



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

[26.07.2023]

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

EROD o skutkach ram ochrony danych UE-USA

02

Na cudzą tożsamość próbowano wyłudzić łącznie 50 mln zł

03

Rząd chce stworzyć wielką platformę przetwarzania informacji o obywatelach

04

Kara 47 tys. zł brak wdrożenia odpowiednich środków

05

Kary Prezesa UOKiK za "nękanie" telefonami

01 EROD o skutkach ram ochrony danych UE-USA

- Europejska Rada Ochrony Danych (EROD), podczas 82. posiedzenia plenarnego, przyjęła notę informacyjną dla osób fizycznych i podmiotów przekazujących dane do USA.
- W nocie informacyjnej wyjaśniono, że przekazywanie danych oparte na decyzjach stwierdzających odpowiedni stopień ochrony nie musi być uzupełniane środkami uzupełniającymi. Przekazywanie danych do USA, które nie zostało uwzględnione w „Wykazie ram ochrony danych”, wymaga odpowiednich zabezpieczeń, takich jak standardowe klauzule ochrony danych lub wiążące reguły korporacyjne. W tym względzie EROD podkreśla, że wszystkie zabezpieczenia wprowadzone przez rząd USA w obszarze bezpieczeństwa narodowego (w tym mechanizm dochodzenia roszczeń) mają zastosowanie do wszystkich danych przekazywanych do USA, niezależnie od wykorzystywanego narzędzia przekazywania danych.
- Ponadto w dokumencie podkreślono, że w obszarze bezpieczeństwa narodowego osoby fizyczne z UE mogą złożyć skargę do swojego krajowego organu ochrony danych, aby skorzystać z nowego mechanizmu dochodzenia roszczeń, niezależnie od narzędzia przekazywania danych wykorzystywanego do przekazywania danych osobowych do USA.
- Co to oznacza w praktyce? Dane wytransferowane do USA np. na podstawie SCC będą objęte tymi samymi gwarancjami, co dane przekazane na podstawie Privacy Framework. Nie zwalnia to jednak z obowiązku przeprowadzenia oceny ryzyka transferu danych - TIA (dr. Paweł Litwiński).

Źródło: [Aktualności – UODO; https://www.linkedin.com/posts/pawe%C5%82-litwi%C5%84ski_privacyframework-scc-tia-activity-7089172332480520192-hL_t?utm_source=share&utm_medium=member_desktop](https://www.linkedin.com/posts/pawe%C5%82-litwi%C5%84ski_privacyframework-scc-tia-activity-7089172332480520192-hL_t?utm_source=share&utm_medium=member_desktop)

02 Na cudzą tożsamość próbowano wyłudzić łącznie 50 mln zł

- Związek Banków Polskich podał nowe statystyki dotyczące prób wyłudzeń kredytów na skradzioną tożsamość. W II kwartale 2023 r. złodzieje próbowali w ten sposób ukraść łącznie ponad 50 mln zł. Odnotowano ponad 2,1 tys. prób wyłudzeń.
- - To stosunkowo wysoki poziom, który utrzymuje się od ostatnich czterech kwartałów (17,2 proc. wzrostu r/r) - przeliczyć to można na ok. 23 próby dziennie – mówi Grzegorz Kondek, Koordynator Kampanii Informacyjnej Systemu Dokumenty Zastrzeżone. I dodaje, że łącznie od 2008 r. udaremniono już 112,5 tys. prób wyłudzeń na łączną kwotę 5,6 mld złotych.
- Jednocześnie Polacy zastrzegli w systemie 44,5 tys. dowodów tożsamości. To aż 20 proc. więcej niż rok temu w analogicznym okresie. Statystycznie do bazy trafiało 490 szt. dziennie. Obecnie w bazie międzybankowego systemu Dokumenty Zastrzeżone jest niemal 2,4 miliona danych o zagubionych lub skradzionych dokumentach tożsamości.
- Według Włodzimierza Kicińskiego, wiceprezesa ZBP, wysoka liczba zastrzeganych dokumentów jest pozytywnym zjawiskiem. - Wraz ze wzrostem świadomości Polaków o potrzebie jak najszybszego zastrzegania utraconych dokumentów skuteczność całego systemu antyfraudowego w polskich bankach wyraźnie rośnie – mówi wiceprezes ZBP.

Źródło: [Prawdziwa plaga. Na cudzą tożsamość próbowano wyłudzić łącznie 50 mln zł - Bankier.pl](#)

03 Rząd chce stworzyć wielką platformę przetwarzania informacji o obywatelach

- "Rz" podała, że "w Sejmie czeka na rozpatrzenie rządowy projekt ustawy, który ma usprawnić elektroniczną obsługę urzędów państwowych". "W projekcie tym, zmieniającym równocześnie wiele ustaw, przewidziano m.in. uregulowanie masowego przetwarzania danych na potrzeby tworzenia analiz społeczno-ekonomicznych dla rządu" - dodano. Według projektu nową rolę rządowego think tanku, jakim jest Polski Instytut Ekonomiczny, ma być obsługiwanie tzw. Zintegrowanej Platformy Analitycznej (ZPA)".
- "To budowany właśnie system analiz, zakładający centralne przetwarzanie danych o obywatelach i firmach. Chodzi o bardzo szeroki zakres danych, które dziś przechowuje w różnych miejscach administracja państwowa. PIE ma mieć dostęp do baz z 18 instytucji, w których są m.in. numery PESEL, wyniki egzaminu ósmoklasisty czy data uzyskania habilitacji, przyczyny ustania małżeństwa, stanu zdrowia oraz ile który przedsiębiorca pracowników zatrudnił, czy i na ile z podatkami zalegał" - zwrócono uwagę.
- W projekcie przewidziano zabezpieczenie (anonimizację) tych danych, a nad ich bezpieczeństwem ma czuwać specjalna Rada Polityk Publicznych, w której skład mają wejść także przedstawiciele organizacji pozarządowych.
- Projekt był już wielokrotnie kwestionowany przez ekspertów legislacyjnych pod kątem zgodności z Konstytucją oraz RODO. Jak zauważa dr Maciej Berek, radca prawny, główny legislator Pracodawców RP, "w ostatnich latach okazało się, że nasze państwo używa nowoczesnych narzędzi informatycznych nie zawsze zgodnie z ich przeznaczeniem, czego przykładem było nadużywanie oprogramowania służącego do zwalczania terroryzmu". "Dlatego poważne obawy budzi administrowanie wielką bazą danych o obywatelach przez PIE, państwową osobę prawną nadzorowaną wyłącznie przez premiera" – sugeruje Berek. (PAP)

Źródło: [Rząd chce stworzyć wielką platformę przetwarzania informacji o obywatelach - Bankier.pl](#)

04 Kara 47 tys. zł brak wdrożenia odpowiednich środków

- Do UODO wpłynęła informacja od podmiotu trzeciego, wskazująca na utratę dokumentacji prowadzonej w formie elektronicznej przez administratora. Dokumentacja ta zawierała m.in. dane osobowe pracowników administratora oraz osób będących stronami umów cywilnoprawnych. W związku z tymi informacjami UODO występował do administratora z kolejnymi pismami o udzielenie wyjaśnień. Administrator przyznał, że w wyniku ataku ransomware doszło do zablokowania dostępu do danych osobowych pracowników spółki. Nie umiał rozszyfrować danych, więc przyjął, że najkorzystniej będzie wstrzymać się od ingerowania w system.
- Administrator nie zgłosił naruszenia ochrony danych osobowych do organu nadzorczego. W ocenie administratora zdarzenie nie stanowiło incydentu, mającego znamiona naruszenia ochrony danych osobowych w rozumieniu RODO.
- W ocenie UODO, biorąc pod uwagę zakres przetwarzanych danych osobowych, a także kategorie osób, administrator był zobowiązany wdrożyć odpowiednie środki techniczne i organizacyjne, które zapewniłyby adekwatny poziom ochrony danych. Dobór właściwych środków powinien wynikać z przeprowadzonej analizy ryzyka, niestety w omawianym postępowaniu nic nie wskazywało na to, że administrator przeprowadził ją prawidłowo dla przetwarzanych w formie elektronicznej danych.
- Niezależnie od okoliczności związanych z analizą ryzyka, w przedmiotowej sprawie administrator nie stosował także adekwatnych środków bezpieczeństwa, czego rezultatem było przełamanie zabezpieczeń systemu informatycznego i zaszyfrowanie danych osobowych. Działanie to nie zostało powstrzymane przez przyjęte u niego mechanizmy bezpieczeństwa. Podmiot ten nie podjął niezwłocznych działań zapewniających szybkie i skuteczne przywrócenie dostępu do danych osobowych.

Źródło: [Decyzje Prezesa UODO - UODO](#)

05 Kary Prezesa UOKiK za "nękanie" telefonami

- Po licznych skargach od konsumentów, Prezes UOKiK potwierdził, że Asmanta Call Center wykonywała połączenia telefoniczne nie mając uprzedniej zgody na kontakt. Niechciane telefony dotyczyły fotowoltaiki.
- Jednocześnie firma wprowadzała konsumentów w błąd, znacznie zawyżając kwoty możliwych do pozyskania dotacji. UOKiK ukarał spółkę oraz osoby zarządzające karami w łącznej wysokości blisko 1,5 mln zł.
- Asmanta Call Center zajmuje się telemarketingiem zleconym przez swoich kontrahentów. Połączenia wykonywane są przez konsultantów lub za pośrednictwem udziału oprogramowania do automatyzacji rozmów. Telemarketerzy oraz automatyczne „boty” dzwonią do konsumentów m.in. z ofertą wykonania instalacji fotowoltaicznych oraz zapraszają na spotkania handlowe. Przedsiębiorca zajmuje się również zbieraniem podczas tych rozmów telefonicznych danych potencjalnych klientów (tzw. leadów).
- UOKiK przypomniał, że dzwonienie z informacją handlową do osób, które nie wyraziły na to zgody, jest niedozwolone prawnie, o zgodę nie można również pytać na początku rozmowy. Taką nieuczciwą praktykę stosowała Asmanta, która nie posiadała pozwolenia właścicieli numerów telefonicznych na marketing bezpośredni.

Źródło: [UOKiK - Urząd - Informacje ogólne - Aktualności - Kary Prezesa UOKiK za "nękanie" telefonami](#)

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