
LEX ARTIST

RODO - aktualności

[13.11.2023]

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 Przedsiębiorcy boją się nowych unijnych regulacji z zakresu cyberbezpieczeństwa

02 Firmie łatwiej będzie zmienić dostawcę chmury. UE przyjęła akt w sprawie danych

03 TSUE: Państwo nie ma pełnej swobody w nakładaniu ograniczeń na platformy

04 Subskrypcje na Facebooku pod lupą organów ochrony danych

05 Cyberatak na największy chiński bank uderzył w amerykańskie obligacje

06 Organizacje biją na alarm ws. rozporządzenia UE o sztucznej inteligencji

07 30 najważniejszych statystyk i faktów dotyczących prywatności na rok 2023

01 Przedsiębiorcy boją się nowych unijnych regulacji z zakresu cyberbezpieczeństwa

- W listopadzie ubiegłego roku Komisja Europejska przyjęła dwa ważne akty prawne mające na celu wzmocnienie cyberbezpieczeństwa i cyberodporności państw członkowskich i organizacji w całym bloku. Pierwszym z nich był Digital Operational Resilience Act (DORA), który obejmuje sektor finansowy i firmy świadczące usługi ICT oraz infrastrukturalne dla podmiotów z sektora finansowego. Drugą była długo oczekiwana aktualizacja dyrektywy w sprawie bezpieczeństwa sieci i systemów informatycznych (NIS), znana jako NIS2.
- Do stosowania NIS2 będą zobowiązane również mikroprzedsiębiorstwa i małe przedsiębiorstwa, które spełnią kryteria wskazujące na ich kluczową rolę dla społeczeństwa, gospodarki lub określonych sektorów lub typów usług.
- Z badań IDC wynika, że prawie co trzecia firma w Europie obawia się dostosowania do nowych unijnych regulacji w obszarze cyberbezpieczeństwa. W Polsce ten wynik jest znacznie wyższy – blisko 41% przedsiębiorców uznaje je za najważniejsze wyzwanie z jakim będą musieli się oni zmierzyć na przestrzeni dwóch lat. Bardzo wysoki odsetek firm obawia się także regulacji w obszarze prywatności danych. Tutaj znów te obawy są znacznie silniejsze i w Polsce – na ten aspekt zwraca uwagą aż 37% firm. Dla porównania, w krajach Europy Zachodniej podobne obawy wyraża 24% firm.
- Szczególnie newralgiczna jest obsługa incydentów. Firmy będą musiały przekazać raport „o wczesnym ostrzeżeniu" w ciągu 24 godzin od momentu jego wykrycia, a następnie przeprowadzić wstępną ocenę w ciągu 72 godzin. Mają miesiąc na przedstawienie ostatecznego raportu. Niedopełnienie tego obowiązku może skutkować karami finansowymi w wysokości od 1,4% globalnego obrotu lub 7 milionów euro (w zależności od tego, która kwota jest wyższa) do 2% globalnego obrotu lub 10 milionów euro w przypadku Istotnych podmiotów. Oprócz kar finansowych, NIS2 przewiduje też odpowiedzialność osobistą za nieprzestrzeganie przepisów. Może ona obejmować czasowy zakaz pełnienia funkcji kierowniczych, w tym na stanowiskach prezesów i rad nadzorczych.

Źródło: Firmy boją się nowych unijnych regulacji - ccnews.pl

02 Firmie łatwiej będzie zmienić dostawcę chmury. UE przyjęła akt w sprawie danych

- Europosłowie przyjęli 9 listopada br. tzw. Akt w sprawie danych, który ma dostosować ochronę danych do nowych technologii i uregulować zasady korzystania z usług chmurowych. To odpowiedź na coraz szybciej rozwijające się nowe technologie i coraz szersze wykorzystywanie sztucznej inteligencji, do którego potrzebne jest przetwarzanie ogromnej ilości danych.
- Nowe unijne prawo to korzystne zmiany dotyczące prostszej zmiany dostawców usług chmurowych (czyli firm oferujących usługi sieciowe, infrastrukturę lub aplikacje biznesowe w chmurze). Wprowadza zabezpieczenia przed nielegalnym międzynarodowym przesyłaniem danych przez te firmy. Na etapie prac zapewniono, że nowy akt umożliwi klientom usług w chmurze możliwość negocjowania umów i unikania „uwiązania" z konkretnym dostawcą, a dodatkowo zapewni sprawną i szybką procedurę zmian.
- Istotne będą również przepisy i środki zapobiegające nadużywaniu nierównowagi umownej, które utrudniają sprawiedliwą wymianę danych. Małe i średnie firmy mają być chronione przed narzucaniem niekorzystnych warunków umownych przez silniejszych graczy - mają w tym pomóc m.in. wzorcowe klauzule umowne, które opracuje Komisja Europejska. Z drugiej strony, szersze uprawnienia w niektórych sytuacjach ma zyskać sektor publiczny (czyli organy państwowe i unijne).
- Jeżeli do zapewnienia bezpieczeństwa konieczne będzie skorzystanie z prywatnych danych przedsiębiorstw, organy wyjątkowo będą mogły z nich skorzystać. Posiadacz danych będzie musiał udostępnić je bez zbędnej zwłoki, co do zasady nieodpłatnie. Przepisy są jednak tak skonstruowane, żeby ograniczyć takie sytuacje do wyjątkowych, niezbędnych przypadków.

Źródło: Firmie łatwiej będzie zmienić dostawcę chmury. UE przyjęła akt w sprawie danych (prawo.pl)

03 TSUE: Państwo nie ma pełnej swobody w nakładaniu ograniczeń na platformy

- Państwo członkowskie nie może nałożyć na dostawcę platformy komunikacyjnej mającego siedzibę w innym państwie członkowskim generalnych i abstrakcyjnych obowiązków. Takie podejście krajowe jest sprzeczne z prawem Unii Europejskiej, które gwarantuje swobodny przepływ usług - uznał Trybunał Sprawiedliwości Unii Europejskiej w sprawie, która dotyczyła m.in. Google i Facebooka.
- w 2021 r. Austria wprowadziła ustawę zobowiązującą krajowych i zagranicznych dostawców platform komunikacyjnych do ustanowienia mechanizmów zgłaszania i weryfikacji potencjalnie nielegalnych treści. Przewiduje ona m.in. regularną i przejrzystą publikację zgłoszeń. dotyczących nielegalnych treści. Organ administracyjny zapewnia przestrzeganie przepisów ustawy i może nakładać grzywny w wysokości nawet do 10 mln euro.
- Google Ireland, Meta Platforms Ireland i TikTok, trzy platformy mające siedzibę w Irlandii, stwierdziły, że austriacka ustawa jest sprzeczna z prawem Unii, a mianowicie z dyrektywą o usługach społeczeństwa informacyjnego.
- TSUE zauważył, że państwa członkowskie inne niż państwo pochodzenia danej usługi nie mogą przyjmować środków o charakterze generalnym i abstrakcyjnym, mających zastosowanie, bez rozróżnienia, do każdego podmiotu świadczącego usługi społeczeństwa informacyjnego należące do danej kategorii. Możliwość przyjęcia generalnych i abstrakcyjnych obowiązków podważałaby zasadę kontroli w państwie pochodzenia danej usługi, na której opiera się dyrektywa.
- Gdyby państwo członkowskie przeznaczenia (w tym wypadku Austria) było uprawnione do przyjęcia takich środków, stanowiłoby to ingerencję w kompetencje regulacyjne państwa, z którego pochodzi usługa (w tym wypadku Irlandii).

Źródło: TSUE: Regulacje danego państwa nie mogą naruszać swobodnego przepływu usług (prawo.pl)

04 Subskrypcje na Facebooku pod lupą organów ochrony danych

- Facebook i Instagram zaczęły stawiać swoich użytkowników w Europejskim Obszarze Gospodarczym (EOG – państwa Unii Europejskiej oraz Norwegia, Islandia i Liechtenstein) przed wyborem: albo zapłacą za dostęp do serwisu, albo nadal będą korzystać za darmo – godząc się, by śledzono ich aktywność pod kątem doboru reklam.
- Dotychczas obie platformy wszystkim wyświetlały reklamy, przy czym przetwarzanie danych w celu targetowania reklamy behawioralnej (tj. dopasowanej do zainteresowań) opierały na tzw. uzasadnionym interesie, o którym mówi RODO. Jednak w lipcu br. Trybunał Sprawiedliwości Unii Europejskiej orzekł, że narusza to przepisy i Meta musi wprost pytać internautów o zgodę na śledzenie (sprawa C-252/21). W sierpniu zbierania danych w celach reklamowych bez uzyskania zgody użytkownika zakazał koncernowi organ ochrony danych w Norwegii (Datatilsynet), a w końcu października na jego wniosek Europejska Rada Ochrony Danych (EROD) zleciła organowi w Irlandii rozszerzenie zakazu na cały obszar EOG.
- Wyrok TSUE dopuszcza wprowadzenie świadczenia usług za opłatą jako alternatywy dla zgody na zbieranie danych. Kluczowe w takiej sytuacji jest jednak zapewnienie, aby była to alternatywa równoważna. Część ekspertów ma co do tego wątpliwości – wskazując na wysoką cenę subskrypcji. Za miesięczny dostęp do konta (lub połączonych kont danego użytkownika) przez stronę internetową trzeba bowiem zapłacić 9,99 euro, a za korzystanie z aplikacji – 12,99 euro.
- „Wiele osób wyraziło sceptycyzm co do tego, czy nowe rozwiązanie Meta spełnia te wymagania" – stwierdza norweski organ, dodając, że jest zaniepokojony rozwojem sytuacji. Facebookową wersję modelu „pay or okay" analizuje też organ ochrony danych w Hamburgu.

Źródło: Subskrypcje na Facebooku pod lupą organów ochrony danych - GazetaPrawna.pl

05 Cyberatak na największy chiński bank uderzył w amerykańskie obligacje

- Spółka zależna Industrial and Commercial Bank of China został zaatakowany przez hakerów na tyle poważnie, że zakłócono działanie niektórych systemów, rzekomo ograniczając płynność amerykańskich obligacji skarbowych. Trwa dochodzenie w sprawie incydentu.
- Industrial and Commercial Bank of China jest jednym z największych chińskich banków. Według S&P należy do wielkiej czwórki. Co więcej, jest też największym na świecie pożyczkodawcą pod względem aktywów.
- Atak polegał na zablokowaniu systemów i żądania okupu za ich odblokowanie. Co za tym idzie, mógł on mieć wpływ na zdolność banku do rozliczania transakcji lub prowadzić do przekierowań, co z kolei miały wpływ na płynność rynku skarbowym lub zdolności do szybkiego handlu aktywami.
- Co najmniej jeden bank BNY Mellon z powodu cyberataku ręcznie rozliczał transakcje z ICBC.
- Nie jest jasne, czy incydent przyczynił się do słabej aukcji 30-letnich obligacji, która została w czwartek przeprowadzona przez Departament Skarbu USA. Doszło bowiem do "ostrej przeceny". - Aukcja amerykańskich obligacji niosła ze sobą wiele zmienności, pytań i niepewności - opisała starsza analityk Swissquote Banku Ipek Ozkardeskaya.
- Do ataku przyznała się grupa znana jako LockBit, składająca się m.in. z rosyjskojęzycznych członków. Jeden z podmiotów, wchodzących w jej skład, ma z kolei siedzibę w Chinach. Zakłócono nim handel amerykańskimi obligacjami, którymi żywo zainteresowany jest rząd Chin. Stąd też zdaniem ekspertów można wysnuć wniosek, że hakerzy „nadepnęli Pekinowi na odcisk", który będzie chciał ukarać odpowiedzialnych.

Źródło: Cyberatak na największy chiński bank uderzył w amerykańskie obligacje - Bankier.pl

06 Organizacje biją na alarm ws. rozporządzenia UE o sztucznej inteligencji

- Wersja rozporządzenia o sztucznej inteligencji (AI Act) przyjęta przez Parlament Europejski zakłada całkowity zakaz systemów zdalnego rozpoznawania twarzy. Organizacje pozarządowe biją na alarm, że może on zostać zniesiony w czasie tzw. trilogu (trójstronne negocjacje między Parlamentem, Komisją a Radą UE).
- Jednym z kluczowych założeń AI Act był całkowity zakaz m.in. systemów AI do zdalnej identyfikacji biometrycznej. W maju Parlament Europejski odrzucił poprawki mające wprowadzić możliwość stosowania takich technologii np. w celu odnajdywania zaginionych osób i zwalczania terroryzmu lub innych poważnych przestępstw. Teraz jednak pomysł poluzowania zakazu wrócił w trilogu, podnoszony przez niektóre państwa członkowskie.
- Jak informuje portal Euroactive, miałoby to być dopuszczalne w ściganiu przestępstw z zamkniętej listy, zagrożonych karą powyżej pięciu lat więzienia. System musiałby przejść ocenę wpływu na prawa podstawowe, a jego użycie byłoby zatwierdzane przez sąd (czasem ex post w ciągu 48 godz.).
- Eksperci wskazują na fakt, że międzynarodowe standardy praw człowieka wymagają, żeby każda ingerencja w nie była niezbędna i proporcjonalna. Wspomniane systemy zaś jej zdaniem nie spełniają tych wymogów, ponieważ istnieją bardziej skuteczne i mniej ingerujące w prawo do prywatności metody utrzymywania bezpieczeństwa. Naruszają one istotę prawa do prywatności, a przez to i innych praw obywatelskich, np. wolności słowa i zgromadzeń.
- Potwierdził to europejski inspektor ochrony danych osobowych, który podniósł, że to zastosowanie sztucznej inteligencji pozbawia ludzi anonimowości w przestrzeni publicznej, niezbędnej do tego, żeby bezpiecznie protestować i wyrażać obywatelskie niezadowolenie bez obawy o potencjalne reperkusje.

Źródło: Rozporządzenie o sztucznej inteligencji przyjęte przez PE. Organizacje biją na alarm - rp.pl

07 Garść najważniejszych statystyk dotyczących prywatności na rok 2023

- 63% konsumentów na całym świecie uważa, że firmy nie są uczciwe w kwestii tego, jak wykorzystują ich dane osobowe, a prawie 48% przestało korzystać z usług firm z powodu obaw o prywatność.
- 33% użytkowników zerwało więzi z firmami z powodu obaw o prywatność. Przestali korzystać z mediów społecznościowych, dostawców usług internetowych, sklepów, firm obsługujących karty kredytowe i instytucji finansowych.
- Wielu konsumentów uważa, że nie otrzymuje wystarczających informacji o tym, jak firmy wykorzystują ich dane. 43% konsumentów zgłosiło brak bezpieczeństwa danych, a 79% uważa, że śledzenie, w jaki sposób różne firmy wykorzystują ich dane osobowe, jest zbyt skomplikowane.
- 71% krajów na całym świecie posiada przepisy dotyczące ochrony danych osobowych, a tylko 15% ich nie ma.
- Firmy odnotowują średni zwrot z inwestycji (ROI) w wysokości 1,8% z wydatków związanych z prywatnością, a 92% przyznaje, że ma moralny obowiązek uczciwego i przejrzystego wykorzystywania danych konsumentów.
- 60% konsumentów twierdzi, że wydałoby więcej pieniędzy na markę, której ufają, aby odpowiedzialnie obchodzić się z ich danymi osobowymi.
- 11% firm potrzebowało do 6 miesięcy lub roku (5%) na poinformowanie konsumenta o naruszeniu ochrony danych osobowych.
- 33% konsumentów na całym świecie doświadczyło naruszenia bezpieczeństwa danych.
- 54% konsumentów uważa, że firmy powinny być zmuszone do wprowadzenia obowiązkowych środków zabezpieczających dane osobowe, takich jak szyfrowanie i uwierzytelnianie dwuskładnikowe po naruszeniu ochrony danych osobowych.

Źródło: 30 most important privacy statistics and facts for 2023 (dataguard.co.uk)