

Cyber24 Days - potrzebujemy certyfikacji podmiotów przetwarzających dane wrażliwe?

Datum 9.10.2026
Subjekt Urząd Ochrony Danych Osobowych
Region Polsko
Kategorie IT a komunikace, Státní instituce, Bezpečnost

7 października prezes Urzędu Ochrony Danych Osobowych Mirosław Wróblewski oraz pracownicy Urzędu wzięli udział w Cyber24 Days, organizowanych przez Cyberdefence24. Wydarzenie obejmowało liczne debaty, dyskusje i rozmowy o bezpieczeństwie cyfrowym i nowych technologiach. Na wydarzeniu wystąpił także dr hab. Wojciech Wiewiórowski, Europejski Inspektor Ochrony Danych (EIOD).

Prezes UODO oraz EIOD wspólnie uczestniczyli w „Fireside chat” (forma swobodnej dyskusji na żywo). Rozmowa zaczęła się od kwestii bezprecedensowych cyberataków na dane medyczne, które dotknęły milionów obywateli. Choć reakcja na takie incydenty to przede wszystkim zadanie organu krajowego, Europejski Inspektor Ochrony Danych zaoferował wsparcie zaraz po tym, jak Minister Cyfryzacji ogłosił, że doszło do wycieku.

Mirosław Wróblewski wskazał, że wycieki te pokazują niebezpieczeństwo płynące z dużej koncentracji danych – zamiast atakować kilkanaście tysięcy małych podmiotów, cyberprzestępcy mogą uderzyć w jeden, który obsługuje je wszystkie. Dlatego konieczne wydaje się wymuszenie wyższych standardów ochrony danych na takich podmiotach – czy to przez system certyfikacji, przede wszystkim przez objęcie ich obowiązkami z ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa. Jednocześnie prezes UODO wskazał, że zaproponowana przez Ministra Cyfryzacji granica 100 tys. rekordów, od której podmiot byłby objęty bardziej wymagającymi restrykcjami, w przypadku danych szczególnych (w szczególności danych o zdrowiu) być może mogłaby zostać obniżona.

Przestępcy uderzają w najsłabsze ogniwo

„Wnioski, które przedstawiłem Ministrowi Cyfryzacji, dotyczą potrzeby uregulowania, bardziej ścisłego, przede wszystkim w kontekście ustawy prawach pacjenta – nie blankietowo, jak ma to miejsce dotychczas – kwestii powierzania przetwarzania danych osobowych. Choćby poprzez stosowanie ustawy o krajowym systemie certyfikacji cyberbezpieczeństwa. Jest to po prostu niezbędne, bo okazuje się, że przestępcy zorientowali się w potencjale danych o stanie zdrowia” – mówił Mirosław Wróblewski, prezes UODO. „Mamy do czynienia z pewnym paradoksem w naszym prawie. Administratorzy-lekarze/przychodnie lekarskie, są zobowiązani do przestrzegania tajemnicy lekarskiej, ale ustawa o prawach pacjenta pozwala na powierzenie przetwarzania tych danych podmiotom przetwarzającym dosyć lekką ręką. Wykształcił się model biznesowy takich „aplikacji gabinetowych”, które są zobowiązane do zachowania poufności, ale nie jest to już standard tajemnicy lekarskiej. Można powiedzieć, że znaleziono najsłabszy element systemu i tam przeprowadzono atak – dodał prezes UODO.

Podkreślił, że administratorzy mają swoje obowiązki i mogą powierzać przetwarzanie danych tylko podmiotom zapewniającym odpowiednie gwarancje oraz przeprowadzać ich audyty. Ale w praktyce biznesowej jest to fasadowa ochrona, bo lekarze często nie mają dostatecznej wiedzy do takiej

weryfikacji. Korzystają z usług firm zewnętrznych, oczekując od nich pewnej jakości – a ostatnie wydarzenia tę jakość poddają w wątpliwość.

Z kolei Wojciech Wiewiórowski wskazał, że po angielsku administrator danych nazywany jest „controlerem” – i lepiej, by nasze dane medyczne kontrolowali lekarze. Jednocześnie zwrócił uwagę, że ważną rolę w tej kwestii mają samorządy zawodowe, jak było to w przypadku prawników – to one muszą tworzyć standardy ochrony danych w branży i egzekwować ich przestrzeganie.

Świadomość zgody i problemy z odszkodowaniami

Obaj rozmówcy zgodzili się, że obecne przepisy RODO są wciąż wystarczające, mimo postępu technologicznego. Problemem jest więc ich odpowiednie egzekwowanie. Mirosław Wróblewski zwrócił jednak uwagę, że pewne konstrukcje okazały się mało praktyczne – UODO otrzymał dziesiątki tysięcy zgłoszeń od administratorów, podczas gdy problem dotyczy przede wszystkim jednej firmy przetwarzającej dane.

Z kolei EIOD wskazał, że brak uregulowania kwestii odszkodowań i pozwów zbiorowych za naruszenie ochrony danych – to mogłoby zapobiec powtarzaniu tych samych błędów przez administratorów w przyszłości.

Na zakończenie padło pytanie czy zgoda na przetwarzanie danych ma jeszcze sens w 2026 r., gdy mogą być one przetwarzane przez algorytmy bez wiedzy osób, których dotyczą. W odpowiedzi Wojciech Wiewiórowski wskazał, że zgoda to tylko jedna z sześciu dopuszczalnych w RODO podstaw przetwarzania, i warto zwrócić uwagę także na pozostałe pięć i korzystać z nich, gdy jest to możliwe.

Z kolei Mirosław Wróblewski wskazał, że właśnie dziś niezwykle ważne jest, by zgodę wyrażać świadomie, a nie bezrefleksyjnie „przeklikiwać” kolejne oświadczenia.

Jak cyberataki wpływają na konsumentów?

Prezes UODO wziął też udział w kolejnym panelu dyskusyjnym pt.: „System padł, dane wyciekły, konto puste. Anatomia kryzysu w świecie cyfrowego konsumenta”. Tę część rozpoczęto od przedstawienia i danych, zgodnie z którymi do września br. krajowe CSIRT-y zarejestrowały łącznie 207 tys. incydentów cyberbezpieczeństwa, a liczba ta będzie zapewne rosnąć w ostatnich miesiącach w związku z m.in. Black Friday czy zakupami świątecznymi. W zeszłym roku liczba zgłoszeń do zespołu CERT przekroczyła 658 tys., co stanowi wzrost o 10 proc. względem roku poprzedniego.

Mirosław Wróblewski potwierdził, że incydentów przybywa i zapewne będzie ich niestety jeszcze więcej, czego najlepiej dowodzą niedawne cyberataki na sektor medyczny. Przywołał też najnowsze badania ENISA (Agencji UE ds. Cyberbezpieczeństwa), z których wynika, że połowa organizacji traktuje cyberbezpieczeństwo tylko jako element utrzymania ciągłości działania, a tylko jedna trzecia przeprowadza audyt zabezpieczeń częściej niż raz do roku. Tymczasem przy tak szybkim rozwoju technologii, nowe zagrożenia i formy ataków pojawiają się niemal ciągle.

Patriotyzm to też ochrona cyberbezpieczeństwa i zaufania

W odpowiedzi na pytanie o największą lukę w obecnym systemie, Mirosław Wróblewski wskazał, że wciąż skupiamy się na pojedynczych przypadkach cyberataków, nie dostrzegając ich skutków w skali makro. Tymczasem wspomniane badania agencji ENISA wskazały, że incydenty tego typu w 2024 r. spowodowały niedostępność różnych systemów w całej UE przez łącznie pół miliarda godzin (dla porównania, rok ma 8760 godzin). Suma indywidualnych problemów organizacji przekłada się więc na kondycję poszczególnych państw, a nawet całej Unii Europejskiej.

„Funkcjonujemy w warunkach quasi-wojennych, jeśli chodzi o ilość cyberataków. W XXI w. patriotyzm wymaga także dbania o cyberbezpieczeństwo własnej organizacji oraz o ochronę praw osób, które korzystają z jej usług. Nasi wrogowie chcą bowiem destabilizacji i to w bardzo różnych obszarach” – mówił Mirosław Wróblewski.

Tymczasem sposób komunikowania o incydentach może takiej destabilizacji zapobiec albo ją pogłębić. Jeden z podmiotów przetwarzających po ostatnim wycieku wysyłał SMS-y informujące osoby, których dane wyciekły. Wysyłali go jednak konkretni administratorzy i na tym poziomie dochodziło do zniekształceń – m.in. czasem nie wskazywano, której przychodni dotyczy ta informacja. W efekcie mogło to jedynie wprowadzić większy chaos i przyczynić się do spadku zaufania informowanych w taki sposób osób. Realizacja obowiązków informacyjnych powinna więc być precyzyjna.

Prezes UODO podkreślił, że w przypadku stwierdzenia cyberataku najpilniejsze jest zapobieżenie temu, by sytuacja eskalowała. Następnie trzeba się skupić na przywróceniu działania usługi. We współpracy z odpowiednimi organami trzeba też starać się naprawić szkody oraz wykryć sprawców ataku. Mirosław Wróblewski po raz kolejny zwrócił uwagę na potrzebę wprowadzenia systemu certyfikowania podmiotów przetwarzających duże ilości danych, zwłaszcza tych szczególnej kategorii. Dodał, że jest na to szansa w ramach zapowiadanej tzw. „piątki Gawkowskiego.”

Udział innych ekspertów UODO w Cyber24 Days

Prócz Prezesa Urzędu w wydarzeniu uczestniczyli także Andrzej Zieliński, zastępca dyrektora Departamentu Kontroli i Naruszeń oraz Piotr Drobek, dyrektor Departamentu Innowacyjności i Zarządzania Danymi. Pierwszy wziął udział w panelu pt. „Kapitanie, toniemy!”. Wycieki danych plagą naszych czasów”. Piotr Drobek z kolei zabrał głos w ramach panelu „Innowacje a regulacje. Kto korzysta na deregulacja rynku cyfrowego?”.

<https://uodo.gov.pl/pl/531/4599>