
LEX ARTIST

RODO - aktualności

Data publikacji: 31.10.2024

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 NSA: trzy miesięczny termin z RODO odnosi się do rozpatrzenia skargi

02 Opublikowano wytyczne EROD dotyczące stosowania art. 5(3) dyrektywy ePrivacy do różnych rozwiązań technicznych

03 "Nie da się zawrzeć umowy tylko trochę albo niechcący". Bezprecedensowy wyrok w sprawie cyberoszustwa

04 Oszuści doskonale znają polskie realia. Jak się przed nimi chronić?

05 Ochrona danych osobowych a bezpieczeństwo państwa – wnioski po seminarium UODO i ZUS

06 Polskie przepisy o sztucznej inteligencji będą przyjmować się powoli

07 Dane z ksiąg wieczystych będą lepiej chronione

08 Atak hakerski na Super-Pharm. Wyciekły dane klientów

09 WSA: nowa, wyższa kara za naruszenie danych osobowych jest prawidłowa

10 Koniec 6-letniej epopei. LinkedIn ukarany za naruszenie RODO

11 WSA podziela stanowisko Prezesa UODO, co do zgody na kanał komunikacji

12 Takiej kary świat nie widział. Google musi zapłacić Rosji 2 undecyliony rubli

LEX ARTIST

Czytaj. Wdrażaj. Automatyzuj.

RODOLOGIA + SODO

tylko do 29.11.24!

- Autorska koncepcja pięciu filarów
- Prosty język, przykłady i schematy
- Gotowe sprawdzone rozwiązania
- Myślenie procesowe by default
- Automatyzacja rozwiązań
- Ponad 500 stron w jakości premium

www.rodologia.com.pl

01 NSA: trzy miesięczny termin z RODO odnosi się do rozpatrzenia skargi

- **Kontekst**: **sprawy**: Artykuł omawia orzeczenie Naczelnego Sądu Administracyjnego (NSA) dotyczące terminów, w jakich organ nadzorczy (Prezes Urzędu Ochrony Danych Osobowych, UODO) powinien reagować na skargi obywateli w świetle przepisów RODO.
- **Początek postępowania**: Skarga została złożona przez obywatela na przetwarzanie jego danych osobowych przez spółkę P. S.A. na rzecz Ubezpieczeniowego Funduszu Gwarancyjnego (UFG). Procedura skargowa rozpoczęła się we wrześniu 2021 roku.
- **Korespondencja organów**: Prezes UODO skierował prośby o wyjaśnienia do P. i UFG już w październiku 2021 roku, ale odpowiedzi w tej sprawie były opóźnione, co następnie skutkowało skargą obywatela na przewlekłość postępowania.
- **Skarga na przewlekłość**: W grudniu 2021 roku skarżący wniosł do Wojewódzkiego Sądu Administracyjnego w Warszawie skargę na przewlekłość i bezczynność organu, domagając się m.in. wyznaczenia terminu wydania decyzji oraz ukarania UODO za naruszenia.
- **Orzeczenie WSA**: Sąd stwierdził przewlekłość w postępowaniu, ale oddalił wniosek o rażące naruszenie prawa oraz inne żądania skarżącego. UODO zostało zobowiązane do zwrotu 100 zł kosztów postępowania.
- **Odwołanie do NSA**: Naczelny Sąd Administracyjny uchylił wyrok WSA w zakresie dotyczący przewlekłości i kosztów postępowania.
- **Wykładnia NSA**: NSA podkreślił, że art. 78 ust. 2 RODO określa trzymiesięczny termin nie tylko do poinformowania skarżącego o postępach, ale także do rozpatrzenia skargi, co oznacza wydanie decyzji administracyjnej.
- **Znaczenie wyroku**: Wyrok NSA ma istotne znaczenie dla praktyki działania organów nadzorczych z zakresu ochrony danych osobowych w Polsce oraz określa konkretne obowiązki czasowe wynikające z RODO..

Źródło: https://judykatura.pl/nsa-trzy-miesieczny-termin-z-rodo-odnosi-sie-do-rozpatrzenia-skargi/

02 Opublikowano wytyczne EROD dotyczące stosowania art. 5(3) dyrektywy ePrivacy do różnych rozwiązań technicznych

- **Wprowadzenie.** Wytyczne Europejskiej Rady Ochrony Danych (EDPB) dotyczą stosowania art. 5(3) dyrektywy ePrivacy do różnych rozwiązań technicznych. Rozszerzają one opinię Grupy Roboczej Art. 29 z 2014 roku dotyczącą stosowania dyrektywy ePrivacy do odcisków palców urządzeń i mają na celu zapewnienie jasnego zrozumienia operacji technicznych objętych art. 5(3) dyrektywy ePrivacy.
- Kluczowe elementy stosowania art. 5(3) dyrektywy ePrivacy

1. Informacje: Termin "informacje" obejmuje zarówno dane osobowe, jak i nieosobowe. Ochrona prywatności użytkowników obejmuje wszelkie informacje przechowywane na urządzeniach końcowych, niezależnie od tego, czy są to dane osobowe.
2. Urządzenie końcowe użytkownika: Obejmuje każde urządzenie podłączone do publicznej sieci komunikacyjnej. Definicja obejmuje każde urządzenie zdolne do połączenia z publiczną siecią komunikacyjną, niezależnie od tego, czy jest aktualnie połączone.
3. Dostęp i przechowywanie informacji: Dotyczy zarówno przechowywania informacji, jak i uzyskiwania dostępu do już przechowywanych informacji. Przechowywanie informacji odnosi się do umieszczania informacji na fizycznym nośniku pamięci będącym częścią urządzenia końcowego użytkownika.

- Informacje
- Zakres: Ochrona prywatności użytkowników obejmuje wszelkie informacje przechowywane na urządzeniach końcowych, niezależnie od tego, czy są to dane osobowe. Przykłady: Scenariusze obejmują przechowywanie wirusów na urządzeniu użytkownika, co pokazuje, że definicja terminu "informacje" nie powinna być ograniczona do danych osobowych.

Źródło: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en

02 cd. Opublikowano wytyczne EROD dotyczące stosowania art. 5(3) dyrektywy ePrivacy do różnych rozwiązań technicznych

- Urządzenie końcowe użytkownika
- **Definicja**: Urządzenie końcowe to każde urządzenie podłączone do interfejsu publicznej sieci telekomunikacyjnej w celu wysyłania, przetwarzania lub odbierania informacji.
- **Ochrona**: Ochrona prywatności użytkowników obejmuje nie tylko poufność ich informacji, ale także integralność urządzeń końcowych użytkowników.
- Przechowywanie informacji
- **Definicja**: Przechowywanie informacji odnosi się do umieszczania informacji na fizycznym nośniku pamięci będącym częścią urządzenia końcowego użytkownika.
- **Zakres**: Obejmuje wszelkie informacje przechowywane na urządzeniu końcowym, niezależnie od źródła lub charakteru tych informacji.
- Śledzenie URL i pikseli
- **Opis**: Piksel śledzący to hiperłącze do zasobu, zwykle pliku graficznego, osadzone w treści, takiej jak strona internetowa lub e-mail.
- **Zastosowanie**: Piksele śledzące mogą być używane do śledzenia aktywności użytkowników, np. kiedy odbiorca otwiera e-mail.
- **Wnioski.** Wytyczne mają na celu wyjaśnienie technicznego zakresu stosowania art. 5(3) dyrektywy ePrivacy, aby zapewnić lepszą ochronę prywatności użytkowników w kontekście nowych technologii śledzenia.

Źródło: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-22023-technical-scope-art-53-eprivacy-directive_en

03 "Nie da się zawrzeć umowy tylko trochę albo niechcący". Bezprecedensowy wyrok w sprawie cyberoszustwa

- **Kontekst**: Ofiara padła ofiarą cyberoszustwa, w wyniku którego przestępcy zaciągnęli na nią kredyty o wartości 80 tys. zł, wykorzystując narzędzie AnyDesk do zdalnego przejęcia jej komputera. Bank początkowo zażądał spłaty zadłużenia od ofiary, jednak po 3 latach sąd orzekł na jej korzyść.
- **Przebieg oszustwa**: Oszuści przekonali ofiarę, że zarobiła na rzekomych inwestycjach i potrzebne jest zainstalowanie dodatkowego oprogramowania (AnyDesk), aby wypłacić zyski. Następnie przejęli kontrolę nad jej komputerem, zaciągnęli pożyczki oraz przelali pieniądze za granicę.
- **Reakcja banku**: Bank odmówił anulowania pożyczek zaciągniętych przez oszustów, a także nie uznał reklamacji poszkodowanej. Postępowanie karne zostało umorzone z braku wykrycia sprawców.
- **Sprawa sądowa**: Poszkodowana wniosła pozew przeciwko bankowi, argumentując, że instytucja nie zareagowała w odpowiedni sposób na podejrzane transakcje. Mimo wyraźnie nietypowej aktywności na koncie (nagłe zadłużenie i przelewy zagraniczne), bank nie zablokował operacji ani nie skontaktował się z klientką w celu weryfikacji transakcji.
- **Wyrok sądu**: Sąd Okręgowy w Rybniku uznał, że bank nie wypełnił swojego obowiązku ochrony środków klienta. Wyrok ten jest prawomocny i prawdopodobnie pierwszy w Polsce dotyczący zaciągnięcia przez oszustów pożyczek w bankowości elektronicznej.
- **Znaczenie wyroku**: Wyrok może stanowić precedens w sprawach odpowiedzialności banków za transakcje zainicjowane przez oszustów. W innych przypadkach spłata środków była przeważnie związana z kradzieżą z kont, a nie kredytami zaciąganymi przez oszustów.
- **Problemy prawne**: Przed sądem pojawiły się trudności, m.in. związane z dostępem do logów bankowych, a także z opiniami biegłych, przez co sprawa trwała ponad trzy lata.

Źródło: https://www.bankier.pl/wiadomosc/Oszusci-zaciagneli-na-nia-kredyt-Bank-kazal-go-splacic-ale-przegral-w-sadzie-8829092.html

04 Oszuści doskonale znają polskie realia. Jak się przed nimi chronić?

- Przestępcy finansowi szybko dostosowują treść swoich kampanii do aktualnych wydarzeń i rynkowych trendów, co sprawia, że są trudni do uchwycenia.
- Na początku roku przestępcy często wykorzystywali wizerunki polityków (np. w czasie popularności Sejmflixa), natomiast w późniejszym okresie roku coraz częściej pojawiały się reklamy z wizerunkami celebrytów.
- Oszuści stosują różnorodne metody działania: od słabo znających technologię indywidualnych przestępców po zorganizowane grupy ze specjalizacjami (technologie, skrypty, dzwonienie). Mogą operować zarówno w kraju, jak i za granicą.
- Oszuści na bieżąco zmieniają treść kampanii, gdy społeczeństwo nabiera świadomości określonych schematów oszustw – np. zmieniają reklamy z Baltic Pipe na te wykorzystujące celebrytów.
- W oszukańczych komunikatach charakterystyczne są błędy językowe lub nienaturalne sformułowania, co pomaga je rozpoznać (np. "12 tysiąców", "pioniodze").
- Przestępcy działają w grupach międzynarodowych – część operacji odbywa się za granicą (np. call center), ale aktywności w Polsce, takie jak wypłacanie pieniędzy, mogą być zlecone lokalnym osobom.
- W przestępczych kampaniach coraz częściej używa się wizerunków znanych osób, aby nadać fałszywym treściom większej wiarygodności.

Źródło: https://www.bankier.pl/wiadomosc/Oszusci-doskonale-znaja-polskie-realia-Jak-chronic-sie-przed-oszustwami-w-Polsce-8831195.html

04 cd. Oszuści doskonale znają polskie realia. Jak się przed nimi chronić?

- Wzrost świadomości społeczeństwa o scamach jest kluczowy. Dzięki zgłoszeniom użytkowników, przestępcze strony są szybciej blokowane – to powoduje, że oszuści muszą ponosić coraz większe koszty ich działalności.
- Rośnie liczba zgłoszeń dotyczących oszustw – w pierwszej połowie 2023 r. zgłoszono 53 tys. podejrzanych stron, wobec 79 tys. zgłoszeń w całym 2023r.
- Od sierpnia 2023 r. można zgłaszać próby oszustw przez aplikację mObywatel, a od zeszłego roku dostępna jest specjalna infolinia pod numerem 8080.

Źródło: https://www.bankier.pl/wiadomosc/Oszusci-doskonale-znaja-polskie-realia-Jak-chronic-sie-przed-oszustwami-w-Polsce-8831195.html

05 Ochrona danych osobowych a bezpieczeństwo państwa – wnioski po seminarium UODO i ZUS

- **Data i miejsce wydarzenia**: 7 października w Centrali ZUS w Warszawie odbyło się seminarium „Ochrona danych jako element odporności społeczeństwa i państwa".
- **Główne organizacje**: Urząd Ochrony Danych Osobowych (UODO), Zakład Ubezpieczeń Społecznych (ZUS), Społeczny Zespół Ekspertów przy PUODO.
- **Tematy seminarium**:
- Wzrost liczby cyberataków – szczególnie w kontekście konfliktów międzynarodowych, takich jak wojna w Ukrainie i konflikt na Bliskim Wschodzie.
- Nowe metody ataków phishingowych i socjotechnicznych.
- Wpływ wycieków danych osobowych na dezinformację oraz procesy demokratyczne.
- Rola nowych technologii (np. sztuczna inteligencja, dane biometryczne) w kształtowaniu wyzwań dla ochrony prywatności.
- **Znaczenie Europejskiego Miesiąca Cyberbezpieczeństwa**: Seminarium odbyło się w ramach tej inicjatywy, której celem jest popularyzacja wiedzy oraz promowanie dobrych praktyk w zakresie cyberbezpieczeństwa.
- **Edukacja jako klucz do bezpieczeństwa**: Techniki zwiększania cyberhigieny: częste zmienianie haseł, ostrożność w korzystaniu ze sprzętu służbowego do celów prywatnych, edukacja pracowników i młodzieży.
- **Rola współpracy**:
- Współpraca organów publicznych (UODO, CSIRT) i sektora prywatnego ma kluczowe znaczenie w zwiększaniu odporności na cyberataki.

Źródło: https://uodo.gov.pl/pl/138/3396

05 cd. Ochrona danych osobowych a bezpieczeństwo państwa – wnioski po seminarium UODO i ZUS

- Znaczenie dyrektywy NIS2 w podnoszeniu poziomu bezpieczeństwa operatorów usług kluczowych, takich jak energetyka czy bankowość.
- Wzrost liczby incydentów cybernetycznych: Wzrost liczby zgłoszonych incydentów ochrony danych – od 10 tysięcy w 2020 roku, do 80 tysięcy do września 2024 roku, co świadczy o rosnącej skali zagrożeń.
- Phishing – duże zagrożenie: Podkreślono rozwój technik phishingowych poprzez podszywanie się pod firmy kurierskie, urzędy administracji czy znajomych ofiary w celu wyłudzenia danych logowania.
- Rozwój Systemu S46: Projekt wspierający podniesienie poziomu cyberbezpieczeństwa w Polsce, zgodny z Ustawą o Krajowym Systemie Cyberbezpieczeństwa (KSC).
- Nowe regulacje i wsparcie UODO: Zapowiedziano system „jednego okienka", który ułatwi proces zgłaszania naruszeń ochrony danych oraz poprawi współpracę z instytucjami Unii Europejskiej.
- Najważniejsze wnioski:
- Potrzeba wzmocnienia regulacji prawnych z uwagi na zmieniające się technologie i nowe zagrożenia cybernetyczne.
- Konieczność zwiększenia współpracy międzynarodowej i usprawnienia procedur reagowania na incydenty.
- Zwiększenie świadomości obywateli i edukacja pracowników publicznych w zakresie ochrony danych osobowych..

Źródło: https://uodo.gov.pl/pl/138/3396

06 Polskie przepisy o sztucznej inteligencji będą przyjmować się powoli

- Kontekst: – Artykuł porusza temat wprowadzania nowej ustawy o systemach sztucznej inteligencji (SSI), której celem jest dostosowanie polskiego prawa do unijnego rozporządzenia 2024/1689 (Artificial Intelligence Act, AIA). Ma to na celu zapewnienie bezpiecznego i etycznego wykorzystania sztucznej inteligencji.
- Stopniowe wdrażanie przepisów – Eksperci uspokajają, że regulacje będą wprowadzane stopniowo. Kluczowe terminy dotyczące implementacji przepisów obejmują m.in. 2 sierpnia 2025 r., kiedy to zaczną obowiązywać przepisy o krajowych organach nadzorujących rynek.
- Nowy organ nadzorczy: KRiBSI – Projekt ustawy przewiduje powołanie Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji (KRiBSI). Będzie ona monitorować rynek, wspierać przedsiębiorców, a także nadzorować przestrzeganie przepisów związanych z AI.
- Decyzje komisji i rola sądu – Odwołania od decyzji KRiBSI będą rozpatrywane przez sąd ochrony konkurencji i konsumentów, co jest oceniane pozytywnie przez ekspertów ze względu na specyficzną wiedzę wymaganą w takich sprawach.
- Regulacje dla określonych podmiotów – Nowa ustawa ma dotyczyć głównie przedsiębiorców korzystających z systemów sztucznej inteligencji w działalności zawodowej, w tym także małych i średnich przedsiębiorstw (MŚP). Wyłączone z regulacji będą systemy SI wykorzystywane przez osoby fizyczne na własne potrzeby.
- Kategorie ryzyka w systemach AI – Przyszłe kontrole KRiBSI będą skierowane przede wszystkim na systemy wysokiego ryzyka, systemy generatywne oraz te, które wymagają dodatkowych obowiązków informacyjnych. Większość innych systemów AI pozostanie poza zakresem tej regulacji, ale może podlegać innym przepisom, np. RODO.

Źródło: https://www.prawo.pl/biznes/ustawa-o-sztucznej-inteligencji-skierowana-do-konsultacji,529563.html

07 Dane z ksiąg wieczystych będą lepiej chronione

- **Kontekst**: Prezes Urzędu Ochrony Danych Osobowych (UODO), Mirosław Wróblewski, wspiera wprowadzenie systemu uwierzytelniania przed uzyskaniem dostępu do bazy danych ksiąg wieczystych.
- **Cele zmian**: Wprowadzenie obowiązku uwierzytelniania ma na celu utrudnienie masowego i automatycznego pobierania danych osobowych oraz zapewnienie lepszej ochrony tych danych, zgodnie z wymaganiami RODO.
- **Obecny problem**: Model jawności ksiąg wieczystych przyjęty w Polsce 11 lat temu umożliwia powszechny dostęp do danych osobowych przez Internet, co stwarza ryzyko ich wykorzystywania przez podmioty komercyjne w sposób niezgodny z przeznaczeniem.
- **Zagrożenia**: Generalny Inspektor Ochrony Danych Osobowych (GIODO) już w 2010 roku ostrzegał przed potencjalnym masowym wykorzystaniem danych z ksiąg wieczystych przez firmy, co mogło prowadzić do tworzenia narzędzi do wyszukiwania danych osobowych oraz ich łącznia z bazami spoza jurysdykcji Polski.
- **Wdrażanie ochrony**: UODO wielokrotnie sygnalizował potrzebę zmiany modelu udostępniania danych, a obecna propozycja Ministerstwa Sprawiedliwości przewiduje systematyczne wprowadzenie obowiązku uwierzytelniania użytkowników.
- **Współpraca z Ministerstwem**: W odpowiedzi na kroki Ministerstwa Sprawiedliwości, UODO wspiera wszelkie inicjatywy mające na celu poprawę ochrony danych osobowych w księgach wieczystych.
- **Korzyści ze zmian**: Proponowane rozwiązanie ograniczy używanie zautomatyzowanych narzędzi do pobierania danych oraz ułatwi wdrożenie technicznych zabezpieczeń, które są wymagane przez art. 24 ust. 1 RODO.

Źródło: https://uodo.gov.pl/pl/138/3402

08 Atak hakerski na Super-Pharm. Wyciekły dane klientów

- **Atak hakerski na Super-Pharm**: Hakerzy wykorzystali lukę w systemie Adobe Commerce obsługiwanym przez zewnętrznego dostawcę, co doprowadziło do wycieku danych klientów drogerii i aptek Super-Pharm.
- **Komunikat do klientów**: Firma poinformowała o incydencie 25 października, wysyłając maila do klientów, w którym przeproszono za niedogodności i zapewniono o podjętych działaniach bezpieczeństwa.
- **Zakres wycieku**: Wyciek danych dotyczył bazy z danymi klientów, w tym zamówień, imienia, nazwiska, adresu e-mail, adresu dostawy oraz numeru telefonu. Dotyczy to zarówno zarejestrowanych klientów, jak i tych, którzy kupowali bez rejestracji.
- **Brak dowodów na pobranie danych**: Super-Pharm poinformował, że aktualnie nie ma dowodów na pobranie danych przez cyberprzestępców.
- **Działania po incydencie**: Firma zablokowała dostęp do systemu, usunęła lukę, wzmocniła zabezpieczenia oraz zgłosiła incydent do odpowiednich instytucji – Prezesa Urzędu Ochrony Danych Osobowych (UODO), CERT Polska oraz na policję.
- **Ryzyko dla klientów**: W wyniku wycieku danych istnieje zagrożenie takie jak phishing (oszukańcze wiadomości), spoofing, spam oraz potencjalne wykorzystanie prywatnych danych do dalszych ataków.
- **Zalecenia dla klientów**: Super-Pharm ostrzega o możliwych konsekwencjach, takich jak ujawnienie danych związanych z zamówieniami czy wykorzystanie ich w sposób naruszający prywatność klientów.

Źródło: https://cyberdefence24.pl/cyberbezpieczenstwo/atak-hakerski-na-super-pharm-wyciekly-dane-klientow

09 WSA: nowa, wyższa kara za naruszenie danych osobowych jest prawidłowa

- W listopadzie 2018 r. administrator danych prowadzący sklep internetowy zgłosił naruszenie ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych (UODO).
- Prezes UODO po przeprowadzeniu postępowania administracyjnego nałożył na Spółkę XYZ karę pieniężną w wysokości 2 830 410 PLN za naruszenie przepisów RODO, w tym zasady poufności danych osobowych.
- Wojewódzki Sąd Administracyjny (WSA) w Warszawie oddalił skargę administratora w 2020 r., podkreślając, że głównym naruszeniem była niewystarczająca ochrona danych klientów spółki, co umożliwiło nieuprawniony dostęp do tych danych.
- WSA zgodził się z oceną, że Spółka XYZ nie dostatecznie oceniła ryzyka związane z dostępem do danych i używała nieskutecznych metod zabezpieczenia, jak tylko login i hasło do panelu pracownika.
- Naczelny Sąd Administracyjny (NSA) w 2023 r. uchylił wyrok WSA i decyzję Prezesa UODO, uznając, że kara dotyczyć powinna braku odpowiednich środków bezpieczeństwa, a nie sam fakt naruszenia danych.
- W związku z decyzją NSA, Prezes UODO ponownie rozpatrzył sprawę i w 2024 r. nałożył na Spółkę XYZ wyższą karę w wysokości 3 819 960 PLN, wskazując, że spółka mogła zapobiec naruszeniom, wdrażając skuteczniejsze środki ochrony danych osobowych.
- Sąd wskazał, że kara pieniężna ma być proporcjonalna, skuteczna i odstraszająca, co uzasadniło podniesienie kwoty kary w odpowiedzi na poważne naruszenia zasad RODO.

Źródło: https://www.bankier.pl/wiadomosc/UE-blokuje-sztuczna-inteligencje-od-Zuckerberga-w-Wielkiej-Brytanii-funkcja-juz-dziala-8826764.html

09 cd. WSA: nowa, wyższa kara za naruszenie danych osobowych jest prawidłowa

- Sąd wskazał, że kara pieniężna ma być proporcjonalna, skuteczna i odstraszająca, co uzasadniło podniesienie kwoty kary w odpowiedzi na poważne naruszenia zasad RODOwa trafiła ponownie do WSA, który we wrześniu 2024 r. oddalił skargę administratora, uznając, że Prezes UODO odpowiednio zastosował przepisy i uzasadnił nałożenie wyższej kary.
- Sąd uznał, że spółka nie wykazała, iż wdrożyła odpowiednich środków bezpieczeństwa adekwatnych do skali ryzyk związanych z przetwarzaniem danych osobowych.
- Orzeczenie w tej sprawie wskazuje, że brak odpowiednich rozwiązań technicznych i organizacyjnych w zakresie ochrony danych może skutkować poważnymi karami finansowymi.

Źródło: https://www.bankier.pl/wiadomosc/UE-blokuje-sztuczna-inteligencje-od-Zuckerberga-w-Wielkiej-Brytanii-funkcja-juz-dziala-8826764.html

10 Koniec 6-letniej epopei. LinkedIn ukarany za naruszenie RODO

- Kontekst: Irlandzka Komisja Ochrony Danych (IKOD) nałożyła karę w wysokości 310 mln euro na LinkedIn za naruszenie przepisów RODO poprzez nieprawidłowe praktyki reklamowe.
- Platforma LinkedIn została ukarana za praktyki profilowania reklam, które nie spełniały wymogów dyrektywy Unii Europejskiej dotyczącej ochrony danych osobowych.
- Proces dotyczący tej sprawy rozpoczął się w 2018 roku i dotyczył naruszeń związanych z przetwarzaniem danych użytkowników w niezgodny z prawem sposób.
- Decyzja Komisji: Na podstawie art. 58 ust. 2 pkt. i i art. 83 RODO, LinkedIn nałożono grzywnę w wysokości 310 mln euro (ok. 1,348 mld zł), reprymendę oraz nakaz dostosowania praktyk reklamowych do przepisów prawa.
- IKOD zwróciła uwagę na „wyraźne i poważne naruszenie" prawa do ochrony danych osobowych, które jest kluczowym prawem każdej osoby.
- Reakcja LinkedIn: Według oświadczenia LinkedIn, platforma wierzy, że jej działania były zgodne z RODO, jednak zobowiązała się współpracować z IKOD, aby poprawić swoje działania reklamowe w wyznaczonym terminie.
- Warto przypomnieć, że LinkedIn już wcześniej znajdował się w centrum uwagi ze względu na trenowanie modeli sztucznej inteligencji na danych użytkowników, co dotyczyło również kwestii ochrony danych.

Źródło: https://cyberdefence24.pl/polityka-i-prawo/koniec-6-letniej-epopei-linkedin-ukarany-za-naruszenie-rodo

11 WSA podziela stanowisko Prezesa UODO, co do zgody na kanał komunikacji

- Sprawa dotyczy prośby o ocenę satysfakcji z zakupu, wysłanej drogą mailową przez sklep internetowy w 2019 roku, co doprowadziło do skargi klienta do Prezesa UODO. Skarga klienta odnosiła się do nieprawidłowości w przetwarzaniu jego danych osobowych (w tym adresu e-mail) przez E. Sp. z o.o., w szczególności bez odpowiedniej podstawy prawnej do celów marketingowych.
- Prezes UODO uznał częściowe naruszenie RODO przez spółkę, wydając decyzję upominającą w marcu 2022 roku, z zastrzeżeniem dotyczącym braku poinformowania klientki o niemożliwości zidentyfikowania jej osoby na nagraniu monitoringu.
- WSA w Warszawie uchylił decyzję Prezesa UODO z 2022 roku w zakresie odmowy uznania naruszenia przepisów dotyczących przetwarzania danych do celów marketingowych. WSA stwierdził, że chociaż art. 10 ustawy o usługach elektronicznych wymaga zgody na przesyłanie informacji handlowych, to inne operacje na danych mogą być oparte na uzasadnionym interesie administratora zgodnie z art. 6 ust. 1 lit. f RODO.
- Rozstrzygnięto, że zgoda na przesyłanie informacji handlowej zgodnie z ustawą o usługach elektronicznych nie jest równoznaczna ze zgodą na przetwarzanie danych osobowych w rozumieniu art. 6 ust. 1 lit. a RODO.
- W listopadzie 2023 r. Prezes UODO ponownie rozpoznał sprawę i wydał decyzję, w której udzielił upomnienia dla spółki za przetwarzanie adresu e-mail w celach marketingowych bez prawnej podstawy. Prezes UODO podkreślił, że przesyłanie e-maili z prośbą o opinię na temat zakupu może być uznane za działania marketingowe, które wymagają spełnienia warunków określonych w przepisach o ochronie danych osobowych.
- WSA w Warszawie ostatecznie oddalił skargę spółki na decyzję Prezesa UODO, uznając, że przesłana wiadomość e-mail rzeczywiście miała charakter handlowy i wymagała odpowiedniej zgody adresata.

Źródło: https://judykatura.pl/wsa-podziela-stanowisko-prezesa-uodo-co-do-zgody-na-kanal-komunikacji/

12 Takiej kary świat nie widział. Google musi zapłacić Rosji 2 undecyliony rubli

- Kontekst: Rosyjskie sądy nałożyły na Google grzywnę w wysokości 2 undercylionów rubli (36 zer za dwójką), co przeliczając na dolary, wynosi około 2,5 decyliona dolarów. Jest to największa kara w historii.
- Powód kary: Google odmówiło przywrócenia kont związanych z rosyjskim reżimem na YouTube, w tym takich kont jak Channel One, Zvezda, Tsargrad czy RIA FAN, które były zablokowane w ramach sankcji po agresji Rosji na Ukrainę w 2020 roku.
- Sprawa sądowa: 17 rosyjskich podmiotów, w tym prorządowe media, złożyło pozew zbiorowy przeciwko Google'owi przed moskiewskim sądem.
- Wysokość kary: Grzywna rosła w systemie codziennym, zwiększając się o 100 tys. rubli każdego dnia, co doprowadziło do obecnej astronomicznej kwoty.
- Google a kara: Alphabet, spółka-matka Google'a, osiągnęła w 2023 roku przychody na poziomie 307 mld dolarów, jednak nawet takie przychody nie pozwolą pokryć nałożonej kary, której spłata jest nierealna.
- Stan prawny: Rosyjska spółka zależna Google’a ogłosiła upadłość w 2022 roku, a bankructwo firmy zostało oficjalnie potwierdzone we wrześniu 2023 roku.
- Reakcja rynku: Pomimo tych wydarzeń i decyzji rosyjskich władz, notowania akcji Google wzrosły o ponad 4% po publikacji wyników finansowych.

Źródło: https://www.bankier.pl/wiadomosc/Takiej-kary-swiat-nie-widzial-Google-musi-zaplacic-Rosji-2-undecyliony-rubli-8836956.html