URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 1/26

www.uodo.gov.pl

SPIS TREŚCI

SPIS TREŚCI

Szanowni Państwo!

dwa lata temu objąłem stanowisko Prezesa UODO. Rozliczam się z tych dwóch lat w wywiadzie, który znajdą Państwo w tym Biuletynie. Prawdziwym podsumowaniem półmetka kadencji - i postawieniem sobie zadań na następne dwa lata był jednak Kongres Ochrony Danych i Nowych Technologii, który 28 stycznia odbył się w Muzeum Historii Polski.

Współorganizowaliśmy go wraz z Krajową Izbą Radców Prawnych w 20. Europejskim Dniu Ochrony Danych Osobowych. Na wydarzenie to przyjęło zaproszenie wielu specjalistów od sztucznej inteligencji, nowych technologii, ekspertów od unijnych regulacji cyfrowych, środowiska i instytucje współtworzące bezpieczną przestrzeń ochrony danych w Polsce.

Wystąpienia i panele dotyczyły przyszłości RODO, przyszłości regulacyjnej sztucznej inteligencji, nowych technologie w zatrudnieniu, ochrony małoletnich w internecie, deepfake'ów, cyberprzestępczości, technologii kwantowych, nowych technologii w medycynie czy unijnego pakietu Omnibus. https://uodo.gov.pl/pl/138/4029
Wydarzenie to cieszyło się ogromnym zainteresowaniem i było doskonałą okazją do dyskusji, wymiany poglądów. Dla wielu osób okazało się inspiracją do kolejnych działań naukowych czy edukacyjnych.

W styczniu Urząd Ochrony Danych Osobowych przedstawił plan kontroli sektorowych na ten rok. Obejmie on organy, które przetwarzają dane osobowe w Wielkoskalowych Systemach Unii, podmioty lecznicze (monitoring wizyjny), podmioty prowadzące Biuletyn Informacji Publicznej (anonimizacja danych), podmioty marketingowe (przetwarzania danych osobowych w celach marketingowych), internetowe platformy dostaw.

Ważne sprawy

- Prokuratura w styczniu przyjęła nasze argumenty i zajęła się sprawą naruszenia praw dziewczynki, której szkolni koledzy wygenerowali nagie zdjęcie i rozsyłali je sobie. Sprawą zajmujemy się od połowy 2025 r. Wcześniej organy ścigania odmówiły wszczęcia śledztwa, argumentując, że przecież nie doszło do nagiej sesji fotograficznej z udziałem nieletniej. Moim zdaniem wykorzystanie wizerunku młodej dziewczyny drastycznie naruszyło jej prywatność oraz zagroziło naruszeniem jej elementarnych interesów życiowych w przyszłości. Dlatego państwo powinno stanąć w obronie jej praw.

- W styczniu wydałem decyzję w sprawie z 2023 r., gdy Policja ujawniła na konferencji prasowej dane kobiety, w tym dane dotyczące jej stanu zdrowia. W sprawie tej nałożyłem w 2025 r. karę na Komendanta Głównego Policji, której prawidłowość potwierdził w styczniu tego roku Wojewódzki Sąd Administracyjny. W dalszym postępowaniu badaliśmy, jak mogło dojść do takiego naruszenia prywatności. Okazało się, że Komendant Miejski Policji w Krakowie nie sporządził analizy ryzyka, więc też nie wprowadził odpowiednich zabezpieczeń dla danych. Policja zbiera dane o obywatelach w Systemie Wspomagania Dowodzenia Policji (SWD). Komendant Miejski przyznał również, że naruszenie ochrony danych osobowych mogło spowodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej. W krakowskiej komendzie nie było jednak reguł gwarantujących, że dane osobowe z tej bazy nie zostaną użyte – jak w tym przypadku – w komunikacie zespołu prasowego. To, że dane kobiety zostały upublicznione, nie jest skutkiem incydentu czy błędu jednostki, ale systemowym zaniechaniem.
- W styczniu nałożyłem także karę na Pocztę Polską za wadliwe organizacyjne umiejscowienie IOD, że nie miał on gwarancji niezależności i szansy na dobre wykonywanie zadań. IOD jednocześnie pracował na stanowisku kierowniczym bezpośredniego związanym z przetwarzaniem danych osobowych. IOD może pełnić też inne funkcje w organizacji. Należy jednak wcześniej – i to na piśmie – zanalizować ryzyko i ustalić reguły pracy, które wykluczą konflikt interesów oraz zapewnią, że IOD będzie miał czas na wykonywanie swoich zadań.
- Prezes UODO upomniał Sąd Rejonowy w Lublinie. Sąd nie przeprowadził właściwej analizy ryzyka. Skończyło się to incydentem w postaci ujawnienia danych w odpowiedzi na wniosek o dostęp do informacji publicznej. Wnioskodawca dostał plik z danymi razem z ukrytymi w nim kolumnami z danymi osobowymi.
- WSA podtrzymał decyzję Pereza UODO o nałożeniu kary na przedsiębiorstwo pogrzebowe. Chodziło o sprawę zagubienia dokumentacji z nazwiskami członków rodzin zmarłych w czasie transportu (spadła z niezabezpieczonej naczepy i znalazła ją w rowie policja). PUODO wskazał, że incydentowi zapobiegłaby prawidłowo przeprowadzona analiza ryzyka. WSA podzielił ten pogląd.

Prezes UODO złożył także zażalenie na postanowienie o umorzeniu dochodzenia w sprawie monitoringu w szpitalu w Przemyślu. Monitoring był założony bez zgody dyrekcji, a więc nie objęty został zabezpieczeniami chroniącymi dane osobowe. Pracownicy szpitala chcieli po prostu ustalić, kto „podbiera" leki z szafki. Prokuratura uznała, że nie jest w stanie ustalić sprawcy, więc umorzyła postępowanie. Prezes UODO wskazał jej błędy w rozumowaniu i wskazał, dlaczego sprawa ta wymaga jednak wyjaśnienia.

Legislacja

W styczniu zgłosiłem uwagi m.in. do projektu ustawy o sprawiedliwym dostępie do danych, do projektu ustawy pozwalającej badać trzeźwość parlamentarzystów (jego konsekwencją będzie przetwarzanie danych) oraz do projektu ustawy o osobistych kontach inwestycyjnych.

Przedstawiliśmy też analizę konsekwencji wyroku Trybunał EFTA w sprawie E-5/25 Silbernagl dotyczącej zasad rozwiązywania stosunku pracy z IOD. Wyrok ten dotyczył przepisów Księstwa Luksemburg. Polska takich regulacji nie ma – opiera się wyłącznie na dyspozycjach RODO. Jednak należałoby sprecyzować zasady rozwiązywania stosunków pracy z osobami pełniącymi funkcję IOD.

UODO w Polsce

W styczniu kontynuowaliśmy akcję „UODO rusza w kraj" – tym razem 23 stycznia spotkaliśmy się z mieszkańcami, IOD-am i administratorami z Suwałk i województwa podlaskiego.

W ramach naszej akcji promującej wiedzę o prawie do prywatności i danych osobowych odwiedziliśmy już Kraków, Tarnów, Katowice, Rzeszów, Kwidzyn, Gdynię i Gdańsk, Płock, Poznań, Olsztyn oraz Gorzów Wielkopolski.

Mirosław Wróblewski
Prezes UODO

Szanowni Państwo!

Na drugą rocznicę objęcia stanowiska Prezesa UODO Mirosława Wróblewskiego przeprowadziłem z nim rozmowę o tym, co nam się udało, a co przed nami. Serdecznie zachęcam do lektury.
W tym numerze rozpoczynamy również cykl publikacji na temat Europejskiej strategii w zakresie danych oraz nowej Europejskiej strategii w zakresie unii danych.

Na początku przybliżymy Państwu DGA, czyli rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danym, oraz omówimy nowe zadania Prezesa UODO wynikające z projektowanych przepisów ustawy o zarządzaniu danymi. Zachęcam też do zapoznania się z materiałem wyjaśniającym, jak przeprowadzać analizę ryzyka zgodnie z zasadą rozliczalności. Ryzyko w rozumieniu RODO zawsze powinno być analizowane z perspektywy osoby, której dane dotyczą, a nie organizacji, która te dane przetwarza (np. przez pryzmat ryzyka finansowego, wizerunkowego lub operacyjnego). Ma to szczególne znaczenie przy określaniu wagi skutków urzeczywistnienia się określonych zagrożeń.

Odpowiadamy także na pytanie, czy przedszkola mogą pozyskiwać numery PESEL rodziców. Odpowiedź brzmi „nie”, a uzasadnienie znajdą Państwo niżej.

Ekspertów zajmujących się badaniami opinii publicznej powinien zainteresować materiał o „liście Robinsona”, narzędziu pozwalającym skutecznie respektować wolę osób, które nie życzą sobie kontaktu z ankieterami. Jest to element zatwierdzonego przez Prezesa UODO w listopadzie 2025 r. Kodeksu postępowania dotyczącego przetwarzania danych osobowych przez prywatne agencje badawcze.

Proponujemy też Państwu materiał o tym, jak prowadzić badania społeczne z udziałem dzieci.

Na ile narusza prywatność publikowanie w mediach społecznościowych numerów rejestracyjnych samochodów? Zajmował się tym czeski organ nadzorczy – materiał o jego ustaleniach zamieszczamy w tym numerze.

Publikujemy również informacje o działaniach (i karach) nakładanych przez organy nadzorcze Francji, Finlandii, Włoch.

Podczas ostatniej sesji plenarnej EROD przyjął opinię dotyczącą projektu decyzji Komisji Europejskiej w sprawie odpowiedniego poziomu ochrony danych osobowych w Brazylii. Po jej przyjęciu decyzja zapewni swobodny przepływ danych osobowych z Europy do Brazylii oraz umożliwi jednostkom zachowanie kontroli nad swoimi danymi.

14 listopada 2025 r. w Warszawie odbyła się konferencja „Privacy, AI and Innovation Roundtable”, zorganizowana przez kancelarię Bird & Bird. Publikujemy z niej relację. Wydarzenie zgromadziło ekspertów z obszaru prawa, ochrony danych i nowych technologii, którzy wspólnie zastanawiali się nad przyszłością regulacji dotyczących prywatności i sztucznej inteligencji w Europie. Spotkanie miało charakter interaktywny – uczestnicy nie tylko wysłuchali wystąpień, ale także współtworzyli rekomendacje, które zostaną opublikowane w raporcie końcowym.

Zapraszam do lektury.

Karol Witowski
Dyrektor Departamentu Komunikacji Społecznej
Rzecznik Prasowy UODO

DWA LATA WALKI O ŚWIADOMOŚĆ OCHRONY DANYCH – Z PREZESEM UODO MIROSŁAWEM WRÓBLEWSKIM ROZMAWIA KAROL WITOWSKI

26 stycznia 2024 r. objął Pan stanowisko Prezesa UODO. Jakie osiągnięcia z pierwszej połowy swojej kadencji uważa Pan za kluczowe?

Trudno wyróżnić jedno takie osiągnięcie, ale przede wszystkim jestem zadowolony z tego, że przez ten czas udało nam się zwiększyć świadomość obywateli dotyczącą ochrony danych osobowych i zaufanie do Urzędu Ochrony Danych Osobowych – o czym świadczą też liczby: wzrosła liczba skarg zgłaszanych do Prezesa UODO. Jeszcze w 2023 r. było to niecałe 7 tys., natomiast w 2025 zgłoszono prawie 13 tys. skarg. Podobnie wzrosła liczba zgłaszanych przez administratorów danych naruszeń. W 2023 r. było to ponad 14 tys., a w 2025 r. zgłoszono ponad 22 tys. naruszeń ochrony danych osobowych. Tu znaczenie ma ogólna sytuacja na rynku, a także wypracowanie przejrzystej i jednoznacznej wykładni przepisów RODO, co znalazło swój wyraz w opublikowanym przez Urząd nowym poradniku.

Udało się także polepszyć i wzmocnić komunikację z obywatelami: UODO opublikował w 2025 r. ponad 300 komunikatów o swojej działalności (w porównaniu z rokiem 2023, kiedy było ich około 80). Zwiększyła się również nasza obecność w mediach społecznościowych. Znacznie częściej pisze się także o Urzędzie i o jego aktywnościach oraz ochronie danych osobowych w samych mediach: w 2025 r. było w publikacjach ponad 24 tys. wzmianek o UODO. Ważny jest też fakt, że wspomniane publikacje w ogromnej większości dotyczą spraw merytorycznych i tematów ważnych społecznie. Skierowano również do Urzędu znaczną liczbę zapytań dziennikarskich: prawie 650 w porównaniu np. z rokiem 2023, kiedy było ich ponad 400. To pokazuje skalę naszego działania i rosnącą rolę ochrony danych w życiu społeczno-gospodarczym.

1 ROZMOWA Z EKSPERTEM

Jedna ze spraw miała wyjątkowy oddźwięk społeczny i poruszała ważne kwestie. Mam na myśli przypadek wygenerowania, za pomocą sztucznej inteligencji, nagich zdjęć dziewczynki. Zrobili to jej koledzy ze szkoły. Sprawa jest skomplikowana, ponieważ organy ścigania odmówiły zajęcia się nią. Wykazał się Pan determinacją i ostatecznie doprowadził do tego, że prokuratura podjęła postępowanie. Czy jest to sprawa, którą postrzega Pan jako szczególnie istotną w kontekście działalności UODO w tym czasie?

Rzeczywiście udało się doprowadzić do tego, że prokuratura na nowo podjęła sprawę dotyczącą wygenerowania oraz upubliczniania nagiego wizerunku uczennicy; to sprawa, w której wcześniej organy ścigania odmówiły wszczęcia postępowania, mimo że zawiadomień do prokuratury było kilka, moje zawiadomienie nie było jedyne. Podjęcie przez prokuraturę czynności jest efektem działań, w których zwracałem uwagę na konieczność kompleksowego zbadania okoliczności zdarzenia oraz zapewnienia skutecznej ochrony praw osoby, której dane dotyczą.

Zresztą ta sprawa ma dla mnie i całego Urzędu wyjątkowy kontekst, bo bezpieczeństwo dzieci i młodzieży i ich ochrona przez niebezpieczeństwami związanymi z wykorzystywaniem nowoczesnych technologii, w tym zwłaszcza sztucznej inteligencji do tworzenia deepfake'ów, jest przedmiotem naszej wyjątkowej troski od początku mojej obecności w UODO.

Dzieci i młodzież nie mają dostatecznej świadomości wagi ochrony danych osobowych, nie przewidują też najczęściej w pełni wszystkich ryzyk, które dotyczą korzystania z internetu. W sprawie wprowadzenia do polskiego prawa przepisów uwzględniających takie zjawiska jak deepfake apelowałem już wielokrotnie, ostatnio nawet na Sejmowej Komisji ds. Dzieci i Młodzieży miałem wystąpienie, a posłowie przyjęli projekt dezyderatu ws. zwiększenia ochrony wizerunku małoletnich w przestrzeni cyfrowej, co dotyczy również takich praktyk w sieci jak sharenting.

Odnoszę wrażenie, że moje apele, a także wszelkie aktywności Urzędu skupiające się na ochronie dzieci i młodzieży odnoszą coraz większy skutek i coraz częściej mówi się o konieczności kompleksowej zmiany polskiego prawa. Ostatnia decyzja prokuratury też pokazuje, że organy ścigania powoli – pod naciskiem rzeczowych argumentów – przestają się wahać i podejmują te sprawy, mimo że nie są one łatwe właśnie z powodu luk w prawie. Wypada mi również podziękować organizacjom, które przez te dwa lata wspierały Urząd w działaniach na rzecz zapewnienia bezpieczeństwa najmłodszym w kontekście ochrony ich danych – np. wspólnie z Fundacją Orange wydaliśmy już wcześniej publikację „Wizerunek dziecka w internecie". W tych działaniach wspiera nas także Społeczny Zespół Ekspertów przy Prezesie UODO.

1 ROZMOWA Z EKSPERTEM

Jakie inne sprawy z minionych dwóch lat są w Pana opinii szczególnie istotne?

Z innych ważnych dla ochrony danych kwestii chciałbym wskazać na sprawę, w której nałożyłem na firmę Meta zakaz wyświetlania oszukańczych reklam z wizerunkiem dwóch osób, pana Rafała Brzoski i pani Omeny Mensah. Gigant nie zgadzał się z moimi postanowieniami wydanymi w związku z działaniami oszustów na Facebooku i Instagramie i wystosował do sądu skargi, które jednak wycofał po czterech porażkach w sądzie pierwszej instancji. W związku z tym Wojewódzki Sąd Administracyjny zakończył postępowanie. Ma to donośne znaczenie, bo sprawa ta jest jednym z przykładów niebezpieczeństwa, jakim w ostatnich latach jest praktyka deepfake'ów oraz tzw. clickbaitu. Doceniam to, że Meta w późniejszym okresie nawiązała współpracę i wprowadziła systemowe rozwiązania techniczne dostępne dla każdego, pozwalające na szybsze rozpatrywanie zgłaszanych reklam tego typu, aczkolwiek skuteczność tego mechanizmu nie jest pewna i będzie przez nas monitorowana.

Na uwagę zasługują też wyroki Naczelnego Sądu Administracyjnego w sprawach skargowych, dotyczące przetwarzania danych osobowych niedoszłych lub byłych klientów banków. NSA podtrzymał stanowisko Prezesa UODO, że nie można przetwarzać danych wnioskodawcy o kredyt, jeżeli nie doszło do zawarcia umowy klienta z bankiem; podobnie ewentualne przyszłe roszczenia byłego klienta nie uzasadniają przetwarzania jego danych osobowych przez bank i Biuro Informacji Kredytowej. Ta sprawa miała również szeroki oddźwięk społeczny, bo w bardzo dużej skali dotyczy relacji obywateli z bankami.

Cieszę się też, że już z początkiem mojej kadencji udało mi się zmienić – uwzględniając orzecznictwo TSUE – stanowisko procesowe poprzedniego Prezesa UODO w postępowaniu przed Naczelnym Sądem Administracyjnym w sprawie ze skargi Rzecznika Praw Obywatelskich, dotyczącej przepisów tzw. ustawy kagańcowej nakazującej sędziom i prokuratorom ujawniać przynależność do zrzeszeń, co obejmować mogło także ujawnianie przynależności do kościoła lub związku wyznaniowego. W nowym stanowisku podkreśliłem konieczność ochrony prywatności sędziów i prokuratorów, a NSA przyznał rację zarówno mnie, jak i Rzecznikowi Praw Obywatelskich.

Oczywiście te sprawy przychodzą mi do głowy pierwsze. Równie ważnych było całe mnóstwo, to np. także wiele ważnych i wygranych spraw dotyczących ochrony danych w związku ze stosowaniem monitoringu wizyjnego.

1 ROZMOWA Z EKSPERTEM

Powołał Pan Społeczny Zespół Ekspertów przy Prezesie UODO. Takich kroków nie podjął nikt wcześniej. Członkowie SZE są bardzo aktywni i zaangażowani. Jak z perspektywy czasu ocenia Pan pracę zespołu?

Społeczny Zespół Ekspertów powołałem w czerwcu 2024 r. Od tego momentu Zespół jest fenomenalnym ciałem doradczym, opiniującym i konsultującym społecznie działania Urzędu. Mapuje także bieżące problemy, które pojawiają się w przestrzeni publicznej, i stara się na nie reagować w sensie głosu eksperckiego. Wspólnie z SZE zorganizowaliśmy już wiele seminariów, konferencji i webinariów, podczas których omawiamy i wyjaśniamy palące kwestie dotyczące ochrony danych. Ostatnio takim tematem jest również sztuczna inteligencja – w obrębie SZE powołaliśmy oddzielną grupę, które zajmuje się tą tematyką.

Pragnę podkreślić, że praca Prezesa UODO, wspieranego przez dwóch znakomitych zastępców, dyrektorów, naczelników i innych ekspertów Urzędu, jest pracą zespołową. Kraje członkowskie tworząc organ ochrony danych, mogły decydować, czy tworzyć instytucje kolektywne (np. komisje), czy organy monokratyczne. W Polsce mamy organ jednoosobowy i wydaje mi się istotne, aby oprócz wsparcia urzędowego mógł on konsultować kierunki działań oraz wyjątkowo ważne obszary, jak np. styk ochrony danych z nowymi technologiami, z przedstawicielami różnych środowisk oraz ekspertami prawnymi i technicznymi.

Często mówi się o tym, że UODO w roku 2025 nałożył finansowe kary administracyjne w rekordowej kwocie ponad 64 mln zł. Niektórzy kojarzą Urząd właśnie z takich działań…

Kary finansowe nigdy nie są celem samym w sobie, nie stanową misji UODO. Organ nadzorczy nakłada je tylko wtedy, gdy nie widzi już innego narzędzia, by zmobilizować instytucję, firmę czy organizację do odpowiednich działań w obszarze ochrony danych. To najczęściej przypadki najpoważniejszych zaniedbań procedur bezpieczeństwa i braku analizy ryzyka. A wysokość łączna kar w roku 2025 wynika z tego, że kilka z nich zostało nałożonych na bardzo duże podmioty – a trzeba pamiętać, że kwoty kar są proporcjonalne do możliwości danego podmiotu. Samych kar było 32 – o kilka więcej niż we wcześniejszych latach – a zatem tym bardziej trzeba zwracać uwagę na wielkość podmiotów. Fundamentem misji UODO jest jednak zwiększanie świadomości w zakresie bezpieczeństwa i ochrony danych, a nie kary administracyjne, które, tak jak zaznaczyłem, są ostatecznością.

1 ROZMOWA Z EKSPERTEM

Wśród podmiotów ukaranych w 2025 r. znalazła się Poczta Polska. Sprawa dotyczy prezydenckich „wyborów kopertowych" z 2020 r. Pojawia się jednak argument, że wówczas PP podjęła się próby organizacji wyborów z powodu wyższej konieczności.

Interpretacje tego rodzaju nie są przedmiotem analizy Urzędu, musielibyśmy zagłębiać się w cały kontekst polityczny, a dotyczy to wielu spraw. Decydujące jest przestrzeganie prawa i standardów ochrony danych. Istotne jest jedynie to, że Poczta Polska pozyskała z rejestru PESEL dane 30 mln obywateli do przeprowadzenia głosowania. Dane osobowe tak potężnej liczby obywateli RP zostały jednak udostępnione bez podstawy prawnej, co jednoznacznie przesądziły wyroki sądów administracyjnych, potwierdzając, że doszło do rażącego naruszenia prawa. Decyzje o karze były logiczną i konieczną konsekwencją tych wyroków. Mówię o decyzjach, ponieważ karę otrzymał także Minister Cyfryzacji, również za bezpodstawne przetwarzanie danych obywateli, który – co odebrałem z uznaniem – przyjął w pełni moją decyzję i wcześniejszy prawomocny wyrok NSA. Chcę też podkreślić, że działania UODO w tej sprawie zostały uruchomione z powodu setek skarg, które zaczęły napływać od obywateli, jednak ówczesny prezes UODO uznał je za bezpodstawne. Jednak w mojej opinii, ale także w opinii Rzecznika Praw Obywatelskich, działania związane z ochroną danych jak najbardziej należało podjąć.

Podobnie musiałem podjąć działania wobec jednego z banków, który przez ponad rok stosował praktykę powszechnego kopiowania dowodów tożsamości, a obejmowała ona każdego klienta niezależnie od charakteru sprawy. Kara była w tej sprawie konieczna, bo doszło do fundamentalnego złamania reguł legalności operacji na danych, ich ograniczenia do niezbędnego minimum. Przy tak znaczących naruszeniach prawa, niezależnie od wielkości podmiotu, których się ich dopuścił, reagowanie i egzekwowanie prawa jest konieczne.

Mówi Pan, że UODO stoi na dwóch nogach, jedną z nich jest egzekucja prawa, drugą edukacja. Jak przedstawia się działalność edukacyjna UODO za Pana kadencji?

Odbywa się w wielu obszarach. To rozwijanie ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa", który – co warto podkreślić – został wyróżniony w 2025 r. podczas gali finałowej konkursu Nauczyciela Roku „Głosu Nauczycielskiego" w kategorii Inicjatywa Edukacyjna. To także warsztaty dla seniorów dotyczące bezpieczeństwa ich danych, organizowane przez UODO od chwili podpisania przeze mnie porozumienia o współpracy z Ogólnopolską Federacją Stowarzyszeń Uniwersytetów Trzeciego Wieku.

Organizujemy również warsztaty dla studentów, konkursy dla studentów prawa, wizyty szkoleniowe dla studentów w Urzędzie. Bardzo ważny jest dla mnie program „UODO rusza w kraj", w ramach którego spotykamy się z samorządem terytorialnym w danym regionie, biznesem i jego organizacjami, organizacjami społecznymi i wreszcie z ekspertami uczelni wyższych i ośrodków naukowych – dotychczas odwiedziliśmy już dziewięć województw. Chciałbym wspomnieć, że w listopadzie otworzyłem, dzięki gościnności Okręgowej Izby Radców Prawnych w Rzeszowie, pierwszy stały punkt konsultacyjny UODO poza Warszawą.

Wreszcie, od dwóch lat jesteśmy obecni na wielkim festiwalu „Pol'and'Rock", na którym organizujemy własny program działań edukacyjnych, w warunkach nietypowych dla urzędu – uważam jednak, że z informacją o ochronie danych, prywatności i współczesnymi wyzwaniami trzeba docierać wszędzie tam, gdzie się da. A na takim festiwalu możemy dotrzeć z naszą misją do bardzo wielu osób.

Ta działalność edukacyjna w moim przekonaniu stanowi zasadniczy obszar aktywności UODO na rzecz budowania świadomości ochrony danych i prawa do prywatności. W szeroko pojętym obszarze edukacyjnym należy też umieścić wszystkie konferencje i seminaria zorganizowane przez UODO przez dwa lata mojej kadencji. Do najważniejszych zaliczam konferencje dotyczące sztucznej inteligencji, biometrii, danych osobowych w działalności dziennikarskiej, dotyczące relacji pomiędzy Prezesem UODO a sądami powszechnymi, technologii kwantowych, ochrony danych osobowych w związku z procesem uzgodnienia płci, czy danych osobowych w medycynie i sektorze farmaceutycznym.

Urząd wykazał też szczególną aktywność, jeśli chodzi o podpisane porozumienia z instytucjami na rzecz ochrony danych w różnych obszarach.

To przede wszystkim porozumienia z Prezesem Naczelnej Rady Lekarskiej o współpracy w zakresie ochrony danych w działalności podmiotów medycznych, porozumienie z Rzeczniczką Praw Dziecka w zakresie inicjatyw edukacyjnych na rzecz ochrony danych osobowych dzieci i młodzieży, porozumienie z Naczelną Radą Adwokacką, Polskim Autokefalicznym Kościołem Prawosławnym, Rządowym Centrum Legislacji czy Głównym Inspektorem Sanitarnym. Taka koordynacja działań już przynosi znakomite efekty; działamy w synergii, wymieniając się pomysłami i uwagami, co sprawia, że wspólne zaangażowanie dla ochrony danych przebija się do świadomości także decydentów, i dzięki temu my wszyscy jako instytucje rządowe czy pozarządowe nie jesteśmy postrzegani jako samotne wyspy, kiedy apelujemy w konkretnej sprawie o poszanowanie standardów ochrony praw podstawowych czy odpowiednie wyważenie między interesami administratorów, najczęściej przedsiębiorców i praw osób, których dane dotyczą.

1 ROZMOWA Z EKSPERTEM

Nie da się nie zauważyć, że często pojawia się na konferencjach i seminariach sformułowanie „prawo nie nadąża za technologią”. Jak wygląda działalność UODO, jeśli chodzi o opiniowanie legislacji?

W 2024 r. Prezes UODO zaopiniował 779 projektów aktów prawnych, a w roku 2025 już 962. Liczba pytań dotyczących wykładni prawa ogółem to 2214 w 2024 r. i 2174 w 2025 r. W tym ostatnim obszarze wprowadzamy większość dostępność stanowisk Urzędu, uruchomiliśmy też nową wyszukiwarkę decyzji administracyjnych, pracujemy nad tym, by nasze zasoby skierować na obszary priorytetowe, w których oczekiwana jest większa aktywność Urzędu. Takie oczekiwania podczas komisji i posiedzeń plenarnych kierowali np. posłowie, deklarując chęć podjęcia inicjatyw ustawodawczych związanych z ochroną danych. Dlatego tylko w roku 2025 skierowałem kilkadziesiąt różnych wystąpień dotyczących potrzeby zmian prawnych z związku z zapewnieniem skutecznej ochrony danych, podczas gdy wcześniej rocznie było ich zaledwie kilka. W 2025 r. odpowiedzieliśmy także na 57 zapytań od organów nadzorczych innych państw.

Do najważniejszych tematów legislacyjnych należały na pewno: zwracanie uwagi na przeprowadzanie testów prywatności, w tym oceny skutków dla ochrony danych, czy analiza kolejnych wersji ustawy o systemach sztucznej inteligencji, opiniowanie ustawy o Krajowym Systemie Cyberbezpieczeństwa, a także odnoszenie się do EHDS w pracach Ministerstwa Zdrowia (Europejska Przestrzeń Danych dot. Zdrowia) w celu zapewnienia stosowania tego rozporządzenia, czy opinie odnośnie do stosowania i wykładni przepisów ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, także w kontekście monitoringu wizyjnego w placówkach medycznych.

Zresztą ta ostatnia kwestia – z uwagi na coraz częściej pojawiające się incydenty w tym obszarze – stała się przedmiotem kontroli sektorowych UODO w tym roku: szczególnie ważne będzie dla nas sprawdzenie, na ile placówki medyczne radzą sobie ze stosowaniem monitoringu wizyjnego tam, gdzie może dojść do naruszeń ochrony danych osobowych najmłodszych.

Prezes UODO opiniował też Strategię Cyfryzacji Polski do 2035 r., Strategię informatyzacji Państwa, Strategię Cyberbezpieczeństwa RP do 2029 r.; wypowiadał się także na temat konieczności przeglądu regulacji dotyczących rejestrów publicznych, jawności ksiąg wieczystych i ustawy o ewidencji ludności. Niezwykle istotne mogą się też okazać, mam nadzieję, opinie organu nadzorczego na temat unijnego pakietu „Omnibus”.

Jednak nic nie jest idealne, więc muszę zapytać: co Pana zdaniem się nie udało podczas minionej połowy Pana kadencji?

Nadal, wydaje mi się, nie udaje się do końca przełamać błędnego postrzegania ochrony danych osobowych jako jakiejś formalnej procedury, praktyki urzędniczej, która nie ma przełożenia na ochronę prywatności i jest takim mało istotnym szczegółem w rzeczywistości. Na razie – ale nie tylko w polskiej rzeczywistości, bo dotyczy to także innych regionów – to zagadnienie jest odbierane w dość wąskim rozumieniu, co przekłada się również na deficyt świadomości o konieczności uwzględniania tematyki ochrony danych już na wczesnym etapie prac nad rozwiązaniami legislacyjnymi (organ nadzorczy nie musiałby wydawać tylu opinii, gdyby odbywało się to właśnie na wczesnym etapie). Gdyby przez kolejne dwa lata udało mi się przełamać ten rodzaj myślenia wśród obywateli i decydentów, uznałbym to za swój wielki sukces. Musimy pamiętać, że ochrona danych i prawo do prywatności do jedne z praw podstawowych, a same dane są dziś po prostu walutą. Pamiętajmy też – jakże to ważne w dzisiejszej geopolitycznej sytuacji – o znaczeniu ochrony danych dla bezpieczeństwa państwa w kontekście strategicznym i wojskowym.

Smutkiem napawa mnie również to, że z racji tempa, w jakim rozwijają się najnowsze technologie, nie jesteśmy w stanie jako państwo, ale także jako urząd, nadgonić rzeczywistości, i cierpią przez to choćby najmłodsi, których powinniśmy uwzględniać na pierwszym miejscu, jeśli chodzi o zapewnienie bezpieczeństwa. Dlatego też misję ochrony dzieci i młodzieży w dobie zagrożeń w sieci postrzegam jako fundamentalną dla mnie na czas najbliższych dwóch lat.

Jak ocenia Pan współpracę między UODO a Ministerstwem Edukacji Narodowej, skoro działalność edukacyjna Urzędu jest tak istotna?

Uważam, że obecny kierunek działań MEN odpowiada na realne potrzeby młodych ludzi i stanowi jeden z kluczowych elementów systemowej ochrony ich zdrowia w sensie psychicznym, ich prywatności i praw podstawowych. Dlatego też w apelu, który wystosowałem do dyrektorów szkół, nauczycieli i rodziców, wyraziłem poparcie dla wprowadzenia do szkół przedmiotów edukacja zdrowotna i obywatelska, które promują wiedzę o odpowiedzialnym funkcjonowaniu najmłodszych w sferze cyfrowej. Zresztą w tej sprawie apelowałem także do Pana Prezydenta. Edukacja cyfrowa od najmłodszych lat, pojmowana jako część wiedzy o świecie i własnych prawach, to absolutnie warunek kluczowy do tego, abyśmy w przyszłości żyli w świecie o wiele bezpieczniejszym, ponieważ będziemy mieli do tego znacznie więcej narzędzi, nie będziemy się bać. Przez cały czas organ nadzorczy znakomicie i efektywnie współpracuje też z MEN, jeśli chodzi np. o tak palące problemy, jak monitoring wizyjny w placówkach szkolnych – przekazujemy nasze uwagi do projektów zmian w tym kierunku – czy dostępność danych zdrowotnych uczniów, w tym momencie zbyt szeroko udostępnianych w przestrzeni szkolnej.

1 ROZMOWA Z EKSPERTEM

Jak postrzega Pan swój Urząd w perspektywie dwóch najbliższych lat i możliwie ciągle trwającej wojny za wschodnią granicą, w związku z tym w perspektywie wciąż nasilających się ataków na sferę cyberbezpieczeństwa? Czy ma Pan w tej kwestii jakiś strategiczny pomysł? Mówimy również o wykradaniu podstawowych danych obywateli, takich jak PESEL.

Najbliższe dwa lata to okres zasadniczej zmiany roli Prezesa UODO – od organu koncentrującego się na stosowaniu RODO ku instytucji osadzającej i stabilizującej nową architekturę prawa cyfrowego UE. Wdrożenie AI Act, DGA, EHDS czy DSA wymaga nie tylko transpozycji kompetencji, lecz także spójnego wpisania tych aktów w krajowy model instytucjonalny oraz ścisłej koordynacji z innymi regulatorami rynku cyfrowego.

Priorytetem jest i będzie przeciwdziałanie fragmentaryzacji wdrożeń, nakładaniu się kompetencji i rozbieżnym interpretacjom, które mogłyby osłabić ochronę praw jednostki i sprawne funkcjonowanie biznesu oraz państwa. Dynamiczny rozwój AI, big data, biometrii czy Internetu Rzeczy powoduje, że formalna zgodność z przepisami przestaje wystarczać. Najważniejsze będzie podejmowanie działań (we współpracy z właściwymi resortami i ekspertami) prowadzących do rozumienia technologii jako warunku skutecznej ochrony praw podstawowych oraz przesunięcie ciężaru ochrony na etap projektowania systemów.

Z kolei coraz częstsze wykorzystywanie systemów AI wymaga jednolitych, horyzontalnych standardów stosowania prawa, zwłaszcza dla mniejszych podmiotów. Priorytetem tutaj będzie zapewnienie przewidywalności regulacyjnej, uzyskiwanej poprzez wspólne kryteria oceny ryzyka, jakości danych, przejrzystości algorytmów i odpowiedzialności, tak aby rozwój AI nie prowadził do fragmentaryzacji ochrony praw. W tym celu już teraz bierzemy aktywny udział w europejskich pracach w tym zakresie, ale także prowadzimy we współpracy z ekspertami działania na poziomie krajowym.

Cyberbezpieczeństwo musi być traktowane nie jako problem czysto techniczny, lecz jako integralny element ochrony praw i wolności osób. Doświadczenia z ransomware i naruszeniami w sektorze publicznym pokazują, że analiza ryzyka musi uwzględniać perspektywę osób, których dane dotyczą, a nie wyłącznie interesy organizacji. Kluczowe znaczenie ma regularne testowanie środków bezpieczeństwa i ocena ich skuteczności. Dane osobowe stały się zasobem wykorzystywanym w cyberprzestępczości i działaniach hybrydowych – stąd m.in. tak liczne „wycieki" danych. Moim priorytetem jest dlatego konsekwentne wpisywanie ochrony danych w szerszą koncepcję bezpieczeństwa państwa i odporności instytucji demokratycznych.

1 ROZMOWA Z EKSPERTEM

Wreszcie, obok reform systemowych będę kłaść silny nacisk na działania edukacyjne w zakresie ochrony danych osobowych i przygotowywania wytycznych oraz poradników dla administratorów danych. Kluczową rolę odgrywają tu również inspektorzy ochrony danych, których pozycja powinna być wzmacniana przy jednoczesnym jasnym podkreśleniu, że odpowiedzialność za zgodność z prawem spoczywa na administratorach.

Dziękuję bardzo za rozmowę.

JAK PRZEPROWADZAĆ ANALIZĘ RYZYKA ZGODNIE Z ZASADĄ ROZLICZALNOŚCI?

RODO opiera się na zasadzie rozliczalności, zgodnie z którą administratorzy oraz podmioty przetwarzające są zobowiązani nie tylko do przestrzegania przepisów dotyczących ochrony danych osobowych, lecz także do wykazania, że realizują swoje obowiązki świadomie i adekwatnie wobec ryzyka naruszenia praw lub wolności osób, których dane przetwarzają. Analiza ryzyka odgrywa w tym mechanizmie kluczową rolę, stanowiąc podstawę do podejmowania decyzji dotyczących sposobu przetwarzania danych oraz doboru technicznych i organizacyjnych środków ich ochrony. Poniżej przedstawiamy listę 18 dobrych praktyk, które mogą pomóc w przeprowadzaniu analizy ryzyka w sposób zgodny z zasadą rozliczalności.

1 Stawiaj prawa i wolności człowieka w centrum analizy ryzyka

Ryzyko w rozumieniu RODO zawsze powinno być analizowane z perspektywy osoby, której dane dotyczą, a nie organizacji, która te dane przetwarza (np. przez pryzmat ryzyka finansowego, wizerunkowego lub operacyjnego). Ma to szczególne znaczenie przy określaniu wagi skutków urzeczywistnienia się określonych zagrożeń.

Pomimo że perspektywa organizacji pozostaje istotna na etapie identyfikacji źródeł zagrożeń i podatności mogących prowadzić do naruszenia praw lub wolności jednostki, warto zachować właściwe rozróżnienie pomiędzy źródłem ryzyka a jego skutkami – które zawsze powinny być oceniane z punktu widzenia osób, których dane dotyczą.

Takie podejście jest niezbędne zarówno dla prawidłowego zarządzania ryzykiem, jak i dla wykazania, że analiza ryzyka została przeprowadzona zgodnie z celami RODO. Przykładem błędnej praktyki byłoby uznanie ryzyka za niskie wyłącznie dlatego, że potencjalne negatywne konsekwencje dotyczą niewielkiej liczby osób.

2 NARUSZENIA I KONTROLE

2 Odwołuj się do wymogów i wskazówek zawartych w RODO

Analiza ryzyka nie powinna być prowadzona w oderwaniu od przepisów RODO, lecz osadzona w kryteriach i wskazówkach w nim określonych (np. w art. 24 ust. 1, art. 25 ust. 1, art. 32 ust. 1, art. 35 ust. 7 oraz motywach 74-76 i 83-84). W szczególności należy uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz prawdopodobieństwo i wagę potencjalnych konsekwencji dla praw lub wolności osób fizycznych.

W praktyce oznacza to konieczność odnoszenia analizy ryzyka do rzeczywistego kontekstu danego procesu, w tym do celów, w jakich dane są wykorzystywane, a nie wyłącznie do technicznego sposobu ich przetwarzania. Ten sam system lub narzędzie (np. rozwiązania oparte na sztucznej inteligencji) może się wiązać z różnym poziomem ryzyka w zależności od celu przetwarzania – innym, gdy służy do oceny kandydata do pracy, a innym, gdy wykorzystywany jest np. do porządkowania treści. Uwzględnienie tych kryteriów umożliwia wykazanie, że analiza została przeprowadzona w sposób świadomy, spójny i zgodny z zasadą rozliczalności.

3 Opieraj analizę ryzyka na faktach i dowodach, a nie na intuicji

Ocena ryzyka powinna wynikać z możliwie obiektywnych przesłanek. Każdą wartość – zarówno liczbową, jak i opisową – przypisywaną do poszczególnych parametrów oceny (np. prawdopodobieństwa wystąpienia zagrożeń lub wagi ich skutków) warto uprzednio zdefiniować i oprzeć na konkretnych przesłankach faktycznych lub technicznych, a nie wyłącznie na arbitralnych założeniach. W tym kontekście przydatne mogą się okazać uznane standardy, normy i metodyki (np. ISO).

Taka praktyka sprzyja wykazywaniu, że analiza ryzyka została przeprowadzona w sposób rzetelny i nie ma charakteru abstrakcyjnego ani wyłącznie deklaratywnego oraz pomaga porównywać wyniki analiz przeprowadzanych w różnych okresach.

4 Dokumentuj źródła ocen i przyjętych założeń

Podstawy, na których oparto analizę ryzyka, powinny być możliwe do zidentyfikowania i obejmować uznane normy techniczne, metodyki, wytyczne, doświadczenia organizacyjne lub inne materiały odnoszące się do znanych zagrożeń i dobrych praktyk. Ich dokumentowanie ma istotne znaczenie zwłaszcza w przypadku przyjmowania określonych założeń, uproszczeń lub skal ocen, które mają wpływ na wyniki analizy.

Ma to na celu umożliwienie odtworzenia toku wnioskowania administratora lub podmiotu przetwarzającego oraz wykazanie, że ryzyko zostało oszacowane na podstawie obiektywnych przesłanek.

5 Traktuj analizę ryzyka jako proces ciągły, a nie jednorazowe działanie

Analiza ryzyka nie ma charakteru jednorazowego „ćwiczenia", lecz powinna być postrzegana jako proces towarzyszący przetwarzaniu danych osobowych. Wszelkie zmiany dotyczące przetwarzania mogą wpływać na charakter i poziom ryzyka, a tym samym powodować konieczność weryfikacji przyjętych uprzednio założeń. Sprzyja to utrzymaniu aktualności analizy oraz wykazywaniu, że administrator lub podmiot przetwarzający na bieżąco zarządza ryzykiem związanym z przetwarzaniem.

W związku z tym istotne jest, aby w organizacji istniały mechanizmy pozwalające osobom odpowiedzialnym za procesy biznesowe na identyfikację sytuacji, w których konieczne jest dokonanie ponownej analizy ryzyka. Może to dotyczyć w szczególności wprowadzenia nowych operacji na danych, modyfikacji zakresu przetwarzanych danych, pojawienia się nowych typów zagrożeń, włączenia do procesu nowych zasobów, zmiany osób odpowiedzialnych za przetwarzanie lub zmiany zasad dostępu i ujawniania danych. Mechanizmy te stanowią element zarządzania zmianą w organizacji i pozwalają powiązać analizę ryzyka z rzeczywistymi zmianami zachodzącymi w procesach przetwarzania.

6 Wersjonuj analizy ryzyka i dokumentuj istotne zmiany w ich treści

Dokumentowanie zmian w analizie ryzyka ma szczególne znaczenie w sytuacjach, w których modyfikowany jest sposób przetwarzania danych, stosowane środki ich ochrony lub inne istotne okoliczności towarzyszące procesom przetwarzania.

Wersjonowanie analiz ryzyka pozwala ustalić, jaka ocena obowiązywała w danym momencie oraz na jakiej podstawie były podejmowane określone decyzje. Ma to znaczenie dla wykazania ciągłości i spójności działań podejmowanych przez administratora lub podmiot przetwarzający, zwłaszcza w kontekście ich późniejszej weryfikacji.

2 NARUSZENIA I KONTROLE

7 Opisuj przetwarzanie w sposób kompletny, konkretny i zgodny z realiami

Analiza ryzyka powinna wiernie odzwierciedlać rzeczywisty sposób przetwarzania danych osobowych, a nie jego modelowy lub wyłącznie deklaratywny obraz. Należy więc opierać ją na faktach, uwzględniając wszelkie istotne elementy analizowanego procesu, w tym te, które mogą wpływać niekorzystnie (z perspektywy praw lub wolności osób fizycznych) na ostateczny poziom ryzyka.

W praktyce obraz przetwarzania może różnić się nie tylko ze względu na charakter przetwarzanych danych, ale również ze względu na podmioty, których dane dotyczą. W szczególności odmiennego podejścia wymaga przetwarzanie danych osobowych dzieci.

Nie należy także ograniczać analizy ryzyka do pojedynczego zasobu (np. systemu IT), z pominięciem szerszego kontekstu procesu przetwarzania, który ten zasób wspiera. Nie wyklucza to dokonywania analizy „dla zasobu" – szczególnie w zakresie identyfikacji zagrożeń – jednak bez zrozumienia procesów, które dany zasób wspiera, nie jest możliwe prawidłowe oszacowanie m.in. wagi potencjalnych negatywnych konsekwencji dla praw lub wolności osób fizycznych.

Tylko takie podejście pozwala zapewnić rzetelność analizy ryzyka oraz realną ochronę interesów osób, których dane dotyczą.

8 Analizuj cały cykl życia danych – od pozyskania do usunięcia

Analiza ryzyka powinna obejmować wszystkie etapy przetwarzania danych osobowych – od ich pozyskania, przez przechowywanie, wykorzystywanie i udostępnianie, aż po usunięcie lub anonimizację.

Ryzyka mogą się pojawiać na różnych etapach cyklu życia danych, również na etapie końcowym, np. w związku z błędami w anonimizacji. Pomijanie poszczególnych etapów lub traktowanie całego procesu jednolicie może prowadzić do nieprawidłowych wniosków, ponieważ poziom ryzyka oraz adekwatne środki ochrony danych mogą się istotnie różnić w zależności od etapu przetwarzania.

W praktyce istotne jest także zrozumienie, których zasobów dotyczą poszczególne operacje na danych oraz w jaki sposób są one realizowane. Identyfikacja operacji na danych stanowi punkt wyjścia do rozpoznania dalszych niuansów dotyczących przetwarzania, takich jak sposób realizacji operacji (np. lokalnie na urządzeniu użytkownika lub w ramach usługi chmurowej, w trybie ciągłym lub incydentalnym) czy częstotliwość ich wykonywania. Czynniki te mogą mieć bezpośredni wpływ na prawdopodobieństwo materializacji zagrożeń i powinny być uwzględniane w analizie ryzyka.

2 NARUSZENIA I KONTROLE

9 Uwzględniaj wszystkie zasoby wspierające proces, którego dotyczy analiza ryzyka

Analiza ryzyka powinna uwzględniać wszystkie zasoby zaangażowane w proces przetwarzania danych osobowych. Przede wszystkim dotyczy to osób uczestniczących w przetwarzaniu, stosowanych rozwiązań technicznych oraz procesów organizacyjnych, które mogą wpływać na sposób przetwarzania danych i poziom ryzyka. Pozwala to lepiej identyfikować rzeczywiste źródła zagrożeń oraz wykazywać, że analiza obejmuje pełny kontekst przetwarzania, a nie jedynie jego wybrane aspekty.

10 Nie ograniczaj analizy ryzyka do obszaru bezpieczeństwa danych (poufności, integralności i dostępności)

Analiza ryzyka nie powinna koncentrować się wyłącznie na zagrożeniach związanych z bezpieczeństwem danych, takich jak nieuprawniony dostęp, utrata czy zniszczenie.

Mimo że bezpieczeństwo informacji stanowi fundament ochrony prywatności, ryzyko dla praw lub wolności osób fizycznych może wynikać również ze sposobu przetwarzania danych, zwłaszcza w przypadkach profilowania, automatycznego podejmowania decyzji lub braku przejrzystości. Aspekty te mogą stanowić samodzielne źródła ryzyka i powinny być uwzględniane w analizie niezależnie od poziomu zabezpieczeń technicznych.

W szczególności w kontekście wykorzystywania systemów opartych na sztucznej inteligencji istotne jest zwrócenie uwagi na kwestie przejrzystości przetwarzania, poprawności i jakości danych oraz potencjalne konsekwencje podejmowania decyzji w sposób zautomatyzowany, w tym na bazie profilowania. Mechanizmy te mogą w znaczący sposób wpływać na sytuację osób, których dane dotyczą, nawet przy braku naruszeń ochrony danych osobowych w rozumieniu RODO.

11 Zwróć uwagę na mniej oczywiste, pośrednie i długofalowe skutki przetwarzania dla osób fizycznych

Analizując ryzyko, należy zwrócić uwagę nie tylko na bezpośrednie i natychmiastowe skutki przetwarzania danych, ale również na jego konsekwencje pośrednie lub ujawniające się w dłuższym horyzoncie czasowym, w zakresie, w jakim mogą być one racjonalnie przewidziane. Uwzględnienie takich aspektów pozwala uniknąć zawężenia analizy wyłącznie do najbardziej oczywistych scenariuszy i lepiej odzwierciedlić rzeczywisty wpływ przetwarzania na sytuację osób, których dane dotyczą.

2 NARUSZENIA I KONTROLE

12 Uwzględniaj „stan wiedzy technicznej” oraz „koszt wdrażania” przy doborze środków ochrony danych

Przy doborze technicznych i organizacyjnych środków ochrony danych należy uwzględniać aktualny stan wiedzy technicznej oraz koszt ich wdrażania jako kryteriów pozwalających dopasować środki do specyfiki administratora lub podmiotu przetwarzającego oraz kontekstu przetwarzania. Kryteria te nie mogą jednak stanowić uzasadnienia dla kontynuowania przetwarzania danych pomimo istnienia wysokiego ryzyka naruszenia praw lub wolności osób fizycznych. Ich zastosowanie powinno pozostawać w bezpośrednim związku z wynikami analizy ryzyka i umożliwiać wykazanie zasadności przyjętych rozwiązań.

Stan wiedzy technicznej powinien być przy tym na bieżąco monitorowany, tak aby stosowane środki odpowiadały aktualnym zagrożeniom. W tym kontekście pomocne mogą być materiały publikowane przez wyspecjalizowane instytucje, takie jak ENISA, które w ramach cyklicznych raportów (np. „ENISA Threat Landscape”) prezentują aktualne zagrożenia oraz przykładowe środki ochrony zgodne z obecnym stanem wiedzy technicznej.

13 Monitoruj wdrażanie zaplanowanych środków ochrony danych

Dobór środków ochrony danych powinien prowadzić do ich faktycznego wdrożenia i stosowania, a nie jedynie do formalnego wskazania ich w dokumentacji. Planowanie i monitorowanie wdrażania zaplanowanych środków pozwala potwierdzić, że decyzje podjęte w wyniku analizy ryzyka zostały rzeczywiście zrealizowane oraz że pozostają aktualne w świetle zmieniających się okoliczności towarzyszących przetwarzaniu. Ma to znaczenie zarówno dla skutecznej ochrony danych osobowych, jak i dla wykazania, że administrator lub podmiot przetwarzający sprawuje rzeczywistą kontrolę nad realizacją przyjętych rozwiązań.

Dobrą praktyką jest także określenie ról i odpowiedzialności w zakresie faktycznego wdrażania zabezpieczeń, co ułatwia przypisanie działań do konkretnych osób lub komórek organizacyjnych oraz wspiera zapewnienie zgodności z zasadą rozliczalności.

14 Dokumentuj regularne testowanie skuteczności stosowanych zabezpieczeń

Wdrożenie określonych zabezpieczeń nie jest wystarczające, jeżeli nie towarzyszy mu mierzenie ich rzeczywistej skuteczności. Regularne testowanie środków bezpieczeństwa powinno umożliwiać ocenę, czy założenia przyjęte w ramach analizy ryzyka pozostają aktualne oraz czy stosowane rozwiązania spełniają swoje funkcje.

Dokumentowanie wyników takich testów pozwala wykazać, że administrator lub podmiot przetwarzający w sposób ciągły realizuje swoje obowiązki, monitorując bezpieczeństwo danych i podejmując adekwatne działania w celu ich bieżącej ochrony.

15 Jasno określ role i odpowiedzialność w procesie analizy ryzyka

Role i odpowiedzialności związane z zarządzaniem ryzykiem powinny być jasno określone i realizowane w praktyce, a nie ograniczać się do ogólnych zapisów w dokumentacji. W szczególności istotne jest wskazanie, kto odpowiada za przeprowadzenie analizy ryzyka, kto podejmuje decyzje dotyczące doboru adekwatnych środków ochrony danych oraz kto ostatecznie faktycznie wdraża je w organizacji. Przypisanie ról ma kluczowe znaczenie dla rozliczalności, ponieważ umożliwia ustalenie, na jakim etapie, przez kogo oraz na jakiej podstawie zostały podjęte określone decyzje.

16 Zapewnij realny udział inspektora ochrony danych w procesie oceny ryzyka

Udział inspektora ochrony danych w procesie analizy ryzyka powinien mieć charakter rzeczywisty i być możliwy do wykazania. Inspektor ochrony danych powinien być włączany w proces analizy w zakresie odpowiadającym jego zadaniom i kompetencjom wynikającym z RODO, w szczególności w celu formułowania zaleceń, opiniowania przyjętych rozwiązań oraz monitorowania zgodności przetwarzania z przepisami o ochronie danych osobowych.

Jednocześnie odpowiedzialność za przeprowadzanie analizy ryzyka oraz za podejmowanie decyzji w jej następstwie pozostaje po stronie administratora lub podmiotu przetwarzającego. Zakres udziału inspektora ochrony danych, a także sposób uwzględnienia jego zaleceń lub przyczyny ich nieuwzględnienia powinny znajdować odzwierciedlenie w dokumentacji oraz w praktyce organizacyjnej.

17 Traktuj zatwierdzenie analizy ryzyka jako świadomą i udokumentowaną decyzję zarządczą

Zarządzanie ryzykiem w naturalny sposób prowadzi do sytuacji, w której pomimo zastosowania odpowiednich środków ochrony danych pewien poziom ryzyka dla praw lub wolności osób fizycznych nadal pozostaje. Decyzje dotyczące dalszego przetwarzania danych w takich warunkach powinny mieć charakter świadomy oraz być jednoznacznie przypisane do konkretnej osoby lub organu w ramach organizacji.

2 NARUSZENIA I KONTROLE

Niezależnie od przyjętych rozwiązań ostateczna odpowiedzialność za analizę ryzyka oraz jej konsekwencje zawsze spoczywa na administratorze lub podmiocie przetwarzającym.

18 Dokumentuj i uzasadniaj decyzje o odstąpieniu od dalszych działań związanych z zarządzaniem ryzykiem

Zasada rozliczalności obejmuje nie tylko działania podjęte w następstwie analizy ryzyka, lecz również decyzje o odstąpieniu od określonych działań. W szczególności dotyczy to rezygnacji z przeprowadzenia oceny skutków dla ochrony danych (DPIA), nieuwzględnienia rekomendacji inspektora ochrony danych lub niewdrożenia dodatkowych środków ochrony danych. Decyzje tego rodzaju powinny być udokumentowane i oparte na wynikach analizy, w sposób umożliwiający wykazanie, że zostały podjęte świadomie oraz z uwzględnieniem ochrony praw i wolności osób fizycznych.

Podsumowanie

Analiza ryzyka w rozumieniu RODO nie jest celem samym w sobie ani jedynie formalnym obowiązkiem dokumentacyjnym. Stanowi ona proces, w ramach którego administrator lub podmiot przetwarzający podejmuje świadome decyzje dotyczące przetwarzania danych osobowych. Z perspektywy zasady rozliczalności kluczowe znaczenie ma nie tylko samo przeprowadzenie analizy, lecz również możliwość zapewnienia transparentności w zakresie źródeł przyjętych założeń, dokonanych ocen oraz podjętych decyzji (w tym decyzji o zaniechaniu określonych działań). Powyższe wskazówki mogą stanowić punkt odniesienia przy budowaniu rzetelnego, spójnego i możliwego do wykazania podejścia do realizacji obowiązków wynikających z przepisów o ochronie danych osobowych.

PRZEDSZKOLE PODCZAS REKRUTACJI NIE MA PRAWA POZYSKIWAĆ NUMERÓW PESEL RODZICÓW

Administrator nie może odmawiać zrealizowania przysługującego każdemu z nas prawa do usunięcia danych osobowych, jeśli to żądanie ma uzasadnienie w przepisach prawa. Dane musi usunąć również z kopii zapasowych systemów informatycznych. Dlatego ważne jest, aby korzystać z takich systemów do tworzenia kopii zapasowych, by móc wywiązać się z tego obowiązku.

Przepisy ustawy z 14 grudnia 2016 r. Prawo oświatowe nie dają podstaw prawnych do pozyskiwania numerów PESEL rodziców dzieci na etapie rekrutacji do publicznych przedszkoli czy szkół. Jej artykuły 150 i 151 wprost wskazują, jakie dane osobowe ma zawierać wniosek o przyjęcie do takiej placówki. Nie ma wśród nich numeru PESEL rodziców (w odróżnieniu od numeru PESEL kandydata, czyli dziecka).

Jednocześnie, skoro zakres pozyskiwanych danych jest określony w powołanych przepisach, to wynikające z art. 152 ustawy uprawnienie organu prowadzącego publiczne przedszkola i inne placówki oświatowe do określenia wzoru wniosku lub zgłoszenia, o których mowa w art. 150 i 151, nie może wykraczać poza to, co regulują te przepisy. Innymi słowy, organ prowadzący daną placówkę nie może zmieniać zakresu wymienionych w nich danych oraz celu, dla którego są one pozyskiwane.

Takie działanie naruszałoby nie tylko powołane przepisy, ale także zasady, o których mowa w art. 5 RODO (m.in. legalizmu, proporcjonalności i minimalizacji).

RODO stanowi bowiem, że:

• przetwarzanie (w tym pozyskiwanie) danych osobowych musi się odbywać zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a),

• dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (art. 5 ust. 1 lit. b) oraz

• być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (art. 5 ust. 1 lit. c).

Ponadto ustawodawca w sytuacji, gdy uznaje konieczność podania numeru PESEL, ustanawia przepisy, które wprost nakładają obowiązek jego podania. Z takim przypadkiem mamy do czynienia w art. 27 § 1 pkt 2 ustawy z 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji, który stanowi, że tytuł wykonawczy ma zawierać numer PESEL.

Zatem dopiero niewywiązanie się z obowiązku uiszczenia należności za wyżywienie dziecka w placówce rozpoczęłoby bieg nowej procedury, prowadzonej zgodnie z przepisami o postępowaniu egzekucyjnym w administracji. I to na tym etapie legalne byłoby przetwarzanie (w tym pozyskiwanie) numeru PESEL, który – zgodnie z art. 27 § 1 pkt 2 ustawy o postępowaniu egzekucyjnym w administracji – musi być zamieszczony w wystawionym tytule wykonawczym. Przepis ten jest zatem przesłanką legalizującą proces przetwarzania danych osobowych w odniesieniu do danych zawartych w wystawionym tytule wykonawczym.

Jednocześnie w przypadku problemów z pozyskaniem numeru PESEL bezpośrednio od rodziców zalegających z opłatami warto zwrócić uwagę na przepisy ustawy z 24 września 2010 r. o ewidencji ludności, które wskazują, jakim organom, na jakich zasadach oraz w jakim celu można udostępnić dane z rejestru PESEL (art. 46). Stanowią one m.in., 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 (art. 46 ust. 1 pkt 1), a także państwowym i samorządowym jednostkom organizacyjnym oraz innym podmiotom – w zakresie niezbędnym do realizacji zadań publicznych określonych w odrębnych przepisach (art. 46 ust. 1 pkt 5).

Pamiętać bowiem należy, że numer PESEL to krajowy numer identyfikacyjny, który powinien podlegać szczególnej ochronie (zgodnie z art. 87 RODO). Pozyskiwanie takich danych na zapas, na wszelki wypadek, np. na potrzeby ewentualnego postępowania egzekucyjnego, które jest odrębnym procesem, jeszcze niezaistniałym w momencie prowadzenia rekrutacji do przedszkola, jest działaniem nadmiarowym, naruszającym zasadę legalizmu, zasadę ograniczenia celu oraz zasadę minimalizacji danych.

„LISTA ROBINSONA" – NARZĘDZIE Z KODEKSU POSTĘPOWANIA DLA PRYWATNYCH AGENCJI BADANIA OPINII I RYNKU

„Kodeks postępowania dotyczący przetwarzania danych osobowych przez prywatne agencje badawcze" przewiduje, że podmioty, które do niego przystąpiły, by skutecznie realizować żądania osób, które nie życzą sobie kontaktów telefonicznych od ankieterów, tworzą tzw. Listy Robinsona.

Jak informowaliśmy na naszej stronie internetowej, Prezes UODO 24 listopada 2025 r. zatwierdził kodeks postępowania dotyczący przetwarzania danych osobowych przez prywatne agencje badania opinii i rynku oraz udzielił akredytacji podmiotowi monitorującemu jego stosowanie. W materiale opublikowanym w związku z uroczystym wręczeniem dokumentów poświadczających te fakty omówiliśmy najważniejsze kwestie odnoszące się do nowego kodeksu. Opisaliśmy:

- co reguluje,
- kto może do niego przystąpić,
- kto będzie monitorował jego przestrzeganie,
- jakie korzyści wynikają z jego stosowania.

Tym razem postanowiliśmy przedstawić jedno z przewidzianych w nim rozwiązań – tworzenie tzw. Listy Robinsona. Jej nazwa pochodzi od postaci Robinsona Crusoe z powieści Daniela Defoe. Ten żeglarz, który rozbił się na bezludnej wyspie i został odcięty od świata, stał się symbolem izolacji. Stąd skojarzenie z nim osób, które nie chcą, by się z nimi kontaktowano.

Dla uszanowania woli badanych

W omawianym kodeksie tworzenie tzw. Listy Robinsona odnosi się do badań CATI. Są one przeprowadzane przez telefon ze wspomaganiem komputerowym (tzn. pytania kwestionariusza wyświetlają się na monitorze, a zadaniem ankietera jest odczytanie ich przez telefon respondentowi i zaznaczenie jego odpowiedzi). W czasie ich trwania zdarza się, że osoba, która odbiera połączenie telefoniczne, prosi o niewykonywanie połączeń na jej numer telefonu i/lub usunięcie tego numeru z baz/-y danych służących do realizacji badania

W przypadku całkowitego usunięcia numeru telefonu w przyszłości mogłoby dojść do sytuacji, w której po automatycznym wygenerowaniu numeru telefonu do kolejnego badania (metoda random digit dialing) ponownie wylosowany zostanie numer telefonu osoby, która nie życzyła sobie jakiegokolwiek kontaktu. Wówczas respondent mógłby być przekonany, że jego wola nie została uszanowana. Stąd wprowadzenie rozwiązania, jakim jest „Lista Robinsona".

Dzięki niej przy każdorazowym automatycznym generowaniu nowej próby numerów telefonu do badania, przed jego rozpoczęciem, weryfikowane jest, czy dany numer telefonu nie widnieje na liście. Jeżeli tak jest, numer ten jest usuwany z konkretnej próby do badania, aby nie wykonywać połączenia do osoby, która sobie tego nie życzy.

Zakres danych na liście

Na „Liście Robinsona" zamieszczane są dane takie, jak:

• numer telefonu osoby, która żąda trwałego zaprzestania inicjowania wywiadów telefonicznych,

• data wpisania na listę,

• informacja o sposobie pozyskania numeru telefonu (random digit dialing lub baza danych pochodząca z rynku).

Administrator i podstawa prawna prowadzenia

Jednocześnie kodeks wprost wskazuje, że administratorem danych zgromadzonych na „Liście Robinsona" jest agencja badawcza, która ją prowadzi.

Natomiast podstawą przetwarzania zawartych na niej danych osobowych może być art. 6 ust. 1 lit. f) RODO, tj. prawnie uzasadniony interes agencji. W tym przypadku jest nim zapewnienie profesjonalnej obsługi żądań respondentów i podnoszenie ich zaufania do branży badawczej (ze względu na specyfikę tego typu badań pozyskanie od respondentów takiej zgody na wpisanie na listę, która spełniałaby wymagania z art. 4 pkt 11 i art. 7 RODO, może być utrudnione lub niemożliwe).

Omawiany kodeks stanowi, że każda agencja badawcza zobowiązana jest do przeprowadzenia i udokumentowania analizy testu uzasadnionego interesu, umożliwiającej przetwarzanie danych na podstawie art. 6 ust. 1 lit. f) RODO, zgodnie z zasadami wynikającymi z Wytycznych EROD 1/2024 dotyczących przetwarzania danych na podstawie art. 6 ust. 1 lit. f) RODO.

Procedura umieszczania

Kodeks – jako narzędzie dające praktyczne wskazówki, jak postępować w konkretnych sytuacjach – opisuje, jakie kolejne czynności powinny być podejmowane przy dodawaniu numeru telefonu do „Listy Robinsona". Stanowi zatem, że:

„1. Ankieter CATI w trakcie rozmowy obowiązany jest dopytać respondenta, czy chce on brać udział wyłącznie w określonym badaniu, czy w jakimkolwiek innym badaniu prowadzonym przez agencję w przyszłości;

2. W przypadku, gdy osoba doprecyzuje, że nie chce brać udziału w jakichkolwiek badaniach prowadzonych w przyszłości, ankieter przedstawia respondentowi obowiązek informacyjny odnoszący się do przetwarzania danych na „Liście Robinsona" lub w przypadku braku chęci respondenta do dalszej rozmowy poinformuje co najmniej o dostępności obowiązku informacyjnego na stronie internetowej agencji, w tym możliwości złożenia sprzeciwu i jego konsekwencjach (czyli możliwości dalszych kontaktów telefonicznych z uwagi na stosowanie metody random digit dialing). W przypadku, gdy respondent przerwie połączenie telefoniczne, agencja badawcza wpisuje respondenta na »Listę Robinsona« jedynie, wtedy, gdy respondentowi zostały przekazane powyższe informacje i agencja jest w stanie to wykazać zgodnie z zasadą rozliczalności oraz Wytycznymi EROD 1/2024 dotyczącymi przetwarzania danych na podstawie art. 6 ust. 1 lit. f) RODO.

Każda agencja badawcza przetwarzająca dane respondentów w celu prowadzenia »Listy Robinsona« zobowiązana jest zamieścić na swojej stronie internetowej obowiązek informacyjny zatytułowany „Obowiązek informacyjny dla badań telefonicznych – Lista Robinsona". Obowiązek informacyjny powinien zawierać wszystkie elementy wskazane w art. 13 lub art. 14 RODO, w tym w szczególności wskazanie odbiorów danych (np. firm dostarczających systemy umożliwiające losowe generowanie numerów telefonicznych). Okres przetwarzania danych osobowych Respondenta na »Liście Robinsona« nie powinien przekraczać dwóch lat od daty rozpoczęcia przetwarzania danych na »Liście Robinsona«. W powyższym okresie retencji wyczerpuje się przedstawiony cel przetwarzania danych, biorąc pod uwagę praktykę operatorów komórkowych proponujących standardowe umowy o świadczenie usług telekomunikacyjnych na okres dwóch lat;

3. Następnie Ankieter CATI odnotowuje wolę respondenta poprzez zaznaczenie w systemie teleinformatycznym odpowiedniego statusu »Lista Robinsona«;

4. Ankieter CATI w trybie natychmiastowym informuje o zaistniałej sytuacji kierownika studia CATI bądź supervisora CATI;

5. Supervisor CATI bądź kierownik studia CATI niezwłocznie usuwa numer telefonu z bazy służącej do realizacji danego badania, a następnie dodaje go do »Listy Robinsona«;

6. Po każdym zakończonym badaniu następuje dokładna weryfikacja, czy wszystkie kontakty ze statusem »Lista Robinsona« zostały na niej umieszczone".

Dostęp do listy

Kodeks przewiduje, że dostęp do „Listy Robinsona" powinien zostać nadany wyłącznie:

• osobom, które pracują w działach badań telefonicznych agencji badawczej,

• IOD (który, zgodnie z art. 38 ust. 2 RODO jest uprawniony do dostępu do wszystkich danych osobowych przetwarzanych przez agencję),

• osobie odpowiedzialnej za obsługę systemu automatycznego generowania numerów telefonicznych.

Od wskazanych wyżej osób należy odebrać zobowiązanie do zachowania poufności.

Szczegółowe określenie środków technicznych i organizacyjnych, które zapewnią bezpieczeństwo danych osobowych na „Liście Robinsona", powinno być odnotowane przez agencję badawczą w udokumentowanej analizie testu uzasadnionego interesu, zgodnie z Wytycznymi EROD 1/2024 dotyczącymi przetwarzania danych na podstawie art. 6 ust. 1 lit. f) RODO

Żądanie usunięcia danych

Warto zaznaczyć, że kodeks określa też sposób postępowania w przypadku złożenia przez osobę, której dane dotyczą, wniosku o usunięcie danych osobowych zgodnego z art. 17 ust. 1 RODO.

Jeśli wniosek dotyczy danych przetwarzanych w ramach badania CATI lub dotyczy usunięcia wszystkich danych wnioskodawcy przetwarzanych przez agencję, weryfikuje ona, czy dane osobowe wnioskodawcy znajdują się również na prowadzonej przez nią „Liście Robinsona". Jeżeli tak, zwraca się do wnioskodawcy o sprecyzowanie, czy jego wolą jest także usunięcie danych osobowych z „Listy Robinsona". Wskazuje przy tym termin na udzielenie odpowiedzi. Nie może być on krótszy niż siedem dni kalendarzowych.

W przypadku braku odpowiedzi w wyznaczonym terminie, agencja usuwa dane osobowe również z „Listy Robinsona".

Jednocześnie w ramach dobrej praktyki (w związku z potrzebą udokumentowania realizacji praw osób, których dane dotyczą) agencja powinna odnotować fakt realizacji wniosku o usunięcie danych osobowych w rejestrze zgłoszonych praw osób, których dane dotyczą, a także zachować informacje co do wnioskodawcy oraz sposobie i terminie realizacji wniosku. Agencja powinna określić termin przechowywania ww. informacji i poinformować o nim osobę, której dane dotyczą.

Reasumując, „Lista Robinsona" prowadzona zgodnie z regulacjami „Kodeksu postępowania dotyczącego przetwarzania danych osobowych przez prywatne agencje badawcze" to narzędzie umożliwiające skuteczne blokowanie inicjowania niechcianych rozmów telefonicznych. Umieszczenie numeru telefonu na „Liście Robinsona" daje pewność, że w przyszłości – nawet w przypadku ponownego wygenerowania numeru przez system lub jego obecności w nowo zakupionej lub otrzymanej bazie – nie zostanie zainicjowane niechciane połączenie. Odpowiednia funkcjonalność systemu teleinformatycznego umożliwia zablokowanie wykonania połączenia z numerami telefonów, które są wpisane na „Listę Robinsona". Jest to równoznaczne z uszanowaniem woli respondentów.

JAK PROWADZIĆ BADANIA SPOŁECZNE Z UDZIAŁEM DZIECI

Opracowanie standardów prowadzenia badań społecznych z udziałem dzieci, a także ich promowanie wśród społeczności badaczy to główne zadania specjalnego zespołu działającego przy Rzeczniku Praw Dziecka. Przedstawiciel UODO uczestniczy w jego pracach, udzielając eksperckiego wsparcia w wypracowywaniu rozwiązań mających na celu dbałość o ochronę danych osobowych najmłodszych.

Koniec roku to dobra okazja, by podsumować blisko półtoraroczny okres udziału przedstawiciela UODO w pracach działającego przy Rzeczniku Praw Dziecka Zespołu ds. etyki badań społecznych z udziałem dzieci w Polsce.

Został on powołany 21 lutego 2024 r. na mocy zarządzenia Rzeczniczki Praw Dziecka, Moniki Horny-Cieślak, która 25 lipca 2024 r. wręczyła akty powołania jego członkom.

W skład zespołu wchodzą eksperci z różnych dziedzin, m.in. przedstawiciele świata nauki, instytucji publicznych oraz organizacji pozarządowych prowadzących badania z udziałem dzieci. W jego gronie są też reprezentanci młodego pokolenia.

Dla prezesa UODO, Mirosława Wróblewskiego, udział przedstawiciela Urzędu w jego pracach jest niezwykle ważny.

Dbałość o przestrzeganie praw dzieci, w tym do ochrony ich danych osobowych, to jeden z priorytetów organu nadzorczego. Najmłodsi mają bowiem niewielkie doświadczenie i są najmniej świadomi zagrożeń związanych z pozyskiwaniem i wykorzystywaniem ich danych osobowych. Mają też mniejszą wiedzę o prawach przysługujących im w związku z przetwarzaniem ich danych

PROJEKT DECYZJI O ADEKWATNOŚCI DLA BRAZYLII: EROD PRZYJMUJE OPINIĘ

Podczas ostatniej sesji plenarnej EROD przyjął opinię dotyczącą projektu decyzji Komisji Europejskiej w sprawie odpowiedniego poziomu ochrony danych osobowych w Brazylii. Po jej przyjęciu decyzja zapewni swobodny przepływ danych osobowych z Europy do Brazylii oraz umożliwi jednostkom zachowanie kontroli nad swoimi danymi.

W swojej opinii, o którą zwróciła się Komisja, EROD ocenia, czy brazylijskie ramy ochrony danych oraz przepisy dotyczące dostępu władz do danych osobowych przekazywanych z Europy zapewniają zabezpieczenia zasadniczo równoważne tym przewidzianym w prawie UE. Rada pozytywnie zauważa bliskie dostosowanie do przepisów UE oraz orzecznictwa Trybunału Sprawiedliwości UE. EROD analizuje również, czy zabezpieczenia przewidziane w brazylijskich ramach prawnych są wdrożone i skuteczne.

Jednocześnie EROD pozytywnie zauważa, że brazylijskie prawo o ochronie danych częściowo ma zastosowanie do przetwarzania danych osobowych w kontekście dochodzeń karnych i utrzymania porządku publicznego, zgodnie z interpretacją brazylijskiego Federalnego Sądu Najwyższego w jego orzecznictwie.

Rada zachęca Komisję do dalszego doprecyzowania zakresu stosowania brazylijskiego prawa o ochronie danych, a także uprawnień dochodzeniowych i naprawczych brazylijskiego organu ochrony danych w odniesieniu do organów ścigania. Wreszcie Rada zachęca Komisję do dalszego wyjaśnienia definicji brazylijskiego pojęcia bezpieczeństwa narodowego.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

Draft adequacy decision for Brazil: EDPB adopts opinion | European Data Protection Board

UKRYTE KAMERY: CNIL NAKŁADA SANKCJĘ NA SAMARITAINE

18 września 2025 r. CNIL nałożył na spółkę SAMARITAINE SAS, która prowadzi sklep o tej samej nazwie, karę w wysokości 100 tys. EUR za ukrycie kamer w magazynach sklepu.

Informacje ogólne

W sierpniu 2023 r., w związku ze wzrostem kradzieży towarów w magazynach, spółka SAMARITAINE SAS umieściła nowe kamery w dwóch magazynach. Kamery miały wygląd czujników dymu i umożliwiały nagrywanie dźwięku. Odkryte przez pracowników, zostały usunięte we wrześniu 2023 r.

Uwagę CNIL na te fakty zwrócił artykuł prasowy z 25 listopada 2023 r. Niedługo później organ otrzymał skargę dotyczącą tych samych kwestii. W kolejnych dniach CNIL przeprowadził dochodzenie.

Na podstawie ustaleń dokonanych w trakcie dochodzenia komitet ograniczony – organ CNIL odpowiedzialny za nakładanie sankcji – nałożył na spółkę SAMARITAINE SAS karę w wysokości 100 tys. EUR za kilka naruszeń RODO. W nawiązaniu do orzecznictwa Europejskiego Trybunału Praw Człowieka (ETPCz) komitet ograniczony przypomniał, że pracodawca może instalować ukryte kamery w wyjątkowych okolicznościach pod warunkiem zachowania uczciwej równowagi między realizowanym celem (ochrona mienia i osób) a ochroną prywatności pracowników. Na przykład, aby takie rozwiązanie było proporcjonalne, musi mieć charakter tymczasowy i zostać wdrożone po udokumentowanej analizie jego zgodności z RODO oraz w świetle wyjątkowych okoliczności.

CNIL w szczególności ukarał spółkę za następujące uchybienia:

Naruszenia objęte sankcją

Naruszenie obowiązku zgodnego z prawem przetwarzania danych oraz zasady rozliczalności (art. 5-1-a) i 5-2 RODO).

Komitet ograniczony przypomniał, że co do zasady, aby spełnić wymóg lojalności, kamery monitoringu wizyjnego filmujące pracowników muszą być widoczne i nieukryte. Jednakże, jak uznaje orzecznictwo, w wyjątkowych okolicznościach i pod pewnymi warunkami administrator może tymczasowo instalować kamery niewidoczne dla pracowników. Administrator danych musi wówczas przeanalizować zgodność urządzenia z RODO i być w stanie ją uzasadnić.

W niniejszej sprawie spółka zgłosiła występowanie kradzieży w magazynach i wyjaśniła, że urządzenie miało charakter tymczasowy (co potwierdzają jego cechy techniczne), ale nie przeprowadziła żadnej

wcześniejszej analizy zgodności z RODO ani nie udokumentowała tymczasowego charakteru instalacji - która została odkryta przez pracowników kilka tygodni po wdrożeniu.

Spółka SAMARITAINE SAS nie uwzględniła tego urządzenia ani w rejestrze czynności przetwarzania, ani w ocenie skutków dla ochrony danych. Ponadto spółka nie poinformowała inspektora ochrony danych o zamiarze instalacji ukrytych kamer w magazynach. W związku z tym wdrożenie tego systemu nie zostało poparte odpowiednimi zabezpieczeniami, które zapewniłyby zachowanie równowagi między celem realizowanym przez administratora a ochroną prywatności pracowników.

Naruszenie zasady minimalizacji danych – brak ograniczenia do danych adekwatnych, stosownych i niezbędnych (art. 5-1-c RODO)

Kamery były wyposażone w mikrofony i nagrywały rozmowy pracowników, należące do sfery osobistej. Komitet ograniczony uznał, że nagrywanie dźwięku pracowników było w tym przypadku nadmierne, co stanowi naruszenie zasady minimalizacji.

Naruszenie obowiązku angażowania inspektora ochrony danych w sprawy dotyczące ochrony danych osobowych (art. 38-1 RODO)

Dopiero kilka tygodni po instalacji kamer inspektor ochrony danych został poinformowany o istnieniu urządzenia. Biorąc pod uwagę charakterystykę tego urządzenia, inspektor ochrony danych mógł ostrzec spółkę o środkach, które należało wdrożyć w celu ograniczenia ryzyka dla ochrony danych pracowników, zgodnie ze swoimi zadaniami.

Źródło:

Komunikat Francuskiego Organu Ochrony Danych

Hidden cameras: the CNIL sanctions the SAMARITAINE | CNIL

FIŃSKI ORGAN NADZORCZY: S-BANK UKARANY GRZYWNĄ ZA LUKĘ W ZABEZPIECZENIACH DANYCH

Podsumowanie decyzji

Fiński organ nadzorczy przeprowadził dochodzenie dotyczące naruszenia ochrony danych osobowych po zgłoszeniu przez S-Bank w sierpniu 2022 r. W kwietniu 2022 r. bank wprowadził nową funkcję logowania w swojej usłudze mobilnej. Z powodu błędu oprogramowania w usłudze uwierzytelniania możliwe było logowanie do bankowości internetowej i usług on-line przy użyciu silnego uwierzytelniania z wykorzystaniem danych uwierzytelniających innych klientów. Luka była możliwa do wykorzystania przez ponad trzy miesiące. Część klientów banku padła ofiarą naruszenia danych. W praktyce luka dotyczyła znaczącej części klientów banku.

Kluczowe ustalenia

Dochodzenie wykazało, że bank nie posiadał odpowiednich zabezpieczeń zapewniających bezpieczeństwo danych osobowych. Bank nie przeprowadził wystarczających testów nowego oprogramowania przed jego wdrożeniem ani nie zidentyfikował luki przed uruchomieniem funkcjonalności. Nie zareagował również w odpowiedni sposób na zgłoszenia klientów dotyczące nieprawidłowości podczas logowania do bankowości internetowej. Fiński SA uznał, że działania banku naruszyły art. 5 pkt. 1 lit. f, art. 25 pkt. 1, art. 32 pkt. 1 oraz art. 32 pkt. 2 RODO.

Decyzja

Fiński SA nałożył na administratora grzywnę w wysokości 1,8 mln EUR oraz udzielił upomnienia za nieprzestrzeganie przepisów o ochronie danych. Fiński SA uznał, że kara za naruszenie ochrony danych była konieczna ze względu na potrzebę ochrony praw jednostek, ogólne znaczenie sprawy oraz wcześniejsze upomnienie udzielone bankowi.

Organ uwzględnił decyzję Fińskiego Urzędu Nadzoru Finansowego, wydaną w maju 2025 r., przy ustalaniu wysokości grzywny i odpowiednio ją dostosował. Urząd Nadzoru Finansowego ocenił działania banku w tym samym zestawie zdarzeń pod kątem innych naruszeń i nałożył grzywnę w wysokości 7 670 000 EUR za zaniedbania w zarządzaniu ryzykiem operacyjnym.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

Finnish SA: S-Bank fined for data security vulnerability | European Data Protection Board

FIŃSKI ORGAN NADZORCZY: AKTIA BANK UKARANY GRZYWNĄ ZA NIEDOCIĄGNIĘCIA W ZABEZPIECZENIACH DANYCH W USŁUDZE SILNEGO UWIERZYTELNIANIA ELEKTRONICZNEGO

Podsumowanie decyzji

Usługa silnego uwierzytelniania elektronicznego Aktia Banku uległa zakłóceniu w wyniku zmiany technicznej w styczniu 2023 r. Podczas krótkotrwałego zakłócenia część osób logujących się do różnych usług przy użyciu danych uwierzytelniających bankowości internetowej Aktia uzyskała dostęp do danych osobowych innych klientów, ponieważ usługa myliła tożsamości użytkowników. Naruszenie danych osobowych dotknęło różne usługi publiczne, fundusze bezrobocia, firmy ubezpieczeniowe oraz podmioty opieki zdrowotnej. Wiele z tych usług zawierało informacje o wysokim stopniu prywatności, takie jak dane dotyczące zdrowia i sytuacji finansowej. Naruszenie danych dotyczyło ok. 350 osób. Nie odnotowano przypadków nadużycia danych.

Kluczowe ustalenia

Dochodzenie fińskiego organu nadzorczego wykazało, że bezpieczeństwo usługi uwierzytelniania powinno zostać zapewnione poprzez odpowiednie zarządzanie zmianami. Fiński SA uznał, że bank wykazał niedociągnięcia w projektowaniu, wdrażaniu i testowaniu zmiany technicznej w usłudze. Aktia powinna była zaplanować i wdrożyć zmianę techniczną w usłudze z większą starannością oraz przeprowadzić wystarczające testy. Bardziej rozległe testy mogły zostać wykonane przy użyciu konwencjonalnych i powszechnie stosowanych metod.

Decyzja

Fiński SA nałożył na Aktia grzywnę w wysokości 865 tys. EUR za nieprzestrzeganie wymogów przepisów o ochronie danych dotyczących bezpiecznego przetwarzania danych osobowych oraz ochrony danych w fazie projektowania i domyślnie (art. 32 RODO, art. 5 pkt. 1 lit. f RODO oraz art. 32 RODO). Wydano również upomnienie.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

Finnish SA: Aktia Bank fined for data security shortcomings in its strong electronic authentication service | European Data Protection Board

MAŁOLETNI: WŁOSKI ORGAN NADZORCZY UKARAŁ PRZEDSZKOLE. KAMERY ZAINSTALOWANE BEZ ZABEZPIECZEŃ I ZDJĘCIA DZIECI OPUBLIKOWANE ON-LINE

Podsumowanie decyzji

Postępowanie zostało wszczęte po skardze rodzica, który aby zapisać córkę do przedszkola, musiał wyrazić zgodę na zbieranie i wykorzystywanie wizerunku dziecka. Rodzic zgłosił również obecność systemu monitoringu wideo wewnątrz przedszkola, który działał także podczas zajęć szkolnych i edukacyjnych.

Kluczowe ustalenia

W toku dochodzenia ustalono, że przedszkole publikowało liczne zdjęcia dzieci w różnych momentach „typowego dnia" zarówno na swojej stronie internetowej, jak i w profilu Google Maps, w tym w szczególnie wrażliwych kontekstach (spanie, jedzenie, korzystanie z toalety, przewijanie, masaż niemowlęcy). Były to sytuacje i czynności szczególnie wrażliwe lub przeznaczone do pozostania prywatnymi. Należy również uwzględnić ryzyko związane ze zwiększoną ekspozycją zdjęć w sieci oraz ich możliwym wykorzystaniem przez osoby działające w złej wierze do celów nielegalnych lub przestępstw wobec dzieci.

Garante stwierdził, że przetwarzanie prowadzone przez przedszkole nie mogło być zgodnie z prawem oparte na zgodzie rodziców, ponieważ nadrzędny był interes dzieci, aby ich fotografie w szczególnie intymnych momentach szkolnych i edukacyjnych nie były publikowane on-line w celu promowania działalności przedszkola. Ponadto taka zgoda nie mogła być uznana za świadomą i dobrowolną, gdyż w przypadku odmowy możliwość zapisania dzieci do przedszkola zostałaby wykluczona.

System monitoringu wideo, który rejestrował wizerunki małoletnich, personelu edukacyjnego, a także rodziców, dostawców i odwiedzających, był również używany niezgodnie z europejskimi i włoskimi przepisami o ochronie prywatności.

Decyzja

Uwzględniając fakt, że przedszkole współpracowało z organem, Garante nałożył administracyjną karę pieniężną w wysokości 10 000 EUR, w związku z naruszeniami art. 5 pkt. 1, 6, 7, 12 pkt. 1, 13, 35, 37 pkt. 7 i 38 pkt. 6 RODO oraz art. 2 Kodeksu ochrony danych osobowych.

Włoski organ nadzorczy nałożył również ostateczny zakaz przetwarzania i nakazał przedszkolu usunięcie danych osobowych.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

Minors: Italian SA sanctions nursery school. Cameras installed without safeguards and photos of children published online | European Data Protection Board

PRAWO DOSTĘPU: ORGAN OCHRONY DANYCH NAKŁADA NA BANK KARĘ 100 000 EUR. KLIENCI MOGĄ UZYSKAĆ DOSTĘP DO SWOICH DANYCH ZAWARTYCH W NAGRANIACH ZAMÓWIEŃ TELEFONICZNYCH

Podsumowanie decyzji

Klient, który padł ofiarą oszustwa, zwrócił się do banku o udostępnienie nagrań rozmów prowadzonych z obsługą klienta, które mogłyby być pomocne w zakwestionowaniu przelewu na około 10 tys. EUR oraz w odtworzeniu przebiegu zdarzeń. Nie otrzymawszy satysfakcjonującej odpowiedzi, złożył skargę do Garante. Dopiero po wszczęciu postępowania przez organ bank przekazał nagrania, jednak wówczas 30-dniowy termin przewidziany przez RODO już upłynął.

Kluczowe ustalenia

W toku dochodzenia włoski organ nadzorczy wskazał, że – zgodnie z Wytycznymi Europejskiej Rady Ochrony Danych 01/2022 dotyczącymi prawa dostępu – nawet rozmowy telefoniczne między klientami a bankami mogą być uznane za dane osobowe i jako takie muszą być udostępniane na żądanie, z poszanowaniem praw osób trzecich uczestniczących w rozmowie.

Decyzja

Garante nałożył administracyjną karę pieniężną w wysokości 100 tys. EUR. Przy ustalaniu jej wysokości organ wziął pod uwagę obrót banku, jego współpracę w trakcie dochodzenia oraz brak wcześniejszych naruszeń.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

Right of access: Data Protection Authority fines bank 100 000 EUR. Customers can access their data contained in telephone order recordings | European Data Protection Board

76. POSIEDZENIE GRUPY BERLIŃSKIEJ

19–20 listopada 2025 r. w Montevideo odbyło się 76. posiedzenie Grupy Berlińskiej (International Working Group on Data Protection in Technology – IWGDPT). Spotkanie zorganizowano na zaproszenie urugwajskiego organu ochrony danych Unidad Reguladora y de Control de Datos Personales (URCDP) oraz Biura Specjalnego Sprawozdawcy ONZ ds. Prawa do Prywatności, prof. dr Any Brian Nougreres. W wydarzeniu uczestniczyła również przedstawicielka Urzędu Ochrony Danych Osobowych, reprezentująca Departament Współpracy Międzynarodowej.

Międzynarodowe forum wymiany doświadczeń

Grupa Berlińska od wielu lat stanowi jedno z najważniejszych forów międzynarodowych, w ramach którego organy nadzorcze, eksperci i przedstawiciele świata nauki wspólnie analizują wyzwania związane z ochroną danych osobowych. Posiedzenia Grupy są okazją do wymiany doświadczeń, prezentacji krajowych inicjatyw oraz wypracowywania wspólnych stanowisk wobec dynamicznych zmian technologicznych.

Tegoroczna edycja miała szczególny wymiar – odbywała się w Ameryce Łacińskiej, regionie intensywnie rozwijającym polityki cyfrowe i strategie sztucznej inteligencji. To nadało obradom dodatkowy kontekst strategiczny i pozwoliło uczestnikom lepiej zrozumieć perspektywę państw spoza Europy.

Dzień pierwszy – 19 listopada

Po uroczystym otwarciu przez gospodarzy i przewodniczącego Grupy uczestnicy wysłuchali prezentacji urugwajskiej agencji AGESIC, która przedstawiła model zarządzania danymi w Urugwaju. Szczególną uwagę zwrócono na rozwój krajowej strategii AI oraz polityki chmurowej – od początkowego podejścia restrykcyjnego do obecnego modelu, opartego na transparentności i jasno określonych standardach.

Następnie odbyła się obszerna sesja raportów krajowych i międzynarodowych. W jej trakcie przedstawiciele organów nadzorczych z całego świata zaprezentowali aktualne działania i wyzwania w swoich państwach:

4 SPRAWY MIĘDZYNARODOWE

- Gruzja poinformowała o reorganizacji systemu ochrony danych i planach powołania nowej instytucji.
- Izrael przedstawił nowelizację ustawy o prywatności, obejmującą m.in. regulację danych osób zmarłych.
- Brazylia zaprezentowała nowy sandbox regulacyjny oraz wskazała na oczekiwaną decyzję Komisji Europejskiej o adekwatności.
- Kanada skoncentrowała się na reformach dotyczących cyberbezpieczeństwa i cyfrowych identyfikatorów zdrowotnych.
- Francja omówiła zalecenia dotyczące AI, zarządzania danymi pośmiertnymi oraz działania egzekucyjne wobec naruszeń w zakresie plików cookie i monitoringu.
- Hiszpania zaprezentowała prace nad nowym Planem Strategicznym 2025–2030, którego celem jest umieszczenie godności jednostki w centrum transformacji cyfrowej.
- Polska przedstawiła raport z działań polskiego organu, obejmujących nadzór regulacyjny, legislację, współpracę międzynarodową, edukację oraz analizę ryzyk związanych z AI i cyberbezpieczeństwem.
- Luksemburg poinformował o inicjatywach edukacyjnych dla młodzieży oraz narzędziach wspierających MŚP.
- Włochy podkreśliły ograniczenia stosowania danych biometrycznych w miejscu pracy i wydały opinię o systemie IT-Wallet.
- Szwecja poinformowała o reorganizacji urzędu i działaniach związanych z AI Act.
- Argentyna kontynuuje modernizację ram regulacyjnych zgodnie z Konwencją 108+.
- Katalonia podpisała porozumienie z Brazylią ws. współpracy nad godnymi zaufania systemami AI.
- EIOD poinformował o publikacjach dotyczących nadzoru człowieka w systemach AI oraz portfeli tożsamości cyfrowej.
- Niemcy omówiły rosnącą liczbę skarg związanych z AI.
- Słowenia przekazała informacje o wdrożeniu krajowej ustawy wykonawczej wdrażającej AI Act oraz o największym wycieku danych w historii kraju.

4 SPRAWY MIĘDZYNARODOWE

Ekwador jako obserwator Konwencji 108+ przedstawił krótką aktualizację dotyczącą udziału w inicjatywach międzynarodowych.

- Kalifornia w raporcie przesłanym zdalnie poinformowała o nowych przepisach dotyczących zautomatyzowanego podejmowania decyzji i sygnałów opt-out.
- Wielka Brytania zapowiedziała przegląd banerów cookie oraz publikację wytycznych dla produktów IoT.

Dzięki tak szerokiemu spektrum raportów uczestnicy uzyskali kompleksowy obraz globalnych wyzwań związanych z ochroną danych i sztuczną inteligencją.

Dzień drugi – 20 listopada

Kontynuowano dyskusje nad dokumentami Grupy Berlińskiej, w tym nad technologią 6G (JCAS), poufnymi obliczeniami w chmurze oraz problematyką danych osób zmarłych. Prezentacja CNIL na temat „data post-mortem" wywołała szeroką debatę o tzw. privacy paradox – rosnącej liczbie osób, które chcą pozostawić swoje dane cyfrowe do wykorzystania po śmierci.

Wydarzenia towarzyszące

- 18 listopada – odbyło się tradycyjne, nieformalne spotkanie uczestników, sprzyjające integracji i wymianie doświadczeń.
- 21 listopada – uczestnicy wzięli udział w dorocznej konferencji URCDP poświęconej ochronie danych w kontekście AI i innowacji cyfrowych.

Podsumowanie

76. Posiedzenie Grupy Berlińskiej potwierdziło jej rolę jako kluczowego forum międzynarodowego w zakresie ochrony danych i prywatności. Przyjęcie dokumentu dotyczącego globalnych sygnałów sprzeciwu oraz intensywne prace nad chmurą poufną, technologią 6G i danymi syntetycznymi pokazują, że Grupa koncentruje się zarówno na bieżących problemach technologicznych, jak i na długoterminowych kierunkach rozwoju.

Kolejne posiedzenie Grupy odbędzie się w czerwcu 2026 r. w Warszawie, jego gospodarzem będzie Urząd Ochrony Danych Osobowych – co stanowi wyjątkową okazję do zaprezentowania roli Polski w globalnej debacie o ochronie danych.

PRIVACY, AI AND INNOVATION ROUNDTABLE – RELACJA Z KONFERENCJI

14 listopada 2025 r. w Warszawie odbyła się konferencja „Privacy, AI and Innovation Roundtable", zorganizowana przez kancelarię Bird & Bird. Wydarzenie zgromadziło ekspertów z obszaru prawa, ochrony danych i nowych technologii, którzy wspólnie zastanawiali się nad przyszłością regulacji dotyczących prywatności i sztucznej inteligencji w Europie. Spotkanie miało charakter interaktywny – uczestnicy nie tylko wysłuchali wystąpień, ale także współtworzyli rekomendacje, które zostaną opublikowane w raporcie końcowym.

Konferencję otworzyła Izabela Kowalczuk-Pakuła, partner w Bird & Bird, podkreślając wagę dyskusji w kontekście nadchodzącego pakietu legislacyjnego Digital Omnibus, który Komisja Europejska ma przedstawić w najbliższych dniach. Wystąpienie główne wygłosił dr Stefan Brink z Instytutu WIDA. W swoim wykładzie wskazał, że RODO jest „mieczem obosiecznym": z jednej strony chroni dane osobowe, z drugiej może ograniczać innowacje. Podkreślił potrzebę większej równowagi między rolą Europy w gospodarce cyfrowej a ochroną praw obywateli, zwracając uwagę na problemy z funkcjonowaniem Europejskiej Rady Ochrony Danych oraz na konieczność bardziej widocznego podejścia opartego na ryzyku. Wskazał również na planowane reformy RODO w latach 2026–2027, które powinny wzmocnić rolę Komisji Europejskiej w strukturze EROD.

Centralnym punktem programu był panel dyskusyjny zatytułowany „Reset or Reinvention? The Future Architecture of Data and AI Regulation in Europe", moderowany przez dr Urszulę Góral z Meta. Wzięli w nim udział Mirosław Wróblewski, prezes UODO, dr Julia Sziklay – wiceprezes węgierskiego organu NAIH, Izabela Kowalczuk-Pakuła z Bird & Bird, Mikołaj Barczentewicz z University of Surrey/Oxford oraz Aleksandra Czarnecka z Agora SA. Dyskusja koncentrowała się na przyszłej architekturze regulacji dotyczących danych i sztucznej inteligencji w Europie. Paneliści podkreślali, że rola organów nadzorczych nie powinna ograniczać się do kontroli, ale obejmować także tworzenie wytycznych w obszarach luk prawnych i nowych technologii. Wskazywano na trudności związane z wdrożeniem AI Act, problem nadmiaru nowych regulacji oraz konieczność jasnych interpretacji i przewidywalnego orzecznictwa Trybunału Sprawiedliwości UE.

4 SPRAWY MIĘDZYNARODOWE

Prezes UODO Mirosław Wróblewski zwrócił uwagę na znaczenie Helsinki Statement i konieczność uwzględniania perspektywy biznesu w procesie regulacyjnym. Ostrzegł przed kosztownym mnożeniem nowych regulacji, przypominając, że celem RODO jest nie tylko ochrona danych, ale także zapewnienie swobodnego przepływu informacji. Julia Sziklay wskazała na przypadki nielegalnego wykorzystania AI w sektorze bankowym na Węgrzech i zaznaczyła potrzebę szczególnej ochrony dzieci oraz MŚP. Mikołaj Barczentewicz krytykował brak uporządkowania instytucjonalnego i zbyt ogólne wytyczne EROD, wskazując na praktyczne podejście CNIL jako wzór. Izabela Kowalczuk-Pakuła omówiła problem nakładających się reżimów RODO i ePrivacy, sugerując możliwość uproszczenia systemu poprzez włączenie regulacji cookies do RODO. Z kolei Aleksandra Czarnecka zauważyła praktyczne potrzeby biznesu: uproszczenie procedur, ograniczenie formalności i większe skupienie na osobie, której dane dotyczą.

W końcowej części konferencji dyskutowano o tym, czy uproszczenia dla biznesu mogą osłabić ochronę praw podstawowych. Zwrócono uwagę, że konieczne jest zachowanie równowagi i przestrzeganie prawa unijnego, a jednocześnie wspieranie innowacji poprzez dialog z konkretnymi sektorami. Wskazano, że nadmiar legislacji grozi nieprzestrzeganiem przepisów, dlatego lepsze są klarowne wytyczne niż kolejne akty prawne. Podkreślono także rolę CNIL jako przykładu wspierania innowacji poprzez laboratoria AI i piaskownice regulacyjne.

Podsumowanie

Konferencja „Privacy, AI and Innovation Roundtable” pokazała, że przyszłość regulacji w Europie wymaga równowagi między ochroną danych a wspieraniem innowacji. Dyskusje ekspertów, w tym wystąpienie prezesa UODO, wskazały na konieczność jasnych interpretacji, stabilnych podstaw prawnych oraz większego dialogu między regulatorami a biznesem. Spotkanie stanowiło ważny krok w kierunku wypracowania rekomendacji, które mogą wpłynąć na kształt reform RODO i AI Act w najbliższych latach.

KONFERENCJA RESEARCH@ GOOGLE RESEARCH POLAND – SZTUCZNA INTELIGENCJA W SŁUŻBIE NAUKI I SPOŁECZEŃSTWA

Otwarcie konferencji

Konferencja research@, zorganizowana przez zespół Google Research Poland 12 listopada 2025 r. zgromadziła naukowców wykorzystujących sztuczną inteligencję w badaniach naukowych. Wydarzenie podzielono na trzy główne panele: nauka i zdrowie, edukacja oraz nauka o Ziemi.

Konferencję otworzyła Magda Kotlarczyk, dyrektor krajowa Google Polska. W swoim wystąpieniu zaznaczyła potrzebę tworzenia przestrzeni sprzyjającej współpracy międzynarodowej społeczności naukowej oraz wymianie pomysłów. Zwróciła również uwagę na rosnącą rolę Polski w promowaniu innowacji.

Panel I – nauka i zdrowie

- Dr Susan Thomas zaprezentowała rozwój MedGemma – otwartego modelu AI przeznaczonego do analiz obrazów medycznych. Omówiła jego funkcjonalności oraz kierunki dalszego doskonalenia.
- Dr Annalisa Pawlosky przedstawiła projekt AI co-scientist, system oparty na wielu agentach, który wspiera procesy badawcze: formułowanie hipotez, ewaluację metod, analizę źródeł i wybór optymalnej metodologii.

o Po prezentacji odbyła się dyskusja z udziałem Viveka Natarajana oraz prof. Tiago Dias da Costa z Imperial College – twórców projektu. Podkreślili oni znaczenie systemu w redukowaniu liczby nieudanych eksperymentów, co przekłada się na efektywność badań.

- Kolejna prezentacja dotyczyła wykorzystania AI w mapowaniu mózgu. Przypomniano, że w 2024 r. zakończono mapowanie mózgu muchy owocówki, a w 2021 r. jedynie fragmentu mózgu człowieka. Obecnie trwają prace nad mózgiem myszy, w których uczestniczą także polscy naukowcy.

Panel II – edukacja

- Wilkowski, Liderka Zespołu Pedagogicznego Google, przedstawiła wizję przyszłości edukacji wspieranej przez AI, m.in. poprzez wprowadzenie tutorów AI.
- Omówiono działania Fundacji Raspberry Pi, która promuje naukę sztucznej inteligencji wśród młodzieży, również w Polsce – poprzez szkolenia dla nauczycieli i uczniów, także w mniejszych miejscowościach.
- Ronit Levavi Morad zaprezentowała projekt AI Quests, umożliwiający uczniom szkół ponadpodstawowych rozwijanie kompetencji AI poprzez interaktywne projekty, np. opracowywanie rozwiązań przeciwpowodziowych.

Panel III – nauka o Ziemi

Ostatni panel poświęcono wykorzystaniu AI w projektach takich jak Google Maps i Google Earth. Modele predykcyjne pozwalają na zbieranie kompleksowych danych o pogodzie i ruchach sejsmicznych, co w przyszłości może umożliwić wcześniejsze ostrzeganie przed kataklizmami i ograniczanie ich skutków.

Dyskusja końcowa

Konferencję zakończyła rozmowa między prof. Piotrem Sankowskim a Yossim Matiasem, wiceprezesem Google. Dyskutowano o przyszłości nauki w kontekście najnowszych osiągnięć AI, w tym systemów wieloagentowych oraz sztucznej inteligencji w rzeczywistości postkwantowej. Wskazano m.in. na nowatorską hipotezę dotyczącą zachowania komórek nowotworowych, zaproponowaną przez model Gemma.

Spotkanie kuluarowe – medycyna i regulacje

Po zakończeniu konferencji odbyło się spotkanie interesariuszy poświęcone rozwojowi nauk medycznych z wykorzystaniem sztucznej inteligencji w Polsce. Wzięli w nim udział przedstawiciele start upów medycznych, organów publicznych oraz samorządów zawodowych, w tym Naczelnej Izby Lekarskiej. Urząd Ochrony Danych Osobowych reprezentował Krzysztof Król, zastępca dyrektorki Departamentu Współpracy Międzynarodowej.

Tematy rozmów obejmowały: rozwój AI w medycynie, bariery regulacyjne, propozycje rozwiązań wspierających wdrażanie technologii oraz ryzyko błędów i odpowiedzialność za wyniki generowane przez systemy AI. W ich toku Krzysztof Król podkreślał konieczność zapewnienia wysokiego poziomu ochrony danych medycznych, które są szczególnie cenne i podatne na ataki.

Podsumowanie

Konferencja research@ Google Research Poland pokazała ogromny potencjał sztucznej inteligencji w nauce, edukacji i medycynie. Jednocześnie podkreślono wagę odpowiednich regulacji i ochrony danych osobowych, które pozostają kluczowym elementem w procesie wdrażania nowych technologii.

WZMACNIANIE OCHRONY DANYCH NA CAŁYM ŚWIECIE: EROD SPOTYKA SIĘ Z KRAJAMI I ORGANIZACJAMI POSIADAJĄCYMI DECYZJĘ STWIERDZAJĄCĄ ODPOWIEDNI POZIOM OCHRONY

W ramach grudniowego posiedzenia plenarnego Europejska Rada Ochrony Danych przeprowadziła spotkanie on-line z komisarzami oraz przedstawicielami organów ochrony danych z krajów i organizacji, wobec których obowiązuje decyzja UE stwierdzająca odpowiedni poziom ochrony danych. Było to drugie tego typu spotkanie, po pierwszym, które odbyło się w październiku 2024 r.

Decyzja stwierdzająca odpowiedni poziom ochrony jest kluczowym mechanizmem w unijnych przepisach o ochronie danych, umożliwiającym swobodny przepływ danych osobowych z Europy do państw trzecich lub organizacji międzynarodowych zapewniających odpowiedni poziom ochrony danych. Do tej pory korzystają z niej następujące kraje i organizacje: Andora, Argentyna, Kanada, Wyspy Owcze, Guernsey, Izrael, Wyspa Man, Japonia, Jersey, Nowa Zelandia, Republika Korei, Szwajcaria, Zjednoczone Królestwo, Urugwaj, Stany Zjednoczone oraz Europejska Organizacja Patentowa. Organy ochrony danych z tych krajów oraz Europejska Organizacja Patentowa są kluczowymi partnerami EROD, odgrywając istotną rolę we wspólnych działaniach na rzecz wzmacniania ochrony danych na świecie.

Wzmacnianie współpracy wielostronnej

Rada w październiku 2024 r. zorganizowała pierwsze spotkanie z organami ochrony danych z piętnastu krajów posiadających decyzję o adekwatności.

Po tym spotkaniu EROD oraz organy ochrony danych z krajów i organizacji objętych decyzją o adekwatności zacieśniły współpracę poprzez wymianę informacji dotyczących prac doradczych oraz dzielenie się doświadczeniami w zakresie międzynarodowej współpracy w egzekwowaniu przepisów o ochronie danych.

4 SPRAWY MIĘDZYNARODOWE

„Nasze pierwsze wspólne spotkanie w październiku 2024 r. utorowało drogę do silniejszej współpracy oraz wartościowej wymiany wiedzy i doświadczeń w zakresie ochrony danych. Wysoki poziom zaangażowania, jaki wykazano podczas tego drugiego spotkania przez EROD oraz organy ochrony danych z krajów i organizacji międzynarodowej, wobec których UE przyjęła decyzję o adekwatności, jest wyraźnym sygnałem naszego zobowiązania do dalszej wspólnej pracy w tym kierunku” – zaznaczyła Przewodnicząca EROD, Anu Talus.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

https://www.edpb.europa.eu/news/news/2025/strengthening-data-protection-worldwide-edpb-meets-countries-and-organisation_en

EROD PRZEDSTAWIA ZALECENIA DOTYCZĄCE ZWIĘKSZENIA POSZANOWANIA PRYWATNOŚCI UŻYTKOWNIKÓW W HANDLU INTERNETOWYM, OMAWIA PROPOZYCJĘ DIGITAL OMNIBUS I POWOŁUJE NOWĄ ZASTĘPCZYNIĘ PRZEWODNICZĄCEGO

Podczas ostatniego posiedzenia plenarnego EROD przyjęła zalecenia dotyczące podstawy prawnej wymagania zakładania kont użytkowników na stronach e-commerce. Ponadto Rada przeprowadziła wstępną dyskusję na temat propozycji Digital Omnibus oraz powołała nową Zastępczynię Przewodniczącego EROD.

Użytkownicy internetu odwiedzają strony e-commerce z różnych powodów, w tym aby dokonywać zakupów on-line, korzystać z promocji lub po prostu przeglądać produkty. W trakcie korzystania z takich stron mogą być proszeni o założenie konta, co może prowadzić do gromadzenia i przetwarzania danych osobowych, a także zwiększać ryzyka dla prywatności i bezpieczeństwa.

EROD przyjęła zalecenia mające na celu doprecyzowanie, kiedy strony e-commerce mogą wymagać od użytkowników założenia konta.

Zasadniczo użytkownicy powinni mieć możliwość korzystania ze stron e-commerce, w tym dokonywania zakupów, bez konieczności zakładania konta. W takich przypadkach EROD zaleca, aby strony e-commerce oferowały wybór: tryb „gościa”, umożliwiający dokonanie zakupu bez zakładania konta, lub możliwość dobrowolnego utworzenia konta. Takie podejście minimalizuje zakres gromadzenia i przetwarzania danych osobowych, a tym samym jest zgodne z zasadą ochrony danych w fazie projektowania i domyślnej ochrony danych wynikającą z RODO.

Obowiązkowe zakładanie konta może być jednak uzasadnione w ograniczonej liczbie przypadków, np. przy oferowaniu usług subskrypcyjnych lub zapewnianiu dostępu do ofert ekskluzywnych.

Zalecenia podkreślają wysiłki EROD na rzecz promowania pragmatycznych, przyjaznych użytkownikom i chroniących prywatność praktyk w sektorze e-commerce.

Zalecenia zostaną poddane konsultacjom publicznym, co umożliwi zainteresowanym stronom zgłaszanie uwag i opinii.

4 SPRAWY MIĘDZYNARODOWE

Wstępna dyskusja na temat propozycji Digital Omnibus

EROD przeprowadziła wstępną dyskusję na temat propozycji Digital Omnibus, w sprawie której EROD i EIOD wydadzą wspólną opinię.

W swoim Oświadczeniu Helsińskim EROD przedstawiła propozycje mające na celu zwiększenie przejrzystości, wsparcia i zaangażowania. EROD i EIOD z zadowoleniem przyjmują dyskusję na temat skutecznych regulacji cyfrowych i pozostają zaangażowane w poszukiwanie rozwiązań ułatwiających zgodność z RODO, zwłaszcza dla małych organizacji.

EROD i EIOD skoncentrują się na tym, jak propozycja Komisji Europejskiej wpłynie na podstawowe prawa jednostek oraz czy doprowadzi do uproszczeń dla organizacji i większej pewności prawnej.

Choć wiele kwestii wymaga analizy, na tym etapie EROD i EIOD podkreślają, że proponowana zmiana definicji danych osobowych wydaje się wykraczać poza najnowsze orzecznictwo TSUE i poza zakres ukierunkowanej zmiany RODO, co może negatywnie wpłynąć na fundamentalne prawo do ochrony danych.

EROD przypomina o nadchodzącym wydarzeniu dla interesariuszy publicznych w tej sprawie, które odbędzie się 12 grudnia 2025 r., i podkreśla, że wdrażanie orzecznictwa TSUE poprzez wytyczne uwzględniające opinie interesariuszy zapewnia większą pewność.

Jelena Virant Burnik wybrana nową Zastępczynią Przewodniczącego EROD

Podczas tegorocznego posiedzenia plenarnego członkowie EROD powołali Jelenę Virant Burnik, Komisarz ds. Informacji Republiki Słowenii, na nową Zastępczynię Przewodniczącego Rady.

„Jestem zaszczycona wyborem na stanowisko Zastępczyni Przewodniczącego EROD. Cieszę się, że mogę się przyczynić się do wzmocnienia roli EROD jako centralnego organu w zakresie ochrony danych w UE. Jestem zaangażowana w rozwijanie współpracy między krajowymi organami ochrony danych oraz tworzenie przestrzeni do otwartych dyskusji, które pomagają ujednolicać rozumienie i egzekwowanie przepisów RODO. W stale rozwijającym się krajobrazie regulacji cyfrowych EROD musi pozostać regulatorem, który rozumie złożone powiązania między przepisami i wnosi konstruktywny wkład w dyskusje na poziomie europejskim” – zwróciła uwagę Zastępczyni Przewodniczącego EROD, Jelena Virant Burnik.

4 SPRAWY MIĘDZYNARODOWE

„W ostatnich latach krajobraz, w którym działamy, fundamentalnie się zmienił, przekształcając rolę EROD w cyfrowej przyszłości Europy. W tym dynamicznym środowisku nowa Zastępczyni Przewodniczącego EROD staje przed ekscytującymi wyzwaniami. Jestem przekonana, że EROD odniesie ogromne korzyści z jej wiedzy i zaangażowania. Z niecierpliwością oczekuję współpracy z Jeleną Virant Burnik, aby wspólnie realizować misję EROD: wspieranie innowacji przy jednoczesnej ochronie podstawowych praw jednostek" – powiedziała Przewodnicząca EROD, Anu Talus

W nadchodzących latach Jelena Virant Burnik będzie ściśle współpracować z Przewodniczącą EROD Anu Talus oraz Zastępcą Przewodniczącego Zdravko Vukiciem, aby zapewnić spójne stosowanie unijnych przepisów o ochronie danych i promować skuteczną współpracę między organami ochrony danych w całej Europie.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych
EDPB gives recommendations to make online shopping more respectful of users' privacy, discusses the Digital Omnibus proposal and appoints new Deputy Chair | European Data Protection Board

SPOTKANIE INTERESARIUSZY DOTYCZĄCE ANONIMIZACJI I PSEUDONIMIZACJI

12 grudnia 2025 r. odbyło się zdalne spotkanie interesariuszy zorganizowane przez Europejską Radę Ochrony Danych, poświęcone zagadnieniom anonimizacji i pseudonimizacji oraz konsekwencjom wyroku Trybunału Sprawiedliwości UE ws. EDPS przeciwko Single Resolution Board (SRB). Wydarzenie stanowiło ważny element realizacji programu prac EROD na lata 2024–2025 oraz potwierdziło zaangażowanie Rady w dialog z podmiotami z różnych sektorów, zgodnie z założeniami tzw. deklaracji helsińskiej.

W spotkaniu uczestniczyli przedstawiciele organizacji branżowych, firm, kancelarii prawnych, środowiska akademickiego oraz organizacji pozarządowych. Każda instytucja mogła delegować jednego reprezentanta, przy czym zadbano o zróżnicowanie perspektyw oraz równowagę geograficzną i tematyczną uczestników.

Podczas wydarzenia omówiono praktyczne wyzwania związane z anonimizacją i pseudonimizacją danych, a także wpływ wspomnianego orzeczenia TSUE na stosowanie tych technik w praktyce. Zebrane opinie i doświadczenia mają wesprzeć dalsze prace EROD nad wytycznymi w tym obszarze.

Spotkanie cieszyło się dużym zainteresowaniem, a nabór zgłoszeń został zamknięty po osiągnięciu wysokiej liczby aplikacji. Kolejne działania konsultacyjne EROD zaplanowano na końcówkę pierwszego kwartału 2026 r., a UODO będzie na bieżąco informować o możliwościach udziału w tych inicjatywach.

NEXPUBLICA FRANCE UKARANA GRZYWNĄ W WYSOKOŚCI 1 700 000 EURO

22 grudnia 2025 r. CNIL nałożyła na NEXPUBLICA FRANCE karę w wysokości 1,7 mln euro za niewdrożenie wystarczających środków bezpieczeństwa w oprogramowaniu PCRM, narzędziu do zarządzania relacjami z użytkownikami w sektorze usług społecznych.

Informacje ogólne

NEXPUBLICA FRANCE (wcześniej INETUM SOFTWARE FRANCE), firma specjalizująca się w projektowaniu systemów informatycznych i oprogramowania, opracowuje pakiet oprogramowania o nazwie PCRM, będący narzędziem do zarządzania relacjami z użytkownikami w obszarze pomocy społecznej. Jest on wykorzystywany m.in. przez Departamentalne Domy Osób Niepełnosprawnych („Maisons départementales des personnes handicapées", MDPH) w niektórych departamentach.

Pod koniec listopada 2022 r. klienci NEXPUBLICA zgłosili do CNIL naruszenia ochrony danych osobowych, ponieważ użytkownicy portalu informowali o możliwości dostępu do dokumentów dotyczących osób trzecich. CNIL przeprowadziła następnie kontrolę w firmie, która wykazała, że wdrożone przez nią środki techniczne i organizacyjne mające zapewnić bezpieczeństwo danych przetwarzanych za pośrednictwem oprogramowania PCRM były niewystarczające.

W konsekwencji komitet ograniczony – organ CNIL odpowiedzialny za nakładanie sankcji – nałożył na NEXPUBLICA FRANCE karę w wysokości 1,7 mln euro, biorąc pod uwagę możliwości finansowe firmy, brak znajomości podstawowych zasad bezpieczeństwa, liczbę osób dotkniętych naruszeniem oraz wrażliwość przetwarzanych danych (w szczególności ujawniających niepełnosprawność).

Naruszenie obowiązku zapewnienia bezpieczeństwa danych osobowych (art. 32 RODO)

Artykuł 32 RODO stanowi, że administrator i podmiot przetwarzający muszą wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić poziom bezpieczeństwa odpowiadający ryzyku, uwzględniając stan wiedzy technicznej, koszty wdrożenia, charakter, zakres, kontekst i cele przetwarzania, a także ryzyko naruszenia praw i wolności osób fizycznych.

Komitet ograniczony uznał, że firma nie spełniła tych wymogów przy wdrażaniu PCRM, biorąc pod uwagę ogólną słabość systemu informatycznego oraz zaniedbania, które doprowadziły do utrzymywania się strukturalnych problemów z bezpieczeństwem.

Stwierdzono, że zidentyfikowane w PCRM podatności:

- wynikały głównie z braku znajomości aktualnych standardów i podstawowych zasad bezpieczeństwa,
- były znane i zidentyfikowane przez firmę w kilku raportach audytowych.

Pomimo tych ustaleń luki zostały usunięte dopiero po wystąpieniu naruszeń danych.

Okoliczności te są szczególnie obciążające ze względu na profil działalności firmy, która specjalizuje się w systemach IT i doradztwie w zakresie oprogramowania.

Komitet ograniczony nie wydał nakazu doprowadzenia do zgodności, ponieważ firma podjęła niezbędne działania naprawcze po naruszeniach danych.

Źródło:

Komunikat francuskiego organu nadzorczego

Data security: NEXPUBLICA FRANCE fined €1,700,000 | CNIL

OŚWIADCZENIE IRLANDZKIEJ KOMISJI OCHRONY DANYCH WS. SZKOLENIA MODELI AI PRZEZ LINKEDIN

Irlandzka Komisja Ochrony Danych (DPC) prowadzi stały dialog z wieloma firmami znajdującymi się w czołówce rozwoju sztucznej inteligencji, koncentrując się na zapewnieniu odpowiedzialnego tworzenia i wdrażania tej technologii dla użytkowników w całej UE/EOG.

W marcu 2025 r. LinkedIn poinformował DPC o zamiarze szkolenia własnych, zastrzeżonych modeli generatywnej AI z wykorzystaniem danych osobowych członków LinkedIn z UE/EOG, począwszy od początku listopada 2025 r. Po szczegółowej analizie dokumentacji dotyczącej ochrony danych dostarczonej przez LinkedIn oraz szeroko zakrojonych konsultacjach bezpośrednich DPC zidentyfikowała szereg ryzyk i innych problemów związanych z proponowanym przetwarzaniem danych osobowych przez firmę. DPC przekazała te zastrzeżenia oraz przedstawiła LinkedIn wiele zaleceń mających na celu ograniczenie potencjalnego negatywnego wpływu planowanych działań na prawa osób, których dane dotyczą.

W rezultacie LinkedIn wprowadził liczne zmiany do swojego planu, w tym m.in.:

- ulepszone komunikaty dotyczące przejrzystości, pomagające użytkownikom zrozumieć, jakie dane osobowe LinkedIn będzie przetwarzać w celu szkolenia swoich modeli AI oraz jak mogą oni zrezygnować z takiego przetwarzania, jeśli sobie tego życzą;
- ograniczenie zakresu danych osobowych, które LinkedIn zamierzał wykorzystywać do szkolenia modeli – zarówno pod względem rodzaju danych, jak i okresu, z którego miały być pozyskiwane;
- ulepszone środki zapobiegające wykorzystaniu danych osobowych użytkowników LinkedIn poniżej 18. roku życia do szkolenia modeli;
- ulepszone środki ochrony użytkowników, w tym wdrożenie filtrów zapobiegających gromadzeniu potencjalnie wrażliwych informacji udostępnianych na niektórych stronach i w Grupach LinkedIn, w tym treści związanych ze związkami zawodowymi;
- dostarczenie bardziej szczegółowych ocen ryzyka oraz innej wymaganej dokumentacji zgodnej z RODO, takich jak ocena prawnie uzasadnionego interesu, ocena skutków dla ochrony danych oraz ocena zgodności.

Podobnie jak w przypadku innych administratorów DPC wymaga również od LinkedIn przygotowania raportu w ciągu pięciu miesięcy od rozpoczęcia przetwarzania. Raport ten ma zawierać m.in. zaktualizowaną ocenę skuteczności i adekwatności wdrożonych środków i zabezpieczeń dotyczących prowadzonego przetwarzania.

DPC będzie nadal aktywnie monitorować wdrażanie tego procesu przez LinkedIn, aby zapewnić wszystkim możliwość sprawowania kontroli nad swoimi danymi osobowymi. Użytkownicy powinni otrzymać powiadomienia od LinkedIn, informujące o sposobach skorzystania z prawa do sprzeciwu na mocy RODO poprzez rezygnację z wykorzystywania ich danych osobowych do szkolenia modeli AI LinkedIn. Można to zrobić za pomocą dedykowanego przełącznika w ustawieniach konta lub poprzez formularz sprzeciwu wobec przetwarzania danych dostępny w LinkedIn.

Przypominamy wszystkim osobom korzystającym z platform internetowych o konieczności regularnego przeglądania ustawień prywatności i kontroli, aby odzwierciedlały one ich aktualne preferencje.

Celem DPC w całym tym procesie było zapewnienie, że LinkedIn wdraża innowacje w sposób odpowiedzialny, ograniczając zidentyfikowane szkody i ryzyka dla osób oraz właściwie uwzględniając prawa osób, których dane dotyczą, poprzez równoważenie i ochronę ich podstawowych praw w zestawieniu z interesami firmy.

DPC nie zatwierdziła ani nie uznała za zgodne z przepisami wykorzystywania danych osobowych użytkowników przez LinkedIn do szkolenia generatywnych modeli AI. Jednak dodatkowe środki wdrożone przez LinkedIn wystarczająco rozwiązały zgłoszone przez DPC obawy, tak że dalsza interwencja regulacyjna nie jest obecnie uznawana za konieczną. DPC będzie nadal monitorować zgodność LinkedIn z RODO i podejmie dalsze działania regulacyjne, jeśli zajdzie taka potrzeba.

DPC, jako wiodący organ nadzorczy dla wielu dużych globalnych firm technologicznych mających główną siedzibę w Irlandii, nadal prowadzi regulacje w sposób sprawiedliwy, spójny i przejrzysty, dążąc do zapewnienia, że rozwój i wdrażanie wszystkich modeli AI w UE/EOG są traktowane w jednakowy sposób.

Źródło:

Komunikat irlandzkiego organu nadzorczego

DPC statement on LinkedIn AI Training | 07/11/2025 | Data Protection Commission

TABLICE REJESTRACYJNE – PRZYPADEK UPUBLICZNIENIA PONAD 30 ZDJĘĆ NA PROFILU W SIECI X

Trzy skargi złożone niezależnie od siebie przez osoby fizyczne spowodowały wszczęcie postępowania administracyjnego z urzędu przez czeski organ nadzorczy.

Do czeskiego Urzędu Ochrony Danych Osobowych w okresie od lipca do września 2022 r. trafiły niezależnie od siebie trzy skargi osób fizycznych na przetwarzanie danych osobowych poprzez publiczne udostępnienie zdjęć ponad 30 tablic rejestracyjnych za pomocą sieci Twitter (obecnie X). Organ nadzorczy postanowił wszcząć postępowanie z urzędu i następnie zebrał materiał dowodowy potwierdzający treść uprzednich skarg – zdjęcia przedstawiały samochody z widocznymi tablicami rejestracyjnymi, które nie były w żaden sposób zamazane lub zasłonięte.

W toku postępowania wykazano, że fotografie zostały upublicznione przez radnego jednej z dzielnic Pragi, który w złożonych wyjaśnieniach wskazał, że jedynie udostępnił w sieci X materiał otrzymany od osoby trzeciej za pomocą komunikatora Whatsapp i oprócz publikacji zdjęć na swoim profilu nie miał zamiaru ich przetwarzania. Organ nadzorczy stwierdził nadto, że konto, którym radny się posługiwał, zostało usunięte z końcem 2024 r., co uniemożliwiło organowi skorzystanie z przysługujących mu uprawnień naprawczych.

Czeski Urząd Ochrony Danych Osobowych wydał następnie decyzję stwierdzającą naruszenie przepisów czeskiej ustawy z 12 marca 2019 r. o przetwarzaniu danych osobowych (110/2019 Sb.) poprzez udostępnienie 32 zdjęć samochodów wraz z widocznymi na nich tablicami rejestracyjnymi, co uczynił mimo braku wyrażonej zgody przez poszczególne osoby. Drugim naruszeniem wskazanym przez organ nadzorczy było niespełnienie obowiązku informacyjnego wobec osób, których dane osobowe zostały udostępnione poprzez publikację zdjęć w sieci X. Organ nadzorczy podjął decyzję o nałożeniu kary administracyjnej w wysokości 40 tys. koron czeskich (ok. 7 tys. zł).

W skardze na decyzję podmiot wskazał, że miał uzasadniony interes prawny w przetwarzaniu danych osobowych, polegający na zamiarze rozpoczęcia debaty publicznej o naruszeniach reguł i zasad prawa drogowego w Pradze. Skarżony oparł swoją argumentację na braku porównania wagi jego interesu prawnego z interesem prawnym skarżących.

Odnośnie do przedmiotu postępowania Skarżony wskazał, że mimo uznania, na gruncie rozstrzygnięć czeskiego organu nadzorczego, tablic rejestracyjnych za źródło danych osobowych jego zdaniem jest to jedynie pośrednia forma identyfikatora, który samodzielnie nie jest wystarczający do konkretyzacji właściciela lub posiadacza pojazdu i w tym celu wymaga dodatkowych danych. Skarżony podtrzymał swoje stanowisko, że sama tablica rejestracyjna ma jedynie pośrednie cechy danych osobowych, wskazał również, że jego działanie nie miało znamion szkodliwości społecznej i nie było źródłem żadnej konkretnej szkody po stronie podmiotów danych osobowych upublicznionych na zdjęciach w sieci X.

W skardze na decyzję Skarżony wskazał również na wysokość, nieproporcjonalność i nieadekwatność kary administracyjnej, żądając jej obniżenia do 1 tys. koron czeskich (ok. 180 zł).

W odpowiedzi na skargę organ nadzorczy podtrzymał swoje stanowisko odnośnie do uznania tablic rejestracyjnych za źródło danych osobowych, argumentując, że „numery rejestracyjne" stanowią przedmiot Rejestru Pojazdów, który jest prowadzony przez właściwe w tym zakresie ministerstwo. W wyroku z 12 lutego 2009 r. czeski Najwyższy Sąd Administracyjny (odpowiednik polskiego Naczelnego Sądu Administracyjnego) rozstrzygnął, że możliwość identyfikacji właściciela pojazdu poprzez odczytanie numeru rejestracyjnego w Rejestrze Pojazdów pozwala na bezpośrednie wskazanie osoby fizycznej – właściciela lub posiadacza pojazdu. Organ nadzorczy dodał również, że czeski Najwyższy Sąd Administracyjny w wyroku z 13 sierpnia 2020 r. (AS 387/2019-56) potwierdził, że numery rejestracyjne są danymi osobowymi, ponieważ pojęcie danych osobowych powinno być interpretowane w sposób obiektywny, tzn. znamiona tego pojęcia nie mogą być definiowane przez administratora, który w danej chwili nimi dysponuje, ale należy zbadać, czy oprócz nich istnieją dodatkowe informacje, które razem z nią mogą doprowadzić do identyfikacji podmiotu danych osobowych. Organ nadzorczy idąc w ślad za orzecznictwem sądu administracyjnego, potwierdził swoje stanowisko, że jeśli dana informacja pozwala jakiejkolwiek osobie lub organowi władzy publicznej na identyfikację osoby, to mamy do czynienia z danymi osobowymi.

W postanowieniu odwoławczym od decyzji organu nadzorczego uznano, że żadna z przesłanek tzw. testu równowagi nie pozwala na stwierdzenie, że publikowanie zdjęć samochodów i umieszczonych na nich tablic rejestracyjnych było właściwe do osiągnięcia określonego celu (w tym wypadku publicznej dyskusji o niedogodnościach komunikacyjnych oraz naruszenia prawa drogowego). Po pierwsze, sfotografowane samochody były zaparkowane legalnie, nie znajdowały się w strefach płatnego parkowania lub w strefach przeznaczonych dla wybranej grupy mieszkańców.

Zdaniem organu nadzorczego działanie skarżonego stało w sprzeczności z deklarowanym celem i uznał, że mogło doprowadzić do wzrostu napięcia społecznego lub stygmatyzacji tych konkretnych osób – właścicieli lub posiadaczy tych pojazdów. Organ nadzorczy nie podjął również polemiki z argumentem niskiej szkodliwości społecznej podniesionym przez skarżącego, ponieważ kwestia pozostawała poza jego właściwością i w procesie rozstrzygania o naruszeniu praw i obowiązków w zakresie przetwarzania danych osobowych tą kwestią w ogóle się nie zajmował. Decyzja organu nadzorczego pozostała w mocy oprócz kwestii wymiaru kary administracyjnej – w tym zakresie zadecydowano o obniżeniu wysokości kary administracyjnej do 10 000 koron (ok. 1800 zł), przy czym na obniżenie jej wysokości miały wpływ sytuacja finansowa i warunki osobiste skarżonego. Organ podniósł jednak argument, że kara administracyjna ma mieć charakter nie tylko prewencyjny, ale także represyjny, co wykluczyło możliwość odstąpienia od jej nałożenia.

Robert Karsznia

Źródło:

Úřad pro ochranu osobních údajů (czeskiego organu nadzorczego)

Ostateczna decyzja organu: UOOU-02771/22-28 z dnia 14 października 2024 r.

Decyzja organu wydana w postępowaniu odwoławczym: UOOU-02771/22-34 z 4 lipca 2025 r.

AGENCJA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ SYSTEM WJAZDU/WYJAZDU: WYTYCZNE DLA STRAŻY GRANICZNEJ DOT. PRAW PODSTAWOWYCH (TŁUMACZENIE MASZYNOWE)

Treść

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

System Wjazdu/Wyjazdu a prawa podstawowe

System Wjazdu/Wyjazdu (EES) jest wielkoskalowym systemem informacyjnym Unii Europejskiej służącym do rejestrowania wjazdu i wyjazdu obywateli państw trzecich przebywających na krótkich pobytach w strefie Schengen. Podstawę prawną tego systemu stanowi rozporządzenie w sprawie EES (rozporządzenie (UE) 2017/2226, z późniejszymi zmianami), które rejestruje i przechowuje dane osobowe, w tym wizerunki twarzy i odciski palców. System Wjazdu/Wyjazdu, zaprojektowany w celu wzmocnienia zarządzania granicami i poprawy skuteczności kontroli migracji, zastępuje ręczne stemplowanie paszportów na granicach zautomatyzowanym gromadzeniem i weryfikacją danych.

Komisja Europejska szacuje, że dane dotyczące ok. 300 mln przypadków przekroczenia granicy przez obywateli państw trzecich będą rejestrowane w EES rocznie – zauważając, że liczba ta odnosi się do poszczególnych przypadków przekroczenia granicy, a nie do osób. Zgodnie z decyzją wykonawczą Komisji (UE) 2025/1544 EES zacznie działać 12 października 2025 r. Zgodnie z rozporządzeniem (UE) 2025/1534 nie wszystkie funkcje EES zostaną wdrożone w pierwszym sześciomiesięcznym progresywnym okresie początkowym.

Chociaż EES obiecuje korzyści operacyjne, jego wdrożenie ma również znaczący wpływ na prawa podstawowe obywateli państw trzecich. Wymaga to środków łagodzących, np. zmniejszenia trudności dla pasażerów wymagających szczególnego traktowania. System ten obejmuje szeroki zakres praw zapisanych w Karcie Praw Podstawowych Unii Europejskiej („Karta”), w tym: godności ludzkiej (art. 1), poszanowania życia prywatnego i rodzinnego (art. 7), ochrony danych osobowych (art. 8), niedyskryminacji (art. 21) oraz szczególnej ochrony dzieci, osób w podeszłym wieku i osób niepełnosprawnych (art. 24–26). Może również wpływać na prawo do azylu (art. 18) i zasadę non-refoulement (art. 19).

Wykonywanie prawa do skutecznego środka prawnego (art. 47) od nieprawidłowych decyzji opartych na rejestrach EES jest również kwestią kluczową – biorąc pod uwagę, że pomimo zabezpieczeń mogą wystąpić błędy w dopasowywaniu danych biometrycznych. Wskaźnik fałszywych wyników nigdy nie będzie zerowy. W przypadku systemu, który przetwarza setki milionów rekordów, nawet bardzo mały poziom błędu wpływa na znaczną liczbę osób.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Prawa wynikające z karty, które są zawarte w Europejskiej Konwencji Praw Człowieka (EKPC) i jej protokołach, należy interpretować w taki sam sposób jak równoważne prawa wynikające z EKPC, zgodnie z art. 52 ust. 3 Karty. Oznacza to, że przy określaniu znaczenia i treści praw określonych zarówno w Karcie, jak i w EKPC należy uwzględnić orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPC). Dotyczy to wielu praw wynikających z Karty.

Samo rozporządzenie w sprawie EES zawiera liczne zabezpieczenia praw podstawowych, które należy wdrożyć podczas obsługi systemu. W przypadku obywateli państw trzecich decyzje oparte na danych EES muszą być przejrzyste i sprawiedliwe. Obywatele państw trzecich o szczególnych potrzebach, tacy jak dzieci, nie powinni ponosić dodatkowego obciążenia (art. 10), a w celu zapewnienia dokładności danych (art. 35 i 39), dostępu do informacji (art. 50) oraz prawa do sprostowania lub dochodzenia roszczeń (art. 52) należy wprowadzić skuteczne zabezpieczenia. Zabezpieczenia te nie tylko wypełniają zobowiązania prawne, ale także zwiększają niezawodność i funkcjonalność samego systemu.

System Wjazdu/Wyjazdu jest jednym z sześciu wielkoskalowych systemów informacyjnych, które UE tworzy w celu wspierania zarządzania azylem, granicami i imigracją, policji i bezpieczeństwa wewnętrznego. Systemy te staną się interoperacyjne, co oznacza, że odpowiedzialne organy będą miały dostęp do niektórych danych lub będą mogły je przeglądać we wszystkich systemach, np. w celu ustalenia tożsamości obywatela państwa trzeciego. Luki w wiarygodności i dokładności danych w EES mogą zatem prowadzić do niekorzystnych skutków dla osób fizycznych w innych procedurach, takich jak procedury azylowe lub imigracyjne, w ujęciu bardziej ogólnym. Przegląd zagrożeń dla praw podstawowych i możliwości związanych z wielkoskalowymi systemami informatycznymi UE można znaleźć na internetowej platformie informacyjnej poświęconej unijnym systemom informatycznym do celów migracji i policji oraz ich interoperacyjności, którą Agencja Praw Podstawowych Unii Europejskiej (FRA) opublikowała w 2024 r. Platforma informuje obywateli państw trzecich, prawników i organizacje społeczeństwa obywatelskiego o głównych cechach unijnych systemów informatycznych i zawiera wskazówki, jak pomóc osobom, których dane dotyczą, w korzystaniu z przysługujących im praw.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Wytyczne Agencji Praw Podstawowych Unii Europejskiej

Na podstawie badań przeprowadzonych w okresie od maja do września 2024 r. Agencja Praw Podstawowych UE (FRA) opracowała zestaw zagadnień dotyczących praw podstawowych związanych z funkcjonowaniem systemu EES, które były przedmiotem konsultacji z praktykami i ekspertami podczas warsztatów we wrześniu 2024 r. oraz w trakcie szkoleń organizowanych przez Europejską Agencję Straży Granicznej i Przybrzeżnej.

Niniejsze wytyczne są przeznaczone dla funkcjonariuszy straży granicznej w państwach członkowskich UE, którzy pracują na poziomie operacyjnym. Dotyczy to przede wszystkim personelu pracującego przy kontrolach pierwszej linii. Jego celem jest wspieranie funkcjonowania systemu wjazdu/wyjazdu zgodnego z prawami podstawowymi.

Wytyczne dla straży granicznej koncentrują się na czterech obszarach operacyjnych, które w badaniach uznano za najistotniejsze dla ochrony praw podstawowych:

- informowanie obywateli państw trzecich;
- przetwarzanie danych osobowych;
- wspieranie obywateli państw trzecich o szczególnych potrzebach;
- traktowanie osób przekraczających dozwolony okres pobytu.

Nadal mają zastosowanie zabezpieczenia przewidziane w innych instrumentach prawnych UE, takich jak kodeks graniczny Schengen. Żadne z postanowień niniejszych wytycznych nie ogranicza obowiązujących standardów i zabezpieczeń w zakresie praw podstawowych ani nie wpływa na nie niekorzystnie.

Wytyczne te uzupełniają wytyczne FRA z 2020 r. „Kontrole graniczne a prawa podstawowe na lądowych granicach zewnętrznych”, które mają ogólne zastosowanie do zadań związanych z zarządzaniem granicami i nie odnoszą się do zadań związanych z EES.

Niniejsze wytyczne są publikowane wraz z osobną publikacją wytycznych dla kadry kierowniczej EES i kadry kierowniczej wyższego szczebla na przejściach granicznych, System Wjazdu/Wyjazdu: Wytyczne dla kadry kierowniczej dot. praw podstawowych, 2025 r. Zawiera on wybrane kluczowe wyniki badań.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Metodologia badań

FRA przeprowadziła badania i wniosła wiedzę specjalistyczną w zakresie praw podstawowych do działań szkoleniowych dotyczących EES, ponieważ system ten będzie przetwarzał dane osobowe, w tym wrażliwe dane biometryczne, setek milionów obywateli państw spoza UE każdego roku.

Badania FRA miały na celu zebranie doświadczeń i oczekiwań praktyków i ekspertów w kwestiach istotnych dla wdrożenia EES. Badania objęły gromadzenie i przetwarzanie danych biometrycznych na granicach, np. za pośrednictwem zautomatyzowanych bramek kontroli granicznej, dostarczanie informacji obywatelom państw trzecich lub zarządzanie kolejkami w miejscach o ograniczonej przestrzeni.

Od maja do września 2024 r. FRA gromadziła doświadczenia funkcjonariuszy straży granicznej, organów krajowych, organów ochrony danych i ekspertów ds. praw podstawowych. Badania terenowe przeprowadzono w sześciu państwach członkowskich UE; obejmowały one dziewięć punktów kontroli granicznej na granicach powietrznych, morskich i lądowych z odpowiednim doświadczeniem w przetwarzaniu danych biometrycznych na granicach. Dokładniej rzecz ujmując, zrealizowano następujące zadania badawcze.

- Przeprowadzono wywiady z 30 organami i ekspertami na szczeblu krajowym, po pięciu w każdym z następujących państw członkowskich: Bułgaria, Estonia, Francja, Niemcy, Włochy i Polska.

- W dziewięciu punktach kontroli granicznej przeprowadzono wywiady z 61 kierownikami zmian i 25 innymi zainteresowanymi stronami, takimi jak operatorzy portów lotniczych, przedsiębiorstwa transportowe i organizacje pozarządowe. W tych punktach kontroli granicznej straż graniczna zaoferowała dla badaczy oględziny z przewodnikiem, co umożliwiło przeprowadzenie obserwacji uczestniczącej.

- Na dziewięciu przejściach granicznych, obejmujących łącznie 177 funkcjonariuszy straży granicznej, przeprowadzono ankietę.

- Pracownicy FRA odwiedzili pięć punktów kontroli granicznej (lotniska we Frankfurcie i Wiedniu, terminal Eurostar we Francji oraz porty w Marsylii i Bari), obserwując i omawiając przygotowania do EES z odpowiednimi organami państw członkowskich.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Badania przeprowadzono w następujących punktach kontroli granicznej:

- Bułgaria – Kapitan Andreewo (przejście graniczne) i port lotniczy w Sofii;
- Estonia – Narwa (lądowy punkt graniczny);
- Francja – port w Marsylii i przejście graniczne Eurostar;
- Włochy – port lotniczy Rzym-Fiumicino i port w Bari; oraz
- Polska – Medyka (przejście graniczne) i port lotniczy w Warszawie.

Wyniki badań stanowiły punkt wyjścia do opracowania niniejszych wytycznych FRA.

1. Informowanie obywateli państw trzecich w sposób godny i pełen szacunku

a) Wytyczne

- **Wytyczne 1.1:** Bądź świadomy informacji dotyczących EES, które obywatele państw trzecich muszą otrzymać przy wjeździe do strefy Schengen.
- **Wytyczne 1.2:** Uczestnicz regularnie w szkoleniach dotyczących EES, jego wpływu na prawa podstawowe oraz umiejętności komunikacyjnych.
- **Wytyczne 1.3:** Sprawdzaj, czy standardowy wzór informacji o EES oraz dane kontaktowe administratora, inspektora ochrony danych i organów nadzorczych są widocznie wywieszone i zawsze dostępne w wystarczającej liczbie egzemplarzy.
- **Wytyczne 1.4:** Systematycznie sprawdzaj, czy obywatele państw trzecich rozumieją, jakie dane osobowe są przetwarzane i w jakim celu, kto będzie miał do nich dostęp i z nich korzystał oraz jak długo dane będą przechowywane. Sprawdź również, czy rozumieją, że mają prawo dostępu do swoich danych oraz prawo żądania ich sprostowania.
- **Wytyczne 1.5:** Zachowuj życzliwość i oferuj wsparcie, gdy obywatele państw trzecich mają trudności ze zrozumieniem, jakie informacje muszą przekazać i dlaczego.
- **Wytyczne 1.6:** Odpowiadaj na pytania jasno i uprzejmie, używając języka zrozumiałego dla obywateli państw trzecich.
- **Wytyczne 1.7:** W razie potrzeby korzystaj ze wsparcia mediatorów kulturowych lub innego personelu pomocniczego w celu ułatwienia komunikacji albo identyfikacji i skierowania osób wymagających szczególnej ochrony.
- **Wytyczne 1.8:** Udzielaj jasnych i wyczerpujących odpowiedzi na pytania dotyczące sposobu sprostowania, poprawienia lub usunięcia danych oraz tego, z kim należy się kontaktować w sprawie skarg. W razie potrzeby wezwij przełożonego.

b. Odniesienia prawne

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2017/2226 z dnia 30 listopada 2017 r. ustanawiające system wjazdu/wyjazdu (EES) w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich i danych dotyczących odmowy wjazdu w odniesieniu do takich obywateli oraz określające warunki dostępu do EES na potrzeby ochrony porządku publicznego i zmieniające konwencję wykonawczą do układu z Schengen i rozporządzenia (WE) nr 767/2008 i (UE) nr 1077/2011, Dz.U. UE L 327 z 9.12.2017, s. 20, art. 38 ust. 5 i art. 50.

2. Przetwarzaj dane osobowe z poszanowaniem prywatności i godności

a) Wytyczne

- **Wytyczne 2.1:** Ogranicz ingerencję w prywatność podczas pobierania danych biometrycznych, np. poprzez stosowanie osłon ochronnych lub zapewnienie osłoniętej przestrzeni obywatelom państw trzecich wymagającym szczególnej pomocy, jeżeli jest to zasadne.
- **Wytyczne 2.2:** Zachowuj wrażliwość na wiek, płeć oraz tło kulturowe danej osoby.
- **Wytyczne 2.3:** Zachowuj szczególną czujność przy pobieraniu danych biometrycznych od niektórych grup, które mogą napotykać trudności związane z wiarygodnością danych, np. dzieci, osób o ciemniejszym odcieniu skóry lub osób z urazami twarzy, traktując je z poszanowaniem godności przy jednoczesnym zapewnieniu standardów jakości danych biometrycznych.
- **Wytyczne 2.4:** Rozważ wykorzystanie sprzętu mobilnego do wykonywania zdjęć twarzy lub pobierania odcisków palców, w szczególności w przypadku obywateli państw trzecich o ograniczonej mobilności, podróżujących samochodem.
- **Wytyczne 2.5:** Niezwłocznie koryguj błędy (np. nieprawidłowe daty lub błędy w pisowni) po ich wykryciu lub zgłoszeniu, zgodnie z ustaloną procedurą.
- **Wytyczne 2.6:** Bezzwłocznie przekazuj do dalszej weryfikacji wnioski o sprostowanie wymagające dodatkowego sprawdzenia, zgodnie z ustaloną procedurą, oraz informuj o tym obywatela państwa trzeciego.

b) Odniesienia prawne

- Karta praw podstawowych Unii Europejskiej, art. 1, art. 8, art. 21 ust. 1, art. 22 i art. 24.
- Rozporządzenie (UE) 2017/2226 ws. EES, art.10, art. 38 i art. 57.
- Decyzja wykonawcza Komisji (UE) 2019/329 z dnia 25 lutego 2019 r. określająca specyfikacje dotyczące jakości, rozdzielczości oraz wykorzystania odcisków palców i wizerunku twarzy na potrzeby weryfikacji i identyfikacji biometrycznej w nowym systemie wjazdu/wyjazdu (EES), Dz.U. UE L 57 z 26.2.2019, s. 18–28.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. UE L 119 z 4.5.2016, s. 1–88, rozdział 3.

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. UE L 119 z 4.5.2016, s. 89–131, rozdział 3.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/817 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze granic i polityki wizowej oraz zmieniające rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 767/2008, (UE) 2016/399, (UE) 2017/2226, (UE) 2018/1240, (UE) 2018/1726, (UE) 2018/1861 oraz decyzje Rady 2004/512/WE i 2008/633/WSiSW, Dz.U. UE L 135 z 22.5.2019, s. 27–84.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/818 z dnia 20 maja 2019 r. w sprawie ustanowienia ram interoperacyjności systemów informacyjnych UE w obszarze współpracy policyjnej i sądowej, azylu i migracji oraz zmieniające rozporządzenia (UE) 2018/1726, (UE) 2018/1862 i (UE) 2019/816, Dz.U. UE L 135 z 22.5.2019, s. 85, art. 47–48.

3. Bądź wrażliwy na osoby o szczególnych potrzebach

a) Wytyczne

- **Wytyczne 3.1:** Zachowuj czujność wobec oznak stresu lub dyskomfortu oraz udzielaj wsparcia obywatelom państw trzecich o szczególnych potrzebach, takim jak dzieci, osoby starsze oraz osoby z niepełnosprawnościami.
- **Wytyczne 3.2:** Zapewnij, aby osoby z niepełnosprawnościami oraz osoby o ograniczonych umiejętnościach cyfrowych miały dostęp do informacji i mogły je zrozumieć.
- **Wytyczne 3.3:** Zapewnij dodatkowy czas i/lub pomoc oraz stosuj dostępne procedury alternatywne (np. odroczenie pobrania danych biometrycznych do momentu wyjazdu danej osoby z UE w przypadku tymczasowych urazów lub pozyskanie wizerunku twarzy z chipa paszportu), gdy pobranie danych biometrycznych jest niemożliwe lub utrudnione z powodu urazów, niepełnosprawności, wieku lub innych cech fizycznych.
- **Wytyczne 3.4:** Zaproponuj bardziej dyskretne pobranie danych od podróżnych, którzy odczuwają dyskomfort związany z procesem gromadzenia danych z powodu niepełnosprawności, stroju religijnego lub innych przyczyn.
- **Wytyczne 3.5:** Używaj języka przyjaznego dzieciom w kontaktach z dziećmi.
- **Wytyczne 3.6:** Stosuj ustalone procedury kierowania do odpowiednich form wsparcia w przypadku obywateli państw trzecich wymagających pomocy, np. gdy potrzebują oni większej prywatności, dodatkowego czasu lub wsparcia tłumacza.

b) Odniesienia prawne

- Karta praw podstawowych Unii Europejskiej, art.1, art. 21 ust. 1, art. 22, art. 24, art. 25, art. 26.
- Rozporządzenie (UE) 2017/2226 ws. EES, art. 10 ust. 2, art. 17 ust. 3.

4) Traktuj osoby przekraczające okres dozwolonego pobytu z szacunkiem i nie wyciągaj pochopnych wniosków

a) Wytyczne

- **Wytyczne 4.1:** W życzliwy sposób poinformuj obywateli państw trzecich o fakcie, że dana osoba przekroczyła okres dozwolonego pobytu, oraz o możliwych konsekwencjach tego faktu.
- **Wytyczne 4.2:** Umożliwiaj obywatelom państw trzecich przedstawienie dowodów w celu obalenia domniemania wcześniejszego nielegalnego wjazdu lub przekroczenia okresu dozwolonego pobytu oraz poinformuj ich o takiej możliwości.
- **Wytyczne 4.3:** Nie przyjmuj dokładności danych EES jako pewnika. Pamiętaj, że ryzyko błędów może występować pomimo zastosowania zabezpieczeń technologicznych, a odsetek wyników fałszywych nigdy nie będzie zerowy.
- **Wytyczne 4.4:** Przekaż informacje o prawie do odwołania oraz o sposobach kontaktu z właściwymi służbami w celu uzyskania wsparcia w przypadku odmowy wjazdu, zgodnie z art. 14 ust. 3 Kodeksu granicznego Schengen.
- **Wytyczne 4.5:** Kieruj osoby wyrażające wolę ubiegania się o azyl, w tym osoby przekraczające okres dozwolonego pobytu lub osoby, które nie wydają się spełniać warunków wjazdu, do krajowej procedury azylowej oraz respektuj zasadę non-refoulement.

b) Odniesienia prawne

- Karta praw podstawowych Unii Europejskiej, art. 1, art. 18, art. 19 ust. 2, art. 21 ust. 1.
- Rozporządzenie (UE) 2017/2226 ws. EES, art.2 ust. 3, art. 9 ust. 2, art. 10 art. 12 ust. 3, art. 41.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 z dnia 9 marca 2016 r. w sprawie unijnego kodeksu zasad regulujących przepływ osób przez granice (kodeks graniczny Schengen), Dz.U. UE L 77 z 23.3.2016, s. 1, art. 2 pkt 16 i art. 14 ust. 3.
- Dyrektywa Parlamentu Europejskiego i Rady 2013/32/UE z dnia 26 czerwca 2013 r. w sprawie wspólnych procedur udzielania i cofania ochrony międzynarodowej (przekształcenie) Dz.U. UE L 180 z 29.6.2013, s. 60–95, motyw 18, art. 31 ust. 2 i art. 43, od lipca 2026 r.: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1348 z dnia 14 maja 2024 r. w sprawie ustanowienia wspólnej procedury ubiegania się o ochronę międzynarodową w Unii i uchylenia dyrektywy 2013/32/UE, Dz. U. UE L z 22.05.2024 r., art. 34 ust. 2 i art. 43.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

- Dyrektywa Parlamentu Europejskiego i Rady 2011/95/UE z dnia 13 grudnia 2011 r. w sprawie norm dotyczących kwalifikowania obywateli państw trzecich lub bezpaństwowców jako beneficjentów ochrony międzynarodowej, jednolitego statusu uchodźców lub osób kwalifikujących się do otrzymania ochrony uzupełniającej oraz zakresu udzielanej ochrony (wersja przekształcona), Dz.U. L 337 z 20.12.2011, s. 9–26, art. 25, od lipca 2026 r.: Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1347 z dnia 14 maja 2024 r. w sprawie norm dotyczących kwalifikowania obywateli państw trzecich lub bezpaństwowców jako osób korzystających z ochrony międzynarodowej, jednolitego statusu uchodźców lub osób kwalifikujących się do otrzymania ochrony uzupełniającej oraz zakresu udzielanej ochrony, zmieniające dyrektywę Rady 2003/109/WE oraz uchylające dyrektywę Parlamentu Europejskiego i Rady 2011/95/UE, Dz.U. UE L, poz. 1347z 22.5.2024 r., art. 25.
- Rozporządzenie Rady (WE) nr 1030/2002 z dnia 13 czerwca 2002 r. ustanawiające jednolity wzór dokumentów pobytowych dla obywateli państw trzecich, Dz.U. L 157 z 15.6.2002, s. 1–7, art. 1 ust. 2 lit. a pkt ii.

Informacje o tej publikacji

Luksemburg: Urząd Publikacji Unii Europejskiej, 2025 r.

html

- TK-01-25-032-PL-Q
- ISBN: 978-92-9489-685-8
- DOI: 10.2811/9691582

PDF

- TK-01-25-032-EN-N
- ISBN: 978-92-9489-686-5
- DOI: 10.2811/8877592

Zdjęcia (okładka):

- Okładka: © FRA

FRA – AGENCJA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ

Schwarzenbergplatz 11 – 1040 Wiedeń – Austria

T +43 158030-0 – F +43 158030-699

- Strona internetowa
- LinkedIn
- Instagram
- Facebook
- YouTube
- X

Agencja Praw Podstawowych Unii Europejskiej System Wjazdu/Wyjazdu: Wytyczne dla kadry kierowniczej dot. praw podstawowych *(tłumaczenie maszynowe)*

Treść

4. **Przetwarzanie danych biometrycznych w sposób zgodny z prawem**
   a) Wybrane kluczowe wnioski
   b) Odniesienia prawne
   c) Wytyczne
   d) Więcej informacji

5. **Wspieranie obywateli państw spoza UE o szczególnych potrzebach**
   a) Wybrane kluczowe ustalenia
   b) Odniesienia prawne
   c) Wytyczne
   d) Więcej informacji

6. **Wykorzystanie danych z Systemu Wjazdu/Wyjazdu zgodnie z prawami podstawowymi**
   a) Wybrane kluczowe wnioski
   b) Odniesienia prawne
   c) Wytyczne
   d) Więcej informacji

7. **Włączenie praw podstawowych do szkoleń**
   a) Wybrane kluczowe wnioski
   b) Odniesienia prawne
   c) Wytyczne
   d) Więcej informacji

8. **Przypisy końcowe**

9. **Informacje o tej publikacji**

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

System Wjazdu/Wyjazdu a prawa podstawowe

System Wjazdu/Wyjazdu (EES) jest wielkoskalowym systemem informacyjnym Unii Europejskiej służącym do rejestrowania wjazdu i wyjazdu obywateli państw trzecich przebywających na krótkich pobytach w strefie Schengen. Podstawę prawną tego systemu stanowi rozporządzenie w sprawie EES (rozporządzenie (UE) 2017/2226, z późniejszymi zmianami), które rejestruje i przechowuje dane osobowe, w tym wizerunki twarzy i odciski palców. System Wjazdu/Wyjazdu, zaprojektowany w celu wzmocnienia zarządzania granicami i poprawy skuteczności kontroli migracji, zastępuje ręczne stemplowanie paszportów na granicach zautomatyzowanym gromadzeniem i weryfikacją danych.

Komisja Europejska szacuje, że dane dotyczące ok. 300 mln przypadków przekroczenia granicy przez obywateli państw trzecich będą rejestrowane w EES rocznie – zauważając, że liczba ta odnosi się do poszczególnych przypadków przekroczenia granicy, a nie do osób. Zgodnie z decyzją wykonawczą Komisji (UE) 2025/1544 EES zacznie działać 12 października 2025 r. Zgodnie z rozporządzeniem (UE) 2025/1534 nie wszystkie funkcje EES zostaną wdrożone w pierwszym sześciomiesięcznym progresywnym okresie początkowym.

Chociaż EES obiecuje korzyści operacyjne, jego wdrożenie ma również znaczący wpływ na prawa podstawowe obywateli państw trzecich. Wymaga to środków łagodzących, np. zmniejszenia trudności dla pasażerów wymagających szczególnego traktowania. System ten obejmuje szeroki zakres praw zapisanych w Karcie Praw Podstawowych Unii Europejskiej („Karta”), w tym: godności ludzkiej (art. 1), poszanowania życia prywatnego i rodzinnego (art. 7), ochrony danych osobowych (art. 8), niedyskryminacji (art. 21) oraz szczególnej ochrony dzieci, osób w podeszłym wieku i osób niepełnosprawnych (art. 24–26). Może również wpływać na prawo do azylu (art. 18) i zasadę *non-refoulement* (art. 19).

Wykonywanie prawa do skutecznego środka prawnego (art. 47) od nieprawidłowych decyzji opartych na rejestrach EES jest również kwestią kluczową – biorąc pod uwagę, że pomimo zabezpieczeń mogą wystąpić błędy w dopasowywaniu danych biometrycznych. Wskaźnik fałszywych wyników nigdy nie będzie zerowy. W przypadku systemu, który przetwarza setki milionów rekordów, nawet bardzo mały poziom błędu wpływa na znaczną liczbę osób.

Prawa wynikające z karty, które są zawarte w Europejskiej Konwencji Praw Człowieka (EKPC) i jej protokołach, należy interpretować w taki sam sposób jak równoważne prawa wynikające z EKPC, zgodnie z art. 52 ust. 3 Karty. Oznacza to, że przy określaniu znaczenia i treści praw określonych zarówno w Karcie, jak i w EKPC należy uwzględnić orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPC). Dotyczy to wielu praw wynikających z Karty.

Samo rozporządzenie w sprawie EES zawiera liczne zabezpieczenia praw podstawowych, które należy wdrożyć podczas obsługi systemu. W przypadku obywateli państw trzecich decyzje oparte na danych EES muszą być przejrzyste i sprawiedliwe. Obywatele państw trzecich o szczególnych potrzebach, tacy jak dzieci, nie powinni ponosić dodatkowego obciążenia (art. 10), a w celu zapewnienia dokładności danych (art. 35 i 39), dostępu do informacji (art. 50) oraz prawa do sprostowania lub dochodzenia roszczeń (art. 52) należy wprowadzić skuteczne zabezpieczenia. Zabezpieczenia te nie tylko wypełniają zobowiązania prawne, ale także zwiększają niezawodność i funkcjonalność samego systemu.

System Wjazdu/Wyjazdu jest jednym z sześciu wielkoskalowych systemów informacyjnych, które UE tworzy w celu wspierania zarządzania azylem, granicami i imigracją, policji i bezpieczeństwa wewnętrznego. Systemy te staną się interoperacyjne, co oznacza, że odpowiedzialne organy będą miały dostęp do niektórych danych lub będą mogły je przeglądać we wszystkich systemach, np. w celu ustalenia tożsamości obywatela państwa trzeciego. Luki w wiarygodności i dokładności danych w EES mogą zatem prowadzić do niekorzystnych skutków dla osób fizycznych w innych procedurach, takich jak procedury azylowe lub imigracyjne, w ujęciu bardziej ogólnym. Przegląd zagrożeń dla praw podstawowych i możliwości związanych z wielkoskalowymi systemami informatycznymi UE można znaleźć na internetowej platformie informacyjnej poświęconej unijnym systemom informatycznym do celów migracji i policji oraz ich interoperacyjności, którą Agencja Praw Podstawowych Unii Europejskiej (FRA) opublikowała w 2024 r. Platforma informuje obywateli państw trzecich, prawników i organizacje społeczeństwa obywatelskiego o głównych cechach unijnych systemów informatycznych i zawiera wskazówki, jak pomóc osobom, których dane dotyczą, w korzystaniu z przysługujących im praw.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Wytyczne Agencji Praw Podstawowych Unii Europejskiej

Na podstawie badań przeprowadzonych od maja do września 2024 r. Agencja Praw Podstawowych UE (FRA) opracowała zestaw zagadnień dotyczących praw podstawowych związanych z funkcjonowaniem systemu EES, które były przedmiotem konsultacji z praktykami i ekspertami podczas warsztatów we wrześniu 2024 r. oraz w trakcie szkoleń organizowanych przez Europejską Agencję Straży Granicznej i Przybrzeżnej.

Niniejsze wytyczne są przeznaczone dla osób odpowiedzialnych za wdrażanie i funkcjonowanie systemu EES. Są one skierowane do personelu ministerstw i/lub organów zarządzania granicami odpowiedzialnego za EES oraz do kadry kierowniczej służb granicznych na przejściach granicznych (BCP).

Chociaż rozporządzenie w sprawie EES (Rozporządzenie (UE) 2017/2226, ze zmianami) oraz praktyczny podręcznik Komisji Europejskiej dla organów krajowych korzystających z EES na podstawie art. 71 rozporządzenia dostarczają niezbędnych informacji do obsługi systemu, niniejsze wytyczne wprowadzają perspektywę praw podstawowych. Przekształcają wymogi prawne w praktyczne wskazówki, opierając się na rzeczywistych wyzwaniach obserwowanych na granicy.

Nie mając charakteru wyczerpującego, wytyczne te dla osób odpowiedzialnych za EES koncentrują się na siedmiu aspektach operacyjnych, które badania wskazały jako najistotniejsze dla ochrony praw podstawowych:

- skuteczne informowanie obywateli państw trzecich;
- traktowanie osób oczekujących na kontrolę graniczną z poszanowaniem godności;
- przestrzeganie przepisów o ochronie danych;
- pobieranie danych biometrycznych w sposób godny;
- wspieranie obywateli państw trzecich o szczególnych potrzebach;
- korzystanie z danych EES zgodnie z prawami podstawowymi;
- uwzględnianie praw podstawowych w szkoleniach.

Dla każdego z tych obszarów wytyczne FRA rozpoczynają się od przedstawienia kontekstu, prezentują wybrane wyniki badań i opisują kluczowe aspekty ram prawnych UE. Same wytyczne, przedstawione w formie punktów, koncentrują się na zagadnieniach, które badania terenowe FRA i związane z nimi dyskusje wskazały jako najistotniejsze. W zależności od krajowej struktury odpowiedzialności administracyjnej duża część wytycznych może również należeć do kompetencji kadry kierowniczej na poziomie BCP. Takie wytyczne są odpowiednio oznaczone i mogą dotyczyć np. kwestii logistycznych, takich jak organizacja systemów samoobsługowej rejestracji i stref oczekiwania, przygotowanie protokołów obowiązujących na całym BCP oraz umów o współpracy, koordynacja zapotrzebowania kadrowego, określanie potrzeb sprzętowych czy organizacja szkoleń. Część wytycznych może również odnosić się do zadań liderów zmian, którzy bezpośrednio nadzorują, kierują i koordynują pracę funkcjonariuszy pierwszej linii oraz nadzorują kontrole drugiego poziomu, przy których pasażerowie podlegają bardziej szczegółowej weryfikacji. Na końcu każdego rozdziału czytelnik znajdzie odnośniki do literatury i materiałów do dalszego zgłębiania tematu.

Niniejsze wytyczne dla osób odpowiedzialnych za EES są publikowane równocześnie z odrębnym opracowaniem wytycznych dla funkcjonariuszy straży granicznej korzystających z EES podczas kontroli pierwszej linii, System Wjazdu/Wyjazdu: Wytyczne dla straży granicznej dotyczące praw podstawowych, 2025 r. Niniejsze wytyczne FRA obowiązują od momentu wdrożenia systemu EES. Niektóre wskazówki zawarte w danej sekcji stają się istotne dopiero po wdrożeniu wszystkich funkcji EES.

Wytyczne te koncentrują się wyłącznie na zagadnieniach związanych z prawami podstawowymi w kontekście funkcjonowania EES w ramach zarządzania granicami i migracjami. Nie obejmują dostępu organów ścigania do EES w celu zwalczania terroryzmu i poważnej przestępczości, gdyż stanowi to odrębny cel, w który zaangażowane są inne organy niż te, do których adresowane są niniejsze wytyczne.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

W kwestiach związanych z zarządzaniem granicami, które nie zostały objęte tymi wytycznymi, czytelnik może odwołać się do następujących publikacji FRA.

- Agencja Praw Podstawowych Unii Europejskiej, Kontrole graniczne a prawa podstawowe na lądowych granicach zewnętrznych – praktyczne wskazówki, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020 r. Są to praktyczne wskazówki dla funkcjonariuszy straży granicznej.
- Rada Europy, Europejski Trybunał Praw Człowieka i Agencja Praw Podstawowych Unii Europejskiej, Podręcznik europejskiego prawa dotyczącego azylu, granic i imigracji – Wydanie 2020, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020, w szczególności rozdział 2. Aktualizacja zaplanowana na 2026 r.
- Rada Europy, Europejski Trybunał Praw Człowieka, Europejski Inspektor Ochrony Danych i Agencja Praw Podstawowych Unii Europejskiej, Podręcznik europejskiego prawa o ochronie danych – wydanie z 2018 r., Urząd Publikacji Unii Europejskiej, Luksemburg, 2018 r. Wytyczne wyjaśniają odpowiednie standardy ochrony danych.
- Agencja Praw Podstawowych Unii Europejskiej, Skutki zobowiązania do dostarczenia odcisków palców dla systemu Eurodac w kontekście praw podstawowych, Urząd Publikacji Unii Europejskiej, Luksemburg, 2015 r.
- Agencja Praw Podstawowych Unii Europejskiej, Prawo do informacji — Poradnik dla organów pobierających odciski palców do systemu EURODAC, Urząd Publikacji Unii Europejskiej, Luksemburg, 2019 r. Zostało to opublikowane wraz z Grupą ds. Koordynacji Nadzoru nad Eurodac.
- Platforma informacyjna FRA poświęcona unijnym systemom informatycznym w zakresie migracji i policji, zawierająca opis wielkoskalowych systemów informatycznych UE dotyczących granic, wiz, azylu i migracji oraz ich interoperacyjności (grudzień 2024 r.).

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Metodologia badań

FRA przeprowadziła badania i wniosła wiedzę specjalistyczną w zakresie praw podstawowych do działań szkoleniowych dotyczących EES, ponieważ system ten będzie przetwarzał dane osobowe, w tym wrażliwe dane biometryczne, setek milionów obywateli państw spoza UE każdego roku.

Badania FRA miały na celu zebranie doświadczeń i oczekiwań praktyków i ekspertów w kwestiach istotnych dla wdrożenia EES. Badania objęły gromadzenie i przetwarzanie danych biometrycznych na granicach, np. za pośrednictwem zautomatyzowanych bramek kontroli granicznej, dostarczanie informacji obywatelom państw trzecich lub zarządzanie kolejkami w miejscach o ograniczonej przestrzeni.

Od maja do września 2024 r. FRA gromadziła doświadczenia funkcjonariuszy straży granicznej, organów krajowych, organów ochrony danych i ekspertów ds. praw podstawowych. Badania terenowe przeprowadzono w sześciu państwach członkowskich UE; obejmowały one dziewięć punktów kontroli granicznej na granicach powietrznych, morskich i lądowych z odpowiednim doświadczeniem w przetwarzaniu danych biometrycznych na granicach. Dokładniej rzecz ujmując, zrealizowano następujące zadania badawcze.

- Przeprowadzono wywiady z 30 organami i ekspertami na szczeblu krajowym, po pięciu w każdym z następujących państw członkowskich: Bułgaria, Estonia, Francja, Niemcy, Włochy i Polska.
- W dziewięciu punktach kontroli granicznej przeprowadzono wywiady z 61 kierownikami zmian i 25 innymi zainteresowanymi stronami, takimi jak operatorzy portów lotniczych, przedsiębiorstwa transportowe i organizacje pozarządowe. W tych punktach kontroli granicznej straż graniczna zaoferowała dla badaczy oględziny z przewodnikiem, co umożliwiło przeprowadzenie obserwacji uczestniczącej.
- Na dziewięciu przejściach granicznych, obejmujących łącznie 177 funkcjonariuszy straży granicznej, przeprowadzono ankietę.
- Pracownicy FRA odwiedzili pięć punktów kontroli granicznej (lotniska we Frankfurcie i w Wiedniu, terminal Eurostar we Francji oraz porty w Marsylii i Bari), obserwując i omawiając przygotowania do EES z odpowiednimi organami państw członkowskich.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Badania przeprowadzono w następujących punktach kontroli granicznej:

- Bułgaria – Kapitan Andreewo (przejście graniczne) i port lotniczy w Sofii;
- Estonia – Narwa (lądowy punkt graniczny);
- Francja – port w Marsylii i przejście graniczne Eurostar;
- Włochy – port lotniczy Rzym-Fiumicino i port w Bari;
- Polska – Medyka (przejście graniczne) i port lotniczy w Warszawie.

Wyniki badań stanowiły punkt wyjścia do opracowania niniejszych wytycznych FRA.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

1. Skuteczne informowanie obywateli państw spoza UE

Prawo do informacji ma kluczowe znaczenie dla funkcjonowania EES, ponieważ zapewnia przejrzystość i umożliwia ochronę praw podstawowych. Informacje propagują rozliczalność, jasność prawa i zaufanie do unijnego systemu zarządzania granicami.

a) Wybrane kluczowe wnioski

Poniższe wnioski zostały uzyskane w wyniku badań jakościowych.

- Żadne z przejść granicznych (BCP), w których prowadzono badania terenowe, z wyjątkiem Medyki (Polska) i Narwy (Estonia), nie dysponowało tablicami informacyjnymi ani ulotkami przy kontroli pierwszej linii.
- Powszechna opinia we wszystkich BCP objętych badaniami wskazuje na potrzebę przewidywania momentu przekazywania informacji obywatelom państw trzecich.
- Lider zmiany w Estonii zauważył, że „w przyszłości konieczność fotografowania niemowląt w wózkach… sprawi trudności… osobie, która to wykonuje, ponieważ będzie musiała wyjaśnić rodzicowi, dlaczego robi zdjęcie jego dziecku”.
- Naukowcy w Niemczech i we Włoszech zwrócili uwagę, że obywatele państw trzecich mogą nie w pełni rozumieć przekazywane informacje.
- Jeden z naukowców w Bułgarii podkreślił potencjalne ryzyka związane z barierami językowymi i niespójnym przekazywaniem informacji w różnych państwach członkowskich.

Ankieta przeprowadzona wśród funkcjonariuszy straży granicznej ujawniła następujące ustalenia:

- 84% funkcjonariuszy straży granicznej stwierdziło, że na podstawie własnego doświadczenia wcześniejsze udostępnienie pasażerom informacji na temat celu, procedur i praw związanych z gromadzeniem danych w EES jest niezbędne do zapewnienia jakości danych biometrycznych (n = 175) [1].

- 91% funkcjonariuszy uważa, że wcześniejsze udostępnienie obywatelom państw trzecich informacji dotyczących wymogów wjazdowych ułatwiłoby komunikację z nimi podczas kontroli pierwszej linii, wraz z wykorzystaniem wideo informacyjnych podczas oczekiwania (81%), dostępu do narzędzi tłumaczeniowych (77%), pisemnych materiałów informacyjnych udostępnianych podczas oczekiwania (70%) oraz personelu wspierającego w językach obcych (68%) (n = 176).
- 37% funkcjonariuszy wskazało, że wielu lub niektórzy obywatele państw trzecich nie są dobrze poinformowani o procedurach kontroli, co negatywnie wpływa na ich pracę (n = 161).
- Funkcjonariusze wymienili następujące wyzwania związane z przekazywaniem informacji obywatelom państw trzecich: presję czasową (73%), niewystarczającą ilość materiałów informacyjnych (61%), trudności komunikacyjne i językowe (59%) oraz brak wystarczającej wiedzy merytorycznej (43%) (n = 172).

b. Odniesienia prawne

Zgodnie z rozporządzeniem w sprawie EES obywatele państw trzecich muszą być wyraźnie informowani o wykorzystywaniu ich danych osobowych, ich obowiązkach i prawach. W art. 50 ust. 1 rozporządzenia wymieniono, o czym należy informować obywateli państw trzecich i w jaki sposób należy ich informować. Zobowiązuje on państwa członkowskie do informowania ich o potrzebie dostarczenia odcisków palców i wizerunków twarzy, konsekwencjach odmowy oraz możliwości udostępnienia danych organom ścigania lub do celów powrotu. Osoby fizyczne muszą być również informowane o przysługujących im prawach do dostępu do swoich danych, ich poprawiania lub usuwania, o wykorzystywaniu danych do monitorowania przekroczenia dozwolonego okresu pobytu, o okresach zatrzymywania danych oraz o prawie do wnoszenia skarg. W rozporządzeniu wyjaśniono, że informacje muszą mieć formę pisemną, być zwięzłe, przejrzyste, zrozumiałe, łatwo dostępne, muszą być sporządzone prostym językiem oraz muszą być sporządzone w języku zrozumiałym dla obywateli państw trzecich lub co do którego można zasadnie oczekiwać, że zostanie przez nich zrozumiany. W decyzji wykonawczej Komisji (UE) 2022/1337 z dnia 28 lipca 2022 r. określono wzór na potrzeby przekazywania informacji.

Prawo do informacji określone w rozporządzeniu w sprawie EES uzupełnia unijne przepisy o ochronie danych (zob. sekcja 3), w szczególności rozporządzenie (UE) 2016/679 (ogólne rozporządzenie o ochronie danych (RODO)). Rozporządzenie w sprawie EES należy interpretować zgodnie z prawem do poszanowania życia prywatnego i rodzinnego oraz do ochrony danych osobowych określonym w art. 7 i 8 Karty, a także z prawem do skutecznego środka prawnego określonym w art. 47 Karty. Musi ono również być zgodne z prawem do dobrej administracji, które jest ogólną zasadą prawa Unii. Aby promować sprawiedliwość i ochronę prawną przy informowaniu obywateli państw trzecich, organy krajowe muszą unikać dyskryminacji zakazanej na mocy art. 21 Karty i podejmować niezbędne środki w celu poszanowania praw dziecka (art. 24), osób starszych (art. 25) i osób niepełnosprawnych (art. 26).

c) Wytyczne

Poniższe wytyczne mogą pomóc organom krajowym w dostarczaniu informacji na temat EES obywatelom państw trzecich w skuteczny i niedyskryminacyjny sposób, z poszanowaniem praw podstawowych.

- **Wytyczne 1.1:** Udostępnienie europejskiej kampanii informacyjnej na temat EES na oficjalnej krajowej stronie internetowej i uzupełnienie jej, w stosownych przypadkach, o informacje na szczeblu krajowym udostępniane online.

Poniższe wytyczne mogą również wchodzić w zakres kompetencji urzędników wyższego szczebla na przejściach granicznych.

- **Wytyczne 1.2:** Opracowywanie materiałów informacyjnych tak konkretnych i szczegółowych, jak to możliwe, wskazujących osoby odpowiedzialne za kwestie ochrony danych oraz za przyjmowanie skarg, wraz z ich danymi kontaktowymi.
- **Wytyczne 1.3:** Wsparcie BCP w zakresie zakładania punktów informacyjnych na miejscu, zapewnienia informacji w wielu językach i w formatach dostępnych, takich jak kody QR, plakaty,

- ulotki, ekrany z filmami informacyjnymi, stanowiska w alfabecie Braille'a, informacje audio, piktogramy lub symbole dla dzieci.
- **Wytyczne 1.4:** Zachęcanie BCP do dystrybucji kodów QR prowadzących do usługi internetowej umożliwiającej sprawdzenie liczby pozostałych dni dozwolonego pobytu.
- **Wytyczne 1.5:** Regularne monitorowanie, czy materiały informacyjne wywieszone na BCP są łatwo dostępne dla wszystkich obywateli państw trzecich, bez konieczności opuszczania kolejki.
- **Wytyczne 1.6:** Dysponowanie odpowiednią liczbą personelu na BCP, który odpowiada na pytania obywateli państw trzecich w różnych istotnych językach.
- **Wytyczne 1.7:** W razie potrzeby i możliwości udostępnienie mediatorów kulturowych lub podobnego personelu wspierającego na BCP w celu pomocy obywatelom państw trzecich podczas samoobsługowej rejestracji, w szczególności osobom o szczególnych potrzebach i z ograniczonymi umiejętnościami cyfrowymi, oraz w celu ułatwienia identyfikacji i skierowania osób wrażliwych.
- **Wytyczne 1.8:** Udostępnianie odpowiednich materiałów informacyjnych oraz, w razie potrzeby, koordynacja z przewoźnikami, biurami podróży, organami wizowymi oraz sąsiednimi BCP w krajach spoza UE w celu wcześniejszego poinformowania obywateli państw trzecich o systemie EES przed podróżą.

d) Więcej informacji

- „Praktyczny podręcznik EES" Komisji Europejskiej dla organów krajowych (niedostępny publicznie).
- Agencja Praw Podstawowych Unii Europejskiej, Kontrole graniczne a prawa podstawowe na lądowych granicach zewnętrznych – praktyczne wskazówki, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020 r., pkt 7.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

2) Traktowanie obywateli państw trzecich oczekujących na kontrolę graniczną z godnością

Obiekty na przejściach granicznych (BCP) często dysponują ograniczoną przestrzenią. Czas oczekiwania może powodować trudności dla obywateli państw trzecich, co jest problemem wykraczającym poza kontekst EES, ale którego skala może być istotnie zwiększona przez funkcjonowanie systemu. Problem ten wymaga odpowiedniego zaprojektowania przestrzeni i zarządzania kolejką.

a) Wybrane kluczowe wnioski

Poniższe wnioski zostały uzyskane w wyniku badań jakościowych.

- Infrastruktura do kontroli w pierwszej i drugiej linii na badanych BCP różni się znacznie, przy czym lotniska są zazwyczaj lepiej wyposażone w zarządzanie przepływem pasażerów. Na granicach morskich i lądowych duże natężenie ruchu pojazdów i pieszych może wydłużać czas oczekiwania i stawiać obywateli państw trzecich w niewygodnej sytuacji, szczególnie gdy nie zapewniono odpowiedniego schronienia.
- Kierownik zmiany w porcie w Bari (Włochy) zauważył, że: „Liczba pasażerów wzrosła szalenie, nie ma miejsca… A gdy jest tylu ludzi, trudno jest także zidentyfikować sytuacje krytyczne”. Funkcjonariusz z Kapitan Andreewo (Bułgaria) opisał: „Ludzie wysiadają z autobusu, przechodzą przez kontrolę i stoją na boku, podczas gdy autobus odjeżdża… Jeśli kontrola trwa, powiedzmy, dwie godziny, pasażerowie stoją przez ten czas tam, gdzie znajdą miejsce”.
- Kierownik zmiany na lotnisku w Warszawie (Polska) zauważył, że EES może pozytywnie wpływać na kolejki: „Często pasażerowie mają w paszporcie wiele takich stempli i żeby to wszystko policzyć, potrzeba czasu. A jeśli system sam obliczy te dni pobytu, myślę, że na pewno będzie to miało pozytywny wpływ”.
- Władze we Francji wskazały warunki oczekiwania i sposób pobierania danych biometrycznych jako kwestie, które mogą wpływać na poszanowanie godności ludzkiej. Władze bułgarskie zauważyły, że wprowadzenie EES może prowadzić do wydłużenia czasu obsługi na BCP, co potencjalnie może oddziaływać na traktowanie obywateli państw trzecich.

Badanie przeprowadzone przez straż graniczną ujawniło następujące ustalenia.

- Funkcjonariusze straży granicznej mający doświadczenie w obsłudze e-bramek wskazali następujące środki jako skuteczne w celu ułatwienia przepływu pasażerów: obecność instruktorów kolejek na miejscu (79%), czytelne oznaczenia wskazujące, kto może korzystać z bramek (76%), oraz dostępność i możliwość kontaktu z firmą odpowiedzialną za konserwację techniczną (74%) (n = 140) [2].
- Większość ankietowanych funkcjonariuszy (87%) uważa, że dostępność personelu wspierającego, takiego jak asystenci kolejek czy mediatorzy kulturowi, jest pomocna w przeprowadzaniu kontroli w sposób ograniczający trudności dla osób o szczególnych potrzebach w przypadku długich kolejek (n = 177).

b) Odniesienia prawne

Zgodnie z art. 7 kodeksu granicznego Schengen (rozporządzenie (UE) 2016/399) straż graniczna musi w pełni szanować ludzką godność podczas kontroli osób, w szczególności w przypadkach osób wymagającymi szczególnego traktowania. Zgodnie z art. 10 rozporządzenia w sprawie EES korzystanie z EES musi być zgodne z Kartą, EKPC oraz, w przypadku dzieci, z Konwencją ONZ o prawach dziecka. Konwencja ONZ o prawach osób niepełnosprawnych, która jest wiążąca dla UE i wszystkich jej państw członkowskich, chroni prawa osób niepełnosprawnych, np. poprzez zapewnienie dostępności transportu (art. 9).

c) Wytyczne

Poniższe wytyczne mogą pomóc władzom krajowym w promowaniu godnego traktowania obywateli państw trzecich podczas przetwarzania ich danych osobowych w systemie EES. Mogą one również należeć do kompetencji kadry kierowniczej na przejściach granicznych (BCP).

- **Wytyczne 2.1:** Wspieranie, tam gdzie jest to zasadne, negocjacji dotyczących przydziału przestrzeni z podmiotem odpowiedzialnym za infrastrukturę BCP, w celu zapewnienia odpowiedniej przestrzeni dla stref oczekiwania, systemów samoobsługowych oraz kontroli pierwszej i drugiej linii.
- **Wytyczne 2.2:** Udzielanie wytycznych i wsparcia BCP w zakresie zapewnienia właściwych stref oczekiwania z miejscami do siedzenia, wystarczającą liczbą toalet, dostępem do wody pitnej oraz, na lądowych BCP i w portach morskich, zadaszonych miejsc dla pieszych i pasażerów pojazdów, chroniących przed słońcem, deszczem i śniegiem.

- **Wytyczne 2.3:** Dokładanie wszelkich rozsądnych starań, aby wspierać BCP w utrzymywaniu krótkich czasów oczekiwania, np. poprzez skuteczne udostępnianie informacji, zarządzanie kolejką oraz zapewnienie odpowiedniego personelu i wyposażenia.
- **Wytyczne 2.4:** Zachęcanie punktów kontroli granicznej do opracowania procedur awaryjnych, szczególnie na portach morskich i lądowych BCP, w celu zapewnienia przestrzegania praw podstawowych obywateli państw trzecich w przypadku przedłużających się opóźnień.
- **Wytyczne 2.5:** Regularne monitorowanie, czy na przejściach granicznych jest wystarczająco dużo miejsca na kontrole drugiej linii związane z Systemem Wjazdu/Wyjazdu, bez ingerowania w przestrzeń potrzebną do przeprowadzania rozmów z osobami ubiegającymi się o azyl lub do identyfikowania potencjalnych ofiar handlu ludźmi.

d) Więcej informacji

- „Praktyczny podręcznik EES" Komisji Europejskiej dla organów krajowych (niedostępny publicznie).
- Agencja Praw Podstawowych Unii Europejskiej, Kontrole graniczne a prawa podstawowe na lądowych granicach zewnętrznych – praktyczne wskazówki, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020 r., pkt 1

3) Przestrzeganie przepisów dotyczących prywatności i ochrony danych

EES przetwarza dane osobowe, w tym dane biometryczne, a mianowicie odciski palców i wizerunki twarzy. Dane biometryczne są wrażliwymi danymi osobowymi, ponieważ umożliwiają jednoznaczną identyfikację lub uwierzytelnienie osoby fizycznej. Centralne przechowywanie danych setek milionów osób wiąże się z ryzykiem związanym z prawami podstawowymi, które należy ograniczyć za pomocą skutecznych zabezpieczeń w zakresie ochrony danych.

a) Wybrane kluczowe wnioski

Poniższe wnioski zostały uzyskane w wyniku badań jakościowych.

- Badania terenowe na przejściach granicznych sugerują, że ogólnie prywatność jest lepiej chroniona na granicach powietrznych, z pewnymi wyjątkami w okresach intensywnej podróży.
- Zdaniem ekspertów z Niemiec, Francji i Włoch interoperacyjność systemów informatycznych UE zwiększa ryzyko związane z ochroną danych.
- W Bułgarii i Polsce specjaliści ds. ochrony danych i pracownicy naukowi zauważyli, że luki w zakresie zdolności administracyjnych i procedur operacyjnych, w połączeniu z ograniczonym nadzorem, mogą prowadzić do nieuprawnionego dostępu do danych EES, stwarzając ryzyko naruszeń ochrony danych.
- Pewien pracownik naukowy w Bułgarii zidentyfikował zagrożenia dla prawa do dobrej administracji i prawa do skutecznego środka odwoławczego, ponieważ obywatele państw trzecich mogą napotkać trudności w dostępie do własnych danych przechowywanych w EES lub poprawieniu lub usunięciu nieprawidłowych danych.

Ankieta przeprowadzona wśród funkcjonariuszy straży granicznej ujawniła następujące ustalenia.

- 87% funkcjonariuszy straży granicznej uważa, że dostępność komfortowych warunków zapewniających prywatność jest ważnym zabezpieczeniem jakości danych (n = 176) [3].

b) Odniesienia prawne

W art. 16 rozporządzenia w sprawie EES wymieniono dane osobowe przetwarzane przez EES. W art. 39 przedstawiono wytyczne dotyczące zgodnego z prawem przetwarzania danych osobowych w EES.

Ogólniej rzecz ujmując, w art. 49 rozporządzenia w sprawie EES określono, że unijne przepisy o ochronie danych, w szczególności RODO i dyrektywa (UE) 2016/680, mają zastosowanie do przetwarzania danych osobowych w EES przez państwa członkowskie. Zgodnie z art. 5 RODO dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty. Przetwarzanie danych biometrycznych podlega ograniczeniom i zabezpieczeniom określonym w art. 9 RODO.

W art. 52 rozporządzenia w sprawie EES opisano prawa do ochrony danych, takie jak prawo dostępu do przechowywanych danych osobowych lub prawo do żądania sprostowania lub usunięcia danych. Zgodnie z art. 50 ust. 1 lit. l) wszystkie osoby fizyczne muszą zostać poinformowane o przysługującym im prawie do wniesienia skargi do odpowiedniego organu nadzorczego, jeżeli uważają, że ich prawa do ochrony danych zostały naruszone (w celu uzyskania informacji zob. sekcja 1).

c) Wytyczne

Poniższe wytyczne mogą pomóc władzom krajowym w przetwarzaniu danych osobowych w systemie EES zgodnie z przepisami UE dotyczącymi ochrony danych.

- **Wytyczne 3.1:** Przeprowadzanie oceny skutków dla ochrony danych przed uruchomieniem nowych komponentów EES, z udziałem krajowych organów ochrony danych, w zależności od potrzeby.
- **Wytyczne 3.2:** Zapewnienie bezpieczeństwa oraz regularnej konserwacji sprzętu i oprogramowania opracowanego i wdrożonego na poziomie krajowym poprzez ciągłą optymalizację techniczną, proaktywne zabezpieczenia i kontrole systemu.
- **Wytyczne 3.3:** Stosowanie wielowarstwowych środków cyberbezpieczeństwa w celu ochrony danych osobowych przed nieautoryzowanym dostępem, włamaniami lub niewłaściwym użyciem

Niniejsze wytyczne mogą również należeć do kompetencji kadry kierowniczej na przejściach granicznych (BCP).

- **Wytyczne 3.4:** Udzielanie wsparcia i wytycznych BCP w zakresie zapewnienia środowiska, które gwarantuje poufność i prywatność podczas zbierania danych osobowych od obywateli państw trzecich.
- **Wytyczne 3.5:** Wsparcie BCP w instalacji osłon prywatności na systemach samoobsługowych oraz ochronnych folii na ekranach lub oknach kabin kontroli granicznej, jeśli jest to zasadne.
- **Wytyczne 3.6:** Podnoszenie świadomości w zakresie konsekwencji błędów wprowadzania danych i szczególnie poważnego wpływu, jaki mogą mieć na daną osobę.
- **Wytyczne 3.7:** Organizowanie szkoleń i udzielanie wytycznych funkcjonariuszom pierwszej linii dotyczących korekt danych dokonywanych na pierwszej linii (np. błędy w samoobsługowej rejestracji) oraz przypadków do przekazania na drugą linię (np. błędne obliczenie dni pobytu), zgodnie z ustalonymi politykami korekty danych.
- **Wytyczne 3.8:** Organizowanie szkoleń i udzielanie wytycznych funkcjonariuszom, jak skutecznie informować obywateli państw trzecich, którzy zgłaszają żądanie sprostowania, uzupełnienia lub usunięcia danych, o właściwym organie do kontaktu i sposobie postępowania w związku z ich wnioskiem.

d) Więcej informacji

- „Praktyczny podręcznik EES" Komisji Europejskiej dla organów krajowych (niedostępny publicznie).
- Rada Europy, Europejski Trybunał Praw Człowieka i Agencja Praw Podstawowych Unii Europejskiej, Podręcznik europejskiego prawa dotyczącego azylu, granic i imigracji – Wydanie 2020, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020, w szczególności rozdział 2. Aktualizacja zaplanowana na 2026 r.
- Rada Europy, Europejski Trybunał Praw Człowieka, Europejski Inspektor Ochrony Danych i Agencja Praw Podstawowych Unii Europejskiej, Podręcznik europejskiego prawa o ochronie danych – wydanie z 2018 r., Urząd Publikacji Unii Europejskiej, Luksemburg, 2018 r.

4) Przetwarzanie danych biometrycznych w sposób godny i zgodny z prawem

Obywatele państw trzecich muszą dostarczyć swoje odciski palców i wizerunki twarzy przy pierwszym wjeździe do strefy Schengen. Podczas kolejnych wjazdów i wyjazdów gromadzone informacje biometryczne będą weryfikowane i – o ile dane biometryczne nie wymagają aktualizacji – nie będą pobierane żadne nowe informacje biometryczne. Straż graniczna może stanąć przed wyzwaniami, np. pobierając wizerunki twarzy dzieci. Chociaż standardy dokładności są wysokie, błędnego dopasowania biometrycznego nigdy nie można całkowicie wykluczyć. Odpowiednie zabezpieczenia pomagają zapewnić, że każda osoba jest traktowana z godnością w takich sytuacjach.

a) Wybrane kluczowe wnioski

Poniższe wnioski zostały uzyskane w wyniku badań jakościowych.

- Powszechna opinia wśród funkcjonariuszy straży granicznej na badanych BCP wskazuje, że pobieranie odcisków palców jest łatwiejsze niż wykonywanie zdjęć twarzy, zwłaszcza gdy osoby nie stoją nieruchomo.
- Postawa funkcjonariusza odgrywa kluczową rolę w procesie pobierania danych biometrycznych, ponieważ wpływa na współpracę osoby kontrolowanej. Jak zauważył kierownik zmiany w Polsce: „Jeżeli podejdziesz do kogoś z uśmiechem, oni również w pewien sposób odpowiedzą uśmiechem. Ludzie nie sprawiają problemów”.
- Przynajmniej na jednym BCP (lotnisko w Marsylii) funkcjonariusze byli wyposażeni w tablety umożliwiające mobilne kontrole EES, co może ułatwiać kontrolę osób o ograniczonej mobilności.
- Funkcjonariusze straży granicznej opierają się na własnym osądzie i doświadczeniu, aby skutecznie radzić sobie w złożonych sytuacjach. Kierownik zmiany w Bułgarii zauważył: „Nie otrzymaliśmy specjalnego szkolenia ani instrukcji, jak oceniać uszkodzenia dłoni. Po prostu działamy zgodnie z własnym doświadczeniem”.
- Elastyczność jest kluczowa przy obsłudze wyjątkowych okoliczności związanych z czynnikami kulturowymi. Kierownik zmiany na lotnisku w Rzymie-Fiumicino, odnosząc się do kobiety noszącej burkę lub szczególny welon uniemożliwiający weryfikację biometryczną twarzy, stwierdził: „Nie zmusimy jej do jego zdjęcia ani nie skierujemy na drugą linię… jeśli jej odciski palców pozwolą na dopasowanie, to będzie wystarczające”.

- Obawy ekspertów w Niemczech dotyczące poszanowania godności ludzkiej koncentrują się na trzech głównych kwestiach: wykorzystaniu danych biometrycznych, postawie i sposobie komunikacji funkcjonariuszy straży granicznej oraz mechanizmach wsparcia dla podróżnych o szczególnych potrzebach.

Badanie przeprowadzone przez straż graniczną ujawniło następujące ustalenia.

- 87% funkcjonariuszy straży granicznej uważa, że dostępność komfortowego otoczenia zapewniającego prywatność jest ważnym zabezpieczeniem jakości danych (oprócz odpowiedniego wyposażenia, potwierdzonego przez 91% funkcjonariuszy straży granicznej) (n = 176) [4].
- 36% funkcjonariuszy straży granicznej stwierdziło, że potrzebuje szkolenia w zakresie uzyskiwania danych biometrycznych od osób o specjalnych potrzebach (n = 173).
- Straż graniczna z doświadczeniem w przetwarzaniu danych biometrycznych na granicach twierdzi, że wyjaśnienie konsekwencji odmowy dostarczenia danych biometrycznych i dostarczenie większej ilości informacji na temat wykorzystania danych (56%), zapewnienie pasażerowi więcej czasu na rozważenie możliwości (31%), wezwanie kolegi do wsparcia (21%), skierowanie do kierownika zmiany (16%) i wezwanie tłumacza ustnego (14%) pomogło im w sytuacjach, w których pasażerowie odmówili przekazania danych biometrycznych (n = 48).

b) Odniesienia prawne

W art. 39 ust. 1 lit. a) rozporządzenia w sprawie EES zobowiązano państwa członkowskie do zapewnienia, aby dane były gromadzone zgodnie z prawem i przy pełnym poszanowaniu godności ludzkiej.

Zgodnie z art. 10 rozporządzenia w sprawie EES pobieranie danych biometrycznych musi być zgodne z Kartą, EKPC oraz, w przypadku dzieci, z Konwencją o prawach dziecka. Przy pozyskiwaniu danych dziecka należy przede wszystkim uwzględnić jego najlepszy interes. W art. 17 ust. 3 zwalnia się dzieci w wieku poniżej 12 lat z obowiązku pobierania odcisków palców, ale od wszystkich dzieci, w tym od niemowląt, należy pobierać wizerunki twarzy. W art. 17 ust. 4 i 5 ustanowiono wytyczne dla organów w sytuacjach, w których odciski palców nie mogą zostać pobrane fizycznie ani tymczasowo, np. z powodu zranienia ręki, lub na stałe.

Te zabezpieczenia przewidziane w rozporządzeniu w sprawie EES wynikają z art. 1 Karty, zgodnie z którym godność ludzka jest nienaruszalna, oraz z art. 24–26 Karty, dotyczących ochrony dzieci, osób starszych i osób niepełnosprawnych.

Odciski palców i wizerunki twarzy muszą być odpowiedniej jakości, aby uzyskać prawidłowe dopasowanie. W art. 15 rozporządzenia w sprawie EES wymaga się, aby wizerunek twarzy miał wystarczającą rozdzielczość i jakość, aby można go było wykorzystywać w zautomatyzowanym dopasowywaniu danych biometrycznych. Zgodnie z art. 39 – który odzwierciedla bardziej ogólny obowiązek określony w art. 5 ust. 1 lit. d) RODO – państwa członkowskie muszą zapewnić dokładność gromadzonych danych. W decyzji wykonawczej Komisji (UE) 2019/329 z 25 lutego 2019 r. określono specyfikacje dotyczące jakości, rozdzielczości oraz wykorzystywania odcisków palców i wizerunku twarzy na potrzeby weryfikacji i identyfikacji biometrycznej w EES.

c) Wytyczne

Poniższe wytyczne mogą pomóc organom krajowym w pobieraniu odcisków palców i wizerunków twarzy od obywateli państw trzecich w sposób zapewniający poszanowanie godności ludzkiej.

- **Wytyczne 4.1:** Zapewnienie, aby wszelkie wytyczne dotyczące jakości danych w celu pobierania danych biometrycznych były ściśle zgodne z unijnymi normami jakości.

Poniższe wytyczne mogą również wchodzić w zakres kompetencji urzędników wyższego szczebla na przejściach granicznych.

- **Wytyczne 4.2:** Zapewnienie funkcjonariuszom pierwszej linii wytycznych dotyczących sposobu pobierania danych biometrycznych w godny i niedyskryminujący sposób, ze zwróceniem szczególnej uwagi na względy kulturowe lub religijne oraz na kategorie osób, dla których pobieranie danych biometrycznych może być trudniejsze, takie jak małe dzieci, osoby o ciemniejszych odcieniach skóry lub osoby z urazami twarzy lub dłoni.
- **Wytyczne 4.3:** Zapewnienie funkcjonariuszom pierwszej linii wytycznych dotyczących sposobu zapewnienia obywatelom państw trzecich o szczególnych potrzebach prywatności, czasu lub pomocy, których potrzebują do przekazania swoich danych biometrycznych.
- **Wytyczne 4.4:** Zapewnienie funkcjonariuszom pierwszej linii wytycznych dotyczących sposobu reagowania na obywateli państw trzecich odmawiających dostarczenia danych biometrycznych.
- **Wytyczne 4.5:** Wspieranie punktów kontroli granicznej w zapewnieniu wystarczającej liczby pracowników do monitorowania samoobsługowych systemów rejestracji i udzielania pomocy w razie potrzeby.

- **Wytyczne 4.6:** Zapewnienie funkcjonariuszom pierwszej linii wytycznych dotyczących sposobów radzenia sobie z wyzwaniami związanymi z wiarygodnością biometryczną dotykającymi osoby o różnych cechach fizycznych (np. dzieci, osoby starsze, osoby o ciemniejszym odcieniu skóry lub inne osoby o mniej wyraźnych rysach twarzy).
- **Wytyczne 4.7:** Zastosowanie wysokiej jakości infrastruktury informatycznej i oprogramowania zdolnego do szybkiego przechwytywania dokładnych i wysokiej rozdzielczości obrazów i odcisków palców.

d) Więcej informacji

- „Praktyczny podręcznik EES" Komisji Europejskiej dla organów krajowych (niedostępny publicznie).
- Załącznik do zalecenia Komisji ustanawiającego wspólny „Praktyczny podręcznik dla straży granicznej" przeznaczony dla właściwych organów państw członkowskich prowadzących kontrolę osób na granicach i zastępujące zalecenie C(2019) 7131 final z dnia 28 października 2022 r., s. 14, 16.
- Rada Europy, Europejski Trybunał Praw Człowieka i Agencja Praw Podstawowych Unii Europejskiej, Podręcznik europejskiego prawa dotyczącego azylu, granic i imigracji – Wydanie 2020, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020, w szczególności rozdział 2. Aktualizacja zaplanowana na 2026 r.
- Rada Europy, Europejski Trybunał Praw Człowieka, Europejski Inspektor Ochrony Danych i Agencja Praw Podstawowych Unii Europejskiej, Podręcznik europejskiego prawa o ochronie danych – wydanie z 2018 r., Urząd Publikacji Unii Europejskiej, Luksemburg, 2018 r.
- Agencja Praw Podstawowych Unii Europejskiej, Skutki zobowiązania do dostarczenia odcisków palców dla systemu Eurodac w kontekście praw podstawowych, Urząd Publikacji Unii Europejskiej, Luksemburg, 2015 r.

5. Wspieranie obywateli spoza UE o szczególnych potrzebach

Właściwa identyfikacja i udzielanie wsparcia osobom o szczególnych potrzebach przybywającym na przejście graniczne ma zasadnicze znaczenie dla funkcjonowania EES zorientowanego na prawa podstawowe. Zapewnia uczciwość, promuje dokładność danych gromadzonych za pośrednictwem systemu, a jednocześnie minimalizuje ryzyko dyskryminacji i szkód.

a) Wybrane kluczowe wnioski

Poniższe wnioski zostały uzyskane w wyniku badań jakościowych.

- Badania FRA pokazują, że zasoby umożliwiające identyfikację i wspieranie obywateli państw trzecich o szczególnych potrzebach są ograniczone, zwłaszcza na lądowych i morskich przejściach granicznych.
- W odniesieniu do osób z niepełnosprawnościami przedstawiciel władz na lotnisku w Sofii wskazał na praktyczne trudności. Zauważył, że osoby te „przechodzą na przód kolejki wraz z funkcjonariuszem, który im pomaga… ale pod względem infrastrukturalnym nie ma… w całym terminalu żadnych obszarów dostosowanych i odpowiednio oznaczonych dla osób z niepełnosprawnościami".
- Na lotniskach rodziny z dziećmi poniżej 12. roku życia nie mogą korzystać z bramek ABC, ponieważ wymagałoby to rozdzielenia członków rodziny.
- Korzystanie z bramek ABC jest w dużej mierze niepraktyczne dla osób o ograniczonej sprawności ruchowej, zwłaszcza osób na wózkach inwalidzkich.

Badanie przeprowadzone przez straż graniczną ujawniło następujące ustalenia.

- Straż graniczna uczestnicząca w ankiecie FRA przewidziała, że informacje i pomoc związane z EES będą najbardziej potrzebne osobom z niepełnosprawnościami (65%), dzieciom podróżującym samotnie (61%) i osobom starszym (52%), na podstawie ich doświadczenia w sprawdzaniu obywateli państw trzecich o szczególnych potrzebach (n = 176).

b) Odniesienia prawne

Wdrażając EES, organy krajowe muszą przestrzegać zabezpieczeń zawartych w Karcie i EKPC, zgodnie z art. 10 rozporządzenia w sprawie EES. Oznacza to, że muszą one zwracać szczególną uwagę na obywateli państw trzecich o szczególnych potrzebach, takich jak osoby starsze, osoby z niepełnosprawnościami i dzieci – wszystkie kategorie osób chronionych na mocy art. 24–26 Karty. Aby zapewnić zgodność z art. 21 Karty, EES musi działać w sposób niedyskryminacyjny.

Zgodnie z art. 10 rozporządzenia w sprawie EES w przypadku pobierania od dzieci wizerunków twarzy lub odcisków palców organy muszą przede wszystkim brać pod uwagę najlepszy interes dziecka. Zasada ta ma zastosowanie niezależnie od tego, czy dziecko jest samo, czy z kimś.

Rozporządzenie w sprawie EES zapewnia szczególną ochronę młodszym dzieciom. Zgodnie z art. 17 ust. 3 dzieci w wieku poniżej 12 lat są zwolnione z obowiązku składania odcisków palców. Wyłączenie to uwzględnia fakt, że odciski palców dzieci zmieniają się z czasem.

c) Wytyczne

Poniższe wytyczne mogą pomóc organom krajowym we właściwym identyfikowaniu i wspieraniu obywateli państw trzecich o szczególnych potrzebach w sposób zapewniający poszanowanie godności ludzkiej.

- **Wytyczne 5.1:** Ustanowienie systemu umożliwiającego obywatelom państw trzecich na wcześniejsze zgłaszanie ich szczególnych potrzeb i zachęcającego ich do tego, aby umożliwić punktom kontroli granicznej oferowanie niezbędnego wsparcia.
- **Wytyczne 5.2:** Współpraca ze społeczeństwem obywatelskim, organizacjami ochrony dzieci i organami zajmującymi się prawami człowieka w celu uzyskania informacji zwrotnych na temat funkcjonowania EES.

Poniższe wytyczne mogą również wchodzić w zakres kompetencji urzędników wyższego szczebla na przejściach granicznych.

- **Wytyczne 5.3:** Zapewnienie wskazówek i szkoleń dla punktów kontroli granicznej na temat sposobu organizowania poczekalni i kolejek w sposób umożliwiający rodzinom pozostanie razem i umożliwiający osobom starszym siedzenie bez utraty miejsca w kolejce.
- **Wytyczne 5.4:** Zapewnienie wytycznych i szkoleń dla punktów kontroli granicznej w zakresie zarządzania kolejkami, tak aby osoby o szczególnych potrzebach, które nie są w stanie korzystać z bramek ABC lub systemów samoobsługowych, nie były nieproporcjonalnie dotknięte długim czasem oczekiwania.
- **Wytyczne 5.5:** Zapewnienie wytycznych i szkoleń dla punktów kontroli granicznej w zakresie szybkiego identyfikowania obywateli państw trzecich wymagających pomocy, np. poprzez zapewnienie wystarczającego nadzoru nad systemami samoobsługi i kolejkami pierwszej linii.
- **Wytyczne 5.6:** Oferowanie wytycznych i szkoleń dla punktów kontroli granicznej na temat sposobów zapewnienia dostępności dla osób z niepełnosprawnościami, w tym poprzez zapewnienie wystarczającej ilości miejsca dla użytkowników wózków inwalidzkich.
- **Wytyczne 5.7:** Zamawianie i wdrażanie systemów samoobsługowych ze skanerami o regulowanej wysokości, pomocą głosową i dotykową informacją zwrotną, aby pomieścić osoby z niepełnosprawnościami.
- **Wytyczne 5.8:** Współpraca z organizacjami osób niepełnosprawnych przy przygotowywaniu przetargów publicznych na wyposażenie techniczne oraz regularna ocena dostępności pomieszczeń na przejściu granicznym.
- **Wytyczne 5.9:** Zapewnienie wytycznych dla punktów kontroli granicznej dotyczących sposobu zagwarantowania, aby osoby towarzyszące mogły pomagać niepełnosprawnym obywatelom państw trzecich w procesie pobierania danych biometrycznych.

d) Więcej informacji

- „Praktyczny podręcznik EES" Komisji Europejskiej dla organów krajowych (niedostępny publicznie).
- Agencja Praw Podstawowych Unii Europejskiej, Kontrole graniczne a prawa podstawowe na lądowych granicach zewnętrznych – praktyczne wskazówki, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020 r., pkt 1.
- Załącznik do zalecenia Komisji ustanawiającego wspólny „Praktyczny podręcznik dla straży granicznej" przeznaczony dla właściwych organów państw członkowskich prowadzących kontrolę osób na granicach i zastępujące zalecenie C(2019) 7131 final z dnia 28 października 2022 r., s. 15.

6. Wykorzystanie danych z Systemu Wjazdu/Wyjazdu zgodnie z prawami podstawowymi

Informacje i dane z EES wspierają różne procedury imigracyjne. Zachowanie czujności co do możliwej niedokładności wyników porównywania danych biometrycznych i świadomość potencjalnych uzasadnień przekroczenia dozwolonego okresu pobytu zmniejsza ryzyko błędnych decyzji lub działań wywołanych niekompletnymi lub niedokładnymi danymi EES.

a) Wybrane kluczowe wnioski

Poniższe wnioski zostały uzyskane w wyniku badań jakościowych.

- Badania terenowe na przejściach granicznych wskazały na ograniczenia w zakresie zdolności i elastyczności przeprowadzania kontroli drugiej linii na granicach lądowych i morskich, ponieważ często działają one z ograniczonym personelem i muszą zarządzać zarówno ruchem pieszych, jak i pojazdów.
- Ekspert ds. praw człowieka we Francji zauważył, że przyśpieszone procedury mogą naruszać prawo do skutecznego środka odwoławczego, zwłaszcza gdy osoby nie posługują się językiem kraju przyjmującego.

Badanie przeprowadzone wśród straży granicznej ujawniło następujące ustalenia.

- Około 1 na 4 funkcjonariuszy (27%) napotkało błędy w Systemie Informacyjnym Schengen lub innych bazach danych ponad 6 razy w ciągu ostatniego roku, 1 na 5 funkcjonariuszy napotkał takie błędy co najmniej 2–5 razy (n = 177).
- 45% funkcjonariuszy straży granicznej wskazało na potrzebę szkoleń lub wytycznych w zakresie procedur dotyczących osób ubiegających się o azyl i rejestracji w EES (n = 173).

b) Odniesienia prawne

EES oblicza czas dozwolonego pobytu obywateli państw trzecich w strefie Schengen i generuje wpisy po wygaśnięciu dozwolonego pobytu (rozporządzenie w sprawie EES, art. 1). Istnieje automatyczny kalkulator (art. 11), który wskazuje maksymalny czas dozwolonego pobytu danej osoby. Po osiągnięciu maksymalnego okresu pobytu krótkoterminowego obywatele państw trzecich nie będą mogli wjechać do strefy Schengen, chyba że posiadają zezwolenie na pobyt długoterminowy. Artykuł 22 RODO zakazuje podejmowania decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu.

Zgodnie z art. 12 ust. 3 w związku z art. 9 ust. 2 rozporządzenia w sprawie EES, EES generuje listę osób, które przekroczyły dozwolony okres pobytu w strefie Schengen, zwanych osobami przekraczającymi dozwolony okres pobytu. Lista ta jest udostępniana organom granicznym, wizowym i imigracyjnym, umożliwiając im podjęcie odpowiednich działań następczych. W przypadku obywateli państw spoza UE zatrzymanych w strefie Schengen oznacza to zazwyczaj wszczęcie procedury powrotowej.

Aby zapobiec rozpoczęciu procedur egzekwowania prawa imigracyjnego wobec osób przebywających legalnie w strefie Schengen, np. w przypadku przedłużenia pobytu ze względów medycznych lub wniosku o udzielenie azylu, w art. 39 rozporządzenia w sprawie EES przewidziano obowiązek zapewnienia dokładności i aktualności danych EES. Oznacza to również, że należy usunąć wpisy w EES dotyczące obywateli państw trzecich, którzy nie są już osobami odbywającymi krótkoterminowe wizyty – np. jeżeli nabyli obywatelstwo UE, uzyskali dokument pobytowy lub kartę pobytową dla członków rodziny obywateli UE na dyrektywy 2004/38/WE. Te kategorie osób nie wchodzą w zakres EES, jak określono w art. 2 rozporządzenia w sprawie EES.

Rozporządzenie w sprawie EES nie wyłącza z zakresu jego stosowania osób ubiegających się o azyl. Zgodnie z art. 10 rozporządzenia (UE) 2024/1348 (rozporządzenie w sprawie procedury azylowej) osoby ubiegające się o azyl mogą pozostać w trakcie procedury azylowej. Umieszczenie ich na liście osób nadmiernie przedłużających pobyt naraziłoby ich na ryzyko *odesłania,* co byłoby sprzeczne z Kartą.

W art. 35 ust. 5 rozporządzenia w sprawie EES przewidziano zabezpieczenie w odniesieniu do obywateli państw trzecich, którzy przekraczają okres dozwolonego pobytu z przyczyn od nich niezależnych, np. z powodu hospitalizacji lub odwołanego lotu powrotnego. Jeżeli obywatele państw trzecich mogą wykazać, że ich pobyt po upływie dozwolonego okresu był spowodowany nieprzewidywalnymi i poważnymi okolicznościami, muszą zostać usunięci z wykazu osób nadmiernie przedłużających pobyt, a ich dane w EES muszą zostać skorygowane.

Zgodnie z art. 41 rozporządzenia w sprawie EES dane EES mogą być przekazywane do państw niebędących członkami UE, jeżeli jest to konieczne do udowodnienia tożsamości danej osoby w celu przeprowadzenia jej powrotu. Zgodnie z art. 41 ust. 4 takie przekazanie nie może naruszać praw osób ubiegających się o ochronę międzynarodową i osób korzystających z ochrony międzynarodowej, w szczególności w odniesieniu do zakazu *wydalania.*

c) Wytyczne

Poniższe wytyczne mogą pomóc organom krajowym zmniejszyć ryzyko, że niedokładne dane EES spowodują niewłaściwe lub niezgodne z prawem działania następcze.

- **Wytyczne 6.1:** Ustanowienie skutecznych systemów szybkiego korygowania lub usuwania danych z EES w przypadku, gdy obywatele państw trzecich nie są objęci zakresem EES, np. w sytuacji uzyskania dokumentu pobytowego lub uzyskania ochrony międzynarodowej.
- **Wytyczne 6.2:** Ustanowienie systemu monitorowania, czy dane EES obywateli państw trzecich, którzy nie są objęci zakresem EES, są szybko prostowane, uzupełniane lub usuwane.
- **Wytyczne 6.3:** Zapewnianie właściwym organom regularnych wytycznych i szkoleń na temat kroków, które należy podjąć, gdy osoba, której dane znajdują się w EES, ubiega się o azyl, aby uniknąć umieszczenia jej w wykazie osób nadmiernie przedłużających pobyt, ponieważ może to narazić ją na ryzyko *odesłania.*
- **Wytyczne 6.4:** Zapewnianie regularnych wytycznych i szkoleń dla funkcjonariuszy organów ścigania ds. imigracji w celu zapewnienia, aby wszelkie przekazywanie danych EES do państw trzecich w celu powrotu miało miejsce dopiero po wydaniu ostatecznej decyzji nakazującej powrót.

Poniższe wytyczne mogą również wchodzić w zakres kompetencji urzędników wyższego szczebla na przejściach granicznych.

- **Wytyczne 6.5:** Oferowanie szkoleń i wskazówek personelowi pierwszej linii w celu profesjonalnego i godnego traktowania każdej osoby, której dozwolony pobyt wygasł.
- **Wytyczne 6.6:** Oferowanie szkoleń i wytycznych pracownikom pierwszej linii na temat sposobu wdrażania procedur dla obywateli państw trzecich w celu obalenia domniemania przekroczenia dozwolonego okresu pobytu, w tym sposobu zapewnienia obywatelom państw trzecich możliwości przedstawienia wiarygodnych dowodów.
- **Wytyczne 6.7:** Zapewnienie wytycznych dla punktów kontroli granicznej przyjmujących zaproszonych funkcjonariuszy spoza UE w celu utworzenia stanowisk pracy w sposób zapewniający poufność EES i uniemożliwiający im dostęp do danych EES, w szczególności dotyczących osób ubiegających się o azyl.

d) Więcej informacji

- „Praktyczny podręcznik EES" Komisji Europejskiej dla organów krajowych (niedostępny publicznie).
- Rada Europy, Europejski Trybunał Praw Człowieka i Agencja Praw Podstawowych Unii Europejskiej, Podręcznik europejskiego prawa dotyczącego azylu, granic i imigracji – Wydanie 2020, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020, w szczególności rozdział 2. Aktualizacja zaplanowana na 2026 r.
- Agencja Praw Podstawowych Unii Europejskiej, Zatrzymanie migrantów o nieuregulowanym statusie – kwestie związane z prawami podstawowymi, 2012.

7. Włączenie praw podstawowych do szkoleń

Szkolenie ma kluczowe znaczenie dla EES zgodnego z prawami podstawowymi. Gwarantuje to, że cały personel uczy się, jak radzić sobie z różnymi sytuacjami, które mogą napotkać w praktyce, w sposób w pełni szanujący prawa jednostek.

a) Wybrane kluczowe wnioski

Poniższe wnioski zostały uzyskane w wyniku badań jakościowych.

- Na badanych BCP stosunkowo niewielu funkcjonariuszy straży granicznej miało możliwość udziału w specjalistycznych szkoleniach stacjonarnych dotyczących EES. Większość z nich uczestniczyła w szkoleniach on-line, co było postrzegane jako ograniczenie pod względem dostępu do praktycznych ćwiczeń, bezpośredniej informacji zwrotnej oraz możliwości omówienia rzeczywistych scenariuszy z trenerami i współpracownikami.
- W momencie prowadzenia badań na BCP wielu funkcjonariuszy nie wiedziało, jakie kroki należy podjąć w przypadku błędnego wprowadzenia danych do EES.
- W tym samym czasie wielu funkcjonariuszy nie było jeszcze świadomych mechanizmów korekty danych w systemie EES.

Badanie przeprowadzone wśród straży granicznej ujawniło następujące ustalenia.

- Funkcjonariusze straży granicznej wymienili następujące potrzeby szkoleniowe: kategorie pasażerów zwolnionych z systemu wjazdu/wyjazdu (60%), procedury dotyczące osób ubiegających się o azyl i ich rejestracji w systemie wjazdu/wyjazdu (45%), możliwości korekty danych w pierwszej linii i procedury ukierunkowanej pomocy (45%), procedury dotyczące dzieci (42%), przeprowadzanie dokładnych kontroli w przypadku rozbieżności w systemie wjazdu/wyjazdu (41%), pobieranie i weryfikowanie danych biometrycznych od osób o specjalnych potrzebach (36%), skuteczna komunikacja z obywatelami państw trzecich (28%) oraz wykorzystanie przyszłej interoperacyjności wielkoskalowych systemów informacyjnych UE podczas odpraw granicznych (21%) (n = 173).

b) Odniesienia prawne

Art. 38 ust. 5 rozporządzenia w sprawie EES stanowi, że pracownicy, którym zezwolono na dostęp do danych w EES i korzystanie z nich, muszą najpierw przejść odpowiednie szkolenie. Szkolenie to powinno dotyczyć tego, jak zapewnić bezpieczeństwo danych, jak chronić dane osobowe osób i jak przestrzegać ich praw podstawowych.

c) Wytyczne

Poniższe wytyczne mogą pomóc organom krajowym w zwiększeniu wiedzy i umiejętności w zakresie praw podstawowych wszystkich pracowników pracujących z EES.

- **Wytyczne 7.1:** Regularne przeglądanie i aktualizowanie komponentów dotyczących praw podstawowych w szkoleniach EES dla dostosowania ich treści do zmieniających się praktyk i wyciągniętych wniosków.

Poniższe wytyczne mogą również wchodzić w zakres kompetencji urzędników wyższego szczebla na przejściach granicznych.

- **Wytyczne 7.2:** Włączenie praw podstawowych do uczenia się w miejscu pracy w ramach EES w celu pogłębienia wiedzy i dostosowania się do zmieniających się praktyk i obowiązków.
- **Wytyczne 7.3:** Dalsze oferowanie ukierunkowanych szkoleń dla funkcjonariuszy pierwszej linii w zakresie następujących aspektów praw podstawowych dotyczących EES:
  - Jak pobierać odciski palców i wykonywać zdjęcia twarzy w sposób wrażliwy na potrzeby dzieci i uwzględniający płeć;
  - Jak udzielać jasnych i niedyskryminujących wyjaśnień dotyczących celu i przebiegu zbierania danych biometrycznych;
  - Jak stosować komunikację przyjazną dzieciom, w tym prosty i niebudzący lęku język, oraz jak udostępniać materiały informacyjne odpowiednie dla dzieci (np. przewodniki ilustrowane, filmy);

- Jak respektować zasady ochrony danych, przepisy dotyczące cyberbezpieczeństwa, zasady bezpieczeństwa danych oraz przepisy dotyczące sieci i systemów informacyjnych, na podstawie przykładów i symulacji przypadków użycia;
- Jak traktować osoby z poszanowaniem godności i profesjonalizmem podczas pobierania danych biometrycznych, z uwzględnieniem wrażliwości kulturowej i świadomości uprzedzeń niejawnych;
- Jak stosować podejście „człowiek w pętli" („human-in-the-loop") przy ocenie jakości danych oraz ryzyka możliwych błędów wprowadzania lub dopasowywania danych;
- Jak skutecznie informować obywateli państw trzecich, którzy zgłosili żądanie sprostowania, uzupełnienia lub usunięcia swoich danych;
- Jak rozpoznawać oznaki stresu lub dyskomfortu oraz udzielać wsparcia, szczególnie osobom o szczególnych potrzebach, takim jak dzieci, osoby starsze i osoby z niepełnosprawnościami;
- Jak wspierać osoby z niepełnosprawnościami i inne osoby o szczególnych potrzebach w sposób szanujący ich prywatność i bezpieczeństwo oraz profesjonalny;
- Jak oceniać uzasadnione przyczyny przekroczenia okresu pobytu i jak traktować osoby przekraczające dozwolony okres pobytu z godnością i bezstronnie, zgodnie z zasadą niedyskryminacji, niezależnie od ich statusu prawnego;
- Jak traktować wnioskodawców ubiegających się o ochronę międzynarodową, których dane zostały już zarejestrowane w EES, zapewniając poszanowanie ich godności, prawa do azylu oraz zasady *non-refoulement*.

d) Więcej informacji

- „Praktyczny podręcznik EES" Komisji Europejskiej dla organów krajowych (niedostępny publicznie).
- Agencja Praw Podstawowych Unii Europejskiej, Kontrole graniczne a prawa podstawowe na lądowych granicach zewnętrznych – praktyczne wskazówki, Urząd Publikacji Unii Europejskiej, Luksemburg, 2020 r., pkt 10.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Przypisy końcowe

1. „n” oznacza liczbę funkcjonariuszy straży granicznej, którzy odpowiedzieli na konkretne pytanie na wszystkich dziewięciu przejściach granicznych, na których przeprowadzono badania terenowe, spośród 177 uczestników badania. Łączna liczba respondentów w odniesieniu do każdego pytania uwzględnia zarówno respondentów, którzy udzielili istotnych odpowiedzi na pytania, jak i tych, którzy wybrali warianty odpowiedzi „nie wiem” lub „wolę nie mówić”. Nie uwzględniono w nim odpowiedzi na pytania zawarte w kwestionariuszu, w których nie wybrano żadnej opcji odpowiedzi.

2. „n” oznacza liczbę funkcjonariuszy straży granicznej, którzy odpowiedzieli na konkretne pytanie na wszystkich dziewięciu przejściach granicznych, na których przeprowadzono badania terenowe, spośród 177 uczestników badania. Łączna liczba respondentów w odniesieniu do każdego pytania uwzględnia zarówno respondentów, którzy udzielili istotnych odpowiedzi na pytania, jak i tych, którzy wybrali warianty odpowiedzi „nie wiem” lub „wolę nie mówić”. Nie uwzględniono w nim odpowiedzi na pytania zawarte w kwestionariuszu, w których nie wybrano żadnej opcji odpowiedzi.

3. „n” oznacza liczbę funkcjonariuszy straży granicznej, którzy odpowiedzieli na konkretne pytanie na wszystkich dziewięciu przejściach granicznych, na których przeprowadzono badania terenowe, spośród 177 uczestników badania. Łączna liczba respondentów w odniesieniu do każdego pytania uwzględnia zarówno respondentów, którzy udzielili istotnych odpowiedzi na pytania, jak i tych, którzy wybrali warianty odpowiedzi „nie wiem” lub „wolę nie mówić”. Nie uwzględniono w nim odpowiedzi na pytania zawarte w kwestionariuszu, w których nie wybrano żadnej opcji odpowiedzi.

4. „n” oznacza liczbę funkcjonariuszy straży granicznej, którzy odpowiedzieli na konkretne pytanie na wszystkich dziewięciu przejściach granicznych, na których przeprowadzono badania terenowe, spośród 177 uczestników badania. Łączna liczba respondentów w odniesieniu do każdego pytania uwzględnia zarówno respondentów, którzy udzielili istotnych odpowiedzi na pytania, jak i tych, którzy wybrali warianty odpowiedzi „nie wiem” lub „wolę nie mówić”. Nie uwzględniono w nim odpowiedzi na pytania zawarte w kwestionariuszu, w których nie wybrano żadnej opcji odpowiedzi.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Informacje o tej publikacji

Luksemburg: Urząd Publikacji Unii Europejskiej, 2025 r.

html

- TK-01-25-032-PL-Q
- ISBN: 978-92-9489-685-8
- DOI: 10.2811/9691582

PDF

- TK-01-25-032-EN-N
- ISBN: 978-92-9489-686-5
- DOI: 10.2811/8877592

Zdjęcia (okładka):

- Okładka: © FRA

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

FRA – AGENCJA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ

Schwarzenbergplatz 11 – 1040 Wiedeń – Austria

T +43 158030-0 – F +43 158030-699

- Strona internetowa
- LinkedIn
- Instagram
- Facebook
- YouTube
- X

Nowe spojrzenie na zarządzanie danymi

Rozpoczynamy cykl publikacji na temat Europejskiej strategii w zakresie danych oraz nowej Europejskiej strategii w zakresie unii danych. Na początku przybliżymy Państwu rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danym (Akt ws. zarządzania danymi Dz. Urz. UE L 152 z 3.6.2022, s. 1–44), określane jako DGA, oraz omówimy nowe zadania Prezesa UODO wynikające z projektowanych przepisów ustawy o zarządzaniu danymi.

Akt ws. zarządzania danymi w pełni obowiązuje od 23 września 2023 r. Jednakże jego pełne stosowanie jest uzależnione od przyjęcia przepisów krajowych, nad którymi obecnie trwają prace legislacyjne. Rządowy projekt ustawy o zarządzaniu danymi (Druk 2060) wpłynął do Sejmu RP 2 grudnia 2025 r.

Kolejnym aktem prawnym, który został przyjęty w ramach Europejskiej strategii w zakresie danych, jest rozporządzenie Parlamentu i Rady (UE) 2023/2854 z 13 grudnia 2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (Akt ws. Danych Dz. Urz. UE L 2023/2854, 22.12.2023.). To rozporządzenie jest bezpośrednio stosowane od 12 września 2025 r., a w ramach rządowego procesu legislacyjnego rozpoczęły się prace nad projektem ustawy o sprawiedliwym dostępie do danych i ich wykorzystywaniu (UC114).

Komisja Europejska opublikowała 19 listopada 2025 r. pakiet zmian unijnych regulacji, zwany Cyfrowym Omnibusem, który zakłada istotne zmiany ww. rozporządzeń.

Sukcesywnie będziemy omawiali obecnie obowiązujące przepisy prawa oraz przebieg procesu legislacyjnego na poziomie unijnym i krajowym.

6 INNOWACJE I ZARZĄDZENIE DANYMI

DGA w pigułce

1. Ogólne informacje o DGA

Akt w sprawie zarządzania danymi ma na celu zwiększenie zaufania do dzielenia się danymi poprzez ustanowienie odpowiednich mechanizmów kontroli sprawowanej przez osoby, których dane dotyczą, i posiadaczy danych nad danymi, które ich dotyczą, oraz w celu usunięcia innych barier dla dobrze funkcjonującej i konkurencyjnej gospodarki opartej na danych (Motyw 5 DGA). Jest to akt o charakterze międzysektorowym, którego celem jest ustanowienie ram prawnych wzmacniających zaufanie do dobrowolnego udostępniania danych.

DGA wprowadza szereg mechanizmów mających zapewnić bezpieczny i przejrzysty przepływ danych, w szczególności poprzez:

- uregulowanie zasad ponownego wykorzystywania określonych kategorii danych pozostających w posiadaniu podmiotów sektora publicznego, które podlegają ochronie praw osób trzecich (tzw. dane chronione);
- ustanowienie ram prawnych dla działalności dostawców usług pośrednictwa w zakresie danych w celu zwiększenia zaufania między podmiotami udostępniającymi i korzystającymi z danych;
- zachęcanie do udostępniania danych w interesie publicznym (altruizm danych);
- ustanowienie Europejskiej Rady ds. Innowacji w zakresie Danych, której zadaniem jest wspieranie spójnego stosowania przepisów i wymiany dobrych praktyk między państwami członkowskimi.

1. Nowe zadania Prezesa UODO

Zgodnie z brzmieniem projektu ustawy o zarządzaniu danymi Prezesowi UODO powierzono rolę organu właściwego zarówno do spraw usług pośrednictwa danych, jak i rejestracji organizacji altruizmu danych. Projekt ustawy przyznaje także Prezesowi UODO kompetencje w zakresie prowadzenia postępowań dotyczących naruszeń zasad przekazywania danych nieosobowych do państw trzecich.

6 INNOWACJE I ZARZĄDZENIE DANYMI

1. DGA a RODO

Akt w sprawie zarządzania danymi i rozporządzenie (UE) 2016/679 (RODO) są wobec siebie komplementarne w ten sposób, że RODO reguluje zasady ochrony danych osobowych, natomiast DGA ustanawia ramy prawne dla ich ponownego wykorzystywania i udostępniania.

Zgodnie z art. 1 ust. 3 DGA to rozporządzenie pozostaje bez uszczerbku dla RODO, w tym z uwzględnieniem uprawnień i kompetencji organów nadzorczych. W przypadku kolizji pomiędzy niniejszym rozporządzenia a prawem Unii w dziedzinie ochrony danych osobowych lub prawem krajowym przyjętym zgodnie z takim prawem Unii pierwszeństwo ma odpowiednie prawo Unii lub prawo krajowe w dziedzinie ochrony danych osobowych. Jednocześnie DGA nie tworzy podstawy prawnej do przetwarzania danych osobowych ani nie ma wpływu na obowiązki i prawa określone w RODO.

1. Wybrane definicje

Artykuł 2 DGA określa katalog definicji, odwołując się do pojęć zdefiniowanych w RODO, jak i wprowadzając nowe kategorie pojęciowe.

Dzielenie się danymi to dostarczanie danych przez osobę, której dane dotyczą, lub przez posiadacza danych użytkownikowi danych do celów wspólnego lub indywidualnego wykorzystywania takich danych na bazie dobrowolnych umów lub na podstawie prawa Unii lub prawa krajowego, bezpośrednio lub z udziałem pośrednika, np. w ramach licencji otwartych lub handlowych, bezpłatnie lub za opłatą (pkt 10).

Usługa pośrednictwa danych oznacza usługę, która ma na celu ustanowienie – za pomocą środków technicznych, prawnych lub innych – stosunków handlowych między – z jednej strony – nieokreśloną liczbą osób, których dane dotyczą, i posiadaczy danych, oraz – z drugiej strony – użytkownikami danych do celów dzielenia się danymi, w tym do celów wykonywania praw osób, których dane dotyczą, w odniesieniu do danych osobowych (pkt 11).

Pojęcie to nie obejmuje: a) usług, w ramach których dane są pozyskiwane od posiadaczy danych i agregowane, wzbogacane lub przekształcane w celu dodania im znaczącej wartości, a następnie użytkownikom danych udzielana jest licencja na wykorzystanie uzyskanych w ten sposób danych bez ustanawiania stosunku handlowego między nimi a posiadaczami danych; b) usług skoncentrowanych na pośrednictwie treści chronionych prawem autorskim; c) usług, z których korzysta wyłącznie jeden posiadacz danych w celu umożliwienia wykorzystywania danych będących w jego posiadaniu, lub usługi, z których korzysta wiele osób prawnych w zamkniętej grupie, w tym w ramach stosunków z dostawcami lub klientami lub współpracy nawiązanej na podstawie umowy, w szczególności usług, których głównym celem jest zapewnienie funkcjonalności przedmiotów i urządzeń podłączonych do internetu rzeczy; d) usług dzielenia się danymi oferowanych przez podmioty sektora publicznego, które to usługi nie mają na celu ustanowienia stosunków handlowych.

6 INNOWACJE I ZARZĄDZENIE DANYMI

Zgodnie z art. 10 DGA, usługi pośrednictwa danych obejmują:

a) usługi pośrednictwa między posiadaczami danych a potencjalnymi użytkownikami danych, w tym udostępnianie środków technicznych lub innych umożliwiających świadczenie takich usług; usługi te mogą obejmować dwustronną lub wielostronną wymianę danych lub tworzenie platform lub baz danych umożliwiających wymianę lub wspólne wykorzystywanie danych, jak również tworzenie innej specjalnej infrastruktury do stworzenia powiązań między posiadaczami danych a użytkownikami danych;

a) usługi pośrednictwa między osobami, których dane dotyczą, zamierzającymi udostępnić swoje dane osobowe, lub osobami fizycznymi zamierzającymi udostępnić dane nieosobowe a potencjalnymi użytkownikami danych, w tym udostępnianie środków technicznych lub innych umożliwiających świadczenie takich usług, w szczególności umożliwiających wykonywanie ustanowionych w RODO praw osób, których dane dotyczą;
b) usługi świadczone przez spółdzielnie danych.

Altruizm danych oznacza dobrowolne dzielenie się danymi na podstawie wyrażonej przez osoby, których dane dotyczą, zgody na przetwarzanie dotyczących ich danych osobowych lub na podstawie udzielonego przez posiadaczy danych pozwolenia na wykorzystywanie ich danych nieosobowych, bez żądania ani otrzymania za to wynagrodzenia wykraczającego poza zwrot kosztów poniesionych przez te osoby lub posiadaczy w związku z udostępnieniem ich danych do celów leżących w interesie ogólnym określonych – w stosownych przypadkach – w prawie krajowym, takich jak opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawa świadczenia usług publicznych, kształtowanie polityki publicznej lub do celów badań naukowych leżących w interesie ogólnym (pkt 16).

1. Więcej informacji

Zachęcamy Państwa do zapoznania się z dodatkowymi materiałami poświęconymi Aktowi w sprawie zarządzania danymi:

- Wytyczne KE w sprawie DGA
- Webinarium UODO pt. „Nowe zadania Prezesa UODO w zakresie zarządzania danymi.”
- Konferencja naukowa DGA – Innowacyjne zarządzanie danymi

przepisy prawa oraz przebieg procesu legislacyjnego na poziomie unijnym i krajowym.

Uczestnicy programu „Twoje dane – Twoja sprawa” świętują XX Dzień Ochrony Danych Osobowych – edukacja, świadomość i odpowiedzialność za dane osobowe w cyfrowym świecie

Na przełomie stycznia i lutego 2026 r. już po raz dwudziesty obchodziliśmy Dzień Ochrony Danych Osobowych. To święto, ustanowione przez Komitet Ministrów Rady Europy w rocznicę przyjęcia Konwencji nr 108, które przypomina o fundamentalnym znaczeniu prawa do prywatności i ochrony danych osobowych w życiu każdego człowieka. Obchody z tej okazji, organizowane przez szkoły oraz placówki doskonalenia nauczycieli, służą wzmacnianiu świadomości młodych ludzi w zakresie ochrony danych osobowych oraz kształtowaniu odpowiedzialnych postaw w świecie nowych technologii. Uczestnicy programu podejmują liczne działania informacyjne i społeczne, które nie tylko zwiększają wiedzę uczniów o przysługujących im prawach, w szczególności do ochrony danych osobowych, lecz także promują dobre praktyki w zakresie ochrony prywatności. Program edukacyjny „Twoje dane – Twoja sprawa” od lat wspiera szkoły i placówki doskonalenia nauczycieli w budowaniu kultury poszanowania danych osobowych, a jednocześnie rozwija kompetencje cyfrowe uczniów i nauczycieli, odpowiadając na wyzwania współczesnej rzeczywistości.

W ramach tegorocznych obchodów przygotowano i udostępniono szkołom materiały edukacyjne, w tym krótką poradę z cyklu „Warto wiedzieć” oraz webinarium poświęcone technologii deepfake i konsekwencjom, do jakich może doprowadzić jej niewłaściwe użytkowanie. Przygotowane dla uczestników programu materiały są wykorzystywane podczas lekcji, zajęć wychowawczych, wydarzeń tematycznych oraz w szkolnych gazetkach, stając się impulsem do rozmów o bezpieczeństwie w sieci, odpowiedzialnym korzystaniu z technologii i świadomym podejmowaniu decyzji w środowisku cyfrowym. **W niniejszym biuletynie publikujemy również treść porady przekazanej uczestnikom programu, aby mogła służyć jako wsparcie do kolejnych działań edukacyjnych dla wszystkich osób zainteresowanych ochroną danych osobowych dzieci i młodzieży.**

Deepfake – nowe wyzwania dla ochrony danych osobowych i bezpieczeństwa dzieci

Szczególne miejsce w tegorocznych obchodach zajęło webinarium skierowane do przedstawicieli szkół, placówek doskonalenia nauczycieli oraz rodziców i opiekunów, zatytułowane: **„Deepfake – nowe wyzwania w cyfrowym świecie. Jak zapobiegać i reagować w trosce o bezpieczeństwo dzieci”.** Podczas spotkania omówiono wyzwania, jakie dla ochrony danych osobowych stwarza technologia deepfake, tj. treści audio i wideo generowanych z wykorzystaniem sztucznej inteligencji, które mogą

wprowadzać odbiorców w błąd, naruszać prywatność oraz prowadzić do poważnych konsekwencji dla osób, których dane osobowe, w szczególności wizerunek, zostały wykorzystane.
Uczestnicy poznali metody rozpoznawania fałszywych materiałów, zagrożenia związane z dezinformacją oraz sposoby reagowania w sytuacjach kryzysowych w środowisku szkolnym.

W pierwszej części webinarium Michał Sajdak (Sekurak.pl) przedstawił techniczne aspekty funkcjonowania deepfake'ów, ich wykrywania oraz przykłady wykorzystania tej technologii w cyberatakach. **Materiał ukierunkowany był na zwiększenie świadomości uczestników programu odnośnie do możliwości skuteczniejszego rozpoznawania i osłabiania wpływu tego rodzaju ataków.** Druga część, prowadzona przez Natalię Misiuk – zastępcę Dyrektora Departamentu Inicjatyw Edukacyjnych UODO – dotyczyła relacji pomiędzy deepfake'ami a ochroną danych osobowych, roli Prezesa UODO, znaczenia rozmów z dziećmi i młodzieżą oraz praktycznych wskazówek dotyczących reagowania na niebezpieczne treści.

„Warto wiedzieć" – praktyczne wskazówki dla uczniów

Integralną częścią działań edukacyjnych była porada z cyklu „Warto wiedzieć", która w przystępny sposób wyjaśnia, czym jest deepfake, jakie zagrożenia może powodować oraz jak bezpiecznie korzystać z narzędzi opartych na sztucznej inteligencji. Podejmowane działania podkreślają znaczenie krytycznego podejścia do treści publikowanych w internecie, konieczność weryfikowania źródeł informacji oraz potrzebę reagowania na sytuacje budzące niepokój.

Wspólna odpowiedzialność za przyszłość

Z okazji jubileuszowych obchodów XX Dnia Ochrony Danych Osobowych do uczestników programu „Twoje dane – Twoja sprawa", skierowany został list od Mirosława Wróblewskiego, prezesa UODO, który wyraził w nim uznanie dla dyrektorów, nauczycieli i uczniów za ich konsekwentne zaangażowanie w budowanie kultury ochrony danych osobowych. Podkreślił, że edukacja – rzetelna, atrakcyjna i oparta na wartościach – stanowi jedno z najskuteczniejszych narzędzi przygotowujących młode pokolenie do świadomego i bezpiecznego funkcjonowania w cyfrowym świecie.
Tegoroczne obchody po raz kolejny dowiodły, że ochrona danych osobowych to nie tylko przepisy prawa, lecz przede wszystkim codzienne wybory, postawy i odpowiedzialność każdego z nas. Dzięki wspólnym inicjatywom edukacyjnym oraz zaangażowaniu środowiska oświatowego możliwe jest skuteczne budowanie świadomości, która przynosi realne korzyści już dziś i przekłada się na długofalowe pozytywne zmiany społeczne.

Warto wiedzieć…

Deepfake

Nowe wyzwania dla ochrony danych osobowych i bezpieczeństwa

Deepfake to technologia wykorzystująca sztuczną inteligencję, która pozwala na tworzenie fałszywych, ale bardzo realistycznych obrazów, filmów lub dźwięków. Może sprawiać wrażenie, że ktoś powiedział lub zrobił coś, co w rzeczywistości nigdy się nie wydarzyło. Technologia ta jest niestety również wykorzystywana w działalności przestępczej, kradzieży tożsamości, wyłudzeniach pieniędzy lub danych osobowych.

Przykłady zagrożeń:

- może kogoś ośmieszyć lub skrzywdzić np. przez przerabianie zdjęć konkretnej osoby,
- może być używana do oszukiwania ludzi np. do tworzenia fałszywych wiadomości lub podszywania się pod kogoś w celu wyłudzenia danych osobowych lub pieniędzy,
- może stać się narzędziem hejtu, szantażu lub zastraszania,
- może sprawić, że trudno odróżnić to, co prawdziwe, od tego, co zostało zmanipulowane.

Jak rozpoznać deepfake? Zwróć uwagę na szczegóły m.in:

- twarz, która wygląda nienaturalnie, jest zniekształcona lub „nie pasuje" do reszty ciała,
- ruchy ust, które nie pokrywają się z tym, co słyszysz,
- ruchy ciała, które mogą być bardzo nienaturalne lub nierealistyczne,
- źródło pochodzenia nagrania – sprawdź, czy materiał pochodzi z wiarygodnego i zaufanego źródła,
- treść, która brzmi nierealnie, absurdalnie albo sprzecznie z tym, co wiesz o świecie.

Jak bezpiecznie korzystać z takich narzędzi?

- nie używaj zdjęć prawdziwych osób,
- nie twórz materiałów, które kogoś ośmieszają lub mogą przestraszyć,
- jeśli tworzysz deepfake na potrzeby zabawy – wyraźnie zaznacz, że materiał jest fałszywy.

Technologia jest narzędziem — decyduj świadomie, w jakim celu jej używasz.

PAMIĘTAJ!

Technologia deepfake może być wykorzystana w zarówno dobrych, jak i złych celach. Z jednej strony może pomóc np. w poprawie jakości produkcji filmowych i dźwiękowych. Z drugiej jednak – może służyć do tworzenia fałszywych treści, które szerzą dezinformację. Należy pamiętać, że nie wszystko, co znajduje się w internecie, jest prawdziwe, a wiele deepfake'ów do złudzenia przypomina prawdziwe materiały. Jeśli coś wzbudza Twoje wątpliwości lub niepokój – porozmawiaj o tym z osobą dorosłą.

URZĄD OCHRONY DANYCH OSOBOWYCH

Warto wiedzieć…

Trudne słowa – proste wyjaśnienia

Co oznaczają słowa, które pojawiają się w poradzie?

•**Deepfake** – to technologia wykorzystująca sztuczną inteligencję do tworzenia fałszywych, ale bardzo realistycznych obrazów, filmów lub dźwięków w celu pokazania czegoś, co nigdy się nie wydarzyło. Wykorzystuje do tego techniki uczenia (deep learning) i fałszowania (fake).

•**Deepfake audio** – koncentruje się na manipulacji dźwiękiem i ludzkim głosem. Za pomocą tej technologii można tworzyć fałszywe nagrania głosowe, w których osoba wydaje się mówić lub śpiewać coś, czego w rzeczywistości nie powiedziała lub nie zaśpiewała. Deepfake audio jest często wykorzystywany w tworzeniu fałszywych nagrań rozmów telefonicznych lub przemówień.

•**Deepfake video** – polega na manipulacji materiałami filmowymi, w szczególności twarzami i ciałami. Dzięki tej technologii można stworzyć nieprawdziwe materiały video. Deepfake video jest używane do różnych celów np. do manipulacji informacjami i tworzenia fałszywych treści.

•**Dezinformacja** – to celowe rozpowszechnianie fałszywych lub wprowadzających w błąd treści, informacji, tzw. fake newsów. Technologia deepfake bardzo często jest wykorzystywana do tworzenia takich treści.

•**Sztuczna inteligencja** – zwana również AI (ang. Artificial Intelligence), to dziedzina informatyki zajmująca się tworzeniem maszyn i systemów, które potrafią wykonywać zadania wymagające ludzkiej inteligencji. Obejmuje to takie umiejętności jak rozumowanie, uczenie się, rozwiązywanie problemów, postrzeganie i podejmowanie decyzji.

•**Dane osobowe** – to informacje, które mogą pomóc kogoś zidentyfikować, np. imię i nazwisko, adres, numer telefonu, e-mail, głos czy wizerunek. Takich danych nie powinno się udostępniać nieznanym osobom i aplikacjom bez potrzeby.

W lutym 2026 Prezes UODO zaprasza na wydarzenie towarzyszące obchodom 20. Dnia Ochrony Danych Osobowych.

28 stycznia 1981 r.

W Strasburgu otwarto do podpisu Konwencję nr 108 Rady Europy – pierwszy prawnie wiążący międzynarodowy akt dotyczący ochrony danych osobowych. Dokument wyznaczył podstawowe standardy ochrony prywatności w Europie i na świecie. Na jego cześć 28 stycznia ustanowiono Dzień Ochrony Danych Osobowych.

XII Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej

Termin: **6 lutego 2026 r.**

Miejsce: **Akademia WSB w Dąbrowie Górniczej**, ul. Cieplaka 1c.

Wystąpienie Prezesa UODO Mirosława Wróblewskiego, pt. ,,Deepfake – ochrona danych w kontekście nowych technologii".

W lutym 2026 Prezes UODO zaprasza na wydarzenie towarzyszące obchodom 20. Dnia Ochrony Danych Osobowych.

28 stycznia 1981 r.

W Strasburgu otwarto do podpisu Konwencję nr 108 Rady Europy – pierwszy prawnie wiążący międzynarodowy akt dotyczący ochrony danych osobowych. Dokument wyznaczył podstawowe standardy ochrony prywatności w Europie i na świecie. Na jego cześć 28 stycznia ustanowiono Dzień Ochrony Danych Osobowych.

XII Dzień Otwarty Urzędu Ochrony Danych Osobowych w Akademii WSB w Dąbrowie Górniczej

Termin: **6 lutego 2026 r.**

Miejsce: **Akademia WSB w Dąbrowie Górniczej**, ul. Cieplaka 1c.

Wystąpienie Prezesa UODO Mirosława Wróblewskiego, pt. ,,Deepfake – ochrona danych w kontekście nowych technologii".

X Konferencja „Dzień Ochrony Danych Osobowych w sektorze medycznym".

Termin: **9 marca 2026 r.**

Organizator: **Abi Expert i wydawnictwo Presscom**

Miejsce: **Arche Hotel Puławska Residence, Warszawa, ul. Puławska 361.**

Wystąpienie eksperta Departamentu Prawa i Nowych Technologii UODO, pt. „Projektowanie ochrony danych medycznych w świetle deficytów legislacyjnych w prawie krajowym".

Pozostałe wydarzenia UODO

Konferencja „EHDS 2026. Wtórne przetwarzanie danych osobowych oraz prawa osób fizycznych”

Termin: **24 marca 2026 r.**

Formuła: **online**

Organizatorzy: **Wydział Prawa i Administracji Uniwersytetu Warszawskiego, Instytut Nauk Prawnych Polskiej Akademii Nauk, Prezes Urzędu Ochrony Danych Osobowych, Wydział Medyczny Uniwersytetu Warszawskiego**

Europejska przestrzeń danych dotyczących zdrowia (EHDS) ma na celu uwolnienie wartości danych medycznych poprzez umożliwienie zgodnego z prawem, bezpiecznego i efektywnego wtórnego wykorzystania danych do celów badań i innowacji. Jej wdrożenie fundamentalnie zmienia podział obowiązków między właściwymi organami, świadczeniodawcami opieki zdrowotnej, naukowcami i podmiotami prywatnymi oraz na nowo definiuje ochronę praw podstawowych w obszarze zdrowia cyfrowego. W trakcie konferencji planowane są wystąpienia, które krytycznie przeanalizują prawne, instytucjonalne i praktyczne implikacje wtórnego wykorzystania danych medycznych w ramach EHDS.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl