

# Podsumowanie miesiąca - październik 2024 r.

Posted on 2024-10-31

Szanowni Państwo, często powtarzamy, że dane osobowe są paliwem dla nowoczesnej gospodarki i społeczeństwa. Nie zawsze jednak dociera do nas, że oznacza to konieczność mierzenia się z nowymi wyzwaniami i problemami. Ochrona danych osobowych to nie tylko żmudne wdrażanie procedur zabezpieczających nas przed już rozpoznanymi ryzykami. Świat, w który wkracza sztuczna inteligencja, musimy wszyscy rozpoznać na nowo.

## Seminarium „Ochrona danych jako element odporności społeczeństwa i państwa”

Przekonaliśmy się o tym w tym miesiącu na organizowanym przez Prezesa UODO i ZUS seminarium „Ochrona danych jako element odporności społeczeństwa i państwa”.

Rozmawialiśmy na nim 7 października o nowych rodzajach ataków cybernetycznych, wpływie działań wojennych w Ukrainie na liczbę naruszeń danych osobowych czy o nowych metodach ataków phishingowych i socjotechnicznych. Zastanawialiśmy się, jakie wyzwania dla ochrony prywatności niosą nowe technologie takie jak sztuczna inteligencja, uczenie maszynowe i przetwarzanie danych biometrycznych. Dyskutowaliśmy o konsekwencjach wycieków danych osobowych - dezinformacji lub ingerencji w procesy demokratyczne.

Według danych NASK liczba incydentów ochrony danych osobowych drastycznie rośnie. W 2020 roku odnotowano 10 tysięcy, dwa lata później - 38 tysięcy, podczas gdy do września 2024 roku zarejestrowano ich już 80 tysięcy! Wniosek z dyskusji jest jasny: ochrona danych osobowych musi być integralną częścią myślenia o bezpieczeństwie państwa. Najslabszym ogniwem w tym łańcuszku jest zawsze człowiek. Dlatego budowanie świadomości zagrożeń, którym możemy przeciwdziałać, jest kluczowe. Czasem wystarczy niewiele: odpowiednio częste zmiany hasła, sprawdzanie, kiedy ktoś ostatni raz logował się na nasze konto, ostrożność w korzystaniu ze sprzętu służbowego do celów prywatnych lub prywatnego do celów służbowych.

Nieprzeszkoleni pracownicy to najslabsze ogniwo w systemie zabezpieczeń danych osobowych w każdej firmie i organizacji, niezależnie od jej wielkości. Obszerną relację z tego wydarzenia można znaleźć na naszej stronie internetowej.

# Ochrona danych w robotyce medycznej w dobie AI ACT i

# EHDS

15 października zorganizowaliśmy natomiast konferencję UODO i Fundacji AI One Health „Ochrona danych w robotyce medycznej w dobie Aktu o Sztucznej Inteligencji i Europejskiej przestrzeni danych dotyczących zdrowia (EHDS)”. Naszym partnerem były tu Izba POLMED i Ośrodek Przetwarzania Informacji - Państwowy Instytut Badawczy. Rozmawialiśmy o takich zagadnieniach jak operacje z udziałem robotów. Harmonijne połączenie bezpieczeństwa danych medycznych, jakie daje EHDS, z ich innowacyjnym wykorzystaniem może przyczynić się do znacznego postępu w medycynie. Technologię trzeba jednak wdrażać w sposób przemyślany. Ataki hakerskie na roboty medyczne są już poważnym zagrożeniem. Niewłaściwe zabezpieczenia oraz luki np. w systemach operacyjnych robotów mogą prowadzić do dramatycznych konsekwencji. Wprowadzenie fałszywych informacji lub nieprawidłowych parametrów może prowadzić do błędnych decyzji medycznych!

## Dane stanowią szansę, jeśli zminimalizujemy zagrożenia

Rozwój medycyny, ale też i biznesu, zależy dziś w dużej mierze od tego, jak szybko zyskamy nowe kompetencje nie tylko z zakresu nowych technologii, ale i ochrony danych. Jeśli chodzi o służbę zdrowia, mamy dużo do nadrobienia. Z raportu NIK przedstawionego na naszej konferencji medycznej wynika, że większość szpitali nie zapewnia odpowiedniego poziomu bezpieczeństwa danych medycznych. Aż 3/5 małych i średnich firm szkoli swoich pracowników z ochrony danych osobowych tylko raz - po przyjęciu do pracy. Co piąte przedsiębiorstwo nie robi tego wcale. Takie są wyniki badania przeprowadzonego na zlecenie serwisu ChronPESEL.pl i Krajowego Rejestru Długów pod patronatem Urzędu

Ochrony Danych Osobowych. Pamiętajmy: brak szkoleń lub ich sporadyczne przeprowadzanie może być bardzo kosztowne, ponieważ często niezamierzone błędy ludzkie są przyczyną wycieku lub kradzieży danych przez hakerów. Ryzyko jest naprawdę bardzo realne.

# Współpraca z Jednostkami samorządu terytorialnego

Ustalenie odpowiednich procedur i zabezpieczeń jest gwarantem rozwoju obejmującym zarówno sektor prywatny, jak i publiczny. Dlatego doskonalenie wiedzy z zakresu bezpieczeństwa danych ważne jest także dla samorządów terytorialnych. Z ich przedstawicielami także spotykamy się regularnie. 21 października 2024 r. mój zastępca, Konrad Komornicki, spotkał się z przedstawicielami Związku Województw RP. Rozmawiali o powstającym kodeksie postępowania dla jednostek samorządu terytorialnego. W założeniu ma on stanowić drogowskaz, jak skutecznie chronić dane osobowe. Dla UODO ważne jest, by jak najwięcej podmiotów wzięło udział w konsultacjach tego kodeksu. Było to kolejne spotkanie z reprezentantami jednostek samorządu terytorialnego. Poprzez takie spotkania UODO chce podkreślić jak ważny jest kontakt z samorządami w kwestii ochrony danych osobowych. Na różnych szczeblach samorządu przetwarzane są ogromne ilości danych i niezmiernie istotna jest kwestia odpowiedniej dbałości o nie.

## Start XV edycji

# ogólnopolskiego programu „Twoje dane - Twoja sprawa”

Dbając o rozwój umiejętności cyfrowych uruchomiliśmy kolejną edycję programu edukacyjnego dla szkół. W tym roku weźmie z nich udział 349 placówek. Na koniec - miło mi poinformować, że sejmowa Komisja Sprawiedliwości i Praw Człowieka pozytywnie zaopiniowała projekt budżetu UODO na 2025 r. Także ustawodawca docenia znaczenie ochrony danych osobowych dla bezpieczeństwa państwa i rozwoju gospodarki.

*Mirosław Wróblewski*

*Prezes UODO*