URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 10/10/24

www.uodo.gov.pl

SPIS TREŚCI

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. Najsłabszym 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 najsłabsze 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

Drodzy Czytelnicy!

W październiku wciąż krążymy wokół tematu edukacji, szczególnie że jesteśmy świeżo po szkoleniu dla koordynatorów ogólnopolskiego Programu „Twoje dane – Twoja sprawa". Patronat honorowy nad XV edycją Programu objął Minister Edukacji Narodowej i Rzeczniczka Praw Dziecka. Więcej o szkoleniu, które było okazją do wymiany doświadczeń, wiedzy i sprawdzonych rozwiązań w edukacji dotyczących ochrony danych osobowych piszemy w tym numerze Biuletynu.

Wywiad z Tomaszem Izydorczykiem, członkiem Społecznego Zespołu Ekspertów przy PUODO, pasjonatem ochrony danych wprowadzi Was w świat RODO, sztucznej inteligencji i zależności między nimi. Z pewnością na długo zostanie Wam w głowie refleksja nad tym, co może się zdarzyć, jeśli terroryści czy cyberprzestępcy dostaną się do systemu zarządzającego urządzeniami medycznymi, takimi jak roboty asystujące przy operacjach… Nasz ekspert tłumaczy m.in. jak ważne jest uświadamianie społeczeństwu, że na podstawie zwykłych danych można wyciągnąć wnioski dotyczące tzw. danych wrażliwych, o tym, jakie zadania w przyszłości będą mogły powierzyć sztucznej inteligencji takie instytucje użyteczności publicznej jak ZUS czy dlaczego musimy na poważnie potraktować wdrożenie przepisów NIS2 / KSC, by zagwarantować nam wszystkim cyberbezpieczeństwo.

Rola inspektora ochrony danych (IOD) w zapewnieniu zgodności działań organizacji z przepisami RODO jest kluczowa. Jakie są jego obowiązki w przypadku naruszeń ochrony danych osobowych? Czy może działać w imieniu administratora? Wyjaśniamy, jakie zadania może w takich sytuacjach wykonywać, a jakich powinien unikać, aby nie naruszać przepisów prawa.

Udostępnienie przez bank stanu rachunku bankowego sądowi w postępowaniu rozwodowym nie narusza przepisów o ochronie danych. Prezes UODO odmówił wszczęcia sprawy ze skargi obywatela, którego dane o stanie rachunku bankowego i numer rachunku bank udostępnił sądowi. Jak opisujemy w wybranej decyzji Urzędu, to sąd prowadząc postępowanie ocenił, jaki zakres danych osobowych skarżącego, stanowiących tajemnicę bankową był mu niezbędny do rozstrzygnięcia postępowania.

Jak działają publiczne sieci Wi-Fi, jakie zagrożenia mogą wynikać z ich użytkowania oraz jak można chronić swoje dane przed nieautoryzowanym dostępem? Zachęcamy do zapoznania się z materiałem z działu „Nowe Technologie".

W tym wydaniu Biuletynu UODO odpowiada na wątpliwości IOD-a jednego ze starostw, dotyczące

podstawy prawnej pozyskiwania numeru PESEL dłużnika w celu wystawienia tytułu egzekucyjnego od poszczególnych jednostek organizacyjnych funkcjonujących u administratora. Urząd potwierdza, że nie ma przeszkód, by na potrzeby prowadzonego przez starostę postępowania egzekucyjnego wykorzystać numer PESEL dłużnika, który jest przetwarzany w poszczególnych wydziałach starostwa.

Duża liczba skarg, brak zasobów ludzkich i finansowych oraz rosnące obciążenie pracą – to niektóre z wyzwań, przed którymi stoi większość organów ochrony danych przy wdrażaniu RODO – stwierdza nowy raport Agencji Praw Podstawowych UE. Agencja wzywa kraje UE do zapewnienia organom ochrony danych zasobów niezbędnych do zagwarantowania ochrony danych osobowych obywateli.

Komisja Europejska ogłosiła zaproszenie do tworzenia fabryk sztucznej inteligencji w celu zwiększenia wiodącej roli Europy w dziedzinie godnej zaufania sztucznej inteligencji (AI). Fabryki sztucznej inteligencji zostaną utworzone przy użyciu światowej klasy sieci europejskich superkomputerów obliczeniowych o wysokiej wydajności (HPC) i będą dostępne dla szeregu europejskich użytkowników, takich jak startupy, przemysł i naukowcy. Będą połączone z inicjatywami państw członkowskich w zakresie sztucznej inteligencji, tworząc tętniący życiem ekosystem AI.

Na koniec serdecznie zachęcamy do śledzenia kolejnego seminarium organizowanego przez UODO i Społeczny Zespół Ekspertów przy PUODO, tym razem z Konfederacją Lewiatan – „Ochrona zdrowia w zatrudnieniu a RODO". Podczas wydarzenia będziemy rozmawiać o tym, czy obowiązujące regulacje prawne są należycie dostosowane do aktualnych potrzeb i zagrożeń dla zdrowia pracujących, a także czy RODO jest barierą dla aktywnego włączenia sią pracodawców w system ochrony zdrowia publicznego.

Po więcej szczegółów zapraszamy jak zawsze na stronę UODO.

Karol Witowski
p.o. Rzecznika Prasowego UODO

ZASTOSOWANIE SI BĘDZIE BARDZO SZEROKIE, A TO CO NAS OGRANICZA, TO ŚRODKI FINANSOWE I WYOBRAŹNIA

Z Tomaszem Izydorczykiem, członkiem Społecznego Zespołu Ekspertów przy PUODO rozmawiał Karol Witowski, p.o. Rzecznika Prasowego UODO

9 października br. w Chorzowie odbyło się seminarium ZUS i UODO „Czas wyzwań – projektowanie systemów AI oraz wdrożenie NIS2 w organizacji". Poprowadził Pan wykład „Analiza ryzyka przy projektowaniu systemów AI". Powiedział Pan na wstępie, że „technologia nie jest niebezpieczna, tylko ludzie, którzy jej używają". Boimy się błędów ludzkich przy wdrażaniu AI, a nie sztucznej inteligencji samej w sobie?

Do takiego wniosku doszedłem podczas jednego z wspólnie organizowanych przez UODO i Społeczny Zespół Ekspertów seminariów. Rozmawiając o ocenie ryzyka, zawsze musimy osadzić te ryzyka w jakimś kontekście, w stanie faktycznym. Wtedy zastanawiamy się jak używana w danym procesie technologia może wpływać na nas, na ludzi, czyli podmiot danych. Aby na to pytanie udzielić odpowiedzi, trzeba najpierw zrozumieć, w jaki sposób dochodzi do przetwarzania danych osobowych z pomocą tej technologii.

Gdy już wiemy, jak wygląda proces przetwarzania, to dochodzimy do naturalnego wniosku, że to nie technologia decyduje o tym, co zrobi z naszymi danymi czy naszą prywatnością. To właśnie człowiek, który korzysta z tej technologii może wpływać na poziom ochrony naszych praw. Spójrzmy na to od strony praktycznej: otrzymujemy spam za pomocą systemu pocztowego nie dlatego, że to ten system podjął taką decyzję. To człowiek ustawił system pocztowy, aby rozsyłał duże ilości wiadomości, które zaśmiecają nasze skrzynki.

Podobnie będzie w przypadku zastosowania sztucznej inteligencji. Ten sam system oparty o sztuczną inteligencję, bazujący na tysiącach doświadczeń nauczycieli i procesach edukacyjnych różnych poziomów edukacyjnych może z jednej strony wspierać system edukacji dostosowany do indywidualnych warunków i potrzeb młodego człowieka, a z drugiej strony może zostać wykorzystany do stygmatyzowania, oceniania lub dyskryminowania określonych grup uczniów, z uwagi na pewne cechy indywidualne. Ten sam system zarządzający bezpieczeństwem migracji czy kontroli granic może posłużyć do zapewnienia bezpieczeństwa granic Unii Europejskiej,

ale równocześnie może być wykorzystany do dyskryminacji na tle rasowym lub etnicznym.

Rolą naszą – osób biorących udział w ocenie ryzyka takich systemów jest dogłębne poznanie możliwości danego systemu sztucznej inteligencji i przewidywanie, jak może on być wykorzystany (przypadkowo lub intencjonalnie) z negatywnym skutkiem dla praw lub wolności ludzi.

Mówi się, że Europa wpadła w pułapkę przeregulowania sztucznej inteligencji przez co jest w tyle za Ameryką, jeśli chodzi o rozwój AI. Wymagania, jakie sobie stawia UE stale rosną, w związku z tym wciąż pracuje nad nowymi rozwiązaniami prawnymi – to sugeruje, że zawsze będziemy w tyle za Stanami. Tymczasem wspomniał Pan, że USA również intensywnie zajmują się projektami aktów prawnych, które mają dotyczyć sztucznej inteligencji.

30 października 2023 r. Prezydent Stanów Zjednoczonych Ameryki wydał Rozporządzenie wykonawcze w sprawie bezpiecznego, pewnego i godnego zaufania rozwoju i użytkowania sztucznej inteligencji[1]. W rozporządzeniu Prezydent Biden podkreśla to, co wcześniej już zostało wspomniane: „Ostatecznie AI odzwierciedla zasady ludzi, którzy ją budują, ludzi, którzy jej używają, i danych, na których jest zbudowana.” Na dedykowanej stronie rządu USA ai.gov możemy monitorować postępy w realizacji rozporządzenia prezydenta.

Z kolei organizacja IAPP[2] także monitoruje globalne polityki prawa w zakresie AI na całym świecie. To są już setki aktów lub projektów aktów prawnych, działań o charakterze legislacyjnym lub tzw. „miękkich wytycznych”. Uniwersytet Stanforda odnotował ogromny wzrost liczby krajów, których prawa zawierają termin „AI” – z 25 krajów w 2022 r. do 127 w 2023 r.[3] Europejczycy uchwalili AI Act (najprawdopodobniej pierwsi), ale czeka nas jeszcze długa droga uzupełnienia regulacji o krajowe przepisy i uruchomienie operacyjne urzędów ds. sztucznej inteligencji w każdym kraju członkowskim.

Z kolei MIT Technology Review[4] podaje, że „Ponad 120 projektów ustaw związanych z regulacją sztucznej inteligencji krąży obecnie w Kongresie USA”. Jak widać cały świat już to robi lub zamierza

[1] Źródło: https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/ oraz https://www.govinfo.gov/content/pkg/FR-2023-11-01/pdf/2023-24283.pdf

[2] Global AI Law and Policy Tracker https://iapp.org/media/pdf/resource_center/global_ai_legislation_tracker.pdf

[3] Źródło: https://www.europarl.europa.eu/RegData/etudes/ATAG/2024/757605/EPRS_ATA(2024)757605_EN.pdf

[4] Źródło: https://www.technologyreview.com/2024/09/18/1104135/the-download-congresss-ai-bills-and-snaps-new-ar-spectacles/

„regulować” sztuczną inteligencję, a właściwie jej tworzenie i użytkowanie.

I właśnie, żeby nie pozostawać za Stanami Zjednoczonymi, nasza rola jest taka, aby dokładnie poznać, jak działa sztuczna inteligencja, bardzo dobrze znać przepisy i umieć je interpretować. Można by zapytać: dlaczego? Jeśli okaże się, że SI wymyka się nam spod kontroli albo nadmierna regulacja SI blokuje konkurencyjność czy efektywność europejskiego wykorzystania sztucznej inteligencji, to będzie nam – praktykom, ekspertom bardzo łatwo pokazać prawodawcom czy decydentom politycznym, jakie zmiany w prawie trzeba zrobić, aby nie pozostawać w tyle. Jedną z dróg do osiągnięcia tego celu jest właśnie edukacja poprzez debaty, konferencje, seminaria, artykuły i każda inna forma uświadamiana – w tym właśnie także Biuletyn UODO.

Zwrócił Pan uwagę na badania prof. Kosińskiego, który publikował swoje prace nt. wyciągania wniosków statystycznych na podstawie dużych baz danych. Wnioski z tych badań dają dużo do myślenia. Na pewno, żeby przesadnie nie dzielić się informacjami o sobie w mediach społecznościowych.

Z jednej strony jesteśmy „ekshibicjonistami” i lubimy publikować w sieci nasze zdjęcia, komentarze czy inne treści pochodzące od nas, z drugiej strony chcemy, aby „pewne” informacje nie ujrzały światła dziennego lub pozostały w wąskim gronie najbliższych osób.

Niestety mam przykrą wiadomość dla nas wszystkich. To, co wydaje nam się, że jest głęboko ukryte, można wywnioskować z innych informacji, z pozoru nieistotnych, oczywistych czy nie naruszających naszą prywatność nadmiernie. Badania prof. Kosińskiego, ale i wiele innych badań naukowców dowodzą, że przy dużych zbiorach danych/ informacji oraz zestawieniu różnych zbiorów danych nieosobowych z danymi osobowymi, można wywnioskować inne dane, w tym dane szczególnej kategorii. Zrozumienie, że na podstawie danych zwykłych można wyciągnąć wnioski dotyczące tzw. danych wrażliwych przebija się także do świadomości sądów (np. orzeczenia TSUE sygn. C-184/20[5] czy C-252/21[6]). Jeśli tylko do świadomości organów ochrony danych i sądów, a tym samym społeczeństwa dotrze, jaki potencjał drzemie w danych i co na ich podstawie korporacje są w stanie wywnioskować, (co widać na bazie badań naukowych opartych o statystyczne metody ilościowe), może zaczniemy bardziej dbać o to, co udostępniamy w internecie i jakie ślady cyfrowe

[5] Źródło: C-184/20 OT przeciwko Vyriausioji tarnybinės etikos komisja https://curia.europa.eu/juris/document/document.jsf?text=&docid=267507&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=7395047

[6] C-252/21 Meta Platforms Inc., dawniej Facebook Inc., Meta Platforms Ireland Limited, dawniej Facebook Ireland Ltd., Facebook Deutschland GmbH przeciwko przeciwko Verbraucherzentrale Bundesverband eV https://curia.europa.eu/juris/document/document.jsf?text=&docid=276478&pageIndex=0&doclang=PL&mode=req&dir=&occ=first&part=1&cid=7395826

po sobie zostawiamy.

RODO jest podstawową regulacją, na której opierają się pozostałe przepisy: AI Act, DSA, Dora, NIS2, KSC. Jaka jest między nimi relacja i kogo dotyczy AI Act?

Kiedyś w rozmowie z przedstawicielką UODO usłyszałem bardzo ciekawą metaforę. Otóż RODO miało być w tej metaforze dywanem – czyli taką podstawą dla wszystkiego, co na nim stoi. Inne regulacje prawne miały być meblami, które znajdują na tym dywanie. Te meble to właśnie AI Act, DSA, DGA, DA, Dora czy NIS2 i wiele innych regulacji. Wszystko, co łączy te akty prawne to dane. Zarówno dane osobowe, jak i nieosobowe.

W dzisiejszym świecie, mocno technologicznym, trudno jest mówić o danych bez danych osobowych. Nawet smart TV, lodówka podłączona do internetu, czy samochód użytkowane są przez ludzi. Dane, które są generowane przez te urządzenia pochodzą przecież od ludzi i wynikają ze sposobu użytkowania tych urządzeń.

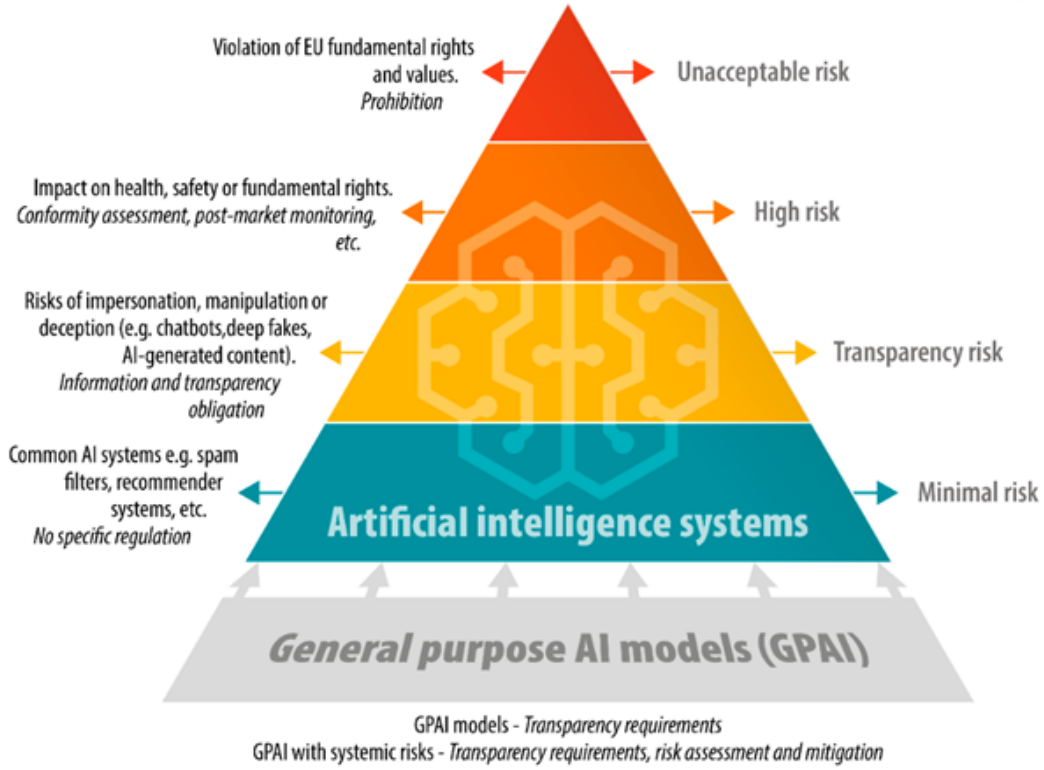
Jeśli chodzi o relacje pomiędzy AI Act a innymi regulacjami, to możemy zobrazować sobie, że za pomocą sztucznej inteligencji możemy realizować obowiązki wynikające ze wszystkich innych aktów prawnych. Możemy wyobrazić sobie, że sztuczna inteligencja będzie realizowała wnioski podmiotów danych o dostęp do danych czy uzyskania kopii danych na podstawie RODO. Podobnie można zaimplementować rozwiązania oparte o sztuczną inteligencję, które będą rozpatrywały wnioski o usunięcie treści nielegalnych na platformach internetowych w oparciu o przepisy DSA.

Automatyczne decyzje dotyczące cyberzagrożeń mogą być rozpoznawane, analizowane przez sztuczną inteligencję, a to będzie realizacja wymogów DORA, NIS2. Jak widać wszystkie te regulacje, które są realizacją strategii Unii Europejskiej polegającej na gospodarce opartej o dane, gospodarce opartej o usługi cyfrowe, przeplatają się między sobą i zazębiają.

Jak unijne rozporządzenie AI Act klasyfikuje systemy sztucznej inteligencji? Jakie są poziomy ryzyka? Jak zarządzać ryzykiem zgodnie z AI Act? Inna jest perspektywa ryzyka z punktu widzenia RODO, a inna z AI Act.

Na bazie lektury Rozporządzenia UE nr 2024/1689 w sprawie sztucznej inteligencji można system SI z uwagi na ryzyko podzielić na cztery klasy systemu o: nieakceptowalnym ryzyku, wysokim ryzyku, transparentnym ryzyku i minimalnym ryzyku.

1 ROZMOWA Z EKSPERTEM



Źródło: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

Zarządzanie ryzykiem w systemach sztucznej inteligencji jest o wiele bardziej sformalizowane i poukładane niż wynikałoby to z przepisów RODO. Organizacje, które będą podlegały pod AI Act będą zmuszone do wprowadzenia systemowego zarządzania ryzykiem, o czym mowa w art. 8 tego rozporządzenia.

Systemowość oznacza ciągły, iteracyjny proces, planowany i realizowany przez cały cykl życia systemu AI wymagający regularnego systematycznego przeglądu i aktualizacji. Proces ten obejmuje następujące cztery główne etapy:

1) identyfikację i analizę znanego i dającego się racjonalnie przewidzieć ryzyka,

2) oszacowanie i ocenę ryzyka, jakie może wystąpić podczas wykorzystywania systemu AI,

3) ocenę innego mogącego wystąpić ryzyka na podstawie analizy danych zebranych z systemu monitorowania,

4) przyjęcie odpowiednich i ukierunkowanych środków zarządzania ryzykiem.

Dla nas, praktyków ochrony danych, nie jest to nic zaskakującego czy nowatorskiego. Jeśli mówimy o prawdziwym systemie ochrony dany osobowych zgodnym z RODO, wydaje się że systemowe podejście do zarządzania ryzykiem jest kluczem do zapewnienia zgodności, nawet jeśli ta „systemowość” nie jest wymuszana regulacją. W przypadku systemów sztucznej inteligencji,

w szczególności wysokiego ryzyka, ta systemowość będzie wymuszona przez przepisy.

Perspektywa ryzyka zarówno z RODO, jak i AI Act jest bardzo zbliżona do siebie. Zarówno w przepisach o ochronie danych, jak i w przepisach o sztucznie inteligencji w centrum zainteresowania jest człowiek i jego prawa. W przypadku RODO mówimy o ochronie praw każdej pojedynczej jednostki, natomiast w przypadku systemów sztucznej inteligencji będziemy minimalizować skutki, jakie mogą mieć wpływ nie tylko na ludzi, ale i poziom ochrony zdrowia, bezpieczeństwa, praworządności i ochrony środowiska, co wynika z art. 1 ust. 1 AIA.

To, że rozporządzenie ws. sztucznej inteligencji wprowadza regulacje dotyczące oceny ryzyka, nie oznacza że jej przeprowadzenie zwalniać będzie administratora z ogólnej oceny ryzyka naruszenia praw i wolności wynikających z RODO. Dlatego nie zapominajmy, że ten sam proces / system, jeśli będzie oparty o sztuczną inteligencję i jednocześnie przetwarzał dane osobowe, będziemy musieli dokonać oceny z dwóch punktów widzenia (dwóch regulacji).

Wykorzystanie sztucznej inteligencji do analizy wniosków o wypłatę świadczeń w ZUS-ie to możliwa niedługa przyszłość? Jakie jeszcze zadania będziemy mogli powierzyć sztucznej inteligencji?

Wierzę, że jest to możliwe. Już teraz wiele typów wniosków o wypłatę świadczeń zostało w wysokim stopniu zautomatyzowanych. Do takiego modelu dąży nie tylko ZUS, ale i cały sektor ubezpieczeń, mając na celu obniżanie kosztów procesu, przyspieszanie jego realizacji i wykrywania nadużyć.

Wydaje się, że zadania, jakie będziemy mogli powierzyć sztucznej inteligencji nie mają końca. Zaczęliśmy od prostych rzeczy jak gry w szachy, analizowanie obrazów, wykrywanie chorób na zdjęciach rentgenowskich. Aktualnie za pomocą AI generujemy treści (teksty), obrazy, nawet muzykę. Już dziś możemy korzystać z prostych rozwiązań jak podpowiedzi w treści e-maili, które na co dzień piszemy w systemach pocztowych, korektę tekstu, który wpisujemy za pomocą klawiatury, zamianę treści rozmów nagranych za pomocą plików audio na tekst pisany (tzw. transkrypcji), a nawet tłumaczenia symultaniczne. Napominajmy o tym, że SI może być wykorzystywana do generowania fajowych zdjęć, treści czy postów w mediach społecznościowych. Z pewnością zastosowanie sztucznej inteligencji będzie bardzo szerokie, a to co nas ogranicza, to środki finansowe i wyobraźnia.

Łatwo nam wyobrazić sobie zastosowanie AI w komercji. Z jakich zastosowań sztucznej inteligencji mógłby teoretycznie skorzystać ZUS czy inne instytucje użyteczności publicznej? Jakie korzyści mogą płynąć z tej technologii dla obywatela?

1 ROZMOWA Z EKSPERTEM

Myślę, że duże podmioty publiczne takie jak właśnie ZUS mogą skorzystać z zastosowania sztucznej inteligencji wszędzie tam, gdzie posiadają duże ilości danych, a obsługiwane procesy są w miarę powtarzalne, jednakże wymagają analizy informacji wpływających do urzędu.

Jeżeli do danego podmiotu wpływają masowo podobne wnioski i podmiot ten posiada wiedzę na temat tego, jakie one były do tej pory, to sztuczna inteligencja mogłaby takie wnioski analizować i rozpatrywać. W ten sposób najbardziej żmudną pracę, którą muszą wykonywać ludzie można zastąpić algorytmami SI. Oczywiście wymagałoby to wprowadzenia systemu kontroli jakości i prawidłowości rozpatrywanych spraw.

Wyobrażam sobie, że równolegle do systemu opartego o sztuczną inteligencję pracowałby merytoryczny zespół pracowników kontrolujący efekty pracy SI oraz rozpatrujący odwołania lub sprzeciwy co do wyłącznie zautomatyzowanego podejmowania decyzji. Na końcu takiej usługi publicznej obywatel o wiele szybciej załatwia tę sprawę, z uwagi na to, że systemy AI mogą pracować 24 h na dobę. Zaoszczędzony w ten sposób czas można poświęcić na bardziej dokładne analizowanie tych spraw, które będą kierowane do rozpatrywania przez zespoły ludzi. Pracownicy nie będą przeładowani ilością spraw i będą mieli więcej czasu na merytoryczne rozpoznanie danej sprawy. I może dzięki tym sposobom uda nam się w przyszłości pracować cztery, a nie pięć dni w tygodniu.

Na jakie kwestie szczególnie muszą uważać instytucje przy wdrażaniu rozwiązań opartych na AI?

Moim zdaniem najważniejszą kwestią, na którą muszą zwrócić uwagę instytucje przy wdrażaniu rozwiązań opartych o sztuczną inteligencję jest zagadnienie danych treningowych.

Mamy takie polskie powiedzenie „Czego Jaś się nie nauczy, tego Jan nie będzie umiał”. To powiedzenie idealnie pasuje do ryzyka, jakie mamy w związku z rozwojem sztucznej inteligencji. W zależności od tego, jakie dane wejściowe zostaną wykorzystane do nauki sztucznej inteligencji, możemy otrzymać w rezultacie lepsze lub gorsze wyniki działania takiego systemu. Oczywiście jest to istotne pod warunkiem, że osoby, które będą trenowały sztuczną inteligencję, a następnie ją wykorzystywały mają dobre intencje i będą to robiły w celu poprawy jakości życia ludzi, a nie przeciwko nam.

W czasie konferencji „Ochrona danych w robotyce medycznej w dobie AI ACT i EHDS” prowadził Pan debatę o robotach medycznych w kontekście cyberzagrożeń. Jakie są najważniejsze wnioski z tej dyskusji?

1 ROZMOWA Z EKSPERTEM

Z mojego punktu widzenia najważniejsze wnioski, jakie płyną z tej konferencji są dwa.

Pierwszy to taki, że niezależnie od tego, ile milionów złotych wydamy na najnowocześniejsze i najlepsze roboty ratujące zdrowie i życie ludzi, mogą one nie być zdolne do leczenia, jeśli nie zadbamy o cały ekosystem cyberbezpieczeństwa i cyberhigieny w zakresie całego podmiotu medycznego.

Drugi wniosek nasuwa się taki, że w kontekście ostatnich wydarzeń na Bliskim Wschodzie (wybuchające pagery, telefony i inne urządzenia ICT), musimy na serio potraktować wdrożenie przepisów NIS2 / KSC i zapewnić cyberbezpieczeństwo w całym łańcuchu dostaw.

Jeśli tak małe i tanie urządzenia mogą wyrządzać ludziom taką krzywdę, to wyobraźmy sobie co może się zdarzyć, jeśli terroryści czy cyberprzestępcy dostaną się do systemu zarządzającego robotem medycznym czy innymi urządzeniami medycznymi?

To już nie chodzi tylko o życie czy zdrowie jednego człowieka, który będzie operowany takim robotem medycznym. Ale chodzi o tysiące urządzeń diagnostycznych, monitorujących czy dawkujących leki. Dla terrorystów czy przestępców nie ma żadnej granicy, której by nie przekroczyli, a rozwój nowoczesnej medycyny jest silnie skorelowany i zależy od urządzeń przetwarzających dane i podłączanych do internetu.

Branża medyczna należy do jednej z ulubionych ofiar hakerów. Czy da się w ogóle w pełni zapewnić bezpieczeństwo danych medycznych? Z optymistycznych konkluzji w trakcie spotkania paneliści poruszyli temat certyfikacji robotów medycznych, które dają pewne gwarancje ochrony danych.

Zapewnienie bezpieczeństwa danych to nie jest stan zero-jedynkowy. To proces nieustannej analizy zagrożeń, oceny ryzyka, wprowadzania środków bezpieczeństwa, monitorowania i wdrażania działań korygujących i zapobiegawczych.

Podobnie jak w medycynie coraz częściej podchodzi się do pacjenta holistycznie, tak samo my w ochronie i bezpieczeństwie danych musimy podchodzić całościowo i kompleksowo. To może oznaczać, że przy obsłudze takiego skomplikowanego i bardzo nowoczesnego robota medycznego musimy zapewnić nie tylko kompetentnych i wyszkolonych lekarzy, inżynierów utrzymujących i rozwijających takiego robota, ale także naszych „zakładowych informatyków", którzy zagwarantują, że ten robot będzie miał możliwość egzystencji w ekosystemie podmiotu medycznego.

Nie zapominajmy w tym holistycznym podejściu o inspektorach ochrony danych, którzy muszą wykazać się wyjątkowo interdyscyplinarną wiedzą na temat ochrony danych w związku z całym ekosystemem szpitala, nie tylko ich pracownikami, systemami informatycznymi, ale także

urządzeniami, które przetwarzają dane pacjentów. Wyroby czy roboty medyczne, systemy zarządzania bezpieczeństwem informacji należy certyfikować i regularnie poddawać audytom zewnętrznym.

Jestem ciekawy, jak Pan odpowie na pytanie, które sam Pan zadał uczestnikom swojego panelu: Poufność, dostępność, integralność danych. Który z tych trzech elementów jest najbardziej istotny dla człowieka, który korzysta z usług sektora medycznego?

Biorąc pod uwagę nasz kontekst kulturowy, my Polacy często rozmawiamy z wieloma osobami na temat naszego stanu zdrowia. Dlatego nie uważam, aby poufność była najistotniejsza, w sytuacji kiedy integralność danych może oddziaływać bezpośrednio na zdrowie lub życie pacjenta w podmiocie medycznym. Oczywiście nie mówię o sytuacji, kiedy wyciekają dane dotyczące zdrowia osób eksponowanych np. politycznie lub biznesowo.

Myślę, że przeciętny Kowalski nie będzie tak bardzo zirytowany czy zestresowany w momencie, kiedy dowie się, że wyciekły jego wyniki badań diagnostycznych. Natomiast jeśli ten sam Kowalski zobaczy nie swoje wyniki badań, które zostały przypisane jemu (naruszenie integralności) poziom stresu takiego Kowalskiego może doprowadzić do opłakanych skutków.

Podobnie będzie w przypadku leczenia wady wzroku. To, że noszę okulary widać i raczej nie mam z tym problemu, aby ktoś dowiedział się o tym, że leczę się u okulisty. Jednakże bardzo chciałbym wierzyć w to, że program, który został przygotowany do laserowej korekty wzroku nie miał żadnej ingerencji z zewnątrz i podane parametry działania tego urządzenia nie zostały zmienione i są dostosowane do mojej wady wzroku.

Biorąc pod uwagę ten właśnie kontekst uważam, że w przypadku podmiotów medycznych integralność danych, a także ciągłość dostępu do danych oraz ciągłość realizacji usług przez systemy informatyczne szpitala są kluczowe z punktu widzenia zdrowia i życia podmiotów danych, czyli pacjentów podmiotów leczniczych.

W Społecznym Zespole Ekspertów przy PUODO podnosi Pan świadomość społeczną na temat ochrony danych osobowych. To ważna rola. Dodam, że jest Pan bardzo aktywnym członkiem zespołu. Przypomnijmy, że wziął Pan również udział w innym seminarium UODO i ZUS „Ochrona danych jako element odporności społeczeństwa i państwa", w bardzo dla nas ważnym spotkaniu ekspertów dotyczącym praktycznych problemów w stosowaniu przepisów ustawy o ochronie sygnalistów z perspektywy

1 ROZMOWA Z EKSPERTEM

RODO, a także w konferencji „Świat robotyki medycznej a ochrona danych osobowych". Jak ocenia Pan działanie zespołu i efekty jego pracy?

Trudno jest mi oceniać efekty pracy zespołu, gdy jestem jego częścią. Jeszcze trudniej oceniać mi efekty, ponieważ będą one o wiele bardziej widoczne najprawdopodobniej w kolejnych latach naszej działalności.

To, co mogę powiedzieć to, że jestem dumy z zaangażowania członków naszego zespołu, bo poświęcają sporo czasu na to, abyśmy mogli zrealizować choć część naszych pomysłów. Jestem pod wrażeniem ilości inicjatyw, które uruchomiliśmy lub które jeszcze czekają na otwarcie we współpracy z Urzędem Ochrony Danych Osobowych. Bardzo pozytywnie oceniam otwartość naszych ekspertów na wszelkie prośby, wnioski czy sugestie zarówno ze strony kierownictwa UODO, jak i pracowników urzędu.

Nie jest żadną tajemnicą, że wielu z nas często krytykowało działania UODO, a między nami nie zawsze istnieje zgodność i jednolitość poglądów. To, co jest jednak budujące, to że potrafimy wspólnie rozmawiać, spierać się na argumenty w przyjaznej atmosferze, a przede wszystkim przyjmować i analizować poglądy organu ochrony danych. Dla mnie osobiście pozytywnym efektem, który już ma miejsce, a który może nie łatwo dostrzec, jest wzajemna wymiana poglądów pomiędzy urzędnikami a nami, reprezentującymi świat nauki, doktryny i rynku.

Osobiście otrzymuję też dużo pozytywnych sygnałów od środowisk inspektorów ochrony danych na temat wspólnie organizowanych konferencji i seminariów, które mają przede wszystkim cele edukacyjne, co uważam za najważniejsze z punktu widzenia systemów ochrony danych osobowych.

Jako członek Społecznego Zespołu Ekspertów przy PUODO aktywnie uczestniczy Pan w pracach nad poradnikiem ds. zgłaszania naruszeń. Jak się pracuje w tak dużym i zróżnicowanym zespole?

Praca w dużym zespole zawsze jest wyzwaniem. Przede wszystkim w wymiarze logistyczno-czasowym. Ilość materiału, która jest do przeczytania lub do skomentowania nie ma końca.

Mam ogromną potrzebę rozmowy z każdym i konfrontowania poglądów, szczególnie z tymi osobami, z których podglądami na dany temat się nie zgadzam. Tylko w ten sposób mogę przekonać się, czy moje myślenie jest prawidłowe czy może jest obarczone jakimś błędem.

Ale najważniejsze jest to, że taka pozytywna konformacja poglądów i spór na argumenty jest najlepszą formą tworzenia wartościowych treści, które powinny się znaleźć w poradnikach, które przecież będą czytane przez setki, jak nie tysiące osób. Natomiast zróżnicowanie zespołu nie odbieram jako coś negatywnego czy utrudniającego, wręcz przeciwnie, jako coś co może poprawić jakość naszej pracy.

1 ROZMOWA Z EKSPERTEM

Nie od dziś wiadomo, że różnorodność środowiska /otoczenia ma wiele zalet i pozytywny wpływ na rozwój ludzi. Dlatego jestem przekonany, że uda nam się wspólnymi siłami oddać w ręce nie tylko inspektorów, wartościowy materiał do pracy.

Poza pełnieniem funkcji członka SZE, prowadzi Pan bloga, kanał na YouTube, szkolenia, konsultacje, jest Pan inspektorem ochrony danych, wykładowcą, audytorem, autorem licznych publikacji, członkiem zarządu w NewTechLaw.eu sp. z o.o. Pomimo tylu obowiązków, podchodzi Pan do kolejnych wyzwań pełen niesłabnącej energii. Czy kluczem do tego jest pasja, której z pewnością Panu nie brakuje?

Pamiętam pierwszy dzień – 4 czerwca, gdy otrzymaliśmy powołanie do Społecznego Zespołu Ekspertów od pana prezesa Mirosława Wróblewskiego. Po zakończeniu całego dnia, jechaliśmy windą wspólnie z prawnikami UODO i padło stwierdzenie, że spotkanie naszego zespołu odbyło się w bardzo miłej i sympatycznej atmosferze. Odpowiedziałem wtedy, że my wszyscy mniej lub bardziej znamy się, często spieramy się merytorycznie i nie zawsze się ze sobą zgadzamy, ale za to się lubimy. A to, co nas wszystkich łączy, to właśnie pasja do ochrony danych osobowych i my naprawdę lubimy to, co robimy.

Dla mnie ochrona danych osobowych to wielowymiarowa i interdyscyplinarna dziedzina (prawa, informatyki, nowych technologii i zarządzania), w której nie da się nudzić, zawsze jest coś do zrobienia, ale można też poznać bardzo ciekawych i wyjątkowo sympatycznych ludzi.

Peter F. Drucker twierdził, że najmniej wydajna jest praca niewolnika, a najbardziej wydajna jest praca ochotnika. W takiej dziedzinie jak ochrona danych osobowych, z takimi ludźmi, praca i cała moja aktywność jest dla mnie przyjemnością, a nie obowiązkiem.

Dziękuję za rozmowę.

PRZEKAZYWANIE NUMERU PESEL NA POTRZEBY PROWADZENIA POSTĘPOWANIA EGZEKUCYJNEGO

Nie ma przeszkód, by na potrzeby prowadzonego przez starostę postępowania egzekucyjnego wykorzystać numer PESEL dłużnika, który jest przetwarzany w poszczególnych wydziałach starostwa.

Przepisy Prawa o ruchu drogowym (art. 73aa, art. 78 ust. 2 pkt 1, art. 140mb) zobowiązują właścicieli pojazdów do złożenia odpowiednio wniosku o ich rejestrację po nabyciu lub zawiadomienia o zbyciu pojazdu. Za niedopełnienie tego obowiązku przewidziane są kary pieniężne nakładane w drodze decyzji administracyjnej. Jednak zgodnie z art. 107 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego oraz stanowiskiem UODO (zawartym m.in. w decyzji ZSPU.440.379.2018 oraz wyrażonym w materiale „Czy rozsyłanie „rozdzielników" do uczestników postępowań administracyjnych nie narusza przepisów ustawy o ochronie danych osobowych?") decyzje te nie zawierają numeru PESEL karanego. Gdy właściciel pojazdu nie zapłaci nałożonej kary, starosta wszczyna postępowanie egzekucyjne. Jednak stosownie do art. 27 ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji w tytule wykonawczym wierzyciel (w tym przypadku starosta) musi podać m.in. numer PESEL dłużnika.

W tej sytuacji IOD jednego ze starostw nabrał wątpliwości, jaka jest podstawa prawna pozyskiwania numeru PESEL dłużnika w celu wystawienia tytułu egzekucyjnego od poszczególnych jednostek organizacyjnych funkcjonujących u administratora. Czy wydział komunikacji, który przetwarza numer PESEL danej osoby w związku z realizacją zadań określonych w Prawie o ruchu drogowym, może udostępnić go wydziałowi finansowemu w celu wystawienia tytułu wykonawczego?

W odpowiedzi UODO podkreślił, że organy administracji publicznej są zobowiązane działać w granicach i na podstawie obowiązujących przepisów prawa regulujących ich funkcjonowanie. Zgodnie zaś z art. 6 ust. 1 RODO przetwarzanie danych (w tym ich udostępnianie) jest zgodne z prawem m.in. wtedy, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze (lit. c).

Przepisy ustawy – Prawo o ruchu drogowym (art. 73 i nast.) stanowią, że w sprawie rejestracji pojazdów właściwym organem jest starosta, który na te potrzeby przetwarza dane osobowe ich właścicieli. Wyraźnie wskazują też (art. 80b), jakie dane osobowe są gromadzone w ewidencji

pojazdów, wymieniając wśród nich m.in. numer PESEL właściciela czy posiadacza pojazdu. Ponadto określają, jakie podmioty i w jakim zakresie wprowadzają dane do ewidencji (art. 80ba) oraz jakie podmioty mają dostęp do tych danych (art. 80bb), a także komu i w jakim zakresie można je udostępnić (art.80c). Zgodnie z art. 80c ust. 1 dane zgromadzone w ewidencji udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, m.in. organom właściwym w sprawach rejestracji pojazdów czy administracyjnym organom egzekucyjnym oraz organom podatkowym. Jeśli zaś starosta występuje w roli organu egzekucyjnego, to istnieje podstawa prawna do pozyskania numeru PESEL z ewidencji pojazdów.

Niewykonanie zobowiązania wynikającego z decyzji administracyjnej, tj. niezapłacenie kary, rozpoczyna bieg nowej procedury, zgodnie z przepisami o egzekucji administracyjnej. Stosownie do art. 27 § 1 pkt 2 ustawy o postępowaniu egzekucyjnym w administracji tytuł wykonawczy powinien zawierać m.in. wskazanie imienia, nazwiska lub firmy zobowiązanego i jego adresu, a także NIP-u lub numeru PESEL, jeżeli zobowiązany taki numer posiada. Przepis ten jest przesłanką legalizującą proces przetwarzania danych osobowych w odniesieniu do danych zawartych w wystawionym tytule wykonawczym. Konieczność przetwarzania numeru PESEL w tytule wykonawczym przez organ egzekucyjny (np. starostę) wynikająca z ww. przepisu prawa spełnia jednocześnie przesłankę z art. 6 ust. 1 lit. c RODO.

Także przepisy ustawy z dnia 24 września 2010 r. o ewidencji ludności wskazują, jakim organom i na jakich zasadach oraz w jakim celu można udostępnić dane z rejestru PESEL (art. 46) oraz określają zasady udostępniania danych w drodze teletransmisji danych (art. 48, art. 49). Stanowią (art. 46 ust. 1), że dane z rejestru PESEL oraz rejestrów mieszkańców w zakresie niezbędnym do realizacji ich ustawowych zadań udostępnia się m.in. organom administracji publicznej, sądom i prokuraturze (pkt 1).

Skoro zatem starosta, jako administrator ma prawo przetwarzać numer PESEL w ramach swoich ustawowych zadań wykonywanych jako organ egzekucyjny wobec administracyjnych kar pieniężnych, to kwestia przekazywania danych pomiędzy wydziałami tego administratora nie powinna być rozpatrywana w kategoriach udostępniania danych. Mamy bowiem cały czas do czynienia z przetwarzaniem danych w ramach struktury organizacyjnej jednego administratora.

UDOSTĘPNIENIE PRZEZ BANK STANU RACHUNKU BANKOWEGO SĄDOWI W POSTĘPOWANIU ROZWODOWYM NIE NARUSZA PRZEPISÓW O OCHRONIE DANYCH

Prezes UODO odmówił wszczęcia sprawy ze skargi obywatela, którego dane o stanie rachunku bankowego i numer rachunku bank udostępnił sądowi. Bank zrobił to na wniosek sądu w sprawie o podział majątku po rozwodzie.

Skarżący uważał, że wezwanie sądowe dotyczyło tylko jego danych związanych z podziałem majątku wspólnego – jego i byłej żony. Tymczasem bank przekazał też informacje dotyczące okresu po ustaniu małżeństwa. Wykraczało to poza okres pozostawania we wspólnocie małżeńskiej, tym samym stanowiło naruszenie tajemnicy bankowej.

Bank zaś argumentował, że wykonał postanowienie sądu i przekazał mu dokładnie takie dane, jakich sąd potrzebował.

Prezes UODO uznał po analizie sprawy, że rzeczywiście bank nie był uprawniony do kwestionowania zakresu żądanych przez sąd danych osobowych. To sąd prowadząc postępowanie ocenił, jaki zakres danych osobowych skarżącego, stanowiących tajemnicę bankową, był mu niezbędny do rozstrzygnięcia postępowania cywilnego w przedmiocie podziału majątku wspólnego.

Argumentacja PUODO

Decyzją z 25 lipca 2025 r. Prezes UODO odmówił uwzględnienia wniosku wskazując m.in., że zgodnie z art. 105 ust. 1 pkt 2 lit. d Prawa bankowego, bank ma obowiązek udzielenia informacji stanowiących tajemnicę bankową wyłącznie na żądanie sądu w związku z prowadzonym postępowaniem spadkowym lub o podział majątku między małżonkami albo prowadzoną przeciwko osobie fizycznej będącej stroną umowy sprawą o alimenty lub o rentę o charakterze alimentacyjnym.

Sąd posiada uprawnienie do żądania udostępnienia przez bank informacji objętych tajemnicą bankową w związku z prowadzonym postępowaniem. Uprawnienie to określone przepisem art. 105 Prawa bankowego nie budzi wątpliwości.

Jak wskazuje się w doktrynie, sąd może uzyskiwać wszelkie informacje bankowe, nieograniczone

jedynie do tych związanych z danym rachunkiem bankowym. Banki posiadają zatem uprawnienie, ale też i obowiązek, do udzielania informacji objętych tajemnicą bankową wyłącznie na rzecz sądu, nie zaś uczestników czy wnioskodawców tego postępowania (K. Osajda (red. serii), J. Dybiński (red. tomu), Prawo bankowe. Wyd. 1, Warszawa 2023). (…)

Podkreślić należy, że art. 105 ust. 1 pkt 2 lit. d Prawa bankowego nie zawiera ograniczenia co do zakresu danych, stanowiących tajemnicę bankową, których może żądać sąd w związku z prowadzonym postępowaniem o podział majątku między małżonkami. Należy więc uznać, że bank udzielając odpowiedzi na żądanie sądu, który wskazał w wezwaniu na żądanie informacji w związku z postępowaniem o podział majątku, nie był uprawniony do kwestionowania zakresu żądanych przez sąd danych osobowych skarżącego zawartych w wyciągach z rachunków bankowych za pełny dostępny okres oraz informacji o stanie rachunku na dzień 23 lipca 2018 r.

To sąd prowadząc postępowanie ocenił bowiem jaki zakres danych osobowych skarżącego, stanowiących tajemnicę bankową był mu niezbędny do rozstrzygnięcia postępowania cywilnego w przedmiocie podziału majątku wspólnego. Bank w ocenie organu był zatem zobowiązany do spełnienia obowiązku prawnego i wykonania wezwania sądu. Dlatego udostępnienie przez bank danych osobowych zawartych w wyciągach bankowych na rzecz sądu miało oparcie w art. 6 ust.1 lit. c RODO, gdyż było niezbędne do realizacji obowiązku prawnego wynikającego z art. 105 ust. 1 pkt 2 lit. d Prawa bankowego.

Sygnatura sprawy: DS.523.4463.2023

Fot. pixabay

ROLA IOD PRZY NARUSZENIACH OCHRONY DANYCH OSOBOWYCH

Rola inspektora ochrony danych (IOD) w zapewnieniu zgodności działań organizacji z przepisami RODO jest kluczowa. Jakie są jego obowiązki w przypadku naruszeń ochrony danych osobowych? Czy może działać w imieniu administratora? Wyjaśniamy, jakie zadania może w takich sytuacjach wykonywać, a jakich powinien unikać, aby nie naruszać przepisów prawa.

Jak IOD może wspierać administratora?

IOD jest ważnym uczestnikiem procesu zarządzania naruszeniami ochrony danych osobowych. Jego zadania w tym obszarze obejmują przede wszystkim:

• **doradzanie** administratorowi (art. 39 ust. 1 lit. a) RODO);

• **monitorowanie** zgodności działań podejmowanych przez administratora z przepisami RODO i przyjętymi procedurami (art. 39 ust. 1 lit. b) RODO);

• **pełnienie funkcji punktu kontaktowego**, od którego organ nadzorczy i osoby, których dane dotyczą, mogą uzyskać dodatkowe informacje (art. 39 ust. 1 lit. e) RODO i art. 34 ust. 2 RODO w zw. z art. 33 ust. 3 lit. b) RODO);

• **zwiększanie świadomości** personelu administratora, organizowanie szkoleń oraz inne inicjatywy, które przyczyniają się do **zapobiegania** powstawaniu naruszeń ochrony danych osobowych (art. 39 ust. 1 lit. b) RODO).

Czego IOD powinien unikać?

Jednocześnie IOD nie może realizować obowiązków, za których wykonanie zgodnie z RODO odpowiada wyłącznie administrator. W praktyce oznacza to, że IOD **nie powinien**:

• **zgłaszać** naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratora, w tym także podpisywać i wysyłać takich zgłoszeń (art. 33 ust. 1 RODO);

• **dokumentować** naruszeń ochrony danych osobowych (art. 33 ust. 5 RODO);

• **zawiadamiać** osób, których dane dotyczą, o naruszeniach ochrony danych osobowych (art. 34 ust. 1 RODO);

• **podpisywać** pism, w których zobowiązuje się do podjęcia określonych działań w imieniu administratora, np. dotyczących bezpieczeństwa przetwarzania (art. 32 ust. 1 RODO);

• oraz w inny sposób **działać na podstawie pełnomocnictwa** udzielonego przez administratora w sprawach dotyczących ochrony danych osobowych.

Dlaczego nakładanie tych obowiązków na IOD jest niewłaściwe?

Wykonywanie przez IOD zadań zarezerwowanych dla administratora jest sprzeczne z RODO i wywołuje pewne problemy:

• **Ograniczenie niezależności:** Udzielanie IOD pełnomocnictwa do działania w imieniu administratora narusza jego niezależność. Pełnomocnictwo wiąże się z koniecznością realizacji określonych poleceń, co stoi w sprzeczności z przepisami RODO, które zabraniają wydawania IOD instrukcji dotyczących wykonywania jego zadań (art. 38 ust. 3 RODO).

• **Konflikt interesów:** IOD ma nadzorować zgodność przetwarzania z przepisami o ochronie danych osobowych. Jeżeli samodzielnie realizuje zadania spoczywające na administratorze lub działa w jego imieniu, traci zdolność dokonywania obiektywnej oceny. Prowadzi to do konfliktu interesów. RODO zakazuje takich praktyk (art. 38 ust. 6 RODO).

Konsekwencje naruszania przepisów RODO

Łamanie przepisów dotyczących statusu IOD może mieć poważne konsekwencje dla organizacji. To m.in. utrata zaufania ze strony pracowników, klientów i partnerów biznesowych, ale także możliwość zastosowania przez Prezesa UODO uprawnień naprawczych, takich jak administracyjna kara pieniężna.

O czym warto pamiętać?

Podsumowując, IOD pełni w organizacji funkcję informacyjną, doradczą, monitorującą i nadzorczą. Aby skutecznie wykonywać swoje zadania, musi zachować autonomię, obiektywizm oraz unikać konfliktu interesów. Właściwe zrozumienie i respektowanie roli IOD to nie tylko wymóg prawny, ale także kluczowy element systemu bezpieczeństwa danych. Odpowiedni podział obowiązków pozwoli na efektywniejsze zarządzanie naruszeniami ochrony danych osobowych.

PUBLICZNE SIECI WI-FI – JAK CHRONIĆ SWOJE DANE?

Jak działają publiczne sieci Wi-Fi, jakie zagrożenia mogą wynikać z ich użytkowania oraz jak można chronić swoje dane przed nieautoryzowanym dostępem?

Jednym z kluczowych elementów, które ułatwiają nam korzystanie z internetu, są publiczne sieci Wi-Fi. Spotykamy je np. kawiarniach, na lotniskach, w hotelach, a nawet w parkach. Dzięki nim możemy bez problemu przeglądać strony internetowe, sprawdzać pocztę elektroniczną, korzystać z mediów społecznościowych czy wykonywać transakcje online.

Jednak korzystanie z publicznych sieci Wi-Fi wiąże się z pewnymi zagrożeniami, zwłaszcza w kontekście ochrony danych osobowych.

Jak działają publiczne sieci Wi-Fi?

Publiczne sieci Wi-Fi to bezprzewodowe sieci lokalne, które umożliwiają użytkownikom łączenie się z internetem na zasadzie radiowej transmisji danych. Sygnał przesyłany jest za pośrednictwem fal radiowych. Sieci te często są otwarte, co oznacza, że każdy, kto znajduje się w zasięgu sygnału, może się do nich podłączyć, często bez potrzeby wprowadzania hasła.

Wi-Fi jest technologią opartą na standardzie IEEE 802.11, która zapewnia różne poziomy bezpieczeństwa, zależnie od konfiguracji sieci i zastosowanych metod szyfrowania. Publiczne sieci Wi-Fi są zazwyczaj mniej zabezpieczone niż sieci prywatne, co czyni je bardziej podatnymi na ataki cybernetyczne. Niska jakość zabezpieczeń wynika z kilku czynników, w tym z potrzeby łatwego i szybkiego dostępu dla użytkowników oraz z braku kontroli nad tym, kto korzysta z sieci.

Zagrożenia związane z korzystaniem z publicznych sieci Wi-Fi

1. Ataki typu Man-in-the-Middle (MITM)

Jednym z najpoważniejszych zagrożeń, na które narażeni są użytkownicy publicznych sieci Wi-Fi, są ataki typu Man-in-the-Middle. Cyberprzestępca przechwytuje i modyfikuje dane przesyłane między użytkownikiem a serwerem. Przejęcie sesji internetowej może prowadzić do kradzieży poufnych informacji, takich jak dane logowania, hasła czy numery kart kredytowych.

Ataki MITM mogą być szczególnie niebezpieczne, ponieważ użytkownik często nie jest świadomy, że jego połączenie zostało przechwycone. Cyberprzestępca może podszywać się pod znaną witrynę internetową, co sprawia, że ofiara czuje się bezpiecznie, wprowadzając swoje dane osobowe.

2. Fałszywe punkty dostępu (Evil Twin)

Innym popularnym zagrożeniem jest tzw. Evil Twin, czyli fałszywy punkt dostępu. Cyberprzestępca tworzy sieć Wi-Fi o nazwie identycznej lub bardzo podobnej do legalnej sieci dostępnej w danym miejscu, np. „Free_Cafe_WiFi". Gdy użytkownik podłącza się do takiej sieci, wszystkie jego dane są przechwytywane przez atakującego. W ten sposób cyberprzestępca może uzyskać dostęp do wrażliwych informacji, takich jak dane bankowe czy hasła do różnych kont.

Nowo odkryta luka w standardzie Wi-Fi IEEE 802.11, nazwana „SSID Confusion" (CVE-2023-52424), pozwala atakującym na przechwytywanie ruchu sieciowego poprzez przekonanie ofiary do połączenia się z fałszywą, mniej bezpieczną siecią Wi-Fi. Atak wpływa na wszystkie systemy operacyjne i typy sieci, w tym domowe i korporacyjne.

Przebieg Ataku

1. Wykrywanie sieci: Atakujący modyfikuje pakiety Wi-Fi, aby zamienić identyfikatory SSID prawdziwej i fałszywej sieci, co wprowadza ofiarę w błąd.

2. Przejęcie uwierzytelnienia: Ofiara uwierzytelnia się do fałszywej sieci myśląc, że jest to zaufana sieć.

3. Trwający MitM: Atakujący przechwytuje ruch ofiary, zmieniając identyfikatory SSID w czasie rzeczywistym.

Skutki

Atak może dezaktywować VPN w przypadku połączenia się z „zaufaną" siecią, co naraża ruch ofiary na ryzyko. Zaleca się uniknięcie ponownego używania danych uwierzytelniających w różnych sieciach oraz stosowanie unikalnych haseł.

3. Brak szyfrowania danych

Większość publicznych sieci Wi-Fi korzysta z nowoczesnych protokołów szyfrowania, takich jak WPA2 lub WPA3, które oferują wysoki poziom ochrony. Protokół WEP (Wired Equivalent Privacy), który był powszechny kilkanaście lat temu, jest już praktycznie nieużywany ze względu na jego słabe zabezpieczenia. Mimo to, w niektórych przypadkach można jeszcze natrafić na sieci korzystające z WEP lub WPA, co może wynikać z nieaktualizowanego oprogramowania routera lub zaniedbań w konfiguracji sieci.

Zastosowanie przestarzałego protokołu niesie ze sobą poważne ryzyko, gdyż dane przesyłane w takiej sieci mogą być łatwo przechwycone przez osoby trzecie. Nawet jeśli sieć korzysta z WPA2 lub WPA3, warto pamiętać, że publiczne sieci Wi-Fi mogą być podatne na różnego rodzaju ataki, takie jak MITM. Dlatego zawsze warto zachować ostrożność i łączyć się tylko z zaufanymi sieciami, szczególnie

przy przesyłaniu poufnych informacji.

4. Sniffing

Sniffing to technika polegająca na przechwytywaniu danych przesyłanych przez sieć. W publicznych sieciach Wi-Fi, gdzie transmisja danych jest często nieszyfrowana, sniffing staje się bardzo prostym narzędziem do wykradania informacji. Sniffery mogą przechwycić takie dane, jak hasła, wiadomości e-mail, a nawet zawartość przeglądanych stron internetowych. Dlatego tak ważne jest korzystanie z usługi VPN, ponieważ szyfruje on cały ruch internetowy, tworząc bezpieczny tunel między urządzeniem użytkownika a serwerem. Dzięki temu nawet jeśli dane zostaną przechwycone, będą one zaszyfrowane i niemożliwe do odczytania przez osoby trzecie.

5. Złośliwe oprogramowanie

Korzystanie z publicznych sieci Wi-Fi może również zwiększyć ryzyko zainfekowania urządzenia złośliwym oprogramowaniem. W otwartych sieciach cyberprzestępcy mogą wprowadzać złośliwe oprogramowanie na urządzenia użytkowników poprzez różnego rodzaju techniki, takie jak drive-by download (automatyczne pobieranie plików bez wiedzy użytkownika) czy fałszywe aktualizacje oprogramowania. Zainfekowane urządzenie może stać się bramą do wykradania danych osobowych lub innych cennych informacji.

Jak chronić swoje dane podczas korzystania z publicznych sieci Wi-Fi?

1. Unikanie przesyłania poufnych informacji

Jednym z najprostszych sposobów na ochronę swoich danych w publicznych sieciach Wi-Fi jest unikanie przesyłania poufnych informacji, takich jak loginy, hasła czy dane bankowe. Dla takich danych należy lepiej skorzystać z sieci mobilnej lub połączyć się z zaufaną, zabezpieczoną siecią prywatną.

2. Używanie VPN (Virtual Private Network)

Wirtualna sieć prywatna jest jednym z najskuteczniejszych narzędzi do ochrony danych w publicznych sieciach Wi-Fi. Szyfruje wszystkie dane przesyłane między urządzeniem użytkownika a serwerem VPN, co znacznie utrudnia ich przechwycenie przez osoby trzecie. Dzięki temu, nawet jeśli cyberprzestępca przechwyci zaszyfrowane dane, nie będzie mógł ich odczytać.

3. Korzystanie z HTTPS

Przy korzystaniu z publicznych sieci Wi-Fi warto zwracać uwagę na to, czy odwiedzane strony internetowe korzystają z protokołu HTTPS, który zapewnia szyfrowanie danych przesyłanych między przeglądarką a serwerem. Adresy stron korzystających z HTTPS zaczynają się od „https://” zamiast

„http://”. Obecność ikony kłódki w pasku adresu przeglądarki jest również sygnałem, że połączenie jest szyfrowane.

4. Wyłączanie udostępniania plików i drukarek

W publicznych sieciach Wi-Fi zaleca się wyłączenie funkcji udostępniania plików i drukarek, która może umożliwić nieautoryzowany dostęp do danych przechowywanych na urządzeniu. W systemie Windows można to zrobić w ustawieniach sieci, natomiast na urządzeniach Apple opcje te znajdują się w preferencjach systemowych.

5. Aktualizacja oprogramowania

Aktualizacje często zawierają poprawki bezpieczeństwa, które naprawiają wykryte luki w zabezpieczeniach. Korzystając z najnowszych wersji oprogramowania, minimalizujemy ryzyko, że nasze urządzenie stanie się ofiarą cyberprzestępcy.

6. Wyłączenie automatycznego łączenia z sieciami Wi-Fi

Wielu użytkowników nie zdaje sobie sprawy, że ich urządzenia mogą automatycznie łączyć się z sieciami Wi-Fi, które wcześniej były używane. Może to prowadzić do sytuacji, w której urządzenie połączy się z fałszywym punktem dostępu, stworzonym przez cyberprzestępcę. Dlatego warto wyłączyć funkcję automatycznego łączenia się z sieciami Wi-Fi i ręcznie wybierać te, do których chcemy się podłączyć.

Podsumowując, korzystanie z publicznych sieci Wi-Fi, choć wygodne, wiąże się z istotnymi zagrożeniami dla prywatności i bezpieczeństwa naszych danych. Świadomość tych zagrożeń oraz stosowanie odpowiednich środków ostrożności, takich jak korzystanie z VPN, zwracanie uwagi na protokół HTTPS, czy regularne aktualizacje oprogramowania, mogą znacząco zmniejszyć ryzyko. Pamiętajmy, że dbanie o bezpieczeństwo naszych informacji w sieci to nasza wspólna odpowiedzialność, a podejmowanie prostych kroków może uchronić nas przed poważnymi konsekwencjami cyberataków.

Fot. pixabay

BRAK ZASOBÓW UTRUDNIA EGZEKWOWANIE OCHRONY DANYCH W UE

Duża liczba skarg, brak zasobów ludzkich i finansowych oraz rosnące obciążenie pracą – to niektóre z wyzwań, przed którymi stoi większość organów ochrony danych przy wdrażaniu RODO – stwierdza nowy raport Agencji Praw Podstawowych UE (FRA). FRA wzywa kraje UE do zapewnienia organom ochrony danych zasobów niezbędnych do zagwarantowania ochrony danych osobowych obywateli.

Raport FRA "RODO w praktyce – doświadczenia organów ochrony danych" podkreśla kluczowe kwestie, przedstawia najlepsze praktyki oraz sugeruje rozwiązania.

W podsumowaniu raportu zwrócono uwagę na następujące kwestie:

1. Brak zasobów – niedofinansowanie i brak personelu utrudniają organom nadzorczym pełne wykonywanie ich zadań. Nowe przepisy UE, takie jak akt w sprawie sztucznej inteligencji lub unijne systemy informacyjne służące zarządzaniu granicami zewnętrznymi, stworzą dla nich dodatkowe zadania. Trudno będzie je wdrożyć bez odpowiednich zasobów. Kraje UE powinny zabezpieczyć niezbędne zasoby finansowe, ludzkie i techniczne, aby umożliwić organom nadzorczym wypełnianie ich roli;

2. Uprawnienia nadzorcze – organy nadzorcze mają już uprawnienia do prowadzenia postępowań, jednak potrzebują więcej narzędzi, aby wzmocnić swoje zdolności nadzorcze. Obejmują one możliwość prowadzenia niejawnych postępowań lub możliwość nakładania kar finansowych na organizacje, które odmawiają współpracy. Komisja Europejska i Europejska Rada Ochrony Danych (EROD) powinny ocenić, jakie narzędzia są potrzebne i w razie potrzeby wzmocnić ramy prawne;

3. Wymiana najlepszych praktyk – z powodu braku zasobów organy nadzorcze często muszą przedkładać rozpatrywanie skarg nad inne zadania. Aby lepiej wspierać organy w rozpatrywaniu dużej liczby skarg, EROD powinna zapewnić więcej wytycznych i ułatwić wymianę najlepszych praktyk. Może to również wymagać przyznania EROD większych zasobów;

4. Konsultacje i udzielanie porad – z organami nadzorczymi często nie konsultuje się nowych przepisów lub wyznacza się im napięte terminy. Niektóre organy publiczne również nie konsultują się z organami nadzorczymi przed rozpoczęciem operacji przetwarzania danych. Aby zapewnić,

że zasady dotyczące ochrony danych są uwzględniane we wnioskach legislacyjnych, kraje UE powinny konsultować się z organami nadzorczymi i zasięgać ich porad z wyprzedzeniem. Powinny również zachęcać instytucje publiczne do bardziej systematycznych konsultacji z organami nadzorczymi;

5. Podnoszenie świadomości – ludzie nie rozumieją w pełni swojego prawa do ochrony danych osobowych. Organizacje przetwarzające dane osobowe mają trudności z identyfikacją i zapobieganiem zagrożeniom dla ochrony danych, zwłaszcza jeśli chodzi o systemy sztucznej inteligencji. Dlatego też przeprowadzanych jest bardzo niewiele ocen skutków dla ochrony danych. Instytucje UE i kraje UE powinny promować wiedzę na temat zasad i obowiązków w zakresie ochrony danych. EROD powinna opracować szczegółowe wytyczne dotyczące przetwarzania danych z wykorzystaniem nowych technologii;

6. Dostęp do danych na potrzeby badań – badacze nadal mają trudności z dostępem do danych, mimo że unijne przepisy o ochronie danych zezwalają na ich przetwarzanie do celów naukowych. EROD powinna opracować szczegółowe wytyczne i wyjaśnić, co jest możliwe na mocy prawa UE;

7. Nowe technologie – RODO zapewnia przydatne narzędzia do radzenia sobie z nowymi wyzwaniami technologicznymi, jednak wiele organów nadzorczych ma trudności z ich właściwym uregulowaniem. Wraz z organami nadzorczymi EROD powinna zidentyfikować konkretne obszary związane z technologią, w których potrzebna jest większa jasność. Organy nadzorcze powinny ściślej współpracować przy doradzaniu w zakresie nowych technologii.

Raport opiera się na 70 rozmowach przeprowadzonych przez FRA z przedstawicielami organów nadzorczych ze wszystkich 27 państw członkowskich UE. Rozmowy odbyły się między czerwcem 2022 r. a czerwcem 2023 r.

Raport dostępny jest po angielsku: Lack of resources undermine EU data protection enforcement | European Union Agency for Fundamental Rights (europa.eu)

Źródło: komunikat Agencji Praw Podstawowych

WYDARZENIE DLA INTERESARIUSZY EDPB DOTYCZĄCE PRZYSZŁYCH WYTYCZNYCH W SPRAWIE „ZGODA LUB ZAPŁATA”

Europejska Rada Ochrony Danych (EROD) organizuje wydarzenie w formule zdalnej dla zainteresowanych stron. Odbędzie się 18 listopada 2024 r. w godzinach od 10:00 do 16:00 czasu środkowoeuropejskiego (dokładna godzina zostanie potwierdzona), w celu zebrania wkładu zainteresowanych stron do przyszłych wytycznych dotyczących stosowania przepisów o ochronie danych w kontekście modeli „Zgoda lub zapłata”.

Celem wydarzenia jest zebranie istotnych spostrzeżeń od organizacji, które mają doświadczenie w modelach „Consent or Pay”, które wymagają od osób, których dane dotyczą, wyboru

- między wyrażeniem zgody na przetwarzanie danych osobowych w określonym celu
- a uiszczeniem opłaty.

Wydarzenie pomoże w wypracowaniu wytycznych EDPB dotyczących modeli „Zgoda lub zapłata”. Wytyczne te stanowią kontynuację opinii EROD 08/2024, która dotyczyła modelu „zgoda lub zapłata” w kontekście dużych platform internetowych. Wytyczne będą miały szerszy zakres zastosowania.

Źródło: komunikat Europejskiej Rady Ochrony Danych

Fot. pexels

IRLANDZKI ORGAN NADZORCZY WSZCZYNA POSTĘPOWANIE W SPRAWIE MODELU GOOGLE AI

Irlandzki organ nadzorczy (DPC) poinformował, że wszczął transgraniczne postępowanie w sprawie Google Ireland Limited (Google) na podstawie sekcji 110 ustawy o ochronie danych z 2018 r.

Przedmiotem postępowania jest ustalenie, czy firma Google wywiązała się z obowiązku przeprowadzenia oceny, zgodnie z art. 35[2] ogólnego rozporządzenia o ochronie danych (ocena skutków dla ochrony danych), przed rozpoczęciem przetwarzania danych osobowych osób, których dane dotyczą w UE/EOG, związanego z opracowaniem jej podstawowego modelu sztucznej inteligencji, Pathways Language Model 2 (PaLM 2).

Ocena skutków dla ochrony danych, jeśli jest wymagana, ma kluczowe znaczenie dla zapewnienia, że podstawowe prawa i wolności osób fizycznych są odpowiednio uwzględniane i chronione, gdy przetwarzanie danych osobowych może powodować wysokie ryzyko.

Niniejsze postępowanie stanowi część szerszych działań DPC, podejmowanych we współpracy z innymi organami regulacyjnymi UE/EOG, mających na celu uregulowanie przetwarzania danych osobowych osób, których dane dotyczą w UE/EOG, w ramach opracowywania modeli i systemów sztucznej inteligencji.

Przetwarzanie transgraniczne oznacza:

• przetwarzanie danych osobowych, które odbywa się w kontekście działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii, jeżeli administrator lub podmiot przetwarzający mają siedzibę w więcej niż jednym państwie członkowskim; albo

• przetwarzanie danych osobowych, które odbywa się w kontekście działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które istotnie wpływa lub może istotnie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim.

Artykuł 35 RODO stanowi, że ocena skutków dla ochrony danych jest wymagana, gdy rodzaj przetwarzania, w szczególności przy użyciu nowych technologii, oraz biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania, może powodować wysokie ryzyko dla praw i wolności osób

fizycznych. Ocena DPIA jest kluczowym procesem budowania i wykazywania zgodności, który zapewnia, że administratorzy danych identyfikują i ograniczają wszelkie zagrożenia dla ochrony danych wynikające z rodzaju przetwarzania, które wiąże się z wysokim ryzykiem. Ma ona na celu zapewnienie, między innymi, że przetwarzanie jest konieczne i proporcjonalne oraz że istnieją odpowiednie zabezpieczenia w świetle ryzyka.

Źródło: komunikat irlandzkiego organu nadzorczego

Fot. pixabay

WIĄŻĄCE REGUŁY KORPORACYJNE (BCR): CNIL PUBLIKUJE NARZĘDZIE MONITOROWANIA

Aby wesprzeć grupy posiadające wiążące reguły korporacyjne w weryfikacji ich wdrożenia, CNIL udostępnia im narzędzie i opisuje etapy jego wdrożenia.

Czym są wiążące reguły korporacyjne i które grupy powinny je wdrożyć?

Wiążące reguły korporacyjne (BCR) wyznaczają wewnątrzgrupową politykę ochrony danych. Umożliwiają podmiotom powiązanym przekazywanie danych osobowych poza Unię Europejską. Jest to jedno z narzędzi zapewniania zgodności przez Ogólne rozporządzenie o ochronie danych (RODO).

Zatwierdzanie wiążących reguł korporacyjnych stanowi część procesu wsparcia wdrażanego przez CNIL.

Grupy holdingowe odpowiadają za skuteczną realizację obowiązków wynikających z BCR. Spółki, których to dotyczy, to międzynarodowe spółki prywatne z siedzibą w kilku krajach Unii Europejskiej i poza nią (patrz lista grup posiadających BCR zatwierdzone przez CNIL).

Nowe narzędzie do monitorowania w celu weryfikacji zgodności z wiążącymi regułami korporacyjnymi

Aby umożliwić grupom posiadającym wiążące reguły korporacyjne sprawdzenie poziomu zgodności z wymogami tych reguł, CNIL opublikował narzędzie monitorowania w języku francuskim i angielskim.

Grupy posiadające BCR będą mogły sprawdzić poziom zgodności z wymogami tych zasad właśnie dzięki opublikowanemu przez CNIL narzędziu monitorującemu.

Należy to wdrożyć w trzech etapach, wykorzystując dwa kwestionariusze, które można dostosować do potrzeb:

1. Inspektor ochrony danych lub osoba odpowiedzialna za grupę wybiera podmioty, które będą podlegać temu monitorowaniu. Mogą, ale nie muszą, znajdować się w UE.

2. Organizacje te wypełniają pierwszy kwestionariusz podmiotu lokalnego i przesyłają go osobie odpowiedzialnej na poziomie grupy. Taka informacja zwrotna zapewnia konkretne i zharmonizowane wdrożenie zasad BCR oraz odpowiednie zarządzanie.

3. Drugi kwestionariusz Grupowy IOD wypełnia bezpośrednio inspektor ochrony danych grupy, na podstawie informacji zwrotnych otrzymanych za pośrednictwem pierwszego kwestionariusza. Musi umożliwiać grupowemu inspektorowi ochrony danych przegląd wdrażania zarządzania.

Na podstawie wyników inspektor ochrony danych lub osoba odpowiedzialna na poziomie grupy może skompletować dokumentację dotyczącą zgodności grupy, zaproponować plan działania lub zwrócić się o przeprowadzenie audytów.

Więcej informacji na ten temat oraz wskazane formularze znajdują się pod adresem francuskiego organu nadzorczego.

Fot. pexels

UE WSPIERA EUROPEJSKICH TWÓRCÓW SZTUCZNEJ INTELIGENCJI POPRZEZ ZAPROSZENIE DO SKŁADANIA WNIOSKÓW AI FACTORIES

Komisja Europejska ogłosiła zaproszenie do tworzenia fabryk sztucznej inteligencji w celu zwiększenia wiodącej roli Europy w dziedzinie godnej zaufania sztucznej inteligencji (AI).

Fabryki sztucznej inteligencji zostaną utworzone przy użyciu światowej klasy sieci europejskich superkomputerów obliczeniowych o wysokiej wydajności (HPC) i będą dostępne dla szeregu europejskich użytkowników, takich jak startupy, przemysł i naukowcy.

Przewodnicząca Komisji Ursula von der Leyen powiedziała: „Europa jest już liderem dzięki EU AI Act, zapewniając, że sztuczna inteligencja jest bezpieczniejsza i bardziej godna zaufania. Na początku tego roku spełniliśmy naszą obietnicę, otwierając nasze wysokowydajne komputery dla europejskich start-upów AI. Teraz Europa musi również stać się światowym liderem innowacji w dziedzinie sztucznej inteligencji. AI Factories pomoże zabezpieczyć naszą pozycję w czołówce tej transformacyjnej technologii".

Fabryki AI będą łączyć ze sobą kluczowe składniki sukcesu w sztucznej inteligencji: moc obliczeniową, dane i talent. Pomogą one programistom AI trenować ich duże generatywne modele AI, wykorzystując superkomputery EuroHPC i zapewniając dostęp do danych, usług obliczeniowych i pamięci masowej. Fabryki będą połączone w sieć w całej Europie, zapewniając unikalne europejskie ramy współpracy w zakresie sztucznej inteligencji.

Fabryki sztucznej inteligencji będą połączone z inicjatywami państw członkowskich w zakresie sztucznej inteligencji, tworząc tętniący życiem ekosystem sztucznej inteligencji. Ponadto będą one korzystać z europejskich ośrodków testowania i eksperymentowania oraz centrów innowacji cyfrowych. Fabryki sztucznej inteligencji mają wspierać rozwój i walidację zastosowań przemysłowych i naukowych sztucznej inteligencji w kluczowych sektorach europejskich, takich jak opieka zdrowotna, energetyka, motoryzacja i transport, obronność i lotnictwo, robotyka i produkcja, czyste technologie i agrotechnika.

Zaproszenie do składania wniosków ogłoszone przez Wspólne Przedsięwzięcie EuroHPC będzie

otwarte do 31 grudnia 2025 r., z pierwszym terminem upływającym 4 listopada 2024 r. i kolejnymi datami granicznymi co trzy miesiące, dopóki dostępne będą środki. Inicjatywa opłacana jest z pieniędzy w wysokości blisko 1 mld euro z programu „Cyfrowa Europa" i „Horyzont Europa" oraz taką samą kwotą finansowania pochodzącą z państw członkowskich.

Źródło: komunikat Komisji Europejskiej

Fot. pexels

RAPORT EKSPERCKI NA TEMAT WPŁYWU WYKORZYSTANIA NEUROTECHNOLOGII I DANYCH NEURONOWYCH NA PRYWATNOŚĆ I OCHRONĘ DANYCH Z PERSPEKTYWY KONWENCJI 108+

Raport naukowy „Wpływ wykorzystania neurotechnologii i danych neuronowych na prywatność i ochronę danych z perspektywy Konwencji 108+" przygotowany przez Eduardo Bertoniego i Marcello lencę został zaprezentowany na 46. posiedzeniu plenarnym Komitetu Konwencji 108 (T-PD), które odbyło się w dniach 5-7 czerwca 2024 r. w Strasburgu. Zawiera on prawny i techniczny opis neurotechnologii i danych neuronowych oraz analizuje wpływ, jaki może ona mieć na prawa człowieka i podstawowe wolności, w szczególności prawo do prywatności i ochrony danych osobowych.

Raport bada obecne i przyszłe możliwości interfejsów neuronowych oraz inicjatywy regulacyjne dotyczące neurotechnologii. Zaproponowano w nim realne rozwiązania mające na celu złagodzenie wyzwań związanych z „prywatnością umysłową". Raport kładzie szczególny nacisk na Konwencję 108+ w odniesieniu do wpływu przetwarzania danych neuronowych na prywatność danych, podkreślając znaczenie ochrony prywatności osób fizycznych przy jednoczesnym promowaniu postępu naukowego i innowacji w neuronauce.

Konwencja 108+ zapewnia solidne ramy wobec wyzwań ery cyfrowej i złożoności badań neuronowych, aby zapewnić odpowiednią ochronę prywatności i danych osobowych osób fizycznych w kontekście neuronauki i badań nad mózgiem.

Źródło: komunikat Rady Europy

SZKOLENIE DLA KOORDYNATORÓW OGÓLNOPOLSKIEGO PROGRAMU EDUKACYJNEGO URZĘDU OCHRONY DANYCH OSOBOWYCH „TWOJE DANE – TWOJA SPRAWA” 24 – 25 PAŹDZIERNIKA 2024 R.

Dwudniowe szkolenie przeznaczone było dla nauczycieli i dyrektorów, biorących udział w tegorocznej, XV edycji Programu.

Poruszono kwestie związane z ochroną danych osobowych w sektorze oświaty oraz w szczególności tematy dotyczące ogromnej potrzeby zabezpieczenia wizerunku dzieci i młodzieży. Celem szkolenia było ukazanie konsekwencji publikacji danych dotyczących młodych osób, a także przedstawienie konkretnych narzędzi i metod pracy z uczniami, aby mogli oni stać się bardziej świadomymi i kompetentnymi użytkownikami internetu.

Szkolenie otworzyła Agnieszka Grzelak, zastępczyni prezesa UODO. W swoim wystąpieniu zaznaczyła, że we współczesnym, szybko rozwijającym się pod względem technologicznym świecie, dane są bezcenne. Brak odpowiedniej reakcji na naruszenie ochrony danych osobowych może skutkować powstaniem szkód majątkowych lub niemajątkowych dla osób fizycznych, takich jak kradzież lub sfałszowanie tożsamości, a w rezultacie straty finansowe, pogwałcenie prywatności i szereg negatywnych konsekwencji psychologicznych dla osoby, której dane dotyczą.

Istotne jest także, aby być dobrze poinformowanym i umieć podejmować odpowiednie kroki, by chronić swoje dane osobowe, ponieważ przetwarzanie danych osobowych jest zjawiskiem dotyczącym wielu dziedzin naszego życia.

Jak realizujemy Program

Realizacja Programu wspomaga w skutecznej ochronie danych osobowych dzieci i młodzieży, ale również podnosi świadomość dorosłych. Placówki zgłoszone do Programu otrzymują od Urzędu materiały edukacyjne – na ich podstawie nauczyciele przekazują wiedzę najmłodszym podczas lekcji poświęconym ochronie danych czy wspólnie realizowanych inicjatyw, często angażujących całe społeczności szkolne.

7 EDUKACJA

Materiały edukacyjne zawierają m.in. informacje dotyczące zasad ochrony danych osobowych i scenariusze lekcji, przygotowują nauczycieli do kształtowania odpowiedzialnych i otwartych postaw wśród uczniów.

To pierwsze spotkanie dla koordynatorów Programu, tymczasem przez cały cykl jego trwania przewidziano wiele innych aktywności: webinariów, szkoleń, celebrację Dnia Ochrony Danych Osobowych, lekcji online dla dzieci, konkursów. Ostatnim etapem Programu jest przygotowanie raportu ewaluacyjnego z podjętych w jego czasie działań.

Każdy uczestnik Programu ma zapewnione:

• bezpłatne szkolenia w ramach doskonalenia zawodowego,

• wsparcie ekspertów Urzędu Ochrony Danych Osobowych,

• bezpłatne materiały edukacyjne służące wprowadzeniu nowych treści podczas zajęć z uczniami.

Sharenting, parental trolling i inne zagrożenia, których chcemy uniknąć

Nadmierne udostępnianie zdjęć, filmów, informacji o dzieciach przez rodziców albo treści uwłaczających ich godności to zagadnienia, z którymi na co dzień mierzą się najmłodsi, których problem ten bezpośrednio dotyczy, ale również takie instytucje publiczne jak UODO, NASK czy Centralne Biuro Zwalczania Cyberprzestępczości. Zaproszeni goście mogli zaprezentować wspomniane problemy ze swojej perspektywy.

CBZC jako jednostka organizacyjna Policji służy zwalczaniu cyberprzestępczości. Zajmuje się zapobieganiem włamaniom na konta, phishingiem, spoofingiem (podszycie się pod inne urządzenie lub innego użytkownika w sieci), wyciekami danych, oszustwami za pośrednictwem portali społecznościowych, ogłoszeniowych i e-maili.

Spośród wszystkich zadań jej najwyższym priorytetem jest walka z wykorzystywaniem seksualnym dzieci w internecie. Nierzadko przestępcy seksualni wymieniają się zdjęciami dzieci publikowanymi w sieci – pochodzą one z portali społecznościowych, a więc ze źródeł powszechnie dostępnych, co pokazuje jak duże są możliwości wykorzystania informacji w sposób niezgodny z intencjami rodziców.

Organy ścigania nie mogą ustępować cyberprzestępcom zarówno w technologii, jak i w metodach stosowanych przez hakerów, którzy z powodzeniem korzystają ze środków, jakie daje sztuczna inteligencja. Stosują m.in. takie zaawansowane techniki manipulacji treściami multimedialnymi jak deep fake czy lip sync przy użyciu AI i głębokiego uczenia maszynowego.

W kontekście obrony przed atakami cyberprzestępców niezwykle ważne jest zachowanie cyfrowej higieny: nieudostępnianie komputera innym osobom, stosowanie uwierzytelniania dwuetapowego,

stosowanie aktualnego i skutecznego oprogramowania antywirusowego.

Koordynatorzy Programu biorący udział w szkoleniu mogli posłuchać o sposobach bezpiecznego wykorzystania sztucznej inteligencji w edukacji. Jak podkreślono: „Każdy system sztucznej inteligencji w jej cyklu życia powinien spełniać łącznie trzy warunki – być zgodny z prawem, zawierać zasady i reguły etyki dla godnej zaufania sztucznej inteligencji oraz być bezpieczny i odporny technicznie".

Z kolei przedstawicielka NASK zaprezentowała zatrważające statystyki dotyczące zjawiska sharentingu w Polsce:

• 40% polskich rodziców udostępnia online zdjęcia i filmy z życia ich dzieci;

• 21% rodziców zamieszcza w sieci takie materiały raz w tygodniu lub częściej;

• 61% robi to raz w miesiącu lub częściej;

• roczna liczba publikacji wynosi średnio 72 zdjęcia i 24 filmy;

• 42% rodziców przyznało, że udostępnia zdjęcia szerszej grupie (bliskim i znajomym), jednak liczącej nie więcej niż 200 osób;

• 20% rodziców dzieli się zdjęciami z dalszym znajomymi i osobami, których nie znają (ponad 200 osób);

• 23,6 % nastolatków czuje zawstydzenie tym, co rodzice publikują o nich w internecie.

Prelegentka przytoczyła rady, które warto zastosować, jeśli publikujemy zdjęcia zawierające wizerunek dzieci: „Ustaw na swoim profilu w mediach społecznościowych pokazywanie swoich wpisów wyłącznie zaufanej grupie odbiorców; nie publikuj nigdy nagich lub półnagich zdjęć swoich dzieci; nie zamieszczaj kompromitujących dziecko materiałów – gdy widać je w kłopotliwej sytuacji; pytaj o zgodę dziecka, także małego, przed publikacją w sieci zdjęć i nagrań, na których występuje. Nawet 4-latek powinien czuć, że ma wpływ na swój wizerunek. Pamiętaj o przyszłości dziecka i jaki na nią może mieć wpływ materiał, umieszczany dzisiaj w internecie".

Podobne wskazówki znajdziemy w poradniku, który powstał we współpracy Urzędu z Fundacją Orange „Wizerunek dziecka w internecie. Publikować czy nie?". Jest on wsparciem dla placówek, organizacji i wszystkich dorosłych w dbaniu o lepszą ochronę dzieci w erze cyfrowej.

Publikacja zdjęć dzieci w sieci to odpowiedzialność, która wymaga rozwagi, aby zapewnić dzieciom bezpieczeństwo oraz poszanowanie ich prawa do prywatności w przyszłości.

Regulacje prawne służące prywatności najmłodszych

W czasie szkolenia omówiono wytyczne Rady Europy, między innymi te dotyczące realizacji zasad

praw dziecka w placówkach oświatowych. Przytoczono główne zadania Europejskiej Rady Ochrony Danych, czyli przede wszystkim wydawanie zaleceń, wytycznych oraz określanie najlepszych praktyk dotyczących istotnych kwestii stosowania RODO w celu wyjaśniania prawa i promowania jednolitej wykładni unijnych przepisów, wspieranie współpracy pomiędzy krajowymi organami nadzorczymi czy przyjmowanie wiążących decyzji skierowanych do Komisji Europejskiej lub do krajowych organów nadzorczych. Przybliżono również działania Grupy Roboczej ds. Edukacji Cyfrowej oraz inicjatywę hiszpańskiego organu nadzorczego w obszarze weryfikacji wieku.

Ciekawym punktem szkolenia było wystąpienie reprezentanta infolinii UODO, który przybliżył odpowiedzi na najczęściej zadawane Urzędowi pytania dyrektorów, nauczycieli oraz rodziców związane z ochroną danych osobowych i wizerunku dzieci w szkołach oraz dotyczące obowiązku informacyjnego w sektorze oświaty. Opowiedział nam o problemach w oświacie z punktu widzenia monitoringu szkolnego, rozpowszechniania wizerunku uczniów oraz tego jak prawidłowo udzielać zgody na publikację wizerunku. Nie zabrakło powołań na odpowiednie regulacje prawne i wniosków, jakie z nich płyną w związku z pytaniami zadawanymi infolinii UODO.

Wyjdźmy poza schemat

Co roku na laureatów konkursu organizowanego w ramach Programu na najciekawszą inicjatywę edukacyjną czeka statuetka „Złotego Pióra”. Innym specjalnym wyróżnieniem, które zdarzyło nam się wręczyć za innowacyjne metody prowadzenia zajęć i praktyczne przybliżanie uczniom problematyki ochrony danych osobowych była nagroda im. Michała Serzyckiego.

Nauczycielki, autorki zwycięskich inicjatyw opowiedziały o swoich działaniach i lekcjach z zakresu ochrony danych osobowych w swoich placówkach. Jak w praktyce wygląda realizacja założeń Programu „Twoje dane – Twoja sprawa” w szkołach? Jak zaplanować i przeprowadzić dziania edukacyjne, aby zainteresować uczniów tematyką ochrony danych i wizerunku? Pomysłowość prowadzących była imponująca i z pewnością będzie inspiracją dla kolejnych uczestników Programu.

Do najbardziej fascynujących lekcji należała ta, podczas której uczniowie wcielali się w rolę detektywa agencji, rozwiązując kryminalną zagadkę. Śledztwo zostało podzielone na kilka etapów. Po każdym z nich uczniowie mieli możliwość sprawdzić swoją znajomość mitologii greckiej, a także rozpoznać, na ile poprawnie analizują fakty i wnioskują na podstawie dostępnych informacji.

Fabułę gry stanowiła współczesna wersja mitu o Syzyfie. Wzbogacono ją treściami z zakresu ochrony danych osobowych i prawa do prywatności. Dzięki oryginalnemu pomysłowi na przedstawienie i wyjaśnienie pojęć z obszaru ochrony danych osobowych i aktywizującej uczestników formule spotkania, młodzież mogła przyswoić wiele praktycznych informacji, pomocnych w codziennej ochronie ich danych osobowych.

To, co jednak najbardziej urzeka w wypowiedziach nagrodzonych koordynatorów Programu, to empatia, podmiotowe traktowanie uczniów i prawdziwa, czuła troska o ich bezpieczeństwo i prawa. Bez tych elementów żadne wykłady i szkolenia nie przyniosą rezultatu. To podstawa, na której stoi Program „Twoje dane – Twoja sprawa" i wszelkie inicjatywy z nim związane.

Na zdjęciu dr Joanna Hałoń – Gnutek wraz z Mirosławem Wróblewskim, prezesem UODO oraz Moniką Horną-Cieślak, Rzeczniczką Praw Dziecka.

Dr Joanna Hałoń – Gnutek jest laureatką Nagrody im. Michała Serzyckiego z 2024 roku. Liderka Programu chętnie dzieli się wiedzą i doświadczeniami, a przygotowane przez nią scenariusze zajęć zostały włączone do bazy materiałów edukacyjnych Programu „Twoje dane – Twoja sprawa" i stanowią wsparcie dla kolejnych uczestników do organizowania interesujących lekcji z uczniami. Dzięki działaniom podjętym przez Panią dr Hałoń-Gnutek Szkoła Podstawowa nr 4 im. Adama Mickiewicza w Lublinie dwukrotnie została nagrodzona statuetką „Złotego Pióra" w konkursie na najlepszą inicjatywę edukacyjną.

URZĄD OCHRONY DANYCH OSOBOWYCH

SPOŁECZNY ZESPÓŁ EKSPERTÓW PRZY PUODO

KONFEDERACJA LEWIATAN

Prezes Urzędu Ochrony Danych Osobowych oraz Społeczny Zespół Ekspertów przy PUODO wraz z Konfederacją Lewiatan zapraszają na seminarium

Ochrona zdrowia w zatrudnieniu a RODO

Seminarium odbędzie się 15 listopada 2024 r. w godz. 10.00 – 16.15 w sali konferencyjnej na 38. piętrze siedziby UODO w Warszawie przy ul. Stawki 2.

Podczas seminarium będziemy rozmawiać o tym, czy obowiązujące regulacje prawne są należycie dostosowane do aktualnych potrzeb i zagrożeń dla zdrowia pracujących, a także czy RODO jest barierą dla aktywnego włączenia się pracodawców w system ochrony zdrowia publicznego. Zakład pracy może bowiem być miejscem, w którym zdrowie osób wykonujących pracę zarobkową nie tylko należy chronić, ale można je także aktywnie wspierać i rozwijać na wielu płaszczyznach, uwzględniając w szczególności zagrożenia psychospołeczne, które szczególnie uwidoczniły się po okresie pandemii.

Do udziału w seminarium zapraszamy przedstawicieli administracji publicznej, ekspertów z zakresu prawa pracy i medycyny pracy, praktyków i przedstawicieli środowisk zaangażowanych w kwestie ochrony zdrowia pracujących.

Ustalenia zebrane w trakcie dyskusji będą miały znaczenie dla aktualizowanego przez Urząd Ochrony Danych Osobowych i Społeczny Zespół Ekspertów przy Prezesie UODO poradnika dla pracodawców, dotyczącego przetwarzania danych osobowych w zatrudnieniu, jak również będą mogły stanowić impuls do podjęcia niezbędnych prac legislacyjnych, jeżeli do takich wniosków dojdziemy podczas tego wydarzenia.

Seminarium odbędzie się w formule hybrydowej z transmisją online za pośrednictwem strony internetowej www.uodo.gov.pl

Po więcej szczegółów zapraszamy na stronę UODO

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl