
LEX ARTIST

RODO - aktualności

[22.11.2023]

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 MSiT: baza "Sportowe talenty" niezbędna, by tworzyć programy aktywizujące młodzież

02 Czy komornik może sprzedać bazę danych klientów spółki, żeby spłacić wierzyciela?

03 Rząd umożliwił zastrzeżenie numeru PESEL m.in. w aplikacji mObywatel 2.0

04 Obrońcy prywatności skarżą Brukselę za mikrotargetowanie

05 Zawrotny rozwój cyfrowy, zwiększone ryzyko. UE stawia nowe wymagania

06 EROD przedst. wyjaśnienia dot. technik śledzenia, podlegających dyrektywie o prywatności i łączności

01 MSiT: baza "Sportowe talenty" niezbędna, by tworzyć programy aktywizujące młodzież

- Do RPO wpływają skargi w sprawie ewidencji „Sportowe talenty", wprowadzonej ustawą z 17 sierpnia 2023 r. o zmianie ustawy o zdrowiu publicznym oraz niektórych innych ustaw. Wątpliwości dotyczą właściwej ochrony danych osobowych przetwarzanych w tej ewidencji, a także celowości i proporcjonalności niektórych przepisów z punktu widzenia poszanowania prawa do prywatności.
- Jak wskazuje RPO, utworzenie publicznej bazy danych gromadzącej dane osobowe wszystkich uczniów, w tym dane wrażliwe. Chodzi o: imię, nazwisko, nr PESEL, rok urodzenia, wiek, płeć, masę ciała, wzrost, wynik testów sprawnościowych i ich datę; klasę, oddział, typ szkoły i jej nazwę i adres, gminę, powiat i województwo, gdzie uczeń uzyskał wynik z testów sprawnościowych. Według uzasadnienia ustawy celem ewidencji jest monitorowanie sprawności fizycznej dzieci i młodzieży oraz możliwość identyfikacji talentów sportowych.
- Bardzo obszerny zakres danych, w tym danych identyfikujących (nr PESEL) – a także danych wrażliwych, gromadzonych w jednym miejscu – budzi zastrzeżenia z punktu widzenia ich bezpieczeństwa. Dane te w pełnym zakresie są udostępniane każdej szkole. Uzupełnia ona dane przekazane przez rodziców i nauczycieli.
- Rzecznik wystąpił o opinię do Urzędu Ochrony Danych Osobowych. UODO poinformował, że zmiany nie zostały skonsultowane z urzędem.
- MEiN podnosi, że testy mają ważny wymiar prozdrowotny i diagnostyczny, a jej głównym celem jest popularyzacja sportu oraz uświadamianie uczniom, że aktywność fizyczna jest ważnym elementem dbałości o zdrowie. Na wątpliwości RPO odpowiada też minister sportu i turystyki - wskazuje, że zmiany mają na celu zapobieganie nadwadze i otyłości oraz popularyzowanie aktywności fizycznej wśród dzieci i młodzieży jest długotrwałym procesem społecznym realizowanym w ważnym interesie publicznym i nie będzie skuteczny bez dokonania populacyjnej diagnozy stanu sprawności fizycznej polskich dzieci i młodzieży.

Źródło: Baza "Sportowe talenty" - RPO (prawo.pl)

02 Czy komornik może sprzedać bazę danych klientów spółki, żeby spłacić wierzyciela?

- 16 listopada br. przed Trybunałem Sprawiedliwości Unii Europejskiej w Luksemburgu odbyła się rozprawa dotycząca wykładni RODO (unijnego rozporządzenia o ochronie danych osobowych). Warszawski sąd w trybie prejudycjalnym zwrócił się do Trybunału z pytaniem, czy przedmiotem postępowania egzekucyjnego może być baza danych klientów spółki oraz, czy przepisy RODO stoją na przeszkodzie sprzedaży takiej bazy danych przez komornika.
- W rozpatrywanej przez warszawski sąd sprawie wierzyciel, mimo prawomocnego nakazu zapłaty, nie mógł odzyskać pieniędzy od pewnej firmy, ponieważ komornik stwierdził, że spółka nie ma majątku i umorzył postępowanie.
- Wierzyciel nie dał za wygraną i wytoczył proces członkowi zarządu firmy, ponieważ zgodnie z Kodeksem spółek handlowych, jeśli nie da się spłacić wierzyciela z majątku przedsiębiorstwa, to odpowiedzialność odszkodowawcza spada właśnie na członka zarządu.
- Pozwany wniósł o oddalenie sprawy i przyznał, że firma posiada majątek: dwie bazy danych z informacjami o setkach tysięcy użytkowników. Jak relacjonuje portal prawo.pl polski sąd ma wątpliwości, czy przepisy RODO pozwalają na to, aby takie bazy sprzedać bez zgody osób, których dane się w nich znajdują. Dlatego skierował sprawę do TSUE.
- Termin ogłoszenia wyroku w tej sprawie nie jest jeszcze znany.

Źródło: W czwartek rozprawa przed TSUE ws. RODO: Czy komornik może sprzedać bazę danych klientów spółki, żeby spłacić wierzyciela? - GazetaPrawna.pl

03 Rząd umożliwił zastrzeżenie numeru PESEL m.in. w aplikacji mObywatel 2.0

- Już od piątku, 17 listopada obywatele mogą skorzystać z nowej usługi i zastrzec swój numer PESEL. Celem ustawy o zmianie niektórych ustaw w celu ograniczania niektórych skutków kradzieży tożsamości jest ograniczanie skutków kradzieży tożsamości. Jak podaje PAP, chodzi m.in. o walkę z wyłudzaniem środków finansowych poprzez zaciąganie np. kredytu na inną osobę bez jej wiedzy i zgody. Zwalczane w ten sposób ma też być zjawisko tzw. SIM swappingu, czyli wyrabiania duplikatu karty SIM, która może być potem użyta do nielegalnego autoryzowania transakcji.
- Nowa usługa, według komentarza Ministerstwa Cyfryzacji, ma więc zapewnić prewencyjną ochronę przed konsekwencjami kradzieży tożsamości.
- Od 1 czerwca 2024 r. podmioty takie jak banki, instytucje kredytowe lub notariusze przed zawarciem umowy lub podjęciem czynności będą musiały sprawdzać w rejestrze, czy PESEL danej osoby został zastrzeżony. Przepisy ustawy wskazują, że obywatele nie będą obciążani za zobowiązanie, które zostało zaciągnięte bez ich wiedzy mimo istniejącego zastrzeżenia.
- Zastrzeżenie numeru PESEL jest bezpłatne. Usługę będzie można aktywować zarówno internetowo, jak i stacjonarnie:
    - w aplikacji mObywatel,
    - na stronie mobywatel.gov.pl,
    - osobiście w dowolnym urzędzie gminy (potrzebny będzie papierowy wniosek),
    - banki krajowe, spółdzielcze kasy oszczędnościowo-kredytowe i poczta będą mogły wprowadzić możliwość zastrzeżenia za ich pośrednictwem numeru PESEL.

Źródło: Zmiany w numerach PESEL. Od piątku dostępna nowa opcja - Bankier.pl

04 Obrońcy prywatności skarżą Brukselę za mikrotargetowanie

- Organizacja NOYB złożyła do europejskiego inspektora ochrony danych (EIOD) skargę przeciwko Komisji Europejskiej, zarzucając jej naruszenie przepisów rozporządzenia 2018/1725 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii (dalej: RODO UE).
- Chodzi o kampanię, którą z oficjalnego konta Dyrekcji Generalnej ds. Migracji i Spraw Wewnętrznych KE prowadzono na platformie X (dawniej: Twitter) we wrześniu tego roku. Komisja promowała wtedy wpis popierający projekt rozporządzenia w sprawie zapobiegania niegodziwemu traktowaniu dzieci w celach seksualnych i zwalczania go (CSAM).
- Na podstawie informacji z repozytorium reklam platformy skarżący ustalił, że Komisja kierowała swój przekaz do użytkowników X z Holandii, którzy mówili po niderlandzku i mieli ponad 18 lat. Odbiorcy byli dodatkowo profilowali według 44 kryteriów. Większość z nich (36) odnosiła się do partii politycznych, polityków lub opinii politycznych, a pozostałych sześć – do przekonań religijnych. Tak mikrotargetowane reklamy w okresie 18–27 września zostały wyświetlone ponad 600 tys. razy.
- Organizacja założona przez austriackiego aktywistę Maxa Schremsa zarzuca KE naruszenie art. 10 i w konsekwencji art. 4 RODO UE. Artykuł 10 co zasady zabrania przetwarzania szczególnych kategorii danych osobowych – w tym właśnie danych ujawniających opinie polityczne i przekonania religijne. Przetwarzanie takich danych jest dopuszczalne wyłącznie pod określonymi warunkami – których, zdaniem NOYB, post Komisji nie spełniał.
- NOYB zwrócił się do EIOD o zakazanie Komisji dalszego przetwarzania danych osobowych skarżącego. Sugeruje ponadto wprowadzenie wobec KE szerszego zakazu – przetwarzania jakichkolwiek szczególnych kategorii danych osobowych na potrzeby internetowych kampanii reklamowych w serwisie X, jak również nałożenie kary pieniężnej za naruszenia.

Źródło: Obrońcy prywatności skarżą Brukselę za mikrotargetowanie - GazetaPrawna.pl

05 Zawrotny rozwój cyfrowy, zwiększone ryzyko. UE stawia nowe wymagania

- Dynamiczny rozwój technologii sprawił, że aspekty związane z implementacją nowych rozwiązań oraz wynikające z nich możliwe zagrożenia dołączyły na stałe do listy zadań rad nadzorczych. Wśród największych ryzyk wskazywanych przez rady nadzorcze firm znalazło się cyberbezpieczeństwa.
- To właśnie świadomość ryzyk odgrywa obecnie kluczową rolę w budowaniu odporności organizacji. Tymczasem, jak pokazują wyniki badania EY Global Board Risk Survey, zaledwie 31% członków rad nadzorczych przyznaje, że ich nadzór nad ryzykiem wynikającym z transformacji cyfrowej jest bardzo skuteczny, a 40% twierdzi, że rozumie największe wirtualne zagrożenia.
- Tylko co trzeci członek rad nadzorczych (31%) przyznał, że skutecznie trzyma pieczę nad tym, aby równoważyć szybkość wdrażania nowych technologii z ekspozycją na ryzyko. Dodatkowo 19% ankietowanych uważa, że ich nadzór jest umiarkowanie skuteczny.
- Zaledwie 34% respondentów jest zadowolonych z poziomu przeszkolenia w zakresie technologii i tematów cyfrowych, przy czym twierdząco odpowiedziało 48% przedstawicieli firm, które są najbardziej świadome ryzyk i zaledwie 20% osób z grona organizacji zidentyfikowanych jako mniej odporne na zakłócenia.
- Kolejnym wyzwaniem dla rad nadzorczych jest bycie na bieżąco z wszelkimi nowymi regulacjami, które dotyczą ich biznesu. Jedną z ważniejszych zmian jest Dyrektywa NIS2, która ma za zadanie podwyższać poziom cyberbezpieczeństwa w krajach Unii Europejskiej. NIS2 w przypadku przedsiębiorców wprowadza rozbudowane wymogi w zakresie bezpieczeństwa i raportowania incydentów, a także bardziej rygorystyczne środki nadzoru ze strony krajowych organów. NIS2 ustanawia również szereg wymagań, które odnoszą się bezpośrednio do kierownictwa organizacji. Pracownicy odpowiedzialni za bezpieczeństwo będą musieli odegrać jeszcze istotniejszą rolę w firmie, nadzorując wdrażanie nowych obowiązków.

Źródło: Zawrotny rozwój cyfrowy, zwiększone ryzyko. UE stawia nowe wymagania - Bankier.pl

06 EROD przedst. wyjaśnienia dot. technik śledzenia, podlegających dyrektywie o prywatności i łączności

- Podczas 87. posiedzenia plenarnego, które odbyło się 14 listopada br. w Brukseli, Europejska Rada Ochrony Danych (EROD) przyjęła Wytyczne w sprawie zakresu technicznego art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Wytyczne te mają na celu wyjaśnienie, które operacje techniczne, w szczególności nowe i powstające techniki śledzenia, są objęte dyrektywą, i zapewnienie większej pewności prawa administratorom i osobom fizycznym.
- Przewodnicząca EROD, Anu Talus, powiedziała: "Nie jest tajemnicą, że śledzenie aktywności użytkowników online może poważnie zaszkodzić prywatności ludzi. Niejasności dotyczące zakresu stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej oraz pojawienie się nowych technik, stanowiących uzupełnienie lub alternatywę dla tradycyjnych plików cookie, doprowadziły do powstania nowych zagrożeń prywatności. Wytyczne te omawiają rozwiązania, takie jak linki śledzące i piksele, przetwarzanie lokalne i unikalne identyfikatory, aby zapewnić, że obowiązki w zakresie zgody, określone w tym artykule, nie będą pomijane”.
- W celu wyjaśnienia zakresu stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej, w wytycznych przeanalizowano kluczowe pojęcia, o których mowa w tym artykule, takie jak "informacja", "terminal abonenta lub użytkownika", "sieć łączności elektronicznej", "uzyskiwanie dostępu" i "informacja przechowana/przechowywanie". Wytyczne zawierają również zestaw praktycznych przykładów przedstawiających popularne techniki śledzenia.
- Wytyczne dotyczą wyłącznie zakresu stosowania art. 5 ust. 3 dyrektywy o prywatności i łączności elektronicznej. Nie odnoszą się one do sposobu uzyskiwania zgody ani do wyjątków określonych w tym artykule.

Źródło: Aktualności - UODO