użytkownika lub prawnie uzasadnionym interesie jako podstawie prawnej przetwarzania tych danych.
- Oprócz tego, Firma oferująca usługi z wykorzystaniem sztucznej inteligencji musi spełnić obowiązek informacyjny wynikający z RODO zarówno wobec osób, których dane zostały zebrane i przetworzone na potrzeby uczenia algorytmów, jak i wobec osób fizycznych będących użytkownikami systemu. Osobom, których dane zostały wykorzystane w celu uczenia algorytmów, jak i użytkownikom usługi należy również zapewnić możliwość skorzystania z tzw. praw jednostki przewidzianych w RODO.

Źródło: Czy PUODO może zajmować się Chatem GPT? (prawo.pl)

03 Organizacja NOYB złożyła do austriackiego organu ochrony danych skargę przeciwko właścicielowi Facebooka i Instagrama

- Od początku listopada europejscy użytkownicy dwóch największych serwisów Mety mają do wyboru: albo nadal będą korzystać ze swoich kont na Facebooku i Instagramie za darmo, godząc się, by śledzono ich aktywność internetową w celu personalizacji reklam, albo wykupią subskrypcję.
- Za miesięczny dostęp do konta (lub połączonych kont danego użytkownika) przez stronę internetową trzeba zapłacić 9,99 euro, a za korzystanie z nich w aplikacji – 12,99 euro. Dodatkowo od marca 2024 r. ma obowiązywać dopłata za każde połączone konto: odpowiednio 6 euro lub 8 euro miesięcznie.
- Założona przez prawnika i aktywistę Maxa Schremsa organizacja NOYB (jej nazwa to akronim wyrażenia: „none of your business" – nie twój interes) uważa, że przy opłacie, która przy kontach w obu serwisach może sięgnąć ponad 251 euro rocznie, wybór użytkowników jest pozorny. Co za tym idzie, wyrażona w ten sposób zgoda na zbieranie danych nie spełnia warunku dobrowolności, a to stanowi naruszenie przepisów RODO.
- „Meta wdrożyła dokładne przeciwieństwo prawdziwie wolnego wyboru" – stwierdza NOYB. Z raportu finansowego spółki wynika, że w III kw. tego roku średni kwartalny przychód Facebooka w Europie w przeliczeniu na użytkownika wyniósł 19 dol., podczas gdy dostęp do aplikacji jest dwukrotnie droższy.
- Big tech zmienił podstawę zbierania danych internautów w EOG, bo metody, jakie stosował poprzednio, zostały zakwestionowane przez organy ochrony danych oraz Trybunał Sprawiedliwości Unii Europejskiej – m.in. w efekcie skarg NOYB.
- – Ile osób nadal korzystałoby z prawa do głosowania, gdyby trzeba było za to zapłacić 250 euro? Były czasy, gdy prawa podstawowe przysługiwały tylko bogatym. Wygląda na to, że Meta chce nas cofnąć o ponad 100 lat – uważa Max Schrems.

Źródło: Skarga na Facebooka. "Meta nie daje prawdziwie wolnego wyboru" - GazetaPrawna.pl

04 Data Act – nowe zasady dostępu do danych

- Rada Unii Europejskiej przyjęła w listopadzie br. Rozporządzenie w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (dalej „Data Act"). Regulacja wejdzie w życie jeszcze w grudniu tego roku, a nowe przepisy zaczną obowiązywać po upływie 20 miesięcy, tj. w drugiej połowie 2025 roku.
- Celem Data Act jest m.in. uregulowanie zasad wykorzystania danych wytwarzanych przez urządzenia skomunikowane (takie jak sprzęty użytku domowego, samochody, w tym pojazdy autonomiczne, maszyny rolnicze, inteligentne gadżety, itp.) tak, aby były one przekazywane szerszej grupie podmiotów, co ma zapewnić bardziej sprawiedliwy dostęp do informacji i wspomóc rozwój technologii.
- Dane, które potencjalnie mogą podlegać obowiązkowi przekazania, to przykładowo lokalizacja GPS samochodów, dane dotyczące ilości prądu pobieranego przez sprzęty użytku domowego czy warunków atmosferycznych, zbierane przez urządzenia rolnicze.
- Data Act ma znieść bariery w przepływie danych, w związku z czym zobowiązuje posiadaczy danych (tj. podmioty które uzyskują dostęp do danych, np. producent urządzenia bądź dostawca usług) do ich udostępniania zarówno użytkownikom, odbiorcom danych (czyli innym przedsiębiorcom, w tym konkurentom posiadaczy urządzeń) jak i w niektórych przypadkach organom publicznym. Udostępnienie generowanych przez urządzenie danych osobowych może natomiast nastąpić wyłącznie na wniosek użytkownika.
- Celem Data Act jest także ułatwienie dostępu do danych, a zatem również do danych osobowych. W związku z powyższym, w projekcie przesądzono, że do przepływu w zakresie danych osobowych zastosowanie nadal znajdują w pierwszej kolejności przepisy RODO, a w przypadku kolizji zastosować należy przepisy unijne bądź krajowe regulujące kwestie przetwarzania danych osobowych.
- W przypadku nieprzestrzegania obowiązków wynikających z Data Act grozić będą kary pieniężne, których wysokość ma zostać ustanowiona przez Państwa członkowskie

Źródło: Legal Alert: Data Act – nowe zasady dostępu do danych - KPMG Poland

05 Irlandia: nowe wytyczne dla administratorów danych w sprawie prowadzenia monitoringu wizyjnego

- Wytyczne Komisji Ochrony Danych mają na celu pomóc właścicielom i najemcom lokali, w szczególności tych, które są miejscami pracy lub są w inny sposób publicznie dostępne, w zrozumieniu ich odpowiedzialności i obowiązków w zakresie ochrony danych podczas korzystania z CCTV.
- Przed zainstalowaniem systemu CCTV potencjalni administratorzy danych powinni rozważyć następujące kwestie:

  a) Cel: Czy istnieje jasno określony cel instalacji CCTV

  b) Zgodność z prawem: Jaka jest podstawa prawna korzystania z CCTV

  c) Konieczność: Czy możesz wykazać, że CCTV jest niezbędne do osiągnięcia Twojego celu?

  d) Proporcjonalność: Jeśli system CCTV ma być wykorzystywany do celów innych niż bezpieczeństwa, czy jesteś w stanie wykazać, że te inne zastosowania są proporcjonalne?

  e) Bezpieczeństwo: Jakie środki zostaną wprowadzone w celu zapewnienia, że nagrania CCTV są bezpieczne;

  f) Retencja: Jak długo będą przechowywane nagrania, biorąc pod uwagę, że powinny być przechowywane nie dłużej niż jest to konieczne

  g) Przejrzystość: W jaki sposób osoby zostaną poinformowane o monitoringu

Źródło: Guidance on the Use of CCTV - For Data Controllers | Data Protection Commissioner

06 TSUE: Jedynie zawinione naruszenie RODO może skutkować nałożeniem administracyjnej kary pieniężnej

- Sąd litewski i sąd niemiecki zwróciły się do Trybunału Sprawiedliwości o dokonanie wykładni przepisów RODO w odniesieniu do możliwości nakładania administracyjnej kary pieniężnej przez krajowe organy nadzorcze na administratora danych.
- W sprawie niemieckiej, spółka nieruchomościowa Deutsche Wohnen, która pośrednio posiada około 163 000 lokali mieszkalnych i 3 000 lokali użytkowych lokali mieszkalnych i 3 000 lokali użytkowych, kwestionuje, między innymi, grzywnę w wysokości ponad 14 milionów euro, która została na nią nałożona na nią w wyniku przechowywania danych osobowych najemców przez okres dłuższy niż to konieczne.
- Trybunał orzekł, że administrator danych nie może zostać obciążony administracyjną karą pieniężną za naruszenie RODO, chyba że naruszenie to zostało popełnione bezprawnie, tj. umyślnie lub przez zaniedbanie.
- W przypadku gdy administrator jest osobą prawną, nie jest konieczne, aby naruszenie zostało popełnione przez jego organ zarządzający. Nie jest też konieczne, aby organ ten wiedział o tym naruszeniu. Wręcz przeciwnie, osoba prawna ponosi odpowiedzialność zarówno za naruszenia popełnione przez jej przedstawicieli, dyrektorów lub kierowników, jak i za naruszenia popełnione przez jakąkolwiek inną osobę działającą w ramach działalności tej osoby prawnej i w jej imieniu.
- Oprócz tego, nałożenie administracyjnej kary pieniężnej na osobę prawną jako administratora danych nie może być uzależnione od wcześniejszego ustalenia, że naruszenie zostało popełnione przez zidentyfikowaną osobę fizyczną.
- Ponadto na administratora może zostać nałożona kara w związku z operacjami wykonywanymi przez podmiot przetwarzający, w zakresie, w jakim administrator może zostać pociągnięty do odpowiedzialności za takie operacje.
- Ponadto, w przypadku gdy adresat grzywny należy do grupy spółek, obliczenie tej grzywny powinno opierać się na obrotach całej grupy.

Źródło: Only a wrongful infringement of the General Data Protection Regulation may result in an administrative fine being imposed (europa.eu)