Raport z Konferencji "Forum Nowych Technologii"

20-21 września 2023 r.

Akademia Ekonomiczno-Humanistyczna, Warszawa

Szanowni Państwo,

z ogromną przyjemnością przedstawiam Państwu raport z konferencji „Forum Nowych Technologii", która odbyła się w Akademii Ekonomiczno-Humanistycznej w Warszawie, w dniach 20-21 września 2023 r. Organizatorem tego wydarzenia był Urząd Ochrony Danych Osobowych, we współpracy ze Stowarzyszeniem Prawa Nowych Technologii i Akademią Ekonomiczno-Humanistyczną w Warszawie.

Celem konferencji „Forum Nowych Technologii", było zgłębienie roli i wpływu postępującej digitalizacji na ochronę danych osobowych. Wydarzenie, które zgromadziło ponad 40 ekspertów z różnych dziedzin, miało na celu stworzenie platformy do dyskusji i wymiany wiedzy na temat aktualnych wyzwań i przyszłych kierunków rozwoju w zakresie nowych technologii i ochrony prywatności.

Podczas dwudniowego „Forum Nowych Technologii" zaproszeni specjaliści zaprezentowali zagadnienia związane z ochroną danych osobowych w erze nowych technologii, w tym trendy i wyzwania związane ze sztuczną inteligencją, chmurą obliczeniową, technologią blockchain, czy technologią śledzenia. Podczas konferencji zgłębiono również temat wyzwań etycznych związanych ze sztuczną inteligencją, w tym wielokrotnie podkreślano kwestię odpowiedzialności w stosowaniu nowych technologii. Eksperci wyjaśniali czym jest bezpieczeństwo informacji w erze cyfrowej. Omówiono również zmiany legislacyjne związane z wejściem w życie aktów, będących częścią unijnego pakietu usług cyfrowych i strategii w zakresie danych. Konferencję podsumowała debata ekspercka, poświęcona najważniejszym trendom nowych technologii w kontekście ochrony danych osobowych.

Poniżej znajdą Państwo podsumowanie przebiegu sesji podczas dwudniowego „Forum Nowych Technologii" i najważniejsze wnioski wynikające z przeprowadzonych dyskusji. Niniejszy raport stanowi podsumowanie konferencji, jak i przegląd wybranych zagadnień dotyczących wyzwań dla ochrony danych związanych z rozwojem nowych technologii.

Jan Nowak
Prezes
Urzędu Ochrony Danych Osobowych

Uroczyste otwarcie i wystąpienie wprowadzające

Uroczyste otwarcie:
Jakub Groszkowski
Zastępca Prezesa Urzędu Ochrony Danych Osobowych

Beata Ostrowska
Przewodnicząca Sektorowej Rady ds. Kompetencji Informatyka oraz Wiceprzewodnicząca Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo

Xawery Konarski
Adwokat, Prezes Stowarzyszenia Prawa Nowych Technologii, Wiceprezes Polskiej Izby Informatyki i Telekomunikacji, Senior Partner w kancelarii Traple Konarski Podrecki i Wspólnicy Sp. J.

Włodzimierz Chróścik
Radca prawny, Prezes Krajowej Rady Radców Prawnych

Wystąpienie wprowadzające:
Maciej Gawroński
Radca prawny, Partner w GP Partners,
Członek Rady Naukowej Instytutu Prawa Ochrony Danych Osobowych

Podczas uroczystego otwarcia konferencji eksperci zgodnie podkreślali, że cyberzagrożenia związane z korzystaniem z nowych technologii stają się coraz bardziej zaawansowane, w związku z tym konieczne jest podjęcie wielokierunkowych działań, celem przeciwstawienia się temu zjawisku.

Wskazywano na rolę inspektorów ochrony danych (IOD) i ich kompetencje w obszarze cyberbezpieczeństwa. Podkreślono w tym zakresie znaczenie rad sektorowych, mających za zadanie śledzić uważnie rynek pracy i na podstawie obserwacji identyfikować, budować potrzeby kompetencyjne IOD, jak również edukować i dopasowywać je do systemu.

Eksperci przedstawili również działalność Stowarzyszenia Prawa Nowych Technologii (SPNT). Organizacja ta, zrzeszająca prawników specjalizujących się w nowych technologiach, prowadzi działalność edukacyjną, wydawniczą i współpracuje z regulatorami. Działalność SPNT odbywa się w grupach roboczych, z których najważniejszą jest grupa „RODO i e-prywatność". Członkowie tej grupy byli licznie reprezentowani na Forum w charakterze mówców.

Prezes Krajowej Rady Radców Prawnych (KRRP) podkreślił, że na kwestie cyberbezpieczeństwa, należy patrzeć z perspektywy etyki i odpowiedzialności jej twórców. KRRP wyraziła ogromne zainteresowanie wnioskami *de lege ferenda*, sformułowanymi w

trakcie konferencji. Zadeklarowano także, że w ramach prac Ośrodka Badań Studiów i Legislacji, KRRP poprze inicjatywy legislacyjne, sygnalizowane w wystąpieniach.

W ramach wystąpienia wprowadzającego, omówione zostały wyzwania dla prywatności i ochrony danych w kontekście rozwoju nowych technologii i digitalizacji, z naciskiem na potencjalne zagrożenia ze strony sztucznej inteligencji (AI), takie jak uprzedmiotowienie ludzi i cyfrowa cenzura. Poruszono też tematykę zastosowania AI w inwigilacji obywateli, jak również obawy związane z jednolitą cyfrową walutą, komputerami kwantowymi i centralizacją zarządzania AI.

Podkreślono, że postęp technologiczny jest nieuchronny, ale ważne jest, aby dominujące firmy technologiczne uwzględniały prawa człowieka, w tym prawo do prywatności i ochrony danych osobowych, oraz dostosowywały swoje rozwiązania do przepisów RODO.

Sesja I: Ochrona danych osobowych w erze nowych technologii

Prelegenci:
Agnieszka Rapcewicz
Adwokat, Fundacja Internet. Czas działać! Akademia Leona Koźmińskiego

Łukasz Jarecki
Zespół Ochrony Danych Osobowych, Grant Thornton

Daria Rychlik
Adwokat, The Attorney Kancelaria Adwokacka

Witold Chomiczewski
Radca prawny, Pełnomocnik Izby Gospodarki Elektronicznej ds. Legislacji

Andrzej Dulka
Prezes Zarządu Polskiej Izby Informatyki i Telekomunikacji

Wiesław Paluszyński
Prezes Polskiego Towarzystwa Informatycznego, Przewodniczący Sektorowej Rady ds. Kompetencji Telekomunikacja i Cyberbezpieczeństwo oraz Członek Sektorowej Rady ds. Kompetencji Informatyka

Barbara Smalarz
Główny Specjalista w Departamencie Bezpieczeństwa i Kontroli Wewnętrznej, KGHM Polska Miedź S.A.

Izabela Kowalczuk-Pakuła
Radca prawny, Stowarzyszenie Prawa Nowych Technologii

Podczas pierwszej sesji zwrócono szczególną uwagę na warunki uzyskania ważnej zgody na zbieranie plików cookies na gruncie obowiązujących przepisów. Przypomniano, że

aby zgoda była ważna, musi być świadoma, dobrowolna, jednoznaczna i konkretna. Co ważne, domyślna zgoda wyklucza świadomą i konkretną zgodę, a jedynie fabryczne ustawienia przeglądarki z automatu odrzucające żądanie utworzenia plików cookies są warunkiem prawidłowego funkcjonowania tego mechanizmu.

Tematem dyskusji była także realizacja prawa do bycia zapomnianym w kontekście technologii blockchain. Co zostało podkreślone, realizacja żądania usunięcia konkretnych danych z blockchainu wiąże się z usunięciem tychże danych wewnątrz wszystkich łańcuchów bloków, które są na urządzeniu. W konsekwencji, skuteczna realizacja prawa do bycia zapomnianym wymaga współpracy i koordynacji działań wszystkich administratorów, co stanowi ogromne wyzwanie i pokazuje, że RODO nie przewidziało skutków przetwarzania danych w ramach takich technologii jak blockchain.

W trakcie sesji skoncentrowano się również na praktycznych aspektach stosowania innych zaawansowanych systemów opartych na sztucznej inteligencji (AI), w tym zwłaszcza modelu ChatGPT, w kontekście obowiązujących i projektowanych regulacji. Uczestnicy konferencji zgłębiali zarówno potencjał, jak i wyzwania związane z wykorzystaniem tych technologii w różnych sektorach. Omówiono szerokie spektrum zastosowań ChatGPT, od automatyzacji obsługi klienta po generowanie treści i wsparcie w procesach decyzyjnych.

Na szczególną uwagę zasługuje kwestia tego, jak ChatGPT i podobne narzędzia AI mogą przyczyniać się do zwiększenia wydajności i innowacyjności, jednocześnie nie pomijając kwestii związanych z odpowiedzialnością za wygenerowane treści i ochroną danych osobowych. Szczególną uwagę należy poświęcić kwestiom prawnym i etycznym aspektom wykorzystania AI, w tym odpowiedzialności za decyzje podejmowane z wykorzystaniem sztucznej inteligencji, praw autorskich do wygenerowanych treści oraz potencjalnym ryzykom nadużyć. Dyskutowano nad tym, jak zapewnić zgodność tych technologii z RODO, szczególnie w zakresie transparentności przetwarzania danych i praw użytkowników do dostępu, sprostowania oraz usunięcia danych.

W tym kontekście należy zwrócić uwagę na działania podjęte dotychczas przez UODO, w związku z rozpatrywaną przez organ skargą na spółkę OpenAI, twórcę modelu ChatGPT. Skarżący podniósł m.in. kwestię braku przejrzystości polityki przetwarzania danych przez OpenAI, zarzucając spółce brak informacji o sposobie i celu przetwarzania jego danych osobowych. UODO prowadzi postępowanie w tej sprawie.

Ponadto, w związku z coraz większą liczbą skarg składanych przez osoby, których dane dotyczą, do europejskich organów nadzorczych na działania spółki OpenAI, w kwietniu 2023 r. organy nadzorcze wspólnie zadecydowały o utworzeniu grupy roboczej ds. ChatGPT. Grupa została powołana w celu wspierania współpracy i wymiany informacji pomiędzy organami, na temat prowadzonych przez nie postępowań, w zakresie przetwarzania danych przez spółkę Open AI, w ramach działania Chatu GPT.

Podczas sesji eksperci poruszyli także temat zwodniczych wzorców projektowych (tzw. *dark patterns* lub *deceptive patterns*). Wskazano na potrzebę jasnego informowania użytkowników o celu przetwarzania, prawach osób, których dane dotyczą, a także poinformowano o ryzykach związanych ze zwodniczymi wzorcami projektowymi. Co podkreślono, za przesłankę legalizującą przetwarzanie danych nie można uznać celu samego w sobie. To, że administrator ma jakiś określony cel pozyskiwania danych nie oznacza, że może już te dane przetwarzać. Administrator może przetwarzać dane osobowe tylko pod warunkiem spełnienia przesłanek legalizujących przetwarzanie, zawartych w RODO (art. 6 i art. 9 RODO).

Na szczególną uwagę w kontekście zwodniczych wzorców, zasługują praktyczne wytyczne przyjmowane w celu rozpoznawania i zapobiegania stosowaniu zwodniczych wzorców projektowych, w tym działania podejmowane przez organy nadzorcze. Europejska Rada Ochrony Danych (EROD), w skład której wchodzą organy nadzorcze, w tym UODO, przyjęła w lutym 2023 r. Wytyczne w sprawie tzw. *deceptive design patterns* w interfejsach platform społecznościowych[1]. Wytyczne zawierają praktyczne zalecenia dla projektantów i użytkowników platform społecznościowych dotyczące tego, jak rozpoznawać i unikać zwodniczych wzorców projektowych w interfejsach mediów społecznościowych, które naruszają wymogi RODO. EROD przedstawiła konkretne przykłady typów zwodniczych wzorców projektowych, rekomendując najlepsze praktyki w odniesieniu do różnych przypadków użycia i zawierając konkretne zalecenia dla projektantów interfejsów użytkownika, które ułatwiają skuteczne wdrożenie RODO.

Eksperci poruszyli także ważny temat ochrony danych osobowych dzieci w przestrzeni cyfrowej w kontekście RODO. Omówiono kwestię reklam internetowych skierowanych do dzieci oraz wyzwań związanych z weryfikacją wieku odbiorców, a także podkreślono

[1] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en

konieczność edukacji i kampanii świadomościowych dotyczących bezpieczeństwa dzieci online.

Sesja II: Sztuczna inteligencja a ochrona danych osobowych – wyzwania prawne i etyczne, ramy regulacyjne i wnioski *de lege ferenda*

Prelegenci: **Ewa Kurowska-Tober** Radca prawny, Stowarzyszenie Prawa Nowych Technologii **Agnieszka Gajewska-Zabój** Radca prawny, Sekretarz Krajowej Rady Radców Prawnych **Dr Dominik Lubasz** Radca prawny, Stowarzyszenie Prawa Nowych Technologii **Dr Maria Jędrzejczak** Uniwersytet im. Adama Mickiewicza w Poznaniu, Członek Rady Naukowej Instytutu Prawa Ochrony Danych Osobowych

Podczas Sesji II skupiono się na analizie roli sztucznej inteligencji w przetwarzaniu danych osobowych. Zwrócono uwagę na to, że systemy oparte na AI bazują na ogromnej ilości danych osobowych, co jest niezbędne do realizacji ich zadań. Jednak ze względu na ich zdolność do przetwarzania danych na niewyobrażalną skalę, stają się one trudne do zrozumienia i kontrolowania.

Uczestnicy konferencji dyskutowali o wyzwaniach związanych z zapewnieniem bezpieczeństwa danych osobowych w kontekście szybko rozwijających się technologii AI. Podkreślono, że kluczowe jest przestrzeganie obowiązków wynikających z RODO, ponieważ projektowane przepisy dotyczące sztucznej inteligencji w dużym stopniu są oparte na tych samych zasadach.

W celu zapewnienia bezpieczeństwa danych osobowych, w związku z rozwojem technologii AI, należy przede wszystkim zadbać o realizację obowiązków wymienionych w RODO, ponieważ projektowany akt w sprawie sztucznej inteligencji został w dużym stopniu skonstruowany na tym wzorcu i przejmuje wiele rozwiązań przyjętych w jego przepisach. Zasada ryzyka, model kar, model obowiązków, organy, które będą zarządzać obszarem sztucznej inteligencji itd., są wzorowane na rozwiązaniach przyjętych w RODO. W oparciu o ten model, obowiązki twórców AI można ująć w 5 głównych obszarach: (1) przestrzeganie podstawowych zasad przetwarzania danych osobowych, (2) zautomatyzowane przetwarzanie

danych, (3) realizacja praw podmiotów danych, (4) obowiązek informacyjny oraz (5) ocena skutków dla ochrony danych. Podstawowe zasady przetwarzania danych osobowych to: legalność, rzetelność i przejrzystość, ograniczenie celów, adekwatność i minimalizacja danych, merytoryczna poprawność, ograniczenie czasowe, integralność i poufność oraz rozliczalność.

W konsekwencji, można zakładać, że RODO naturalnie wypełni lukę w przyszłych przepisach aktu w sprawie sztucznej inteligencji, zapewniając tym samym, że w ramach całego cyklu życia systemu AI będzie brany pod uwagę jego wpływ na prawa i wolności jednostek.

Podczas sesji wskazano na problem braku przejrzystości przetwarzania danych osobowych w technologii sztucznej inteligencji. Taki sam problem pojawia się w odniesieniu do zasady ograniczenia celu, minimalizacji czy adekwatności. Jak wskazywali eksperci, w momencie, gdy sztuczna inteligencja tworzy sztuczne sieci neuronowe, przeszukuje ogromne ilości źródeł w poszukiwaniu informacji. W konsekwencji pojawia się pytanie o to, jak AI ma samoczynnie ograniczyć swój dostęp do informacji i danych osobowych, które prawdopodobnie nie będą jej w ogóle potrzebne do realizacji danego zadania. Stanowi to wyzwanie dla twórców sztucznej inteligencji, w szczególności w świetle zasady *privacy by design*, która zakłada, że AI powinna być tak zaprojektowana u podstaw, żeby zapewnić ochronę danych osobowych. W odniesieniu do zasady minimalizacji określonej w RODO, akt w sprawie sztucznej inteligencji wprowadza dodatkową zasadę - kompletności (art. 10 ust. 3 projektu aktu w sprawie sztucznej inteligencji). Zasada kompletności mówi, że zbiory danych treningowych (czyli takich, z których AI wywodzi swoje umiejętności) muszą być adekwatne, wolne od błędów i kompletne.

Zautomatyzowane podejmowanie decyzji, w tym profilowanie – i związany z tym obowiązek informacyjny – to kolejny ważny aspekt, poruszany przez uczestników sesji, związany z budową systemów sztucznej inteligencji. Modele sztucznej inteligencji w dużym stopniu korzystają z rozwiązań związanych z profilowaniem, dlatego ważnym zadaniem dla twórców AI jest zapewnienie skutecznej realizacji praw podmiotu danych.

Ochrona danych osobowych jest kluczowa dla etycznego wykorzystania sztucznej inteligencji. Podkreślenia wymaga to, że edukacja, wzrost świadomości oraz współpraca ze specjalistami w dziedzinie ochrony danych osobowych są niezbędne przy tworzeniu modeli AI. Co istotne, ocena skutków dla ochrony danych osobowych powinna być przeprowadzona w przypadku każdego zastosowania sztucznej inteligencji, a analiza ryzyka jest jednym z kluczowych narzędzi w procesie wykorzystywania AI. Rozwój nowych technologii jest tak

dynamiczny, iż już niektóre sformułowania przepisów rodzą pytania o ich aktualność, co stanowi kolejne wyzwanie dla twórców i użytkowników AI.

W sesji II zwrócono także uwagę na treść wspólnej opinii EROD i EIOD w sprawie projektu aktu w sprawie sztucznej inteligencji[2]. Należy podkreślić, że EROD i Europejski Inspektor Ochrony Danych (EIOD) w opinii wezwali do zakazu wykorzystywania AI w celu biometrycznej identyfikacji oraz niektórych innych zastosowań, które mogą prowadzić do dyskryminacji i niosą ze sobą ryzyko ingerencji w prawa i wolności jednostek. Co istotne, wiele uwag zostało uwzględnionych przez Parlament Europejski i jest szansa, że proces legislacyjny będzie szedł w wyznaczonym przez EROD i EIOD kierunku ściślejszej ochrony osób, których dane dotyczą.

Sesja III: Etyka i odpowiedzialność w stosowaniu technologii

Prelegenci:
Barbara Podwysocka
Dyrektor Pionu Bezpieczeństwa, Polski Holding Hotelowy Sp. z o.o.

Przemysław Olszewski
Checkbox Sp. z o.o.

Kamil Wojciechowski
Forsafe Sp. z o.o.

Natalia Bender
Warsztatownia.eu

Tematem trzeciej sesji była etyka i odpowiedzialność w wykorzystaniu technologii. W wystąpieniach skupiono się na etycznym zastosowaniu sztucznej inteligencji. Podstawową konkluzją wszystkich wystąpień było uznanie, że sztuczna inteligencja powinna być używana w celu promowania dobrostanu ludzkości.

Podczas sesji przedstawiono temat etyki nowych technologii jako elementu *compliance*. Zdaniem ekspertów sztuczna inteligencja powinna służyć społeczeństwu i stanowić przydatne narzędzie organizacyjne. Twórcy AI powinni oceniać dane rozwiązanie nie tylko od strony zaprojektowania danej technologii, ale również późniejszego jej wykorzystania. Projektanci systemów, korzystający z AI, z założenia muszą tworzyć je z poszanowaniem praw

[2] https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_pl

podstawowych osób fizycznych, w tym prawa do prywatności i ochrony danych. Systemy nie mogą być projektowane w sposób nieetyczny.

Istotne jest, co zostało podkreślone także we wcześniejszej części konferencji, transparentność procesu, gromadzenia danych przez AI. W momencie projektowania i implementacji narzędzia jego twórca musi mieć zaplanowane zarządzanie systemem, a także mieć pełną kontrolę i plan jego działania.

Nowe technologie, takie jak generatywna sztuczna inteligencja, wirtualna rzeczywistość, manipulacja obrazem i dźwiękiem, usługi związane z profilowaniem w marketingu, przetwarzanie danych osobowych dzieci – to realne wyzwania, z którymi muszą się mierzyć użytkownicy. Każda z tych technologii jest oparta na przetwarzaniu danych. Dlatego też w tym kontekście kluczowe jest zrozumienie działania technologii, identyfikacja generowanych ryzyk, kontrola przepływu danych oraz zapewnienie bezpiecznego korzystania z systemu przez użytkowników. Należy także pamiętać o roli inspektorów ochrony danych, którzy wspierają administratorów w realizacji tych założeń w organizacji.

Niezwykle ważnym tematem w kontekście etycznego korzystania z nowych technologii jest także cyberlustracja w procesie rekrutacji do pracy. Przy korzystaniu z narzędzi sztucznej inteligencji w celu znalezienia informacji dostępnych publicznie o kandydatach do pracy, pracodawcy muszą pamiętać, że budowanie opinii o kandydatach na podstawie informacji z mediów społecznościowych lub innych dostępnych publicznie źródeł, może prowadzić do błędów poznawczych i stanowić istotne wyzwanie w procesach rekrutacyjnych. Może również prowadzić do dyskryminacji kandydatów.

Sesja IV: Bezpieczeństwo informacji w erze cyfrowej

Prelegenci:
Jakub Groszkowski
Zastępca Prezesa Urzędu Ochrony Danych Osobowych

Tomasz Ochmiński
Kierownik Zespołu Kontrolnego, Departament Kontroli i Naruszeń, Urząd Ochrony Danych Osobowych

Renata Podlewska
Inspektor Ochrony Danych, Uniwersytet Medyczny im. Karola Marcinkowskiego w Poznaniu

Paweł Ornoch
Dyrektor Biura Bezpieczeństwa w PKO BP Finat

Maciej Jurczyk
Ekspert ds. Bezpieczeństwa w PKO BP Finat

Piotr Kamiński
nFlo Sp. o.o.

Łukasz Bonczek
Dyrektor Biura Analiz Projektów Sprzedażowych, EXATEL S.A.

Nieodłącznym elementem rozwoju technologii jest korzystanie z aplikacji mobilnych. Przyspieszenie transformacji cyfrowej i rozpowszechnianie e-usług w większości branż, stało się okazją do dużej aktywności cyberprzestępców i wzrostu liczby naruszeń ochrony danych osobowych. Dlatego UODO, w ramach planu kontroli sektorowych na 2023 r., zajął się weryfikacją sposobów przetwarzania danych osobowych przy użyciu internetowych oraz mobilnych aplikacji. UODO przeprowadził kontrole u podmiotów z sektorów: medycznego, handlowego, bankowego, gastronomicznego, turystycznego, transportu oraz administracji rządowej. Aplikacje mobilne stanowiły główne narzędzie pracy wykorzystywane np. w branży transportowej, albo były dodatkowym narzędziem – np. w pracy podmiotów sektora finansów.

Kontrole najczęściej obejmowały podstawę prawną przetwarzania danych osobowych w danej organizacji, zakres i rodzaj przetwarzanych danych osobowych, wdrożenie odpowiednich środków technicznych i organizacyjnych dotyczących funkcjonowania aplikacji mobilnych oraz związanych z nią informatycznych zasobów systemowych. Sprawdzano też, czy przeprowadzona została analiza ryzyka oraz to, czy skuteczność zastosowanych środków technicznych była regularnie testowana, mierzona i oceniana. Kontrole wykazały, że kontrolowani administratorzy z reguły wdrożyli odpowiednie środki techniczne i organizacyjne oraz uwzględniali zasadę *privacy by design* i *privacy by default* na etapie projektowania i wdrażania aplikacji mobilnych, zapewniając przy tym skuteczną ochronę przetwarzanych danych osobowych w organizacji.

UODO przedstawił kilka przykładów dobrych praktyk związanych z bezpiecznym wykorzystaniem aplikacji mobilnych w pracy kontrolowanych podmiotów, jak np. audyty bezpieczeństwa aplikacji, w tym testy penetracyjne pod kątem wykrycia potencjalnych podatności. Przytoczono także przykłady niepożądanych praktyk, np. żądania od użytkowników przesłania zdjęcia lub skanu karty kredytowej powiązanej w celu potwierdzenia tożsamości. Wyniki przeprowadzonych kontroli zostaną przedstawione na początku 2024 r.

W trakcie sesji omówiono także różne modele generatywnej sztucznej inteligencji. Podkreślono, że AI nie zawsze jest w stanie udzielić jednoznacznej odpowiedzi, co podkreśla konieczność zachowania ostrożności i weryfikacji informacji przez użytkowników. Eksperci zaakcentowali też wielokrotnie rolę audytu jako jednego z podstawowych narzędzi skutecznego zabezpieczania danych osobowych przed incydentami bezpieczeństwa informacji, cyberatakami i naruszeniami ochrony danych osobowych. Podkreślono ponadto znaczenie "utwardzania" systemu bezpieczeństwa w organizacji oraz skoncentrowano się na roli szkoleń pracowników i skutecznego wdrażania zaleceń poaudytowych.

Podczas sesji zaprezentowano krajobraz bezpieczeństwa polskiego Internetu w Polsce w 2023 r, w szczególności w zakresie małych i średnich przedsiębiorstw. Najczęściej stosowanym przez małe i średnie przedsiębiorstwa środkiem bezpieczeństwa, na co zwracają uwagę eksperci, jest uwierzytelnianie silnym hasłem, za to mniej popularne jest wykonywanie kopii zapasowych i kontrola dostępu do sieci przedsiębiorstwa.

Podczas tej sesji zidentyfikowano także główne problemy związane z zapewnieniem cyberbezpieczeństwa w gospodarce. W opinii ekspertów największe problemy związane z zapewnieniem cyberbezpieczeństwa w gospodarce wynikają z braku świadomości biznesu, nieodpowiedniej alokacji środków na cyberbezpieczeństwo przez podmioty publiczne czy też w ogóle – brak tych środków. Najczęściej wskazuje się na wysokie realne koszty budowy bezpiecznej organizacji: sprzęt, szkolenia, usługi, audyty, zasoby ludzkie. Pewną odpowiedzią na te ograniczenia może być precyzyjne określenie, na co mają być wydane środki budżetowe, opracowanie modeli dobrych praktyk w organizacji, wyznaczanie dobrych trendów w zakresie budowania świadomości zagrożeń oraz skuteczne egzekwowanie przepisów i nagłaśnianie przypadków uchybień.

Sesja V: Najważniejsze zmiany legislacyjne 2023/2024

Prelegenci:
Dr Magdalena Witkowska-Krzymowska
Dyrektor Departamentu Prawnego w Ministerstwie Cyfryzacji

Xawery Konarski
Adwokat, Prezes Stowarzyszenia Prawa Nowych Technologii, Wiceprezes Polskiej Izby Informatyki i Telekomunikacji, senior partner w kancelarii Traple Konarski Podrecki i Wspólnicy Sp. J.

Joanna Litwin
Inspektor Ochrony Danych w Miejskim Ośrodku Pomocy Rodzinie w Szczecinie, Wyższa Szkoła Kształcenia Zawodowego we Wrocławiu

Piotr Drobek
Radca w Urzędzie Ochrony Danych Osobowych

Małgorzata Skórska
Kancelaria WKB Lawyers

Agata Szeliga
Radca prawny, Stowarzyszenie Prawa Nowych Technologii

Sesja V koncentrowała się na najważniejszych zmianach legislacyjnych zaplanowanych na lata 2023 i 2024. Dokonano analizy podstawy prawnej działania aplikacji mObywatel oraz jej funkcjonalności, zauważając wyjątkowe podejście prawodawcy, który stworzył odrębny akt prawny dotyczący tej aplikacji. Następnie zaprezentowano 10 tez dotyczących wzajemnego oddziaływania aktu w sprawie sztucznej inteligencji oraz RODO, podkreślając, że oba akty powinny funkcjonować jako tandem legislacyjny. Przedstawiono projekt europejskiej przestrzeni danych dotyczącej zdrowia (EHDS), wyjaśniając pierwotne i wtórne wykorzystanie elektronicznych danych dotyczących zdrowia.

Podczas sesji poruszono tematykę projektu europejskiej przestrzeni danych dotyczących zdrowia (EHDS), której źródłem jest europejska strategia w zakresie danych, mająca na celu stworzenie jednolitej przestrzeni danych. Głównymi celami EHDS są m.in. zapewnienie osobom fizycznym w UE większej praktycznej kontroli nad ich elektronicznymi danymi dotyczącymi zdrowia i stworzenie prawdziwie jednolitego rynku cyfrowych produktów i usług zdrowotnych dzięki harmonizacji przepisów.

Projekt rozporządzenia w sprawie EHDS obejmuje pierwotne i wtórne wykorzystanie elektronicznych danych dotyczących zdrowia. Pierwotne wykorzystanie – dotyczyć będzie przetwarzania danych osobowych na potrzeby udzielania świadczeń zdrowotnych w celu oceny, utrzymania lub poprawy stanu zdrowia osoby fizycznej, łącznie z przepisywaniem, wydawaniem i udostępnianiem produktów i wyrobów leczniczych, a także na potrzeby różnych usług, np. związanych ze zwrotem kosztów leczenia. Natomiast wtórne wykorzystanie – odnosi się do przetwarzania danych osobowych w działalności edukacyjnej, dydaktycznej i badań naukowych w sektorach ochrony zdrowia lub opieki zdrowotnej. Co istotne, choć EHDS wyraźnie wzmacnia kontrolę i prawa osób, których dane o stanie zdrowia dotyczą, to jednak istnieje niebezpieczeństwo osłabienia prawa ochrony danych osobowych – biorąc głównie pod uwagę kategorie danych i cele związane z ich wtórnym wykorzystaniem.

Podczas Sesji IV omówiono też historię ustanawiania reguł przekazywania danych osobowych do Stanów Zjednoczonych, której początki sięgają czasu dyrektywy 95/46/WE, skupiając się przede wszystkim na założeniach aktualnych Ram Ochrony Danych UE-USA, przyjętych 10 lipca 2023 r. w drodze decyzji KE o zapewnieniu odpowiedniego stopnia ochrony danych osobowych. Wskutek decyzji dane osobowe można przekazywać bez konieczności uzyskiwania dodatkowych zezwoleń, czy zastosowania takich instrumentów prawnych jak standardowe klauzule umowne bądź wiążące reguły korporacyjne tylko do tych podmiotów, które są certyfikowane w ramach tego programu. Ramy Ochrony Danych UE-USA opierają się na samocertyfikacji i uczestniczą w nim tylko te podmioty, które do niego przystąpiły.

Podkreślono, że obecny program w wielu elementach nie różni się od swoich poprzedników. Natomiast głównym problemem zasygnalizowanym w wyroku Schrems II jest dostęp służb amerykańskich do danych przetwarzanych przez podmioty odbierające dane w USA, na zasadach, które nie spełniają m.in. kryterium proporcjonalności, niezbędności oraz nie zapewniają jakichkolwiek mechanizmów gwarantujących możliwość odwołania się do sądu. W celu rozwiązania tego problemu, dekretem wykonawczym Prezydenta USA wprowadzono dodatkowe gwarancje i powołano dodatkowe instytucje, w tym m.in. specjalny sąd odwoławczy do spraw ochrony danych osobowych.

W związku z tym, że złożono już pierwsze skargi związane z funkcjonowaniem Ram Ochrony Danych UE-USA, zdaniem ekspertów, należy, liczyć się, że w perspektywie kilku lat rozstrzygnie się odpowiedź na pytanie o to, czy aktualne Ramy Ochrony Danych UE-USA zapewniają wystarczającą ochronę i są ważne.

Podczas dyskusji przestawiono także perspektywę prawną oraz ujęcie praktyczne nowoczesnego marketingu cyfrowego w kontekście zapewnienia bezpieczeństwa i ochrony danych osobowych. Jak wskazano podczas sesji współczesna gospodarka rynkowa wymaga od przedsiębiorców ciągłego starania o zainteresowanie konsumenta, rywalizacji z konkurentami i rozwijania współpracy z otoczeniem. Do tego potrzebne są informacje, w szczególności te, oddziaływujące na wybory konsumentów. Przedstawiono różnicę pomiędzy reklamą behawioralną, która jest oparta na obserwacji zachowań osoby w danym czasie a targetowaniem, które jest działaniem polegającym na skierowaniu lub ukierunkowaniu danego przekazu do konkretnej grupy osób. W obu przypadkach niewątpliwie dochodzi do przetwarzania danych osobowych i dlatego konieczne jest skuteczne egzekwowanie prawa osób, których dane dotyczą, zagwarantowanych przez RODO.

Uczestnicy sesji wyjaśnili także kwestię wpływu aktu w sprawie danych na RODO i przetwarzanie danych osobowych. Akt w sprawie danych stanowi część strategii UE, która zakłada stworzenie ram prawnych dla gromadzenia, przetwarzania, wtórnego wykorzystania danych osobowych i dzielenia się nimi. Jej celem jest również ułatwienie dostępu do informacji poprzez otwarcie publicznych przestrzeni danych, by w efekcie możliwe było pełne wykorzystanie potencjału cyfrowej gospodarki. Niemniej jednak w opinii wielu ekspertów akt w sprawie danych zawiera przepisy, które mogą szkodzić przejrzystości prawa, ochronie prywatności, ochronie własności intelektualnej i równemu traktowaniu podmiotów tworzących unijny rynek. Podkreślono ogromną szansę gospodarczą i społeczną wynikającą z transformacji cyfrowej, pod warunkiem zapewnienia konstruktywnego dialogu pomiędzy regulatorami a podmiotami, które będą dotknięte nowymi regulacjami.

Sesja VI: Era innowacji jako wyzwanie dla organów ochrony danych

Prelegenci:
Maria Skwarcan
Departament Współpracy Międzynarodowej i Edukacji, Urząd Ochrony Danych Osobowych

Anna Buchta
Kierownik Działu Polityka i Konsultacje, Europejski Inspektor Ochrony Danych

Rocco Panetta
Krajowy Lider IAPP – Włochy, Partner Zarządzający w Kancelarii PANETTA

Kari Laumann
Kierownik Sekcji Badań, Analiz i Polityki, Norweski Urząd Ochrony Danych

Yuliia Derkachenko
Przedstawicielka Rzecznika Praw Obywatelskich Ukrainy ds. praw informacyjnych

Sesję IV rozpoczęto przeglądem działań Europejskiej Rady Ochrony Danych podejmowanych wobec wyzwań związanych z rozwojem nowych technologii. Jednym z punktów strategii na lata 2021-2023 EROD jest podejście, zgodnie z którym ochrona danych osobowych nie powstrzymuje rozwoju innowacji, ale pomaga zapewnić rozwój technologii, nowych modeli biznesowych i społeczeństwa zgodnie z wartościami, takimi jak godność ludzka, autonomia i wolność.

W celu promowania podejścia do nowych technologii w oparciu o prawa podstawowe, EROD przyjęła w ostatnich latach szereg wytycznych (m.in. wytyczne

w sprawie wirtualnych asystentów głosowych[3], wytyczne w sprawie tzw. zwodniczych wzorców projektowych w interfejsach platform społecznościowych[4], o których była mowa we wcześniejszej części konferencji, oraz wytyczne w sprawie stosowania technologii rozpoznawania twarzy w dziedzinie egzekwowania prawa[5]). Prace nad kolejnymi dokumentami trwają.

Eksperci przedstawili także opinie EROD i EIOD dotyczące przedłożonych przez Komisję Europejską projektów aktów prawnych w ramach strategii cyfrowej i strategii w zakresie danych. Co istotne, chociaż zalecenia EROD i EIOD, dotyczące projektów unijnych aktów prawnych, nie są wiążące, to w praktyce mają przełożenie na dalszy przebieg procesu legislacyjnego. W szczególności Parlament Europejski, czasami również Rada UE, coraz częściej wprowadzają poprawki inspirowane zaleceniami EIOD i EROD.

EROD przedstawiła we wskazanych dokumentach szereg obaw i zaleceń dotyczących zgodności wniosków ustawodawczych z obowiązującym prawodawstwem Unii w zakresie ochrony danych, które dotyczyły zasadniczo braku wystarczającej ochrony podstawowych praw i wolności osób fizycznych, fragmentarycznego nadzoru oraz ryzyka wystąpienia niespójności z obecnymi ramami ochrony danych.

Podstawowy aspekt, na który zwraca uwagę EIOD w swoich opiniach, dotyczy tzw. wzajemnego oddziaływania poszczególnych nowych aktów prawnych z obowiązującymi przepisami w zakresie ochrony danych. Dzieje się to pomimo tego, że nieuchronnie wiele nowych regulacji, choć nie reguluje bezpośrednio kwestii ochrony danych osobowych, będzie miało zastosowanie w sytuacjach i w kontekście tych samych modeli biznesowych, które są już przedmiotem postępowań na gruncie RODO.

Uczestnicy sesji podkreślali, że prawo do ochrony danych osobowych wywodzi się z prawa podstawowego Unii Europejskiej i ma bardzo szczególny status w UE, dlatego należy podejmować działania zmierzające do tego, by to prawo było w pełni respektowane, także w kontekście spraw związanych z ochroną konkurencji i konsumentów. W konsekwencji, zarówno EROD, jak i EIOD, podkreślają, aby wdrażanie nowej legislacji unijnej było absolutnie zgodne z treścią RODO, ale również z jego ugruntowaną wykładnią. Co ważne, w niektórych przypadkach, gdzie konieczne było dostosowanie projektowanych regulacji do

[3] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-022021-virtual-voice-assistants_pl
[4] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-032022-deceptive-design-patterns-social-media_en
[5] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052022-use-facial-recognition-technology-area_pl

obowiązującego prawodawstwa, Parlament Europejski i Rada wprowadziły poprawki potwierdzające, że nowe akty prawne będą musiały być stosowane bez uszczerbku dla istniejących przepisów.

Zastrzeżenia budzi także fakt, że organy ochrony danych nie są w nowych instrumentach prawnych wyznaczane jako główne organy właściwe do egzekwowania ich przepisów. Państwa członkowskie mają ograniczony wybór i możliwości zdecydowania jakie organy będą kompetentne w danym zakresie. Jest to uzasadnione tym, że wspomniane nowe akty prawne mają inne cele niż RODO. Nie zmienia to faktu, że ktokolwiek będzie odpowiedzialny za wdrażanie nowych przepisów będzie musiał uwzględniać opinie organów ochrony danych. Jest to konieczne, choćby ze względu na podniesione wcześniej tzw. „wzajemne oddziaływanie". Choć cele regulacji się różnią, to jednocześnie należy zauważyć, że się uzupełniają, są komplementarne.

Eksperci wskazywali także na konieczność pełnego uwzględnienia przepisów RODO jako obowiązującego prawodawstwa w kontekście technologii generatywnej sztucznej inteligencji, opartej całkowicie na danych. Dlatego tak ważne jest, by projekt aktu w sprawie sztucznej inteligencji był zgodny z RODO i opierał się na RODO.

Omówiono także wnioski z postępowań przed włoskim organem ochrony danych dotyczących sztucznej inteligencji. Wniosek płynący ze wskazanych postępowań jest jasny: konieczne jest pełne uwzględnienie przepisów RODO jako obowiązującego prawodawstwa w kontekście technologii generatywnej sztucznej inteligencji. W związku z tym kluczowe jest, aby projekt aktu w sprawie sztucznej inteligencji był zgodny z RODO.

Norweski organ nadzorczy podzielił się swoimi doświadczeniami związanymi z projektem piaskownicy regulacyjnej dla sztucznej inteligencji i ochrony prywatności. Ta inicjatywa wspomogła zbudowanie wewnętrznych kompetencji organu w obszarze sztucznej inteligencji i pomogła pracownikom organu lepiej zrozumieć otoczenie biznesowe związane z AI, co przekłada się na lepszą ocenę tego, w jaki sposób stosować wymogi RODO.

Podczas sesji przedstawiono także rolę i doświadczenie ukraińskiego organu właściwego w sprawach ochrony danych w kontekście rozwoju technologii. Opracowywanie ram prawnych w dziedzinie sztucznej inteligencji w Ukrainie, jak wskazała ekspertka, opiera się na międzynarodowych standardach i zmierza w kierunku europejskiej strategii rozwoju sztucznej inteligencji. Opracowując ramy prawne i stając się kandydatem do UE, Ukraina jest zobowiązana do stworzenia systemu sztucznej inteligencji, który będzie przydatny dla obywateli, przedsiębiorstw i rządu. W związku z obranym przez Ukrainę kursem integracji europejskiej, opracowywanie i dalsze udoskonalanie ustawodawstwa krajowego w zakresie

regulacji prawnych dotyczących wykorzystywania sztucznej inteligencji powinno, opierać się na już ukształtowanych europejskich standardach, zasadach i zaleceniach.

Przedstawiono także istotne działania Ukrainy w sferze sztucznej inteligencji. Ważnym krokiem dla Ukrainy było przyjęcie Europejskiej Karty Etycznej w sprawie wykorzystywania sztucznej inteligencji w systemach sądownictwa i środowiskach pokrewnych przez Europejską Komisję na rzecz Efektywności Wymiaru Sprawiedliwości Rady Europy. W 2020 r. w Ukrainie powstała Koncepcja rozwoju sztucznej inteligencji w Ukrainie, w której po raz pierwszy na poziomie legislacyjnym określono definicję, cel, zasady i zadania rozwoju technologii sztucznej inteligencji w Ukrainie. Ukraina przystąpiła także m.in. do Programu "Cyfrowa Europa" (2021-2027), mającego na celu rozwój wiodących umiejętności cyfrowych i jeszcze większą dostępność usług cyfrowych dla obywateli i instytucji państwowych UE oraz krajów stowarzyszonych.

Ostateczną konkluzją było podkreślenie konieczności stworzenia globalnych (wiążących) międzynarodowych ram prawnych dla rozwoju i wdrażania sztucznej inteligencji, by móc zapobiec niezgodnemu z prawem jej wykorzystywaniu.

Debata: Najważniejsze trendy nowych technologii w kontekście ochrony danych osobowych

Moderator:
Adam Sanocki
Rzecznik Prasowy Urzędu Ochrony Danych Osobowych, Dyrektor Departamentu Komunikacji Społecznej w Urzędzie Ochrony Danych Osobowych

Uczestnicy debaty:
Jakub Groszkowski
Zastępca Prezesa Urzędu Ochrony Danych Osobowych

Monika Krasińska
Dyrektor Departamentu Orzecznictwa i Legislacji, Urząd Ochrony Danych Osobowych

Maciej Gawroński
Radca prawny, Partner w GP Partners, Członek Rady Naukowej Instytutu Prawa Ochrony Danych Osobowych

Xawery Konarski
Adwokat, Stowarzyszenia Prawa Nowych Technologii, Wiceprezes Polskiej Izby Informatyki i Telekomunikacji, Traple Konarski Podrecki i Wspólnicy Sp. J.

Ewa Kurowska-Tober
Radca prawny, Stowarzyszenie Prawa Nowych Technologii

Agnieszka Gajewska-Zabój
Radca prawny, Sekretarz Krajowej Rady Radców Prawnych

Marcin Wysocki
Zastępca Dyrektora Departamentu Cyberbezpieczeństwa, Ministerstwo Cyfryzacji

Debata ekspercka stanowiła podsumowanie konferencji i dotyczyła dynamicznego rozwoju innowacji i ich wpływu na ochronę danych osobowych, ujawniając istotne punkty dotyczące regulacji prawnych i praktyk biznesowych. Uczestnicy debaty podkreślali, że tempo postępu technologicznego wyprzedza aktualne regulacje, co rodzi potrzebę tworzenia standardów i dobrych praktyk, mogących zrównoważyć rozwój technologii z ochroną prywatności.

Podkreślano znaczenie wspierania takich instrumentów jak piaskownice regulacyjne, które pozwalają na identyfikację ryzyka oraz skuteczne reagowanie na nie. Wskazano, że w związku z rozwojem technologii, powstają różnorodne wyzwania, takie jak certyfikacja chmury obliczeniowej, szczególnie w kontekście najważniejszych kategorii danych i potencjalnych szkód ekonomicznych.

Zgodzono się co do tego, że wiele problemów można skutecznie rozwiązać, korzystając z istniejących regulacji, takich jak RODO. Przykładem tego podejścia jest zasada rozliczalności, która dostarcza konkretnego punktu odniesienia. Inna praktyczna wskazówka dotyczy krajowej certyfikacji - nawet niezatwierdzone kodeksy branżowe stanowią wartościowy instrument, wskazówkę właściwego postępowania.

W kontekście istniejących narzędzi, zagwarantowanych przez RODO, zaakcentowano znaczenie oceny wpływu na prywatność i zasady *privacy by design*. Ocena wpływu na prywatność jest często bagatelizowana, podczas gdy eksperci z dziedziny ochrony danych powinni być angażowani na etapie wczesnego projektowania każdego technologicznego przedsięwzięcia.

Eksperci podkreślali także, że nowe technologie powinny stanowić narzędzie rozwoju, a nie być celem samym w sobie. Pytanie o ocenę tego narzędzia staje się zasadnicze. Być może konieczne jest zdecydowane ograniczenie apetytu na dane poprzez środki legislacyjne. Dążenie do maksymalizacji zysku, przekładające się na minimalizację praw, staje się poważnym tematem do refleksji. Ta kwestia powinna być poddawana dyskusji wewnątrz organizacji, i powinna być ona prowadzona w oparciu o zaufanie konsumentów. Warto zaznaczyć, że wciąż brakuje głosu inspektorów ochrony danych w całym procesie.

Uczestnicy debaty wyrazili przekonanie, że prawo zawsze będzie miało trudności z nadążaniem za rozwojem społeczeństwa. Wyrażono pozytywną opinię na temat RODO, które stanowi fundament, na którym można budować działania w obszarze dostosowania nowych technologii do potrzeby ochrony praw jednostki. Odnosząc się do wcześniejszych uwag o potrzebie certyfikacji i zatwierdzania kodeksów postępowania, przypomniano o tym, że pierwszy zatwierdzony kodeks postępowania już istnieje oraz, zapewniono, że Prezes UODO będzie wspierać każdą rzetelnie przygotowaną inicjatywę.

Eksperci wskazywali także, że dyskusja na temat etyki nabiera tempa w kontekście sztucznej inteligencji. Etyka jest uznawana za jeden z głównych celów regulacji, zwłaszcza w kontekście technologii, które mają tendencję do wykorzystywania słabszych jednostek. Wskazano przy tym na potrzebę współistnienia dwóch czynników: dobrej legislacji i aktywnego działania organów nadzorczych.

Kończąc debatę, uczestnicy zgodzili się, że ostatecznie najistotniejsze jest to, by w centrum nowych technologii znalazł się człowiek, jego prawa i wolności. Bezkrytyczna wiara w cyfryzację jest staroświecka, a współczesny udany biznes wymaga dbałości o sferę prywatności konsumentów.

Wnioski ogólne z Konferencji "Forum Nowych Technologii"

Konferencja "Forum Nowych Technologii" była kluczowym wydarzeniem skupiającym się na złożoności i wyzwaniach związanych z ochroną danych osobowych w erze postępującej digitalizacji. Dyskusje i prezentacje przeprowadzone podczas pięciu sesji podkreśliły, że rozwój technologiczny, choć oferuje niespotykane dotąd możliwości, niesie ze sobą również nowe ryzyka dla prywatności i bezpieczeństwa danych osobowych. Uczestnicy konferencji, reprezentujący szeroki wachlarz perspektyw, od technologicznych po prawne, zgodnie podkreślali konieczność holistycznego podejścia do problematyki ochrony danych.

Kluczowe obszary, które wymagają szczególnej uwagi, to m.in. etyczne aspekty stosowania sztucznej inteligencji, wyzwania związane z technologią w kontekście praw osób, oraz potrzeba zapewnienia przejrzystości stosowanych technologii i procesów przetwarzanych danych, w celu umożliwienia sprawowania realnej kontroli przez osoby, których dane dotyczą, nad ich danymi osobowymi.

Równie ważna okazała się kwestia dostosowywania nowych regulacji, powstających w reakcji na szybko zmieniające się realia cyfrowe, do aktualnie obowiązujących ram ochrony

danych osobowych, aby zapewnić zgodność z RODO i jego wykładnią, a tym samym zagwarantować ochronę praw jednostek.

Szczególnie istotne w tym kontekście jest też wzmocnienie współpracy między organami regulacyjnymi, przemysłem technologicznym, środowiskiem akademickim i organizacjami pozarządowymi w celu rozwijania zrównoważonych rozwiązań dotyczących ochrony danych. Należy także rozwijać platformy wymiany wiedzy i doświadczeń, które pomogą w dostosowywaniu przepisów i praktyk do szybko zmieniającego się środowiska technologicznego.

Aby zapewnić rozwój technologii, gwarantując przy tym wzmacnianie praw osób, których dane dotyczą, ważne jest również opracowywanie kodeksów i certyfikacji w branży technologicznej, jak również promowanie najlepszych praktyk wśród administratorów w zakresie etycznego i odpowiedzialnego wykorzystania danych osobowych w zakresie nowych technologii.

Podsumowanie i podziękowania

Konferencja „Forum Nowych Technologii" pokazała jak ważne jest ciągłe śledzenie i reagowanie na zmiany w świecie technologii, zwłaszcza w kontekście ochrony danych osobowych. Przyszłe strategie i działania powinny równoważyć innowacyjność z etycznymi i prawymi aspektami ochrony prywatności, co wymaga wspólnych wysiłków wszystkich zainteresowanych stron.

Urząd Ochrony Danych Osobowych dziękuje wszystkim, którzy przyczynili się do sukcesu konferencji "Forum Nowych Technologii". Składamy serdeczne podziękowania Akademii Ekonomiczno-Humanistycznej w Warszawie oraz Stowarzyszeniu Prawa Nowych Technologii za współorganizację tego wydarzenia. Szczególne podziękowania kierujemy do patronów i sponsorów, którzy wsparli naszą konferencję. Państwa wsparcie było nieocenione dla zapewnienia wysokiej jakości i zasięgu tego wydarzenia.

Dziękujemy wszystkim prelegentom za ich bezcenną wiedze, doświadczenie i wgląd w kwestie związane z nowymi technologiami i ochroną danych osobowych. Państwa prezentacje i dyskusje wniosły istotny wkład w zrozumienie i adresowanie współczesnych wyzwań.

Dziękujemy również wszystkim uczestnikom za liczny udział w konferencji. Państwa zainteresowanie kwestiami związanymi z ochroną danych osobowych i pozytywny odbiór konferencji są najlepszą motywacją dla Urzędu Ochrony Danych Osobowych do organizowania kolejnych tego typu wydarzeń. Jako Urząd Ochrony Danych Osobowych jesteśmy wdzięczni

za możliwość prowadzenia tak ważnego dialogu i podnoszenia świadomości w zakresie ochrony prywatności i danych osobowych w erze cyfrowej w kolejnych latach, zapraszając Państwa na następne, organizowane przez UODO wydarzenia.