



A large, faint fingerprint pattern is visible in the background of the slide, rendered in a dark blue color that matches the overall theme. The fingerprint is centered and occupies most of the frame.

RODO - aktualności

[15.07.2024]

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

UOKiK: Ponad 106 mln zł kary dla PayPal

02

Dostęp do danych innych wierzycieli, zawartych w KRZ został w końcu zmodyfikowany

03

PUODO: Należy ograniczyć dostęp do danych użytkowników łamiących prawa autorskie

04

Akt o sztucznej inteligencji opublikowany w Dzienniku Urzędowym UE

05

Sejm przyjął ustawę Prawo Komunikacji Elektronicznej (PKE)

01 UOKiK: Ponad 106 mln zł kary dla PayPal

- Prezes UOKiK zakwestionował postanowienia w „Umowie z użytkownikiem PayPal”. Wątpliwości wzbudziły klauzule zawierające 34 działania zabronione użytkownikom oraz katalog przykładowych sankcji.
- Wśród nich były m.in. zapisy mówiące o ukaraniu użytkownika choćby za samą próbę skorzystania z zablokowanego konta. PayPal zakładał też, że nie wolno „naruszać żadnych przepisów prawa, ustaw, zarządzeń lub regulacji (np. dotyczących usług finansowych, ochrony konsumentów, nieuczciwej konkurencji, zakazu dyskryminacji i nieuczciwej reklamy)”, bo może się to skończyć nałożeniem niedookreślonych sankcji.
- W praktyce naruszenie dowolnego przepisu w jakimkolwiek państwie upoważniało PayPal do zastosowania sankcji. Naruszenie mogłoby nawet nie mieć związku z korzystaniem z konta PayPal, przez co konsumenci mogliby nie wiedzieć, że zrobili coś niezgodnego z postanowieniami umownymi.
- Otwarty katalog przewidzianych w umowie sankcji, które dodatkowo nie były powiązane z poszczególnymi naruszeniami, oznaczał arbitralność decyzji spółki. Przykładowo, mogła ona „w dowolnej chwili” i „według własnego uznania” zablokować pieniądze użytkownika „w wysokości oraz przez okres tak długi, jak będzie to konieczne”. Co więcej, PayPal mógł jednocześnie nałożyć na konsumenta nawet kilka sankcji: zapłatę kwoty 2500 USD lub większej, zamknięcie konta bez uprzedzenia i odmowę świadczenia usług w przyszłości.
- Zdaniem Prezesa UOKiK zastosowanie kwestionowanych warunków mogło prowadzić do sytuacji, w której konsument był z jednej strony nieświadomy tego jakie działanie może zostać uznane przez spółkę za zabronione. Z drugiej strony nie był w stanie przewidzieć sankcji, które mogą zostać wobec niego zastosowane. Skutkiem mogło być nawet pozbawienie dostępu do pieniędzy zgromadzonych na koncie PayPal na nieokreślony czas.

Źródło: [Ponad 106 mln zł kary dla PayPal \(uokik.gov.pl\)](https://uokik.gov.pl)

02 Dostęp do danych innych wierzycieli, zawartych w Krajowym Rejestrze Zadłużonych (KRZ), został w końcu zmodyfikowany

- Dostęp do danych innych wierzycieli, zawartych w Krajowym Rejestrze Zadłużonych (KRZ), został w końcu zmodyfikowany – wynika z pisma przekazanego rzecznikowi praw obywatelskich (RPO) przez prezesa Urzędu Ochrony Danych Osobowych (UODO).
- Sprawa niekontrolowanego dostępu do danych wierzycieli Getin Noble Bank została ujawniona w sierpniu ub.r. przez DGP. Chodziło o to, że każda z 27 tys. osób, które miały roszczenia względem upadającego banku, mogła zupełnie swobodnie podejrzeć dane należące do pozostałych wierzycieli. Wśród ujawnionych w ten sposób danych znajdowały się nr PESEL, dowodu osobistego lub treść umów kredytowych zawartych z Getin Bankiem.
- Do zbadania tej sprawy prawie natychmiast włączyli się RPO oraz prezes UODO, którzy zażądali od MS wyjaśnień i uszczelnienia systemu. Resort początkowo bagatelizował problem i wskazywał, że przyjęte rozwiązanie jest odzwierciedleniem mechanizmów występujących w przypadku akt papierowych dotyczących uczestników jednego postępowania. Wówczas również, odwiedzając sąd, można otrzymać dane dotyczące innych uczestników.
- „Obecnie po wysłaniu zgłoszenia wierzycielności użytkownik systemu KRZ uzyskuje dostęp ograniczony wyłącznie do podglądu dokumentów złożonych przez siebie (dostęp do własnejteczki wierzyciela). Pełen dostęp do całościowych akt postępowania oraz szczegółów postępowania, w tym danych pozostałych wierzycieli, jest możliwy dopiero po weryfikacji uczestnika przez doradcę restrukturyzacyjnego lub sąd” – czytamy w odpowiedzi nadesłanej przez prezesa UODO. Decyzję o zmianach podjął minister sprawiedliwości (MS).

Źródło: [Dane wierzycieli w KRZ bezpieczniejsze - GazetaPrawna.pl](#)

03 PUODO: Należy ograniczyć dostęp do danych użytkowników łamiących prawa autorskie

- Prezes UODO, uważa, że trzeba zmienić prawo telekomunikacyjne tak, by przy okazji ścigania naruszeń prawa autorskiego, nie pobierać informacji dotyczących innych aspektów życia danej osoby w zakresie dostępu organów ścigania do danych objętych tajemnicą telekomunikacyjną. Takie są konsekwencje wyroku TSUE w sprawie C-470/21.
- TSUE wskazał, że dostęp do takich danych jest możliwy. Jednak muszą one być przechowywane tak, by niemożliwe było wyciągnięcie precyzyjnych wniosków na temat życia prywatnego konkretnych osób. Chodzi o to, by nie było możliwe powiązanie identyfikatora jakim jest np. adres IP z innymi informacjami (np. dotyczącymi płatności kartą kredytową). Bo to już pozwalałoby na tworzenie profilu użytkownika.
- Zdaniem prezesa UODO takie doprecyzowanie należałoby wprowadzić do polskiego prawa telekomunikacyjnego. Jego zdaniem dziś nie mamy gwarancji, że przechowywane dane służyć będą wyłącznie zidentyfikowaniu osoby podejrzewanej o dopuszczenie się czynu zabronionego, i niemożliwe będzie „by, poza sytuacjami nietypowymi, dostęp ten mógł pozwalać na wyciągnięcie precyzyjnych wniosków na temat życia prywatnego posiadaczy adresów IP”.
- W kontekście kontroli sądowej Prezes UODO przypomina także o niedawnym wyroku Europejskiego Trybunału Praw Człowieka z 28 maja 2024 r. w sprawie Pietrzak, Bychawska-Siniarska i inni przeciwko Polsce (skargi nr 72038/17 i 25237/18). Sprawa dotyczyła ustawodawstwa polskiego, pozwalającego służbom na zbieranie informacji o obywatelach pod pretekstem walki z przestępczością i zagrożeniami dla bezpieczeństwa publicznego. ETPCz stwierdził, że w wyniku braku realnej kontroli nad prowadzeniem kontroli operacyjnej w ramach czynności operacyjno-rozpoznawczych oraz zbyt ogólnie sformułowanych przesłanek umożliwiających prowadzenie tej kontroli, doszło do naruszeń prawa do poszanowania życia prywatnego, rodzinnego oraz korespondencji – w odniesieniu do skarg dotyczących m.in. zatrzymywania danych komunikacyjnych do potencjalnego wykorzystania przez właściwe organy lub władze krajowe.

04 Akt o sztucznej inteligencji opublikowany w Dzienniku Urzędowym UE

- „Niniejsze rozporządzenie należy stosować zgodnie z wartościami Unii zapisanymi w Karcie, ułatwiając ochronę osób fizycznych, przedsiębiorstw, demokracji, praworządności oraz ochronę środowiska, a jednocześnie pobudzając innowacje i zatrudnienie oraz czyniąc Unię liderem w upowszechnianiu godnej zaufania AI” – czytamy w dokumencie.
- AI Act wejdzie w życie 1 sierpnia br., ale zacznie być stosowane w kilku transzach: od 2025 do 2027 roku. Jako pierwsze zaczną być stosowane przepisy dotyczące zabronionych systemów AI. Pełny kalendarz:
 - W lutym 2025 r. zaczną być stosowane rozdziały I (przepisy ogólne) i II (zabronione systemy AI);
 - W sierpniu 2025 r. będą miały zastosowanie: rozdział III, sekcja 4 (organy powiadamiające), rozdział V (modele AI ogólnego przeznaczenia), rozdział VII (zarządzanie), rozdział XII (poufność i kary), artykuł 78 (poufność), z wyjątkiem artykułu 101 (grzywny dla dostawców AI ogólnego przeznaczenia);
 - W sierpniu 2026 r. zastosowanie będzie mieć cały Akt o sztucznej inteligencji, z wyjątkiem artykułu 6(1) i odpowiadających mu obowiązków (jedna z kategorii systemów AI wysokiego ryzyka);
 - W sierpniu 2027 r. – zastosowanie będzie mieć też artykuł 6 (1).

Źródło: [Akt o sztucznej inteligencji opublikowany w Dzienniku Urzędowym UE | CyberDefence24](#)

05 Sejm przyjął ustawę Prawo Komunikacji Elektronicznej (PKE)

- Nowe Prawo Komunikacji Elektronicznej (PKE) wprowadza regulacje, które mają poprawić sytuację konsumentów w relacjach z firmami telekomunikacyjnymi. Zmiany te obejmują kilka kluczowych obszarów, które podniosą jakość i transparentność usług telekomunikacyjnych. To fundamentalny akt prawny dla tego sektora gospodarki. Nowa regulacja zastąpi obecną ustawę – Prawo telekomunikacyjne.
- Nowe prawo wprowadza usługę Advanced Mobile Location (AML), dzięki której będzie można przekazywać precyzyjne informacje o lokalizacji osoby dzwoniącej na numer alarmowy 112 oraz inne trzycyfrowe numery alarmowe.
- Prawo zobowiązuje operatorów do tego, aby dostarczali konsumentom prostych i jasnych informacji o warunkach umowy, zanim ją podpiszą. Dzięki temu każdy użytkownik będzie mógł świadomie zdecydować, która oferta jest dla niego najlepsza. Przepisy mają też chronić konsumentów przed nieuczciwymi sprzedawcami usług telekomunikacyjnych, którzy odwiedzają klientów w domach bez wcześniejszego umówienia.
- Ustawa reguluje ponadto kwestię pieniędzy, które pozostają na kartach przedpłaconych (prepaid) po wygaśnięciu ważności konta. Operatorzy będą je zwracać właścicielom prepaidów.
- Nowa regulacja powtarza znany z p.t. model bezwarunkowego gromadzenia przez operatorów danych o wszystkich użytkownikach usług telekomunikacyjnych i ich udostępniania policji i innym uprawnionym podmiotom. Przeciwno tym rozwiązaniom występowali m.in. Urząd Ochrony Danych Osobowych i minister ds. UE. Są one bowiem niezgodne z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej, a także – jak wskazywał UODO – z konstytucją, europejską konwencją praw człowieka i Kartą praw podstawowych Unii Europejskiej.

Źródło: [Nowe Prawo Komunikacji Elektronicznej – co zmieni? - Ministerstwo Cyfryzacji - Portal Gov.pl \(www.gov.pl\)](#); [Prawo komunikacji elektronicznej. Jest ustawa, skończą się kary - GazetaPrawna.pl](#)

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