





RODO - aktualności

Data publikacji: 17.10.2024

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

18. wersja nowelizacji KSC. Polska nie wyrobi się z implementacją NIS2?

02

Zakazane systemy AI - Broszura NASK

03

TSUE wypowiada się o warunkach ukierunkowanej reklamy

04

WSA: PUODO prawidłowo nakazał administratorowi i procesorowi dostosowanie operacji przetwarzania

05

Ustawa Kamilka wymaga korekt. Wystąpienie PUODO do Ministra Sprawiedliwości

06

UODO rusza w kraj – za nami pierwsze spotkania w Krakowie i Tarnowie

07

WSA: Prezes UODO prawidłowo nałożył karę 15 000 zł za brak analizy ryzyka

08

EROD przyjmuje nowe wytyczne, dot. m.in. prawie uzasadnionego interesu

09

UE blokuje sztuczną inteligencję od Zuckerberga, w Wielkiej Brytanii funkcja już działa

10

Co piąta firma nie dba o szkolenia z ochrony danych osobowych

11

WSA: Przetwarzanie numeru telefonu prezesa zarządu nie stanowiło naruszenia

01

18. wersja nowelizacji KSC. Polska nie wyrobi się z implementacją NIS2?

- **Kontekst:** Ministerstwo Cyfryzacji ogłosiło nowelizację ustawy o Krajowym Systemie Cyberbezpieczeństwa (KSC), której uchwalenie planowane jest na 2025 rok. Tymczasem termin wdrożenia dyrektywy NIS2 mija 17 października 2024 roku.
- Konsultacje: W projekcie nowelizacji wzięto pod uwagę ok. 70% z 1567 zgłoszonych uwag.
- **Najważniejsze zmiany:**
 - *Nadzór i kontrola:* Wprowadzenie bardziej przejrzystych zasad nadzoru nad kluczowymi podmiotami, m.in. możliwością wyznaczania jednego organu wiodącego.
 - *Kontrole doraźne:* Nowość - natychmiastowe działania w przypadku zagrożenia, m.in. po zgłoszeniu przez urzędnika monitorującego.
 - *Kary pieniężne:* Zasady zależą od rodzaju naruszenia, czasu jego trwania oraz możliwości finansowych podmiotu. Okresowa kara pieniężna została złagodzona.
 - *Urzędnik monitorujący:* Nowe stanowisko, którego zadania są ograniczone czasowo do miesiąca, a systemy IT mogą być kontrolowane po wcześniejszym powiadomieniu podmiotu.
- **Dodatkowe zmiany:**
 - Obniżenie wymagań dla podmiotów w sektorach produkcji.
 - Możliwość skargi do sądu administracyjnego od środków nadzorczych.

Źródło: <https://cyberdefence24.pl/polityka-i-prawo/18-wersja-nowelizacji-ksc-polska-nie-wyrobi-sie-z-implementacja-nis2>

01 cd. 18. wersja nowelizacji KSC. Polska nie wyrobi się z implementacją NIS2?

- Obowiązkowy audyt cykliczny dla podmiotów kluczowych co 3 lata.
- Modyfikacja przepisów karnych, w tym złagodzenie okresowych kar pieniężnych.
- Zasada mapowania norm zamiast odwołania do ISO.
- **Termin wdrożenia dyrektywy NIS2:** Polska musi implementować ją do 17 października 2024 r. Opóźnienia w przyjęciu przepisów dotyczących Toolbox 5G są oceniane negatywnie przez rząd.
- **Podkreślenie roli cyberbezpieczeństwa:** Nowelizacja ma za zadanie wzmocnić cyberbezpieczeństwo, oferować rynkowe zasady oceny dostawców wysokiego ryzyka oraz chronić przed zagrożeniami cyfrowymi.
- **Finansowa odpowiedzialność:** Ministerstwo przyznaje, że nowe regulacje wiążą się z dużą odpowiedzialnością finansową, zarówno dla państwa, jak i rynku, który musi dostosować się do nowych wymogów dotyczących bezpieczeństwa.

Źródło: <https://cyberdefence24.pl/polityka-i-prawo/18-wersja-nowelizacji-ksc-polska-nie-wyrobi-sie-z-implementacja-nis2>

02 Zakazane systemy AI - Broszura NASK

- Najważniejsze informacje z broszury NASK:
- **1. Wprowadzenie Aktu o AI:**
- Akt o AI (AI Act) wszedł w życie w sierpniu 2024 r. w Unii Europejskiej.
- Celem jest zapewnienie bezpiecznego rozwoju i stosowania sztucznej inteligencji z poszanowaniem praw podstawowych.
- **2. Zakres stosowania:**
- Przepisy dotyczą dostawców, użytkowników, importerów i dystrybutorów systemów AI w UE oraz tych, których wyniki są wykorzystywane w UE.
- Wyłączenia obejmują systemy AI stosowane w obronności, bezpieczeństwie narodowym oraz badaniach naukowych.
- **3. Kategorie ryzyka:**
- Systemy AI są klasyfikowane na podstawie ryzyka: minimalne, ograniczone, wysokie i zakazane praktyki. Rzecznik Generalny TSUE wskazał, że:
- **4. Zakazane praktyki:**
- **Techniki podprogowe, manipulacyjne i wprowadzające w błąd:** Systemy AI, które manipulują zachowaniem osób w sposób powodujący szkody.
- **Wykorzystywanie słabości osób:** Systemy AI, które wykorzystują słabości osób ze względu na wiek, niepełnosprawność lub sytuację społeczną.

Źródło: <https://www.gov.pl/web/ai/zakazane-systemy-ai>

02 cd. Zakazane systemy AI - Broszura NASK

- **Scoring społeczny:** Systemy AI oceniające osoby na podstawie ich zachowań społecznych, prowadzące do krzywdzącego traktowania.
- **Kategoryzacja biometryczna:** Systemy AI kategoryzujące osoby na podstawie danych biometrycznych w celu wywnioskowania informacji o ich cechach osobistych.
- **Ocena ryzyka popełnienia przestępstwa:** Systemy AI oceniające ryzyko popełnienia przestępstwa na podstawie profilowania.
- **Zdalna identyfikacja biometryczna:** Systemy AI identyfikujące osoby w czasie rzeczywistym w przestrzeni publicznej do celów ścigania przestępstw.
- **Scraping:** Systemy AI tworzące bazy danych poprzez niecelowane pozyskiwanie wizerunków twarzy z internetu lub nagrań z telewizji przemysłowej.
- **Rozpoznawanie emocji:** Systemy AI wyciągające wnioski na temat emocji osób w miejscu pracy lub instytucjach edukacyjnych.
- **5. Kary za nieprzestrzeganie przepisów:**
 - Administracyjne kary pieniężne do 35 mln EUR lub 7% całkowitego rocznego światowego obrotu przedsiębiorstwa.
 - **Następne kroki:**
 - Przepisy dotyczące zakazanych praktyk wejdą w życie 2 lutego 2025 r.
 - Przepisy dotyczące systemów wysokiego ryzyka oraz inne kluczowe regulacje wejdą w życie w sierpniu 2025 r. i sierpniu 2026 r.:

Źródło: <https://www.gov.pl/web/ai/zakazane-systemy-ai>

03 TSUE wypowiada się o warunkach ukierunkowanej reklamy

- **Kontekst sprawy:** Pan Max Schrems, aktywista działający na rzecz ochrony danych osobowych, zainicjował kolejną sprawę przed Trybunałem Sprawiedliwości Unii Europejskiej (TSUE). Sprawa dotyczyła naruszeń prywatności związanych z przetwarzaniem jego danych osobowych przez platformę Meta Platforms Ireland.
- **Panelowa dyskusja:** W lutym 2019 roku wziął udział w publicznej dyskusji panelowej w Wiedniu, gdzie otwarcie wypowiedział się na temat swojej orientacji seksualnej. Wydarzenie to było dostępne dla publiczności i transmitowane na żywo, a nagranie z tego wydarzenia miało później szeroką dystrybucję (podcast, YouTube).
- **Zautomatyzowana analiza danych przez Meta:** M. Schrems zaczął otrzymywać reklamy dotyczące osób homoseksualnych, mimo że nie wyrażał wcześniej zainteresowania takimi treściami. Reklamy te były wynikiem analizy jego zachowań na platformie, w szczególności polubień użytkowników wspierających pewną polityczkę.
- **Stanowisko TSUE:**
 - Każde długoterminowe przechowywanie danych osobowych w celu ukierunkowanej reklamy uznano za nieproporcjonalne i naruszające prawa użytkowników zagwarantowane w RODO.
 - Artykuł 9 ust. 2 lit. e) RODO (dotyczący przetwarzania szczególnych kategorii danych osobowych) musi być interpretowany zawężająco – nie można wykorzystywać takich danych bez wyraźnej zgody osoby, której one dotyczą.

Źródło: <https://judykatura.pl/tsue-wypowiada-sie-o-warunkach-ukierunkowanej-reklamy/>

03 cd. TSUE wypowiada się o warunkach ukierunkowanej reklamy

- **Zakres upublicznienia informacji:** Pomimo, że M. Schrems publicznie wypowiedział się na temat swojej orientacji seksualnej, TSUE podkreślił, że nie upoważnia to operatorów platform społecznościowych do przetwarzania innych danych dotyczących jego orientacji w celu oferowania zindywidualizowanej reklamy.
- **Podsumowanie:** TSUE orzekł, że nawet jeśli osoba dobrowolnie wypowiedziała się na temat swojej orientacji podczas publicznej debaty, nie oznacza to, że dane te mogą być bez jej zgody wykorzystywane przez platformy internetowe do celów marketingowych lub analitycznych.

Źródło: <https://judykatura.pl/tsue-wypowiada-sie-o-warunkach-ukierunkowanej-reklamy/>

04 WSA: PUODO prawidłowo nakazał administratorowi i procesorowi dostosowanie operacji przetwarzania

- **Kontekst:** Wojewódzki Sąd Administracyjny w Warszawie rozpoznał skargę Administratora danych i Podmiotu przetwarzającego na decyzję Prezesa Urzędu Ochrony Danych Osobowych (UODO) z lutego 2023 r., dotyczącej przetwarzania danych osobowych bez podstawy prawnej.
- **Zarzuty wobec podmiotów przetwarzających dane:** Skarga została złożona w związku z przetwarzaniem danych osobowych M.W. w celu dochodzenia roszczeń majątkowych, mimo że roszczenia te były już przedawnione.
- **Decyzja Prezesa UODO:** Prezes UODO stwierdził, że Administrator i Podmiot przetwarzający nie mieli podstawy prawnej do dalszego przetwarzania danych osobowych M.W., ponieważ roszczenia, których dochodzili, uległy przedawnieniu już w 2016 roku.
- **Brak uzasadnionego interesu:** Organ uznał, że kontynuowanie przetwarzania danych osobowych w tej sytuacji nie miało uzasadnionego interesu prawnego (zgodnie z art. 6 ust. 1 lit. f RODO), co oznacza naruszenie przepisów dotyczących ochrony danych osobowych.
- **Stanowisko Uczestnika postępowania:** M.W. oświadczył, że nie uznaje roszczenia, co w świetle prawa uchylało możliwość jego dalszego egzekwowania – zarówno w sądzie, jak i w drodze pozasądowej.
- **Stanowisko WSA w Warszawie:** Sąd potwierdził, że z chwilą oświadczenia Uczestnika o przedawnieniu i nieuznaniu roszczenia, Administrator oraz Spółka przetwarzająca dane utracili możliwość powoływania się na możliwość dochodzenia roszczenia na drodze prawnej.
- **Brak określenia retencji danych:** Sąd zwrócił uwagę, że termin przechowywania danych ("retencja") nie został jasno określony – co stanowi dodatkowy problem w kontekście zasad przetwarzania danych.

Źródło: <https://judykatura.pl/wsa-prezes-uodo-prawidlowo-nakazal-administratorowi-i-procesorowi-dostosowanie-operacji-przetwarzania/>

04 cd. WSA: PUODO prawidłowo nakazał administratorowi i procesorowi dostosowanie operacji przetwarzania

- **Końcowe ustalenia:** Przetwarzanie danych osobowych M.W. przez Administratora oraz Spółkę, w szczególności bez wykazania uzasadnionego interesu (art. 6 ust. 1 lit. f RODO), stanowiło naruszenie podstawowych zasad ochrony danych osobowych, w tym zasady przetwarzania zgodnego z prawem (zgodnie z art. 5 ust. 1 lit. a RODO).
- **Ostateczny wniosek:** Prezes UODO miał podstawy, aby nakazać zaprzestanie przetwarzania danych ze względu na brak wystarczającej podstawy prawnej, co potwierdził WSA w Warszawie.

Źródło: <https://judykatura.pl/wsa-prezes-uodo-prawidlowo-nakazal-administratorowi-i-procesorowi-dostosowanie-operacji-przetwarzania/>

05 Ustawa Kamilka wymaga korekt. Wystąpienie PUODO do Ministra Sprawiedliwości

- **Kontekst:** Prezes Urzędu Ochrony Danych Osobowych (UODO) zwrócił się do ministra sprawiedliwości Adama Bodnara w sprawie konieczności doprecyzowania przepisów „ustawy Kamilka” o ochronie małoletnich, aby dostosować je do zasad ochrony danych osobowych zgodnych z RODO.
- **Ustawa Kamilka:** Została stworzona z myślą o zwiększeniu ochrony praw dzieci, m.in. poprzez lepsze zbieranie sygnałów o zagrożeniach oraz weryfikację kompetencji osób pracujących z dziećmi. UODO zwraca jednak uwagę na to, że powinna być bardziej precyzyjna w zakresie przetwarzania danych osobowych.
- **Problemy z przetwarzaniem danych:**
 - Ustawa zawiera nieprecyzyjne przepisy dotyczące podstaw prawnych przetwarzania danych osobowych, co może prowadzić do nadmiernej ingerencji w prywatność (art. 7 i 8 Karty Praw Podstawowych UE).
 - Brak określonych zasad dotyczących okresu przechowywania danych osobowych oraz zabezpieczeń związanych z ich przetwarzaniem.
- **Standardy RODO:**
 - Zasady przetwarzania danych muszą być zgodne z podstawowymi zasadami RODO: legalność, rzetelność, ograniczenie celu, minimalizacja danych, integralność oraz poufność.
 - Prezes UODO sugeruje przeprowadzenie tzw. „testu prywatności” (oceny skutków przetwarzania danych osobowych), aby zapewnić proporcjonalność między ochroną praw dziecka a prywatnością osób fizycznych.

Źródło: <https://uodo.gov.pl/pl/138/3377>

05 cd. Ustawa Kamilka wymaga korekt. Wystąpienie PUODO do Ministra Sprawiedliwości

- **Nieprecyzyjne regulacje:**
 - Weryfikacja tożsamości dziecka i opiekuna/pracownika nie jest dokładnie określona na poziomie ustawowym, zależy od wytycznych, co nie jest wystarczające z punktu widzenia zapewnienia zgodności z RODO.
 - Brak regulacji dotyczących przetwarzania danych na etapie weryfikacji przeszłości kryminalnej pracowników i zakresu tych danych w określonych kontekstach.
 - **Problem przetwarzania danych na zapas:** Wytyczne pozwalają pracodawcom w niektórych przypadkach na zbieranie danych "na wszelki wypadek" (np. od pracowników nie mających bezpośredniego kontaktu z dziećmi), co może prowadzić do nadmiernej ingerencji w prywatność.
- **Kolejne wątpliwości:**
 - Brak precyzji w określeniu, jak i kiedy powinna odbywać się weryfikacja niekaralności pracowników, zarówno nowych, jak i już zatrudnionych.
 - Brak jasnych wytycznych co do przetwarzania danych w przypadku, gdy do zatrudnienia osoby ostatecznie nie dochodzi.
- **Wnioski:**
 - UODO domaga się lepszego zabezpieczenia danych osobowych przetwarzanych na podstawie „ustawy Kamilka”, poprzez bardziej precyzyjne przepisy oraz wprowadzenie odpowiednich mechanizmów ochrony prywatności zgodnych z RODO.
 - Ministerstwo Sprawiedliwości ma 30 dni na odniesienie się do przedstawionych wątpliwości i sugestii UODO.

Źródło: <https://uodo.gov.pl/pl/138/3377>

06 UODO rusza w kraj – za nami pierwsze spotkania w Krakowie i Tarnowie

- **Kontekst:** Prezes UODO, Mirosław Wróblewski, rozpoczął cykl ogólnopolskich spotkań poświęconych ochronie danych osobowych. Inicjatywa dotyczy współpracy z mieszkańcami, władzami samorządowymi oraz inspektorami ochrony danych (IOD).
- **Cel akcji:** Celem spotkań jest przybliżenie tematyki ochrony danych osobowych mieszkańcom oraz wzmocnienie wsparcia dla samorządów i innych instytucji w zakresie cyberbezpieczeństwa i przestrzegania przepisów RODO.
- **Pierwsze spotkania:**
 - W Tarnowie prezesa UODO spotkał się z przedstawicielami władz samorządowych oraz lokalnymi IOD.
 - W Krakowie zorganizowano bezpłatny punkt porad prawnych z zakresu ochrony danych osobowych, co pozwoliło mieszkańcom uzyskać odpowiedzi na konkretne pytania.
 - Prezes UODO spotkał się także z przedstawicielami Archidiecezji Krakowskiej, omawiając współpracę w kontekście ochrony danych osobowych w organizacjach kościelnych.
- **Wzmocnienie współpracy:** Mirosław Wróblewski zapowiedział bliską współpracę z samorządem terytorialnym, mającą na celu efektywniejszą ochronę danych osobowych oraz lepsze cyberbezpieczeństwo.
- **Powiązane działania:** W Tarnowie Monika Młotkiewicz z UODO przeprowadziła szkolenie dla inspektorów ochrony danych z jednostek samorządu terytorialnego (JST), podkreślając rolę efektywnej ochrony danych w administracji lokalnej.

Źródło: <https://uodo.gov.pl/pl/138/3374>

06 UODO rusza w kraj – za nami pierwsze spotkania w Krakowie i Tarnowie

- **Zaangażowanie społeczne:** Kilkudziesięciu mieszkańców Krakowa wzięło udział w spotkaniu z ekspertami UODO, uzyskując informacje i odpowiedzi na pytania związane z ochroną danych osobowych.
- **Plany na przyszłość:** Inicjatywa "UODO rusza w kraj" będzie kontynuowana w innych województwach, gdzie podobne spotkania z mieszkańcami i władzami samorządowymi planowane są w ścisłej współpracy z lokalnymi wojewodami.

Źródło: <https://uodo.gov.pl/pl/138/3374>

07

WSA: Prezes UODO prawidłowo nałożył karę 15 000 zł za brak analizy ryzyka

- **Kontekst sprawy:** Kierownik wyższego szczebla zgłosił kradzież laptopa służbowego, z którego skradziono dane osobowe. Administrator zgłosił incydent do Prezesa UODO, informując jednocześnie, że jest w trakcie wdrażania systemów szyfrujących.
- **Braki w odpowiednich zabezpieczeniach:** Prezes UODO nałożył karę na administratora za brak odpowiednich środków technicznych i organizacyjnych, które mogłyby zapobiec lub zmniejszyć ryzyko kradzieży i nieuprawnionego dostępu do danych osobowych.
- **Niedociągnięcia w dokumentacji:** Administrator przedstawił dokumenty wymagane przez Prezesa UODO, ale zawierały one błędy, były wewnętrznie sprzeczne i nie odpowiadały w pełni na pytania organu nadzorczego.
- **Podstawy prawne:** Na podstawie szeregu artykułów RODO (m.in. art. 5, art. 24 i art. 32), Prezes UODO uznał, że naruszone zostały zasady związane z integralnością, poufnością oraz rozliczalnością danych.
- **Sąd podtrzymał decyzję:** Sąd oddalił skargę administratora, argumentując, że laptop był zabezpieczony jedynie hasłem, a nie zgodnie z zaleceniami szyfrującymi, co mogło prowadzić do naruszenia prywatności.
- **Wysokość kary:** Nałożona kara wyniosła 15 000 zł. Sąd uznał, że kara ta jest skuteczna, proporcjonalna i odstrasżająca, zgodnie z zasadami określonymi w art. 83 ust. 1 RODO.
- **Brak naruszenia zasady równości:** Sąd nie dopatrył się naruszenia zasady równości określonej w art. 32 ust. 1 Konstytucji RP, uznając, że wszystkie podmioty muszą być traktowane w podobnych okolicznościach zgodnie z przepisami prawa.

Źródło: <https://judykatura.pl/wsa-prezes-uodo-prawidlowo-nalozyl-kare-15-000-zl-za-brak-analizy-ryzyka/>

08 EROD przyjmuje nowe wytyczne, dot. m.in. prawnie uzasadnionego interesu

- **Kontekst:** Europejska Rada Ochrony Danych (EROD) podjęła na ostatnim posiedzeniu (7-8 października 2024 r.) istotne decyzje związane z ochroną danych osobowych, dotyczące obowiązków administratorów i podmiotów przetwarzających, wytycznych w sprawie uzasadnionego interesu oraz możliwości usprawnienia egzekwowania przepisów RODO.
- **Opinie ws. podmiotów przetwarzających:** EROD przyjęła opinię dotyczącą obowiązków administratorów korzystających z usług podmiotów przetwarzających i podprzetwarzających. Opinia podkreśla m.in. potrzebę łatwego dostępu do informacji o tych podmiotach oraz odpowiedzialność administratorów za zapewnienie, że te podmioty dają "wystarczające gwarancje" ochrony danych.
- **Wytyczne dotyczące uzasadnionego interesu:** EROD wydała wytyczne szczegółowo omawiające warunki przetwarzania danych osobowych na podstawie uzasadnionego interesu (art. 6 ust. 1 lit. f RODO). Wskazano trzy główne kryteria: konkretność interesu, konieczność przetwarzania i równoważenie interesów administratora z prawami osób fizycznych.
- **Oświadczenie w sprawie egzekwowania przepisów RODO:** EROD z zadowoleniem przyjęła zmiany w projekcie rozporządzenia wprowadzone przez Parlament Europejski i Radę, w tym postulaty dotyczące usprawnienia współpracy organów ochrony danych. Rada podkreśliła też konieczność dalszego uszczegółowienia przepisów dotyczących rozstrzygania sporów.
- **Program prac na lata 2024–2025:** EROD przedstawiła swój program prac na lata 2024–2025, który jest częścią wdrażania długoterminowej strategii na lata 2024–2027. Program ten obejmuje działania priorytetowe, uwzględniając potrzeby kluczowych interesariuszy.
- **Nowy status dla Kosowa:** Rada nadała kosowskiej Agencji Informacji i Prywatności (odpowiednik organu ochrony danych) status obserwatora swoich działań.

Źródło: <https://uodo.gov.pl/pl/185/3387>

09 UE blokuje sztuczną inteligencję od Zuckerberga, w Wielkiej Brytanii funkcja już działa

- Meta AI, darmowy chatbot, został udostępniony użytkownikom w Wielkiej Brytanii od 9 października. Jest wbudowany w aplikacje takie jak Facebook, Messenger i Instagram, choć nie jest jeszcze dostępny w krajach Unii Europejskiej ze względu na regulacje dotyczące sztucznej inteligencji.
- Funkcje chatbota obejmują m.in. generowanie i modyfikowanie grafik oraz układanie list zakupów. Do chatbota można dostać się za pomocą komendy „@MetaAI” lub poprzez specjalną stronę meta.ai.
- Użytkownicy inteligentnych okularów Meta Ray-Ban w Wielkiej Brytanii mogą korzystać z interfejsu głosowego chatbota. Mark Zuckerberg zapowiedział, że do końca 2023 roku Meta AI ma stać się "najczęściej używanym i najlepszym asystentem AI na świecie".
- Meta zapisała, że treści rozmów z chatbotem będą przechowywane, choć istnieje możliwość ręcznego usunięcia historii konwersacji. Meta AI działa od kilku miesięcy w USA, choć spotyka się z ostrzeżeniami o niepewności wyników i możliwych błędach w odpowiedziach.
- Według „New York Times”, chatbot ma ograniczenia, szczególnie w prostych zadaniach, takich jak wyszukiwanie przepisów czy cen biletów lotniczych, i jest podatny na tzw. "halucynacje", czyli generowanie nieprawdziwych informacji.
- Meta AI udostępnia funkcjonalności do różnorodnych zadań, takich jak sugerowanie potraw na bazie podanych składników, pomoc w nauce do egzaminu, generowanie grafik według opisu (promptu) oraz ich modyfikowanie. Wszystkie obrazy stworzone przez AI będą specjalnie oznaczone, a funkcje generowania filmów i dźwięków na razie nie są publicznie dostępne.

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

10 Co piąta firma nie dba o szkolenia z ochrony danych osobowych

- **Wprowadzenie:** Badanie przeprowadzone przez ChronPESEL.pl i Krajowy Rejestr Długów pod patronatem Urzędu Ochrony Danych Osobowych (UODO) na temat szkoleń z ochrony danych osobowych wśród firm z sektora MŚP wskazuje na poważne luki.
- **Ogólne wyniki badania:** 81% firm szkoli swoich pracowników z ochrony danych osobowych, ale 59% z nich robi to tylko raz, na początku zatrudnienia. 20% firm nie prowadzi takich szkoleń wcale.
- **Zagrożenie błędami ludzkimi:** Niedostateczne i niepowtarzane szkolenia pracowników zwiększają ryzyko błędów, takich jak otwieranie podejrzanych e-maili, używanie słabych haseł czy niepoprawne przechowywanie danych, co może prowadzić do wycieku informacji lub cyberataków.
- **Znaczenie cyklicznych szkoleń:** Tylko 22% firm ponawia szkolenia w trakcie zatrudnienia, co znacząco zwiększa ryzyko cyberataków. Przeważają tu małe firmy (41%) w porównaniu do mikro (21%) i średnich (35%).
- **Brak szkoleń a branże:** Najwięcej firm nie organizujących szkoleń jest w sektorze transportowym (32%) oraz produkcyjnym i usługowym (po 20%). Wśród firm, które całkowicie lekceważą konieczność szkoleń, dominują jednoosobowe działalności (25%).
- **Zagrożenia cybernetyczne:** 12% firm z sektora MŚP przyznaje, że doświadczyło próby kradzieży danych osobowych, a 3% doświadczyło udanego ataku. Branże szczególnie narażone to transportowa (32%) i produkcyjna (19%).
- **Dane osobowe w firmach MŚP:** W Polsce firmy przetwarzają głównie dane takie jak imię i nazwisko (86%), numer telefonu (80%), adres zamieszkania (75%) oraz PESEL (75%). Ich wyciek może mieć katastrofalne skutki zarówno prawne, jak i wizerunkowe.

Źródło: <https://uodo.gov.pl/pl/138/3395>

10 cd. Co piąta firma nie dba o szkolenia z ochrony danych osobowych

- **Błędne reakcje na cyberataki:** Mimo że większość firm zgłaszałaby kradzież danych do odpowiednich organów (59%), aż 40% nie wie, jak właściwie się zachować w przypadku incydentu. Tylko 42% zgłosiłoby kradzież danych do UODO.
- **Kary za niezgłoszenie incydentów:** Brak zgłoszenia może oznaczać wysokie kary finansowe od UODO, zwłaszcza w przypadkach mogących prowadzić do kradzieży tożsamości.
- **Rekomendacje ekspertów:** Firmy powinny wprowadzać cykliczne szkolenia i odpowiednie procedury w celu minimalizacji ryzyka cyberataków, szczególnie zważywszy na fakt, że wyciek danych może narazić je zarówno na kary finansowe, jak i utratę zaufania klientów.

Źródło: <https://uodo.gov.pl/pl/138/3395>

11 WSA: Przetwarzanie numeru telefonu prezesa zarządu nie stanowiło naruszenia

- Spółka zadzwoniła do klienta z ofertą handlową, wykorzystując numer telefonu, który był związany z osobą, która wcześniej zażądała jego usunięcia.
- Marek A., prezes zarządu spółki, złożył skargę do prezesa Urzędu Ochrony Danych Osobowych (UODO), twierdząc, że jego dane osobowe zostały niewłaściwie przetworzone przez firmę.
- Prezes UODO stwierdził naruszenie przepisów RODO i udzielił spółce upomnienia za przetwarzanie danych osobowych Marka A. bez jego zgody.
- Wojewódzki Sąd Administracyjny (WSA) w Warszawie uchylił tę decyzję, stwierdzając, że numer telefonu użyty przez spółkę był związany z osobą prawną, a nie fizyczną, więc przepisy RODO nie mają tu zastosowania.
- WSA podkreślił, że RODO chroni dane osobowe tylko osób fizycznych i nie dotyczy danych osób prawnych, takich jak firmy.
- Sąd uznał, że sporny numer telefonu należał do klienta będącego osobą prawną, a prezes zarządu działał w imieniu spółki, co wykluczało możliwość naruszenia RODO.
- Na tej podstawie, sąd orzekł, że kontakt spółki z numerem związanym z osobą prawną nie naruszył przepisów o ochronie danych osobowych.

Źródło: <https://www.prawo.pl/biznes/numer-telefonu-prezesa-zarzadu-nie-stanowil-danych-osobowych-wyrok,529377.html>

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