
LEX ARTIST

RODO - aktualności

[20.08.2024]

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 Kara prawie 1,5 mln złotych dla spółki medycznej po ataku hackerskim

02 Meta nie może publikować na terenie Polski reklam z użyciem danych prezesa InPostu

03 Jak chronić dane sygnalistów – podsumowanie seminarium UODO

04 Skarga na portal X dotarła do UODO. Prezes: Temat coraz bardziej palący

05 To może być największy wyciek w historii. Mowa o miliardach danych osobowych

01 Kara prawie 1,5 mln złotych dla spółki medycznej po ataku hackerskim

- Hackerzy uzyskali dostęp do szczegółowych danych osobowych około 21 tys. osób - pacjentów i pracowników spółki American Heart of Poland S.A.
- Zdarzenie objęło szeroki zakres danych, tj.: nazwisko, imię, imiona rodziców, nazwisko rodowe matki, datę urodzenia, dane dotyczące zarobków lub posiadanego majątku, dane dotyczące zdrowia, numer rachunku bankowego, adres zamieszkania lub pobytu, numer PESEL, nazwę użytkownika lub hasło, seria i numer dowodu osobistego, numer telefonu oraz adres e-mail.
- O wycieku danych spółka dowiedziała się od hakerów, którzy zażądali 3 mln dolarów okupu za nieujawnienie przechwyconych danych. Spółka powiadomiła o incydencie prezesa UODO, a osoby, których dane wyciekły, poinformowała o zagrożeniu związanym z incydentem. PUODO przeprowadził w tej sprawie czynności wyjaśniające i kontrolne, a w ich następstwie wszczął wobec spółki postępowanie administracyjne.
- PUODO w toku przeprowadzonych czynności ustalił m.in., że spółka nie wdrożyła wszystkich niezbędnych środków służących ochronie przetwarzanych przez nią danych, nie była w stanie ustalić przyczyny wycieku, a ponadto nie przestrzegała własnych zaleceń dotyczących bezpieczeństwa danych.
- Spółka założyła, że poziom bezpieczeństwa przetwarzanych przez nią danych jest właściwy, tylko na podstawie przeprowadzonego w niej wewnętrznego audytu, którego celem było przedłużenie ważności certyfikatu ISO/IEC 27001:2013. W opinii UODO założenie to było jednak błędne. Brak prawidłowo przeprowadzonej analizy ryzyka, kluczowej dla ochrony danych, doprowadził do niewdrożenia przez spółkę właściwych środków organizacyjnych i technicznych służących ochronie przetwarzanych danych.
- PUODO wydał decyzję, w której stwierdził nieprawidłowości w przestrzeganiu przez spółkę przepisów o ochronie danych osobowych i nałożył na nią karę pieniężną w wysokości 1 440 549 zł. Spółka odwołała się do Wojewódzkiego Sądu Administracyjnego.

Źródło: Wysoka kara dla spółki po wycieku danych (prawo.pl)

02 Meta nie może publikować na terenie Polski reklam z użyciem danych prezesa InPostu

- Według deefpake'a, który jako reklama pojawił się w serwisach Facebook i Instagram, Rafał Brzoska miał rzekomo założyć platformę, która zapewnia zyski wszystkim „obywatelom Polski". Deepfake'owa reklama używa prawdziwych, aktualnych danych osobowych Pana Rafała Brzoski, prezesa Inpost. To bezprawnie zmodyfikowane nagranie wykorzystujące jego wizerunek.
- Skarżący podkreśla, że Meta rozpowszechnia nagranie bez weryfikacji i oceny wiarygodności danych osobowych. Meta wie o sprawie, bo skarżący zawiadomił ją o problemie 3 lipca. Skargę Pana Rafała Brzoski rozpatrywać będzie organ irlandzki, bo tam ma siedzibę Meta Platforms Ireland Limited.
- Na skutek działań Prezesa UODO, podjętych w związku ze skargą Pana Rafała Brzoski, Meta Platforms Ireland Limited musi wstrzymać wyświetlanie, w serwisach Facebook i Instagram, reklam wykorzystujących prawdziwe dane Pana Rafała Brzoski.
- Zakaz będzie obowiązywał trzy miesiące i dotyczy fałszywych reklam wyświetlanych na terytorium Rzeczpospolitej Polskiej. Prezes UODO Mirosław Wróblewski wydał postanowienie zabezpieczające na podstawie art. 70 ust. 1 i 2 ustawy o ochronie danych osobowych oraz art. 66 ust. 1 RODO, który określa maksymalny czas obowiązywania tego środka właśnie na 3 miesiące oraz w wyjątkowych okolicznościach pozwala PUODO zastosować środek tymczasowy jeśli uzna, że istnieje pilna potrzeba ochrony praw i wolności osób, których dane dotyczą.
- Zgodnie z procedurą Prezes UODO powiadomił o tym pozostałe organy nadzorcze, których sprawa dotyczy, a także Europejską Radę Ochrony Danych i Komisję. Pozostaje także w bezpośrednim kontakcie z wiodącym organem nadzorczym, tj. organem irlandzkim.

Źródło: Aktualności - UODO

03 Jak chronić dane sygnalistów – podsumowanie seminarium UODO

- 7 sierpnia w UODO odbyło się seminarium, podczas którego Mirosław Wróblewski wspólnie z pracownikami Urzędu, przedstawicielami Społecznego Zespołu Ekspertów przy PUODO oraz zewnętrznymi ekspertami omówili uwagi przesłane w ramach konsultacji społecznych i przedstawili propozycje wykładni przepisów ustawy o ochronie sygnalistów w zakresie dotyczącym danych osobowych.
- W pierwszym panelu podkreślono, że tożsamość sygnalisty to nie tylko imię i nazwisko, ale wszelkie dane, na podstawie których można byłoby go pośrednio zidentyfikować, takie jak np. jego miejsce pracy. Ochrona poufności sygnalisty powinna obejmować także te dane.
- Prelegenci poruszyli również wątek obowiązków informacyjnych i ewentualnych wyłączeń w tym zakresie wynikających z ustawy o ochronie sygnalistów oraz samego RODO (w szczególności w kontekście realizacji tych obowiązków względem osób których dotyczy zgłoszenie).
- Pewne wątpliwości mogą wzbudzać zasady naliczania okresu przechowywania danych osobowych sygnalisty, zwłaszcza w przypadku kilku zgłoszeń naruszenia prawa. Przyjęto jednak, że 3-letni okres retencji danych osobowych należy liczyć zawsze od daty przyjęcia zgłoszenia. Dotyczy to także danych osobowych w rejestrze zgłoszeń wewnętrznych.
- Ważnym aspektem ochrony danych osobowych sygnalistów są kanały zgłoszeń regulowane w procedurze zgłoszeń wewnętrznych. W tym temacie poruszono wątek grup kapitałowych, zwracając uwagę na ryzyko ograniczania się jedynie do korporacyjnych kanałów zgłoszeń.
- Ważnym aspektem są także środki bezpieczeństwa danych osobowych sygnalistów m.in. w ramach kanałów zgłoszeń (kontrowersje wśród uczestników seminarium wzbudził zwłaszcza kanał ustny). Podkreślono konieczność uwzględnienia reguł privacy by design i privacy by default w projektowanych procesach przetwarzania danych. Jednocześnie należy zadbać o integralność i dostępność danych.

Źródło: Aktualności – UODO; Ochrona danych osobowych sygnalistów – wyjaśnienia ekspertów - Ochrona danych osobowych (poradyodo.pl)

04 Skarga na portal X dotarła do UODO. Prezes: Temat coraz bardziej palący

- Organizacja pozarządowa NOYB („Non of Your Business") wysłała skargi na portal X do urzędów ochrony danych w 9 krajach, w tym do Polski,
- Portal X (dawny Twitter), którego właścicielem jest Elon Musk, korzystał z danych osobowych użytkowników bez ich wyraźnej zgody, w celu szkolenia modelu sztucznej inteligencji Grok. Taki proces jest zdaniem NYOB naruszeniem RODO.
- Zareagowała Irlandzka Komisja Ochrony Danych, która wszczęła postępowanie wobec X. W efekcie Elon Musk zgodził się zaprzestać przetwarzania danych użytkowników z UE/EOG zaczerpniętych z postów X od 7 maja 2024 r. do 1 sierpnia 2024 r. DPC poinformowało, że postępowanie sądowe będzie kontynuowane we wrześniu.
- Noyb w komunikacie opublikowanym na stronie internetowej, działania DPC nazywa „nieśmiałymi". Zarzuca irlandzkiemu organowi, że nie jest zainteresowany sednem sprawy i zadowala się jedynie „środkami łagodzącymi". „Zwracamy uwagę na fakt, że DPC zdaje się aprobować zastosowanie art. 6 ust. 1 lit. f) RODO jako podstawy prawnej odnośnie przetwarzania danych przez Twittera, gdyż »wynegocjował« wdrożenie »wzmocnionych środków łagodzących« na mocy art. 6 ust. 1 lit. f) RODO. Podkreślamy, że w niniejszej sprawie kategorycznie odrzucamy możliwość posłużenia się przez Twittera art. 6 ust. 1 lit. f) RODO" – czytamy w skardze wystosowanej do UODO.
- Według Noyb, portal X zniechęca także użytkowników do prawa wyboru, stosując formularz opt-out zamiast opt-in, a także do wyrażania sprzeciwu do trenowania AI na naszych danych. Organizacja twierdzi też, że X nie udziela niezbędnych informacji dotyczących przetwarzania danych w sposób „zwięzły, przejrzysty, zrozumiały i łatwo dostępny" i nie używa przy tym „jasnego i prostego języka".
- UODO zbada tę sprawę, aby zapewnić pełną zgodność działań z obowiązującymi przepisami.

Źródło: Skarga na portal X dotarła do UODO. Prezes: Temat coraz bardziej palący | CyberDefence24

05 To może być największy wyciek w historii. Mowa o miliardach danych osobowych

- Naruszenie, które rzekomo miało miejsce w kwietniu, polegało na kradzieży danych, w tym nazwisk, adresów i numerów ubezpieczenia społecznego, które według doniesień pochodzą od firmy, która gromadzi i sprzedaje dane w legalnych celach. Uważa się, że dane zostały skradzione z National Public Data (NPD), firmy zajmującej się sprawdzaniem przeszłości osób, działającej w ramach Jerico Pictures Inc.
- NPD gromadzi informacje z rejestrów publicznych w celu ich sprzedaży oraz świadczenia powiązanych usług. Złożono jednak pozew, w którym zarzucono, że NPD pobierało również dane ze źródeł niepublicznych bez uzyskania zgody osób fizycznych. Jak dotąd NPD nie potwierdziło oficjalnie wycieku, ani nie wyjaśniło, jak do niego doszło.
- Początkowo do kradzieży danych przyznał się haker znany jako USDoD, próbując sprzedać je za 3,5 miliona dolarów. USDoD był już wcześniej powiązany z innymi naruszeniami, w tym z próbą sprzedaży bazy danych użytkowników InfraGard za 50 000 dolarów w grudniu 2023 r. Sytuacja uległa zmianie 6 sierpnia, kiedy użytkownik o imieniu Fenice zamieścił bezpłatnie na forum hakerskim najbardziej kompletną wersję skradzionych danych.
- W odpowiedzi na naruszenie na Florydzie złożono pozew zbiorowy przeciwko NPD. Odwołuje się do VX-Underground, edukacyjnej witryny internetowej o cyberbezpieczeństwie, która podała, że USDoD wystawiła bazę danych na sprzedaż, twierdząc, że zawiera ona 2,9 miliarda rekordów. VX-Underground zweryfikowało dane jako prawdziwe po otrzymaniu zaawansowanej kopii bazy danych – ogromnego pliku o rozmiarze 277,1 GB.
- Chociaż niektóre osoby potwierdziły, że ich dane zostały uwzględnione, problemy takie jak nieprawidłowe numery ubezpieczenia społecznego i nieaktualne dane adresowe sugerują, że informacje mogą pochodzić ze starej kopii zapasowej.

Źródło: To może być największy wyciek w historii. Mowa o miliardach danych osobowych | ITHardware; Major data breach exposes 2.7 billion personal records, experts urge action (msn.com)