URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 02/26

www.uodo.gov.pl

SPIS TREŚCI

SPIS TREŚCI

Szanowni Państwo,
podsumowując nasze prace w lutym 2026 r., chciałbym zwrócić uwagę na jedną ważną sprawę.

W mediach pojawiły się ostatnio informacje, że planowane przez Prezesa UODO sektorowe kontrole, które w tym roku obejmą podmioty prowadzące Biuletyn Informacji Publicznej, mogą się skończyć wysokimi karami administracyjnymi i godzić w przejrzystość działania organów samorządu terytorialnego.

Kontrole PUODO nie są równoznaczne z karami. Prowadzimy je po to, by poprawić ochronę danych osobowych. Z naszych rocznych sprawozdań jasno wynika, że na BIP-ach ujawniane są dane osobowe – na ogół przez pomyłkę albo z pośpiechu, bowiem dokumenty tam publikowane nie są odpowiednio anonimizowane. Wiele samorządów opracowało i wdrożyło odpowiednie polityki ochrony danych, zaczęło dokonywać ich systematycznych przeglądów. Jednak nie dzieje się tak wszędzie i praca UODO ma pomóc w przeprowadzeniu takich zmian.

Prezes UODO sięga po kary tylko w wyjątkowych sytuacjach. Naszym celem jest zapobieganie incydentom z danymi. Mamy do tego wiele narzędzi, a kara finansowa jako sposób na wymuszenie zmian na przyszłość jest ostatecznością.

Edukacja i legislacja

Staramy się przede wszystkim podkreślać, jak zmiany technologiczne wymuszają na nas wszystkich bardziej staranne podejście do problemu danych osobowych. Nie tylko w administracji. Chodzi o wiedzę, procedury i praktyki organizacyjne.

Przykładem takich naszych działań niech będzie ostatnie webinarium o deepfake'ach, dezinformacji i ochronie danych w dobie Al. Zorganizowaliśmy je dla uczestników programu „Twoje dane – Twoja sprawa". Temat deepfake'ów był również jednym z ważnych wątków poruszanych podczas Kongresu Ochrony Danych Osobowych i Nowych Technologii w styczniu. Zagadnienie to omawiano m.in. w ramach paneli poświęconych wyzwaniom prawnym, społecznym i technologicznym, a ja sam moderowałem jeden z paneli. Wykład „Deepfake – ochrona danych w kontekście nowych technologii" wygłosiłem też podczas XII Dnia Otwartego Urzędu Ochrony Danych Osobowych, który odbył się 6 lutego 2026 r. w Akademii WSB w Dąbrowie Górniczej

Innym ważnym działaniem uprzedzającym jest takie przygotowywanie prawa, by tworzyło dla nas wszystkich, a zwłaszcza dla młodych pokoleń, bezpieczne ramy korzystania z nowych technologii. W lutym analizowaliśmy w UODO m.in. projekt podstawy programowej wychowania przedszkolnego oraz kształcenia ogólnego dla szkoły podstawowej. Zgłosiliśmy do niego uwagi.

Temat walki z deepfake'ami oraz ochrony dzieci i młodzieży w cyberprzestrzeni, Prezes UODO poruszył też w piśmie do Ministerstwa Cyfryzacji, zawierającym uwagi do projektu nowelizacji ustawy o świadczeniu usług drogą elektroniczną.

W porównaniu z poprzednią podstawą programową, która jedynie ogólnie odnosiła się do korzystania przez uczniów z technologii, w nowym projekcie zdecydowano się na wprowadzenie konkretnych rozwiązań dotyczących higieny cyfrowej oraz bezpieczeństwa danych. To dobra zmiana. Odnieśliśmy się do kilku ważnych kwestii, w tym do tego, w jaki sposób można by w szkołach wprowadzać zakazy korzystania z telefonów komórkowych. Naszym zdaniem takich regulacji nie można wprowadzać rozporządzeniem, lecz ustawą – mówimy bowiem o korzystaniu z konstytucyjnych wolności i praw. Mogą one podlegać ograniczeniu, ale jeśli są wprowadzane ustawą.

Ważne rozstrzygnięcia

Pragnę zwrócić Państwa uwagę na cztery ważne rozstrzygnięcia:

- Po pierwsze – PUODO nałożył administracyjne kary pieniężne na Fundację Lumus po stwierdzeniu dokonania szeregu naruszeń przepisów o ochronie danych osobowych. Sprawa ta i ustalone w jej toku naruszenia wskazują na szerszy, systemowy charakter problemów organizacji pozarządowych, z którymi spotykają się w obszarze przestrzegania przepisów o ochronie danych osobowych osób fizycznych.

- Po drugie, PUODO nałożył karę finansową na firmę kurierską. Tu wykryte problemy były tak duże, że nie można było postąpić inaczej. Okazało się, że firma używała zewnętrznych pośredników do transportowania przesyłek. Nie miała z nimi umów na przetwarzanie danych – więc w transporcie i przy załadunku nie było odpowiednich procedur bezpieczeństwa dla danych. Sposób nadawania pracownikom spółki uprawnień do przetwarzania danych też wzbudził poważne wątpliwości. Takie uprawnienie dostawało się od systemu informatycznego po zaliczeniu testu kończącego e-szkolenie. Tymczasem uprawnienia musi nadawać człowiek – bo tylko tak można zadbać o bezpieczeństwo procesu przetwarzania danych. Maszynowe upoważnienie nie jest prawdziwym upoważnieniem do przetwarzania danych.

Ujawnione w spółce problemy stanowiły bardzo poważne naruszenie przepisów RODO i rodziły ryzyko dla osób, których dane spółka przetwarzała – a były to dane nadawców i odbiorców przesyłek.

- Po trzecie, WSA podtrzymał decyzję PUODO, który ukarał Komendanta Głównego Policji karą finansową za ujawnienie na konferencji prasowej danych osobowych, w tym danych dotyczących zdrowia. Wcześniej media opisały sprawę pewnej kobiety i pokazały, jak potraktowali ją policjanci. Komendant zwołał konferencję prasową, by bronić podwładnych. I ujawnił dane tej osoby. Nie miał do tego podstawy, a ujawnienie danych stanowiło poważne naruszenie prywatności poszkodowanej.

Sprawa ta sięga 2023 r. Po zbadaniu postępowania Komendanta Głównego Policji sprawdziliśmy, jak dane osobowe pokrzywdzonej trafiły do niego z Komendy Miejskiej. To postepowanie też zakończyło się decyzją o nałożeniu kary. PUODO ustalił bowiem, że dane kobiety trafiły do komunikatu prasowego w Komendzie Miejskiej z wewnętrznego systemu Policji, ponieważ Komenda nie zanalizowała ryzyka ani nie przygotowała wynikających z takiej analizy procedur administracyjnych i technicznych, które chroniłyby dane osobowe przed nieuprawnionym ujawnieniem.

- Po czwarte, NSA oddalił skargę kasacyjną właściciela kliniki stomatologicznej na decyzję Prezesa UODO.

W tej sprawie chodziło o to, że właściciel kliniki zbywał PUODO, który chciał się upewnić, że zrobiono wszystko, by ochronić prawa osób, których dane skopiował pracownik kliniki do prywatnych celów. Skończyło się to karą dla przedsiębiorcy. Miała ona taki skutek, że przedsiębiorca przedstawił następnie PUODO dowody należycie wykonanego obowiązku poinformowania zainteresowanych o incydencie. Teraz NSA potwierdził prawidłowość działania PUODO.

Uwaga, e-doręczenia

Na koniec chciałbym wskazać na to, że uwzględniliśmy już nowe przepisy o e-doręczeniach w wymogach akredytacji podmiotów monitorujących kodeksy postępowania oraz dodatkowych wymogach akredytacji podmiotów certyfikujących.

Zmiany dotyczą wymaganej formy kontaktu z Urzędem Ochrony Danych Osobowych. Skrzynki elektroniczne, które stanowiły formę kontaktu we wcześniejszych wersjach wymogów, zostały wycofane z użycia i zastąpione skrzynkami do e-doręczeń.

Zmiany były konsultowane z Europejską Radą Ochrony Danych.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W najnowszym numerze Biuletynu prezentujemy Wam wywiad z Magdaleną Bigaj – laureatką tegorocznej Nagrody im. Michała Serzyckiego, Prezeską Fundacji Instytut Cyfrowego Obywatelstwa. W rozmowie opowiada m.in., dlaczego lepiej mówić o „higienie cyfrowej" niż uzależnieniach od telefonów czy social mediów, a także o tym, jak kwestię tę rozumieją dzieci i młodzież, a jakie problemy mają z nią dorośli. Rozmawialiśmy też o przemocy rówieśniczej, zakazie używania smartfonów w szkołach, czy też ograbianiu młodego pokolenia z prywatności przez masowe publikowanie ich wizerunku przez szkoły, przedszkola oraz rodziców.

Temat monitoringu w placówkach edukacyjnych i związanych z nim ograniczeń omawiamy również w dziale Nowych Technologii. Przypominamy też niedawny wyrok Naczelnego Sądu Administracyjnego, który podtrzymał decyzję Prezesa UODO w kwestii stosowania monitoringu w altanach śmietnikowych (w celu egzekwowania prawidłowej segregacji śmieci). W sekcji „Orzecznictwo zagraniczne" omawiamy głośny wyrok TSUE, który uznał, iż WhatsApp może zaskarżyć decyzję EROD, oraz stanowisko czeskiego Sądu Najwyższego w sprawie masowego zbierania danych internautów i czasu ich retencji.

Wszystkim administratorom szczególnie polecamy tekst o tym, jak przygotować się do kontroli Prezesa UODO, aby przebiegły one szybko i sprawnie. Z kolei Inspektorów Ochrony Danych zainteresują teksty o roli IOD w sektorze publicznym oraz o konieczności powołania IOD przez sygnatariuszy kodeksu postępowania dla prywatnych agencji badania opinii i rynku. Kontynuujemy także serię tekstów przybliżających Czytelnikom przepisy Aktu o zarządzaniu danymi – „DGA w pigułce". W ramach podsumowania roku przypominamy z kolei najważniejsze statystyki i sprawy z pierwszych dwóch lat kadencji Prezesa UODO.

Sporo miejsca poświęciliśmy również opisowi wkładu Europejskiej Rady Ochrony Danych do cyklicznej ewaluacji stosowania przepisów Dyrektywy policyjnej – i związanym z tym wyzwaniom dla krajowych organów. Osobno omówiliśmy opublikowany niedawno raport z działania Systemu Informacyjnego Schengen w 2024 r. Relacjonujemy także udział Prezesa UODO i innych przedstawicieli Urzędu w wydarzeniach międzynarodowych, szczególnie tych związanych z Dniem Ochrony Danych 2026 r.

Zapraszam serdecznie do lektury!

Karol Witowski
Dyrektor Departamentu Komunikacji Społecznej
Rzecznik Prasowy UODO

TRZEBA ZACZĄĆ DBAĆ O HIGIENĘ CYFROWĄ JAK SIĘ ZOBACZY DWIE KRESKI NA TEŚCIE CIĄŻOWYM

Dobrze by było, żeby przyszli rodzice już mieli pewne zasady higieny cyfrowej wprowadzone w swoim życiu. Bo dzieci uczą się przez naśladowanie. I my często wprowadzamy zamęt w życiu dziecka z jednej strony, oczekując od niego pewnych zachowań, których sami nie przestrzegamy – mówi Magdalena Bigaj, ekspertka od higieny cyfrowej, Prezeska Fundacji Centrum Cyfrowego Obywatelstwa, laureatka nagrody im Michała Serzyckiego.

W tym roku otrzymała Pani nagrodę im. Michała Serzeckiego, zacytuję fragment laudacji: *za wybitne zaangażowanie w ochronę danych osobowych i prawo do prywatności, a w szczególności za działanie edukacyjne, które w istotny sposób przyczyniają się do zwiększenia świadomości zagrożeń* jakie dla najmłodszych użytkowników niosą nowe technologie? A moje pytanie brzmi: za co Pani dałaby sobie nagrodę? Który aspekt Pani pracy jest dla Pani najważniejszy? I który najbardziej satysfakcjonujący?

Magdalena Bigaj: Trudno jest odpowiadać na takie pytania, bo jesteśmy kulturowo wychowywani, żeby się nie chwalić. Ale jakbym miała szczerze i bez fałszywej skromności to powiedzieć, przywołałabym pewnie inny fragment laudacji Prezesa Mirosława Wróblewskiego. Ten, w którym mówił o wprowadzeniu do debaty publicznej i działań systemowych, pojęcia „higieny cyfrowej".
Kiedy ponad 7 lat temu zaczynałam pracę w obszarze, w którym teraz działam, dominowała narracja o „fonoholizmie", czy „e-uzależnieniach". O tym się głównie mówiło w edukacji, która była wtedy prowadzona przede wszystkim w szkołach i skoncentrowana na dzieciach i młodzieży. Ponieważ mam wykształcenie medioznawcze i pracowałam przez ponad dekadę nad tym, jak mówić do ludzi, przekonać ich do czegoś, to pomyślałam: Nikt nie chce być w „fonoholikiem" albo myśleć o sobie, że jest uzależniony od internetu. Ani dorosły, ani dziecko.

Określenie to mocno kojarzy się z „alkoholikiem"…
Dokładnie. I jeżeli wyobrazilibyśmy sobie, że osoba, którą znamy, często sięga po kieliszek wina, to raczej nie powiedzielibyśmy do niej „ Słuchaj, wyglądasz mi na alkoholika". Bo wówczas możemy się spotkać z dużym oporem. Ale jeśli powiemy: „Wiesz, ja też sięgam po alkohol czasami, ale słyszałam, że jak się odstawi, to się lepiej śpi, poprawia się przemiana materii i w ogóle ostatnio czytałam, że alkohol wpływa na stany lękowe" - to jest komunikat neutralny, który nie koncentruje się na słabościach danej osoby, lecz na pozytywach ograniczenia. Odciąża ją trochę z poczucia winy i koncentruje uwagę na tym, że to zachowanie może nie być zdrowe. O ile w przypadku alkoholu, jak pokazują najnowsze badania, nie ma bezpiecznej dawki, o tyle telefon jest narzędziem codziennego użytku – i warto się nauczyć używać go w sposób bezpieczny.

1 ROZMOWA Z EKSPERTEM

Lata temu zdecydowałam, że postawię na higienę cyfrową, o której już trochę się wtedy mówiło, choć raczej w kontekście cyberhigieny, czyli zachowań z obszaru cyberbezpieczeństwa. Ale żeby mówić o tym odpowiedzialnie, rozpoczęłam badania z doktorką Magdaleną Woynarowską z Warszawskiego Uniwersytetu Medycznego.

Co było wynikiem tych badań?

W ramach takich badań trzeba zoperacjonalizować pojęcie, aby właściwie zbadać dane zjawisko. Przyjęłyśmy zasadę: „o rzeczach prostych mów prosto, o trudnych jeszcze prościej." Żeby ludzi do czegoś zachęcić, musisz im to wytłumaczyć. I tak stworzyłyśmy, albo raczej sprecyzowałyśmy definicję „higieny cyfrowej" jako zachowań chroniących zdrowie związanych z używaniem technologii informacyjno-komunikacyjnych, zwłaszcza internetu i urządzeń ekranowych.

A potem promowałam wyniki badań, napisałam pierwszą książkę. I okazało się, że mówienie o dorosłych było naruszeniem jakiegoś tabu. To był swego rodzaju wrzód społeczny, który narastał. I gdy nagle pojawił się komunikat: *Dobra, dzieci mają problem, ale pogadajmy o nas, dorosłych. My mamy problem z higieną cyfrową.* Okazało, że w Polsce ludzie chcą o tym rozmawiać, czytać, mają mnóstwo pytań. Przez ostatnie 4 lata udzieliłam setki wywiadów i wykładów na ten temat, co pokazuje ogromne zainteresowanie społeczne tą kwestią. Ale zmiana musi się zadziać na trzech poziomach.

Jakie to poziomy?

Pierwszy jest indywidualny. Musimy doprowadzić do tego, żeby ludzie chcieli wprowadzać dobre nawyki cyfrowe i aby było to tak oczywiste jak higiena jamy ustnej czy profilaktyka zakażeń. Drugi to poziom społeczny, czyli sprawienie, aby zmieniły się lub w ogóle ukształtowały pewne normy społeczne dotyczące korzystania z telefonów, np. taka, że skrolowanie, gdy ktoś do nas mówi, jest niegrzeczne, a widok dziecka ze smartfonem budził sprzeciw. I wreszcie poziom systemowy, tj. działania podejmowane na poziomie państwa, czy wspólnoty międzynarodowej.

W Fundacji działamy na wszystkich tych poziomach. Po latach widzę, że taka perspektywa to jedyne słuszne podejście. Więc pewnie bym sobie dała nagrodę za to, że lata temu przewidziałam, że warto iść w tę stronę, że to będzie klucz do ludzkich nawyków, ale też do polityków i przede wszystkim, że stanie się to tak ważnym tematem jakim jest dzisiaj.

Książkę oddałam do wydawcy w grudniu 2022 r. i uparłam się, żeby premiera odbyła się jak najwcześniej, bo przeczuwałam, że kolejny rok będzie kluczowy. I faktycznie tak było, w 2023 r. jeszcze przed premierą gruchnęła wieść, że 41 prokuratorów generalnych w USA pozwało firmę Meta za działania na szkodę zdrowia psychicznego nastolatków.

A potem już w zasadzie każdy miesiąc przynosił nowe informacje o nadużyciach ze strony VLOPów, czy innych firm, takich jak rozwijająca się wówczas OpenAI. Gdy patrzę wstecz, to myślę, że przekroczyliśmy pewien Rubikon. To, jak wyglądała debata publiczna 7 lat temu jest nieporównywalne z tym, co dzieje się teraz. Edukatorki naszej fundacji odwiedzając szkoły w całej Polsce widzą, że rodzice się budzą, nauczyciele się budzą, ludzie chcą wprowadzać zmiany. I to jest niesamowite!

Zdecydowanie okazała się Pani trendsetterką i przewidziała koniunkturę. Wspomniała też Pani o rosnącej świadomości nauczycieli i rodziców. A jak to wygląda w przypadku dzieci i młodzieży – na ile mają oni wiedzę o higienie cyfrowej i świadomość tego, że prywatność jest ważna i należy ją chronić?

Jest to pokolenie dużo bardziej świadome niż ich rodzice. Symptomy tego widzimy w mediach społecznościowych - to jak chętnie rodzice dzielą się prywatnością dzieci, a jak rzadko robią to młode osoby. Nastolatki opowiadają głównie o sobie, jakby mieli wrodzoną świadomość ochrony prywatności innych. Gdy wchodzimy na profil nastolatka, to widzimy jego, rzadziej grupy osób. Oczywiście nie mówię tu o sytuacjach używania cudzego wizerunku w sposób przemocowy.

1 ROZMOWA Z EKSPERTEM

Pamiętam sytuację, kiedy przechodziłam obok szkoły moich dzieci, pod którą stało mnóstwo rowerów. Chciałam zrobić temu zdjęcie, ale było tam dwóch chłopców. Stali tyłem i daleko, nie robiłam zdjęcia im, a jednak odwrócili się i krzyknęli do mnie: „RODO!". To było świetne! Aż się roześmiałam. Dzieciaki z szóstej albo siódmej klasy już wiedzą, że ja nie mam prawa zrobić im zdjęcia! Tymczasem pokolenie ich rodziców i nauczycieli często bez problemu publikuje zdjęcia swoich i cudzych dzieci.
Prowadząc z nastolatkami rozmowy do mojej drugiej książki, „Twój telefon, twoje zasady" widziałam ogromną świadomość tego, że dane są wartością. Oczywiście młodzież nie mówi o „danych", operują raczej pojęciem „prywatności". Tylko oni mogą decydować o dzieleniu się informacjami z tego życia, nikt nie może tego robić za nich. Niestety, to wciąż za mało. Nasza Fundacja kończy właśnie przygotowywać raport z pierwszego ogólnopolskiego badania higieny cyfrowej i aktywności fizycznej wśród młodzieży.

Co wykazało to badanie?

Jeden z głównych wniosków jest taki, że młodzież ma dostęp do wiedzy, ale musimy ich wesprzeć w pracy nad dobrymi nawykami. Uczniowie w siódmej klasie szkoły podstawowej przejawiają wyższy poziom higieny cyfrowej niż w trzeciej liceum. Wielu siódmoklasistów znajduje się wciąż pod kuratelą rodziców, sporo wiedzy o higienie cyfrowej czy cyberbezpieczeństwie otrzymują też w szkole. Z kolei licealiści mają już po 17 czy 18 lat, to młodzi dorośli, bez kontroli rodzicielskiej. I widać, że u nich częstość zachowań chroniących zdrowie, w tym prywatność jest znacznie niższa.
Chodzi o to, żeby mieli pewne dobre nawyki, by np. instalując aplikację, zwracali uwagę, do jakich danych dają jej dostęp. Zbyt mała grupa młodzieży przestrzega zasady, by przyjmować do znajomych tylko osoby, które znamy osobiście, zbyt duża natomiast klika w linki z nieznanych źródeł. To rodzi poważne ryzyka pod względem przestępstw na tle seksualnym, przemocy w internecie, czy kradzieży danych.
Już od ponad dekady mówi się, że „dane to nowa ropa". Mamy więc pokolenie, które jest od dziecka okradzione z danych. Dorośli często to bagatelizują, ale gdyby ktoś mi dziś zaserwował reklamę wyborczą, sprytnie stargetowaną na podstawie moich doświadczeń z dzieciństwa – które współcześni rodzice chętnie publikują w sieci – to byłabym wobec tego bezbronna. A z łatwością można sobie wyobrazić, że wraz z rozwojem sztucznej inteligencji, w przyszłości takie precyzyjne targetowanie, na podstawie dostępnych w chmurze danych o człowieku, będzie możliwe.

Powiedziała Pani o różnicach między szkołą podstawową i liceum. Jak to się zmienia, niestety na niekorzyść. Zakładam, że wczesna szkoła podstawowa, czy wiek przedszkolny to jeszcze inne podejście. Kiedy należy rozpocząć edukację higieny cyfrowej? Czy zajęcia z tego zakresu już na poziomie przedszkola to dobry pomysł?

Trzeba zacząć dbać o higienę cyfrową, gdy się zobaczy dwie kreski na teście ciążowym. Dobrze by było, żeby przyszli rodzice już mieli pewne zasady higieny cyfrowej wprowadzone w swoim życiu. Bo dzieci uczą się przez naśladowanie. I sami często wprowadzamy zamęt w życiu dziecka, oczekując od niego pewnych zachowań, których sami nie przestrzegamy. Czyli jeśli dziecko malutkie widzi mamę, czy tatę, których twarz przesłania czarny prostokąt, to uczy się, że człowiek w stadzie funkcjonuje z tym prostokątem. I ono wnioskuje z zachowań starszych w stadzie, że to przedmiot pożądany - jeśli widzi, że to jest coś, co jest lubiane, często używane, to będzie go chciało.
Oczywiście nie chodzi o to, żeby tego telefonu zupełnie nie było przy dziecku, ale o to, żeby nie lekceważyć dziecka z powodu korzystania z urządzenia. Swego czasu duże poruszenie społeczne wywołała kampania Fundacji Dajemy Dzieciom Siłę pod hasłem: „Blisko telefonu, daleko od dziecka". Zwracała ona uwagę na to, że pierwsze trzy lata życia dziecka są kluczowe dla rozwoju jego osobowości i tego, w jaki sposób ono w przyszłości będzie funkcjonować. Patrząc na badania doktorki Magdaleny Rowickiej „Brzdąc w sieci", nie mam wątpliwości, że wiele dzieci we wczesnych latach jest lekceważona przez rodzica, ze względu na to, że mamy ciągle coś ważnego do zrobienia w telefonie.

1 ROZMOWA Z EKSPERTEM

Wracamy do problemu uzależnienia dorosłych od telefonów?

Nie chodzi o uzależnienie - to jest choroba, którą diagnozuje lekarz. I osób klinicznie uzależnionych jest niewiele. Ale na pewno jesteśmy od telefonów zależni. Bardzo wiele rzeczy można, a czasem trzeba dziś zrobić online. To często usprawnia życie, na przykład nie musimy już iść do urzędu, by złożyć pismo, możemy zrobić to online., Ale jesteśmy od telefonu zależni – wiele codziennych spraw wymaga użycia internetu, wzięcia do ręki telefonu. I często przez to lekceważymy dzieci.

A kiedy małe dziecko płacze lub stęka, sygnalizując rodzicowi, że go potrzebuje, a rodzic nie reaguje i dzieje się to często, to dziecko uczy się, że jego potrzeby nie są najważniejsze i nie warto ich sygnalizować. To może mieć poważne konsekwencje dla jego rozwoju emocjonalnego i funkcjonowania społecznego. Gdy dziecko zaczyna więcej rozumieć, trzeba mu już nie tylko dawać dobry przykład – np. brak telefonu w sypialni czy nie chodzenie z nim po domu – ale też, zacząć o tym rozmawiać i zwracać uwagę na dobre i złe nawyki.

Czyli zajęcia z higieny cyfrowej w przedszkolach są potrzebne?

Uważam, że tak, choć oczywiście nie z trzylatkami. Niestety, badania doktorki Rowickiej pokazują, że 12 % dzieci poniżej pierwszego roku życia dostaje już do ręki telefon. A im później, tym bardziej ta grupa rośnie. Natomiast z cztero- czy pięciolatkami można już te zajęcia prowadzić. W Fundacji w ramach Lekcji Higieny Cyfrowej przygotowaliśmy program zajęć dla zerówki, który jednak można zaadaptować dla młodszych dzieci. Oparte są o model odwróconej edukacji, w której dzieci, robiąc pudełko do odkładania telefonów, maja zachęcać do tego domowników.

Ale kiedy mówimy „dziecko”, widzimy różne grupy osób. Warto pamiętać, że inaczej pracujemy z dziećmi szkolnymi, inaczej z nastolatkami. W naszych badaniach higieny cyfrowej widzimy, że internet to dla młodzieży technologia przeźroczysta. Bardzo duże grupy są podpięte do sieci przez cały czas. To widać też w raporcie „Internet dzieci”. To może stanowić wyzwanie dla samokontroli, bo to tak, jakby ktoś nam kazał kontrolować kiedy pierwszy raz w ciągu dnia użyliśmy prądu – zwykle nie zwracamy już na to uwagi. Dlatego głównym problem dla młodych jest motywacja – dlaczego mają w ogóle zacząć wdrażać nawyki higieny cyfrowej.

Tymczasem pojawiają się postulaty zakazu używania social mediów do 16 roku życia. Taki zakaz wprowadziła niedawno Australia, co wywołało duże poruszenie w mediach. Czy to dobry kierunek?

Zależy, kogo ma dotyczyć ten zakaz. Bo Australia nie zakazała używania social mediów przez dzieci. Zakazała udostępniania im takich usług. Tak jak nie ma zakazu kupowania alkoholu przez np. 14-latka, ale zakaz sprzedawania mu tego alkoholu. I to jest właściwe podejście. To jest zgodne z naszym podejściem do higieny cyfrowej, i tego, co nazywamy cyfrowym obywatelstwem, czyli tworzeniem i używaniem technologii w sposób odpowiedzialny, przestrzegania prawa także w przestrzeni cyfrowej. Zajmowanie się bezpieczeństwem obywateli jest obowiązkiem państwa. Ma ono powinność amortyzowania negatywnych skutków rozwoju gospodarczego. A dziś rozwój gospodarczy napędzany jest nowymi technologiami. Powinniśmy, patrzeć i na gospodarkę cyfrową tak jak na inne gałęzi gospodarki.

Tak jak ludność mieszkająca w okolicach kopalni jest objęta rozmaitymi programami albo prewencyjnymi, albo naprawczymi, gdy naruszone są normy jakości powietrza. Tak samo powinniśmy to uregulować w gospodarce cyfrowej. Nie mówić o „świecie wirtualnym”, bo nie tworzymy prawa obowiązującego w grze Sims, tylko w prawdziwym świecie. I mamy w nim internet, który jest jak wielki supermarket, w którym proponuje nam się rozmaite produkty i usługi cyfrowe. I one wszystkie powinny być klasyfikowane pod względem poziomu ryzyka.

1 ROZMOWA Z EKSPERTEM

Na czym miałaby polegać taka klasyfikacja?

Na sprawdzeniu, czy usługa ma algorytmizację treści, czy są elementy hazardowe, czy pozwala na kontakt z obcymi, czy ma opcję „infinity scroll" itd. No nie jest niczym złym, jeśli mówimy o serwisie dla dorosłych. Kwalifikacja powinna się odbywać, gdy taka usługa wchodzi na „teren" internetu danego kraju czy wspólnoty (UE). Bo usługi cyfrowe też są świadczona na danym terytorium, tak jak kiedyś w Polsce nie było np. Netflixa. W kwestii biznesu, finansów czy licencji nikogo nie dziwi, że jakiś serwis nie jest dostępny w danym kraju. A kiedy w grę wchodzi bezpieczeństwo dzieci i młodzieży, nagle podnoszą się krzyki, że cezura, że nadmiar kontroli itd.

Stary internet, tworzony przez pasjonatów jako sfera w pewnym sensie „wyjęta spod prawa" już nie wróci. Jeśli mamy do kogoś mieć o to pretensje, to nie do ludzi, którzy troszczą się o bezpieczeństwo dzieci tylko do firm, które przez ostatnie 20 lat nie wykazały się społeczną odpowiedzialnością. Bo gdyby się wykazały, to my byśmy dzisiaj nie musieli tego regulować. Dlatego tu są potrzebne działania z poziomu państwa i dobrze, że Australia je wprowadziła. Francja też od wielu lat prowadzi tego typu działania, oni jako jeden z pierwszych krajów wprowadzili zakaz telefonów w szkołach. Niedawno Dania, zapowiedziała, że wprowadzi podobny zakaz mediów społecznościowych.

Tego rodzaju pomysły pojawiły się też w Polsce…

Po spotkaniach w sejmowej komisji dzieci i młodzieży, w których regularnie uczestniczymy, widać, że jest już wola we wszystkich resortach, żeby taki zakaz udostępniania wprowadzić. Czy to się uda? Nie wiadomo, bo mówimy w większości o firmach, które są kapitałem amerykańskim, więc wprowadzenie takiej ustawy znacząco wpłynie na zyski tych firm. Trudno mi sobie wyobrazić, żebyśmy podnieśli rękę na amerykańską gospodarkę, w obecnej sytuacji geopolitycznej.

Na przykładzie DSA widzimy zaś, że implementacja przepisów unijnych w tych kwestiach też idzie nam jak po grudzie i jesteśmy w ogonie Europy. Ale jestem przekonana, że tego już się tego procesu nie zatrzyma. I to nie tylko dlatego, że robią to duże państwa zachodnie. Ale też dlatego, że rośnie oddolny ruch w tym kierunku. Przypomina to ruchy klimatyczne sprzed kilku dekad. Prawo krajowe zostało wzięte w „imadło", tzn. z dołu naciskała świadomość ludzi – widzimy coraz więcej rodziców, którzy się troszczą się o bezpieczeństwo dzieci w internecie. A „z góry" Komisja Europejska bardzo odważnie działa wobec vloopów. W ostatnim miesiącu słyszeliśmy, że Infinity scroll na Tik Toku jest funkcją, która powinna być zabroniona na terenie UE.

Niedawno głośny był też postulat zakazu smartfonów w szkołach…

Jesteśmy w fundacji zwolennikami wprowadzania precyzyjnych zasad korzystania z telefonów i prywatnych urządzeń. Akceptowania tego, że część uczniów funkcjonuje z telefonem. W miejscach, gdzie przejeżdżają dwa autobusy dziennie, a dziecko tym autobusem musi samo dojechać do szkoły, telefon jest narzędziem bezpieczeństwa i pozostawania z dzieckiem w kontakcie.

Ale naszym zdaniem, w każdej szkole powinna panować zasada, że możesz wnieść do niej swoje prywatne urządzenie, ale po wejściu musi ono być zdeponowane. Nie mówimy o zakazie przynoszenia telefonów, ale o nakazie ich zdeponownia. Nasze edukatorki odwiedzając szkoły widzą ogromną różnicę w koncentracji uczniów na zajęciach i funkcjonowaniu w szkołach, w których takie zasady zostały wprowadzone – a jest ich coraz więcej.

W raporcie „Internet dzieci" widzimy, że większość czasu ekranowego młodzież i dzieci spędzają po godzinach szkolnych, tj. w domu. Ale dobrze, jeśli szkoła jest miejscem, w którym one są jednak odciążone, no i… nie bójmy się tego słowa - zmuszone do tego, żeby bez ekranów funkcjonować. To dobrze nawet dla ich ciała, dla ich szyi, która nie jest pochylona w tym czasie nad ekranem. Ale też dla ich relacji, bo muszą się czymś zająć, zacząć rozmowę z kimś, gdy nie mają telefonu.

1 ROZMOWA Z EKSPERTEM

Jestem przeciwniczką pokrzykiwania o zakazie i robienia tego w sposób, w który wielu polityków chciało wprowadzać, czyli wyłącznie przez zmiany zapisów w prawie oświatowym. Język tworzy rzeczywistość, więc zniechęcam do używania słowa „zakaz", bo ono stawia ludzi w przeciwnych sobie obozach: zakazujących i tym, którym się zakazało. Ale „zasady" jak najbardziej są potrzebne, w tym zasada nie używania prywatnych urządzeń na terenie szkoły.

A czy same szkoły mogą je wprowadzać, np. w swoich statutach?

Tak, ale dla wielu szkół to trudne zadanie i już dziś popełniają liczne błędy, próbując wprowadzić taki zakaz. Np. wpisują do statutów postanowienia o odbieraniu telefonu uczniowi – do tego szkoła nie ma prawa. Trzeba takie zasady wprowadzać mądrze, obwarować je zgodnymi z prawem sankcjami i przede wszystkim pogodzić się z tym, że zawsze będą ludzie, którzy nie przestrzegają zasad.
W październiku 2025 r. udostępniliśmy bezpłatnie obszerny poradnik „Higiena cyfrowa w szkole i przedszkolu" (na stronie można też znaleźć bezpłatne materiały edukacyjne, aktualne wyniki badań), w którym krok po kroku tłumaczymy, jak te zasady wprowadzić mądrze. Jedną z bardzo ważnych jest to, że ona obowiązują wszystkich – również nauczycieli. Przy tworzeniu tego poradnika słuchaliśmy społeczności szkolnej i uczniowie nam mówili np.: pan od WF rzuca nam piłkę i gra w gry, a pani od innego przedmiotu to daje nam zadania i siedzi na Vinted. To jest bardzo ciekawe, że nauczyciele mocno oporują przeciwko tej zasadzie. O ile kiedyś najtrudniej było nam prowadzić zajęcia z uczniami i rodzicami, to dzisiaj wyzwaniem są często rady pedagogiczne, które chętnie by wprowadzały zasady dla uczniów, ale dla siebie - już nie.

A jak uczniowie odnoszą się do wprowadzania takich zakazów?

Rozmawiając w szkołach, w których takie zasady funkcjonują – a są placówki, w których działają one drugi czy trzeci rok - otrzymujemy informację, że prędzej czy później społeczność przyzwyczaja się do nowego standardu. I łatwo wyłapuje się tych, którzy jednak nie przestrzegają tej zasady. Często sami rezygnują z tego, bo są widoczni na korytarzu – siedzą ze spuszczoną głową i natychmiast ich widać.
Często wprowadzenie zakazu na początku budzi niechęć starszych uczniów, jeżeli mówimy o podstawówce czy liceum, ale z czasem zaczyna im się to podobać. Ci którzy mają odwagę, mówią, że w sumie fajnie, że to zostało wprowadzone, że te telefony są w szafkach, a nie na przykład w toaletach. Bo telefon stał się nowym narzędziem starej przemocy rówieśniczej. Sytuacje, w których ktoś kogoś nagrał w toalecie, ktoś komuś dokuczał, ktoś inny to utrwalał, dzieją się w każdej szkole. Poznańska rzeczniczka praw uczniowskich, Agata Dawidowska, w każdym tygodniu podejmuje interwencję związaną z utrwalaniem wizerunku, albo z jego przerobieniem, co jest powszechne w dobie AI.

Statystyki wskazują, że ofiarami nękania w szkole pada ok.10% uczniów. To średnio 2 osoby na klasę, a w proceder jest zaangażowanych od kilku do kilkunastu osób w każdej klasie. Czy używanie smartfonów zmaga to zjawisko?

Badania, m.in. prowadzone przez profesora Jacka Pyżalskiego pokazują, że sprawców przemocy rówieśniczej nie przybywa, tzn. jest ich mniej więcej ten sam odsetek. I patrząc w ten sposób można uznać, że telefon nie wpływa na przemoc rówieśniczą. Ja mam trochę inne spojrzenie- dzisiaj przemoc rówieśnicza ma sprawcę zbiorowego. Jest sprawca bezpośredni, który inicjuję czy przewodzi tym aktom przemocy, ale mamy też sprawców zbiorowych, którzy te akty utrwalają. Mamy dzisiaj taki odruch, coś się dzieje, to będziemy to nagrywać. To jest wtórna i niekończąca się wiktymizacja osoby, która doświadcza przemocy. Ponieważ ona ma świadomość - to jest przerażające – że to, czego teraz doświadcza, będzie odtwarzane, nieskończoną ilość razy. Bo zostało nagrane i wrzucone do internetu i nie wiadomo, czy kiedykolwiek da się usunąć. A więc narzędzie zachęca do utrwalania, co samo w sobie jest przemocą. Samo to, że wyciągniemy telefon i zaczniemy kogoś nagrywać w szkole już sprawia dyskomfort tej osobie.

1 ROZMOWA Z EKSPERTEM

Często młodzież dołącza do cyberprzemocy, czy przemocy z użyciem telefonu, w obawie przed tym głównym hejterem. Bo jeśli pokażemy, że jesteśmy przeciwko temu, to jego złość może zwrócić się na nas. I stąd mogą się brać też często lajki pod takimi przemocowymi treściami. Zgadzam się z Katarzyną Staciwą, że mamy tu do czynienia z przestępstwem. Z naruszeniem czyjejś nietykalności, dobrego imienia, z pomówieniami czy nękaniem - i powinniśmy nazywać to po imieniu. Zwykle w takich sytuacjach nie trzeba sięgać po radykalne środki, nie zawsze konieczne jest zgłaszanie sprawy na policję, tylko na przykład sięgnięcie do Standardów Ochrony Małoletnich w danej szkole czy statutu. Ale przykra prawda jest taka, że wielokrotnie kończy się tym, że to ofiara zmienia szkołę. Dziecko, którego szkoła nie umie zareagować odpowiednio, czuje się zdradzone przez dorosłych, bo w szkole nikt nie stanął po jego stronie, a sprawcy nie zostali ukarani.
To się nie powinno zdarzać i powinniśmy mieć zasadę „zero tolerancji dla przemocy". I pokazywać, że każde tego typu zachowanie spotyka się z reakcją. A często wciąż wielu dorosłych żywi przekonanie, że to jest jakaś przemoc „wirtualna", czyli ona nie boli tak naprawdę. Zresztą niedawno mieliśmy sytuację, że prokuratura i policja uznały, iż przerobienie zdjęcia nastolatki nie jest nawet wykroczeniem. Tutaj szacunek dla Prezesa Mirosława Wróblewskiego, że pisze pisma odwoławcze w tej sprawie. Bo to jest po prostu demoralizujące dla społeczeństwa, zwłaszcza dla młodych ludzi.

Czy klasowe grupy na komunikatorach sprzyjają tej formie przemocy rówieśniczej? Bo często same szkoły zachęcają do ich zakładania…

W ubiegłym roku ciekawy raport opublikowała Fundacja „Kosmos dla dziewczynek". Jedna z zapytanych uczennic, mówi w nim o ogromnym stresie, który przeżywa, kiedy budzi się rano i widzi na grupie klasowej kilkaset nieprzeczytanych wiadomości. Jej pierwszą myślą jest: „Czy tam się ktoś ze mnie właśnie nie śmieje?"
Zachęcam rodziców, żeby zerknęli co dziesięcio- i dwunastolatki na takiej grupie klasowej robią. Tam generalnie są głównie „głupotki", śmieszne gify, emotikony, „obrazoburcze memy. " Ale zdarza się też, i to wcale nierzadko, że na takich grupach dzieci rozsyłają pornografie, materiały przedstawiające krzywdzenie seksualne nieletnich czy zwierząt, albo z odbierania komuś życia (np. transmisja z egzekucji dokonywanej przez terrorysytów – to przypadek jednej ze szkół). Tego się już nie da odzobaczyć, to są straszne rzeczy, traumatyzujące. To jest odbieranie dzieciństwa.
Natomiast jeśli nie było cię w szkole i chcesz na takiej grupie dowiedzieć się, co jest zadane – to jest to bardzo trudne. Dajemy więc dzieciom narzędzie, z którego nie wiedzą one, jak korzystać. Czas wprost powiedzieć, że to nie są narzędzia dla dzieci. One naprawdę mogą się komunikować w szkole oraz wysyłać do siebie smsy czy zadzwonić. Czyli robić to w sposób nie społecznościowy tylko bezpośredni. Telefon dla dziecka młodszego, jeśli jest potrzebny, powinien być pozbawiony dostępu do internetu.
Relacje społeczne buduje się przede wszystkim poprzez bezpośrednie kontakty. One świetnie tworzą się w szkole, bo szkoła cię uczy, że musisz się dogadać z ludźmi, którymi byś nie dał lajka. Ale musisz z nimi przebywać i znaleźć jakiś wspólny język, żeby się nie pozabijać w tej szkole. Relacje społeczne w tym wieku wymagają wychodzenia z domu, kontaktów, a nie uczenia się tego, że można przez internet napisać coś brzydkiego koleżance, wykluczyć ją z grupy czy przerobić jej zdjęcie. I zakazanie dostępu dzieci do komunikatorów, nie odbiera im możliwości budowania więzi społecznych, jak piszą osoby nieobeznane z tematem.

Często pada też pytanie o upowszechnianie wizerunku dziecka w internecie bez jego woli - przez rodziców, dziadków, czy też takie instytucje jak szkoły czy przedszkola. Czy takie dziecko, jak będzie starsze, może coś zrobić, by chronić ten wizerunek?

To temat z którym powinniśmy się jak najszybciej zmierzyć, dlatego, że dzieci dzisiaj są masowo odzierane z prywatności. Ten problem będzie się nasilał, dlatego że jest nas coraz mniej, a szkoły oraz

przedszkola po raz pierwszy w historii znalazły się w sytuacji, w której za chwilę trzeba będzie się starać o to, żeby mieć uczniów. To będzie skłaniało przedszkola do prowadzenia promocji. Tutaj zgadzam się z Aleksandrą Rodzewicz, która zwraca uwagę, że nigdzie w prawie nie ma przepisu zobowiązującego państwowe placówki do promowania się. A jeśli to robią, to znaczy, że wydają środki na działania nieuwzględnione w ustawie.

Inny argument, który moim zdaniem powinien zjeżyć włos na głowie dyrektorów szkół i przedszkoli jest taki, że już znamy przypadki, gdy nastolatki albo młodzi dorośli piszą do szkół, czy różnych organizacji, które wykorzystywały ich wizerunek z prośbą o jego usunięcie. I współczuję placówkom, które będą musiały dogrzebać się do Facebooka z 2017 roku i po usuwać tam zdjęcia, na których jest dany uczeń. A to jest pokolenie dużo bardziej świadome i wcale bym się nie zdziwiła, jakby zaczęły pojawiać się procesy o to, że ktoś mimo żądania usunięcia wizerunku ze strony nie zrobił tego. Takie nadużycia zdarzają się nawet ze strony kuratorów – znam przypadek, gdy aby odebrać nagrodę w konkursie, uczeń musiał się zgodzić na zrobienie zdjęcia i jego publikację. A przecież możemy to utrwalić w taki sposób, żeby twarz dziecka nie była widoczna.

Bardzo niepokoi mnie to, że trwa okres rekrutacji do przedszkoli i mamy do czynienia z masowym wykorzystywaniem dzieci w filmikach promujących te przedszkola. A w bardzo wielu przypadkach pod tego typu materiałami pojawiają się obrzydliwe komentarze wprost pedofilskie. Rodzice mają z tym ogromny kłopot, bo dzisiaj nie za bardzo mają się na co powołać. Zgody są często na nich wymuszane, albo nawet jak nie wyrażą zgody, widzą swoje dzieci na fanpejdżu szkoły. A nie każdy chce być tym rodzicem, który robi awanturę. To są sytuacje, które wymagają stanowczych działań. Wiem, że takie działania są też prowadzone, zwłaszcza w kontekście szkół i przedszkoli m.in. przez Komisję ds. dzieci i młodzieży, bo to jest stosunkowo łatwo uregulować w przypadku podmiotów publicznych.

Natomiast nie wprowadzimy takiego prawa, które zakaże publikować zdjęcia dzieci rodzicom. Ale myślę, że tutaj świadomość będzie się zmieniała. Każdy rodzic wie, że od pewnego wieku już nie można dziecku od tak sobie zrobić zdjęcia, że nastolatek zrobi nam awanturę, że wysłaliśmy jego nieautoryzowane zdjęcie na grupę rodzinną do dziadków. To prawo do wizerunku najlepiej widać właśnie po nastolatkach, którzy doskonale zdają sobie sprawę do prawa do prywatności i ochrony danych.

Aleksandra Rodzewicz przeprowadziła badanie w szkołach w całej Polsce, z którego wynikało, że większość szkół i przedszkoli publikuje wizerunek w social mediach. Z kolei z badania, przeprowadzonego przez Rzeczniczkę Praw Dziecka dowiadujemy się, że wielu nastolatków deklaruje, iż nie ma to dla nich znaczenia. Być może dlatego, że jest to pokolenie już okradzione z prywatności. Tak bardzo, że jest im już wszystko jedno. Także tutaj też jeszcze nas czeka dużo pracy.

Bardzo dziękuję za rozmowę.

Rozmawiał Karol Witowski

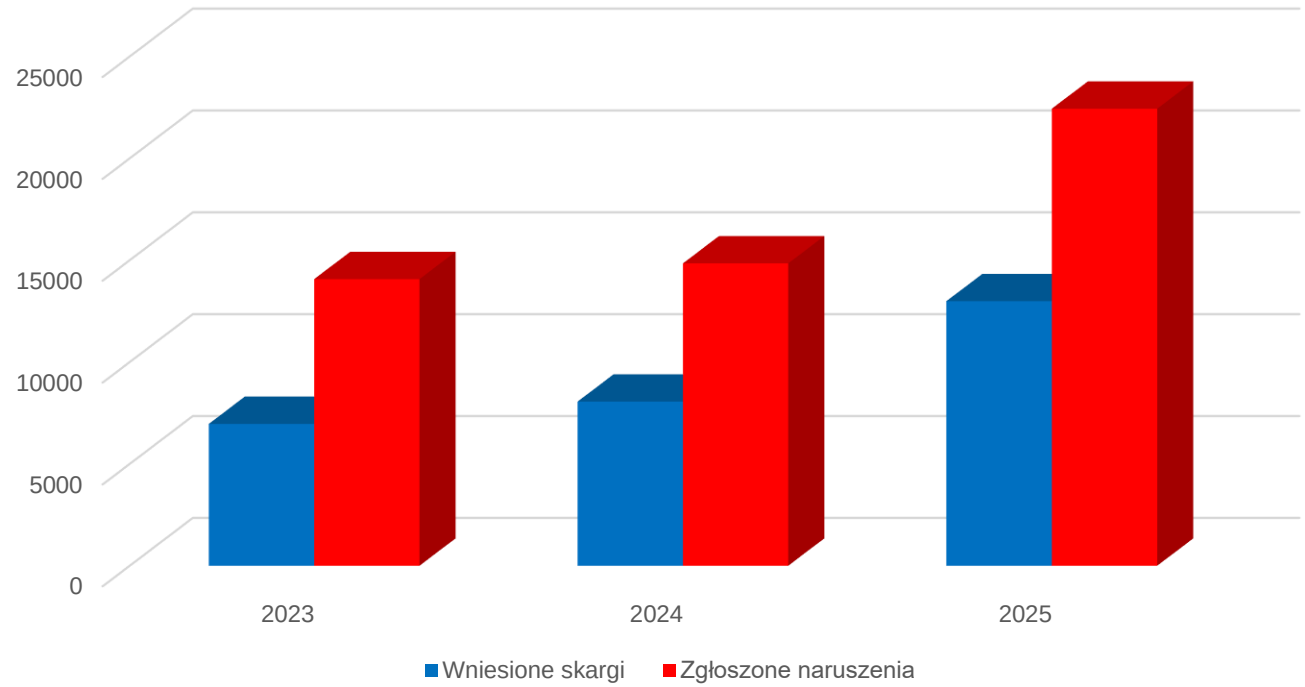
DWA LATA KADENCJI UODO – W LICZBACH

W styczniu minęła połowa czteroletniej kadencji Mirosława Wróblewskiego jako Prezesa UODO. Z tej okazji, podczas przypadającego 28 stycznia 2026 r. Dnia Ochrony Danych Osobowych, Prezes Urzędu podsumował ostatnie dwa lata działalności UODO.

Na uwagę zasługuje przede wszystkim rosnąca z każdym rokiem liczba skarg. Podczas gdy w 2023 r. było ich prawie 7 tys., to w 2024 r. liczba ta przekroczyła 8 tys., a w zeszłym – sięgnęła niemal 13 tys. (patrz wykres 1). Przybywa także naruszeń zgłaszanych przez administratorów w tej kwestii, w 2025 r. wzrost był iście skokowy. O ile w dwóch wcześniejszych latach liczba ta oscylowała w okolicach 15 tys., to w minionym roku przekroczyła 22 tys.

Przyczyn tego stanu rzeczy jest wiele: po części odpowiada za to postępująca cyfryzacja gospodarki, co powoduje, że przetwarzanych jest coraz więcej danych, w tym osobowych. Nie bez znaczenia jest także wzrost świadomości zarówno wśród obywateli, jak i administratorów – do czego przyczynia się również działalność UODO. Zmiany w strukturze Urzędu wprowadzane od stycznia 2025 r. sprawiają zaś, że działa on sprawniej i może rozpatrywać więcej skarg i zgłoszeń. Statystyki wykazują, że rocznie UODO kończy postępowanie w odniesieniu do blisko 6 tys. spraw, z czego tylko ok. 1800 kończy się wydaniem decyzji administracyjnej. W 2024 r. udało się ich zakończyć o 5 proc. więcej niż w roku poprzednim.

SKARGI I NARUSZENIA ZGŁOSZONE DO UODO W LATACH 2023–2025



2 DZIAŁALNOŚĆ UODO

Rekordowe kary za bezprawne przetwarzanie danych

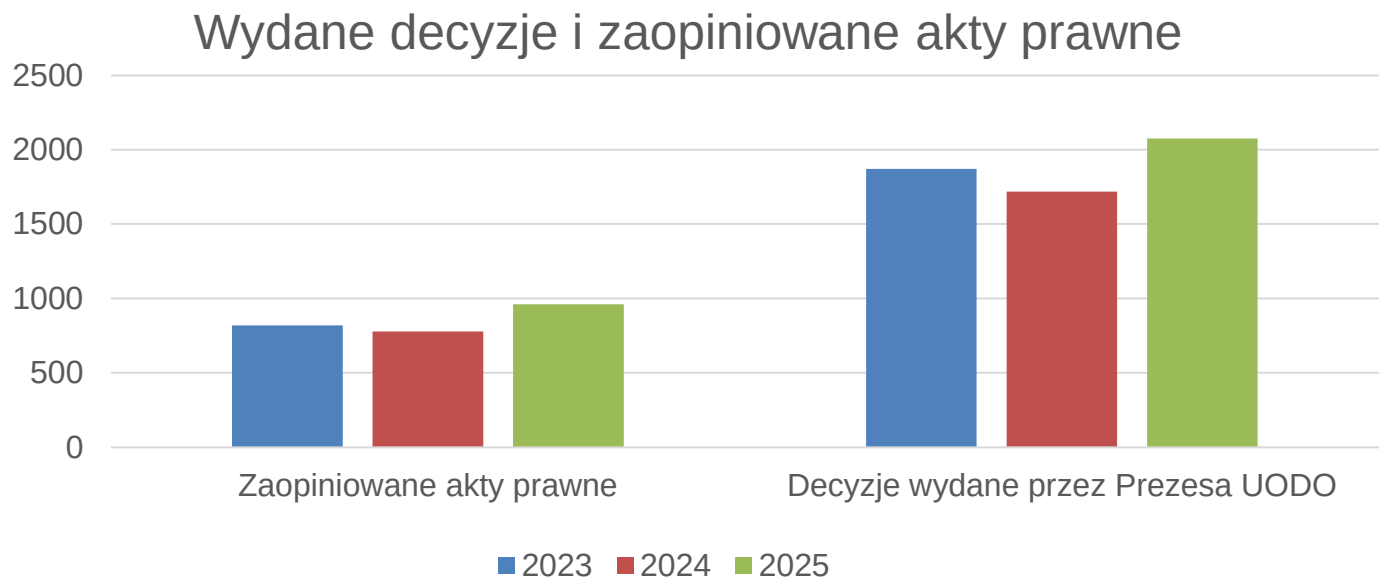
Rośnie także liczba kar pieniężnych nakładanych przez Prezesa UODO. W 2025 r. orzeczono ich 32 (dla porównania: w rok wcześniej było ich 27, a w 2023 r. – 31). Łącznie osiągnęły też rekordową wysokość **64 440 097,25 zł.** Niewątpliwie do tego wyniku przyczyniła się kara w wysokości 27 mln nałożona na Pocztę Polską (oraz dodatkowo 100 tys. zł na Ministerstwo Cyfryzacji) za niezgodne z prawem przetwarzanie danych z rejestru PESEL przy nieudanej próbie zorganizowania wyborów prezydenckich w formie korespondencyjnej (tzw. wybory kopertowe).

W 2025 r. orzeczono też najwyższą do tej pory karę na przedsiębiorstwo prywatne w Polsce – wynoszącą 18,4 mln zł. Nałożona ona została na ING Bank za skanowanie dowodów osobistych bez weryfikacji, czy w danym przypadku jest to konieczne (także np. gdy chodziło o zgłoszenie usterki technicznej bankomatu). Organ nadzorczy stwierdził, że bank działał automatycznie, bez indywidualnej weryfikacji potrzeby zabezpieczenia się przed ryzykiem nielegalnych transakcji finansowych. Przepisy AML wymagają bowiem przeprowadzenia analizy dla każdego przypadku osobno – nie przewidują rutynowego kopiowania dokumentów wszystkich osób. Bank złamał fundamentalne reguły: legalności operacji na danych, ich ograniczania do niezbędnego minimum oraz określonego celu wykorzystania.

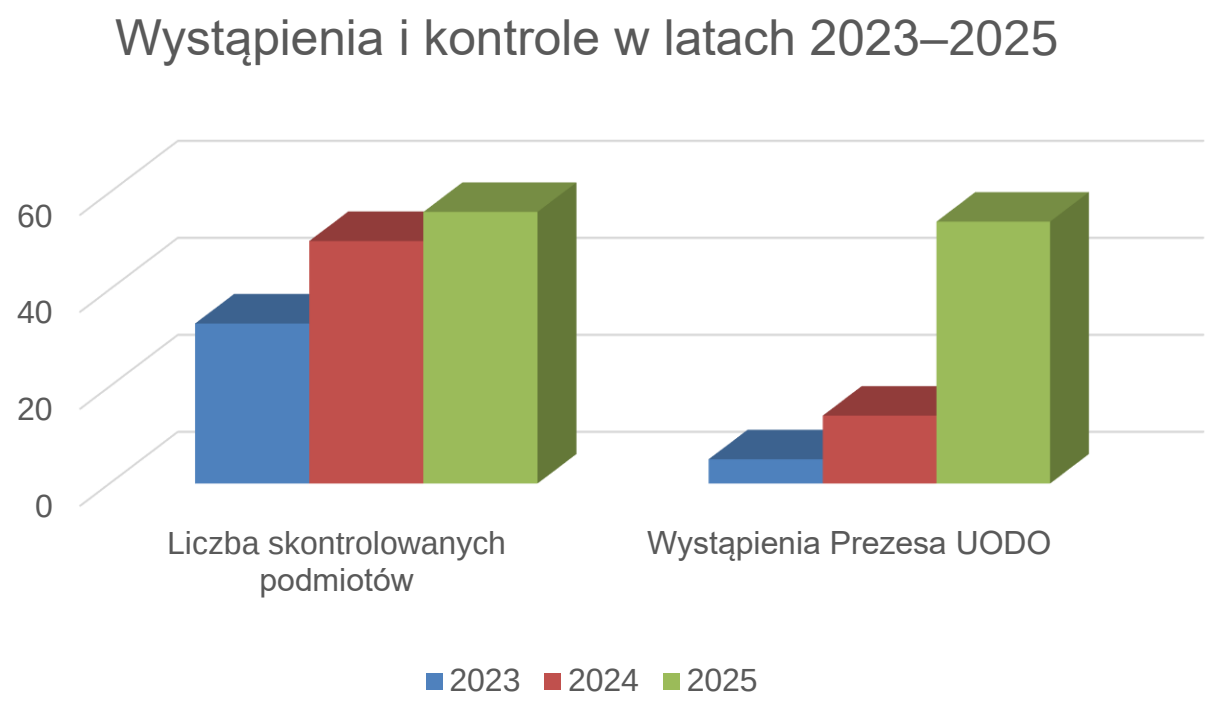
Nieco niższą karę orzeczono w 2025 r. wobec McDonald's, za naruszenie przepisów dotyczących bezpieczeństwa danych. Sieć ta zleciła zewnętrznemu podmiotowi (świadczącemu usług PR) obsługę systemu planowania zmian – bez weryfikacji, czy firma ta posiada odpowiednie kompetencje i środki zabezpieczenia danych. W efekcie tysiące rekordów na temat zatrudnionych w tej sieci osób stały się publicznie dostępne – zawierały one dane pozwalające zidentyfikować pracowników.

Więcej wystąpień i opinii do aktów prawnych

Po niewielkim spadku w 2024 r. wzrosła także liczba decyzji wydanych przez Prezesa UODO (2023 r. – **1870;** 2024 r. – **1719;** 2025 r. – **2076**). Podobnie sytuacja wygląda z zaopiniowanymi aktami prawnymi – w 2023 r. było ich **819**; w 2024 r. – **779; a** 2025 r. **aż 962**. Stale rośnie za to liczba kontrolowanych rocznie podmiotów – o ile w 2023 r. było ich 33, to w 2024 r. już 50, a w zeszłym – 56. Skokowo wzrosła liczba wystąpień UODO – z zaledwie 5 w 2023 r., przez 14 w roku następnym, do 54 w 2025.



Wystąpienia te są ważnym instrumentem w kształtowaniu i podnoszeniu poziomu ochrony danych osobowych. Zawierają one wnioski o zmianę obowiązujących regulacji lub wprowadzenie nowych przepisów dotyczących przetwarzania danych osobowych albo wskazują na konieczność zmodyfikowania praktyk stosowanych w podmiotach, do których są skierowane – tak, by były one zgodne z RODO. W 2025 r. najważniejsze wystąpienia dotyczyły: potrzeby stworzenia przepisów chroniących ludzi przed negatywnym wpływem deepfake'ów, **przeprowadzenia przeglądu rejestrów publicznych,** doprecyzowania przepisów dotyczących stosowania monitoringu wizyjnego w placówkach medycznych, **udostępniania dokumentacji medycznej w celach naukowych, funkcjonowania Krajowego Systemu Informacyjnego Policji (KSIP), a także konieczności zmian** przepisów prawa krajowego stosownie do treści wyroków TSUE**.**

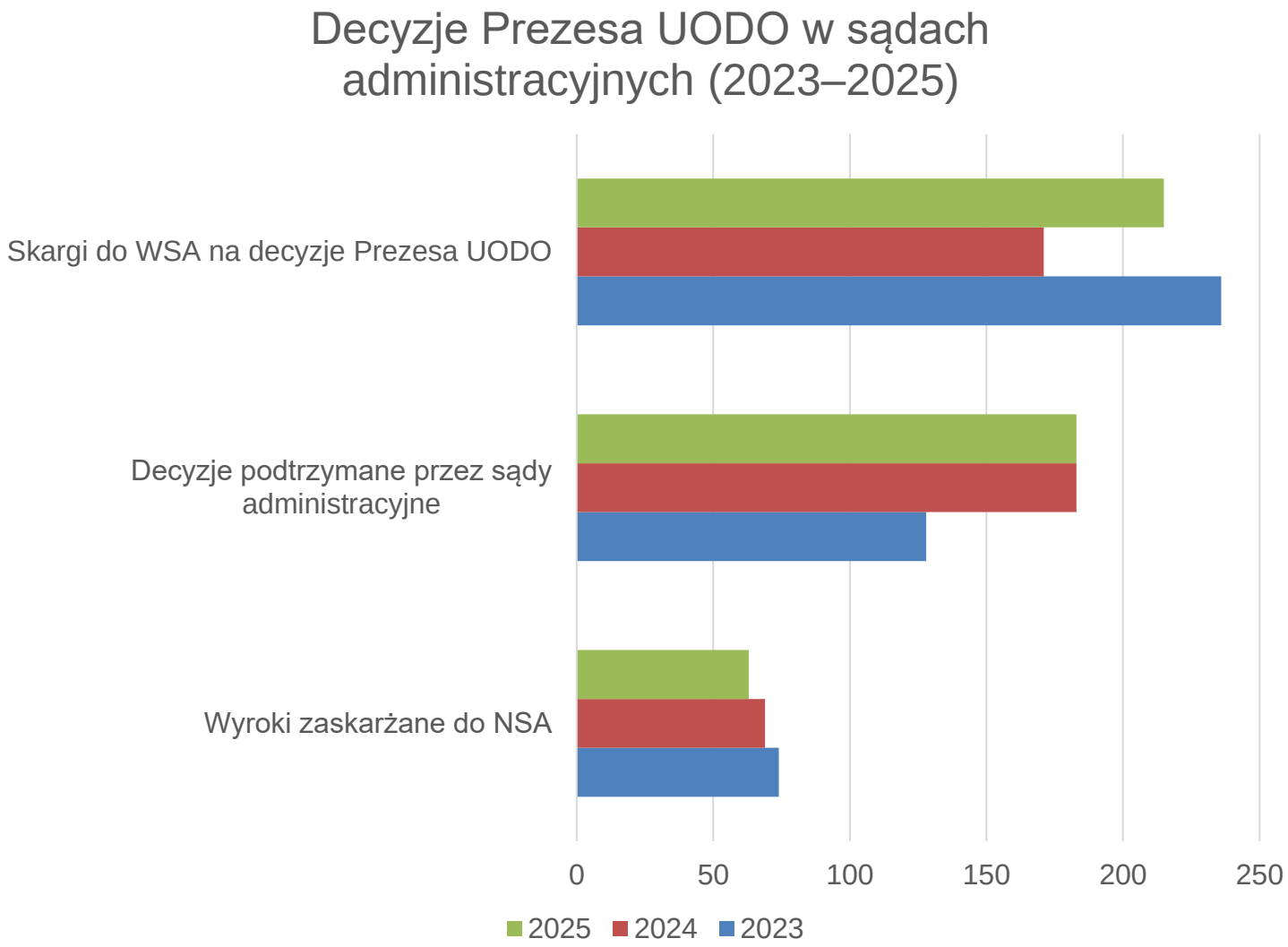


Stała liczba decyzji Prezesa UODO podtrzymanych przez sądy administracyjne

Spada natomiast liczba wyroków zaskarżanych do NSA (2023 r. – **74;** 2024 r. – **69;** 2025 r. – **63**). Jednocześnie w zeszłym roku sądy administracyjne utrzymały w mocy 183 decyzje Prezesa UODO – tyle samo, ile rok wcześniej. W 2025 r. wniesiono też do WSA 215 skarg na decyzje organu. To więcej niż w 2024 r. (171), ale nieco mniej niż w 2023 r. (236). Z najważniejszych orzeczeń sądowych minionego roku z pewnością należy wskazać wyrok dotyczący Morele.net, w którym WSA podtrzymał nałożenie na ten serwis kary za doprowadzenie do wycieku danych 2,2 mln osób (sprawę rozpatruje NSA). Z kolei ws. spółki ClickQuickNow sąd potwierdził, że Prezes UODO skutecznie egzekwuje bezwzględny skutek cofnięcia zgody na przetwarzanie danych.

Z kolei Naczelny Sąd Administracyjny przyznał organowi rację w sprawie spółdzielni mieszkaniowej, która wiadomości ws. rozliczeń z mieszkańcem kierowała także do jego pracodawcy – co stanowiło niezgodne z prawem przetwarzanie danych osobowych. Również w sprawie niedoszłych i byłych klientów banków NSA podzielił stanowisko Prezesa UODO, że przetwarzanie ich danych jest niedopuszczalne.

Szeroki odzew medialny miało natomiast nałożenie na Meta Platforms zakazu przetwarzania danych prezesa InPost i jego małżonki do wyświetlania reklam (będących w rzeczywistości próbami wyłudzenia pieniędzy i danych). Mimo że właściciel Facebooka wniósł skargę, WSA odmówił wstrzymania wykonania decyzji Prezesa.



Więcej porozumień i zawiadomień o podejrzeniu przestępstwa

Znaczące wzrosty odnotowano także w kwestii zawiadomień o podejrzeniu popełnienia przestępstwa przy przetwarzaniu danych osobowych. O ile w ostatnich latach Prezes UODO prawie nie korzystał z tego narzędzia (tylko w 2024 r. złożono jedno takie zawiadomienie), to w minionym roku złożył ich 7. Podobnie sytuacja wygląda z porozumieniami o współpracy – o ile w 2024 r. zawarto tylko dwa (z Rzecznikiem Praw Dziecka i Ogólnopolską Federacją Stowarzyszeń Uniwersytetów Trzeciego Wieku), to w 2025 r. było ich aż 9 – i objęły one takie podmioty, jak: Ministerstwo Cyfryzacji, NRA, GIS, KIODO Polski Autokefaliczny Kościół Prawosławny, Fundacja Polskich Portów Lotniczych, Naczelna Izba Lekarska, RCL, Polskie Towarzystwo Legislacji); w tym jedno porozumienie ze szkołą wyższą (Akademia im. Jakuba z Paradyża).

SYGNATARIUSZE KODEKSU POSTĘPOWANIA DLA PRYWATNYCH AGENCJI BADANIA OPINII I RYNKU MUSZĄ POWOŁAĆ IOD

„Kodeks postępowania dotyczący przetwarzania danych osobowych przez prywatne agencje badawcze" przewiduje, że podmioty, które do niego przystąpią, zobowiązane są do wyznaczenia inspektora ochrony danych. Jednocześnie twórcy kodeksu zadbali, by przepisy tego dokumentu wspierały IOD w niezależnym wykonywaniu zadań, we właściwym wspieraniu administratora, a także w rozwoju zawodowym.

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, a w poprzednim wydaniu Biuletynu UODO opisaliśmy jedno z przewidzianych w nim rozwiązań – tworzenie tzw. Listy Robinsona.

Tym razem chcemy zwrócić uwagę na zawarte w tym dokumencie regulacje poświęcone roli inspektora ochrony danych (IOD).

Docenienie roli IOD

Twórcy kodeksu, dostrzegając szczególny wpływ IOD na właściwe ukształtowanie procesów przetwarzania danych osobowych w organizacji, która go powołuje, poświęcili mu osobny rozdział w tym dokumencie.

Jego przepisy stanowią, że agencje badawcze, które przystąpią do stosowania kodeksu, mają obowiązek wyznaczenia IOD. Wskazują, że **zaletą wyznaczenia IOD jest zapewnienie Agencji badawczej dodatkowego merytorycznego wsparcia na płaszczyźnie zgodności przetwarzania danych osobowych z prawem. Wyznaczenie IOD może także stanowić jeden z elementów wykazywania przez Agencje przestrzegania RODO (zasada rozliczalności).**

Jednocześnie rekomendują, aby osoba pełniąca funkcję IOD wspierała agencję badawczą w zakresie spraw dotyczących ochrony danych osobowych oraz uprawnień IOD wskazanych w RODO.

Łatwy kontakt

Kodeks przewiduje także, **że informacja o wyznaczeniu IOD powinna być łatwo dostępna** dla osób, których dane dotyczą, m.in. **udostępniona na stronie internetowej**. Wskazuje, że każda agencja badawcza powinna dokonać indywidualnej analizy w celu określenia miejsca umieszczenia danych kontaktowych IOD, tak aby umożliwić szybkie i łatwe ich wyszukiwanie. Zaleca jednak, aby taka informacja była zawarta **w wyodrębnionej części strony** internetowej dotyczącej ochrony danych osobowych, np. w zakładce kontakt, RODO itp.

Kodeks stanowi, że należy udostępnić takie dane IOD, jak:

- imię;
- nazwisko oraz
- adres poczty elektronicznej lub numer telefonu IOD.

Przeciwdziałanie konfliktowi interesów

Kodeks dopuszcza **łączenie funkcji IOD z innymi obowiązkami**. Zobowiązuje jednak agencje badawcze do przenalizowania, czy wykluczony został konflikt interesów, o którym mowa w RODO, oraz czy zakres dodatkowych obowiązków nie uniemożliwia IOD faktycznego realizowania jego obowiązków wynikających z przepisów ogólnego rozporządzenia o ochronie danych. Stosownie do Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243 rev. 01; przyjętych 13 grudnia 2016 r.; a następnie zmienionych i przyjętych 5 kwietnia 2017 r. i wciąż obowiązujących na gruncie RODO**) IOD nie może w agencji badawczej zajmować stanowisk, na których są podejmowane decyzje co do celów i sposobów przetwarzania danych osobowych** lub realizowane są obowiązki administratora.

Dlatego w kodeksie przewidziano, że *tym samym, zależnie od rodzaju działalności, rozmiaru i struktury agencji badawczej dobrą praktyką może być m.in.:*

- ***określenie stanowisk niezgodnych z funkcją IOD**;*
- ***opracowanie wewnętrznych zasad** pozwalających uniknąć konfliktu interesów;*
- *zapewnienie bardziej **ogólnego wyjaśnienia dotyczącego konfliktów interesów;***
- *zadeklarowanie, że IOD nie ma konfliktu interesów w odniesieniu do pełnionej przez siebie funkcji, w celu zwiększenia świadomości na temat tego wymogu;*
- ***wprowadzenie zabezpieczeń do wewnętrznych zasad organizacji** oraz zapewnienie, aby ogłoszenie o naborze na stanowisko IOD lub umowa o świadczenie usług były wystarczająco jasne i precyzyjne, aby uniknąć konfliktu interesów. W tym kontekście należy również mieć na uwadze, że **konflikty interesów mogą przybierać różne formy** w zależności od tego, czy rekrutacja na stanowisko IOD ma charakter wewnętrzny lub zewnętrzny.*

Wsparcie ze strony administratora

W kodeksie zadbano też o umożliwienie IOD właściwego wypełniania zadań, w tym rozwoju zawodowego. Zapisano w nim bowiem: *Administrator zobowiązany jest udzielić wsparcia IOD poprzez zapewnienie niezbędnych zasobów do wykonania tych zadań. Szczegółowych wskazówek w tym zakresie agencje badawcze powinny szukać w* ***Wytycznych dotyczących inspektorów ochrony danych, stanowiskach i decyzjach Prezesa Urzędu Ochrony Danych Osobowych*** *oraz orzecznictwie sądowym*.

Podkreślono, że *wytyczne dotyczące inspektorów ochrony danych opowiadają się za szerokim rozumieniem zasobów, do których zaliczyć należy m.in.:*

- ***czas*** *niezbędny do wywiązywania się z przydzielonych obowiązków;*
- *udzielanie* ***wsparcia w postaci zasobów finansowych, infrastruktury*** *(pomieszczenia, urządzenia, wyposażenia)* ***oraz pracowników****;*
- *oficjalne* ***powiadomienie wszystkich pracowników o wyznaczeniu IOD*** *w celu zapewnienia, aby wszyscy w organizacji wiedzieli o jego istnieniu i pełnionej przez niego funkcji;*
- *niezbędny* ***dostęp do innych działów****, np. HR, działu prawnego, informatycznego itd., w celu zapewnienia IOD niezbędnego wsparcia i informacji;*
- ***doskonalenie zawodowe*** *– IOD musi mieć zapewnioną możliwość ciągłego odświeżania wiedzy z dziedziny ochrony danych osobowych. Celem administratora powinno być ciągłe poszerzanie wiedzy IOD oraz zachęcanie go do udziału w kursach szkoleniowych poświęconych ochronie danych i innych formach doskonalenia zawodowego*.

MONITORING WIZYJNY W SALI LEKCYJNEJ – DOPUSZCZALNY CZY NIE?

Stosowanie monitoringu wizyjnego w pomieszczeniach, w których odbywają się zajęcia dydaktyczne, jest co do zasady zabronione. Odstępstwa w tym zakresie są możliwe, ale niezbędne jest spełnienie warunków określonych w przepisach ustawy Prawo oświatowe. Dla legalności jego stosowania konieczne jest również zapewnienie zgodności z RODO.

Wpływające do UODO pytania, a także doniesienia medialne dowodzą, że stosowanie monitoringu wizyjnego w szkołach wciąż przysparza problemów. Wątpliwości jednej z placówek wzbudziła ostatnio kwestia, czy kamery można zamontować w salach lekcyjnych, w których znajduje się specjalistyczny, a zarazem potencjalnie niebezpieczny sprzęt, m.in. piły do cięcia metalu czy palniki gazowe. Władze tej szkoły, mając świadomość, że stosowanie monitoringu wizyjnego w miejscu prowadzenia zajęć dydaktycznych wymaga szczególnej ostrożności, poprosiły UODO o opinię, czy ze względu na bezpieczeństwo oraz ochronę mienia można dopuścić montaż kamer w tych pokojach.

W odpowiedzi UODO wskazał, że dla jednoznacznego rozstrzygnięcia niezbędne byłoby dokonanie wnikliwej, uwzględniającej wszystkie uwarunkowania analizy, w którą powinien zostać włączony inspektor ochrony danych. Niemniej udzielając ogólnych wskazówek, zaznaczył, że **warunki stosowania monitoringu wizyjnego w szkołach publicznych zostały uregulowane w ustawie z 14 grudnia 2016 r. Prawo oświatowe, konkretnie w art.108a ust. 1-9**. Dla zapewnienia legalności i prawidłowości stosowania monitoringu w placówce oświatowej warunki te muszą być spełnione jednocześnie z tymi określonymi w RODO.

Monitoring musi szanować prawo do prywatności uczniów i nauczycieli

Co ważne, przepisy w tym zakresie **podlegają wykładni ścisłej**. **Przedmiotowy i podmiotowy zakres monitoringu oraz cele, w jakich może być on stosowany, nie mogą wykraczać poza dozwolone ramy ustawowe.**

Stosowanie monitoringu obejmującego obszar wnętrza sal dydaktycznych stanowi wyjątkowo inwazyjną metodę przetwarzania danych osobowych, wiążącą się z gromadzeniem i wykorzystywaniem szerokiego zakresu informacji dotyczących zarówno uczniów, jak i pracowników placówki oświatowej. Dlatego stosowanie tego rodzaju technologii może stanowić potencjalnie nadmiarową ingerencję w ich prywatność, jak również budzić wątpliwości z punktu widzenia stałego śledzenia pracownika, a więc zapewnienia gwarancji praw pracowniczych. Z tego powodu decyzja o ewentualnym stosowaniu monitoringu powinna być podejmowana ze szczególną roztropnością, przy zachowaniu zasad proporcjonalności i poszanowania konstytucyjnego prawa do prywatności.

3 PRAWO I NOWE TECHNOLOGIE

Zakaz i odstępstwa w szczególnych okolicznościach

Zgodnie z art. 108a ust. 3 Prawa oświatowego stosowanie monitoringu wizyjnego w pomieszczeniach, w których odbywają się zajęcia dydaktyczne, jest co do zasady zabronione. Odstępstwa od tej reguły są dopuszczalne, przy spełnieniu warunków wskazanych w powołanym przepisie. Przewidują one, że stosowanie monitoringu jest dopuszczalne**, gdy istnieją szczególne okoliczności powodujące wzmożony stopień zagrożenia** dla bezpieczeństwa **uczniów i pracowników lub mienia szkoły**, a w celu zapobiegnięcia tym zagrożeniom **stosowanie monitoringu jest niezbędne**.

Decydując się na zastosowanie monitoringu wizyjnego w salach lekcyjnych szkoła (która staje się administratorem danych przetwarzanych za pomocą kamer) musi wykazać, że **istnieją realne i bieżące zagrożenia dla bezpieczeństwa osób lub mienia** wymagające zastosowania monitoringu, tzn. jest on w tym przypadku środkiem **niezbędnym,** koniecznym dla zminimalizowania zagrożenia, a jednocześnie **nie ma możliwości zastosowania innych, mniej inwazyjnych, racjonalnych środków zaradczych albo są one niewystarczające** dla skutecznego zminimalizowania zagrożenia (np. wzmożona kontrola bieżąca pracowników i uczniów, wprowadzenie zabezpieczeń mechanicznych, elektronicznych, proceduralnych, zastosowanie urządzeń alarmujących o przekroczeniu dopuszczalnej temperatury, nieprawidłowym działaniu urządzeń albo nieautoryzowanej ingerencji).

Ocena skutków dla ochrony danych

Ponieważ tego rodzaju forma monitoringu potencjalnie wiąże się z wysokim ryzykiem naruszenia praw i wolności osób obserwowanych, administrator powinien **przeprowadzić ocenę skutków dla ochrony danych** (stosownie do art. 35 w zw. z art. 24 i art. 32 RODO). Celem przeprowadzenia oceny skutków jest **zidentyfikowanie konkretnych zagrożeń dla praw i wolności** osób, których dane dotyczą w związku ze stosowaniem monitoringu oraz **zaplanowanie konkretnych, adekwatnych środków technicznych i organizacyjnych**, które pozwolą zminimalizować ryzyko wystąpienia tych zagrożeń.

Bez względu na powyższe, przy stosowaniu monitoringu dyrektor szkoły dochować musi pozostałych warunków, o których mowa w art. 108a ust. 1–9 ustawy Prawo oświatowe, takich jak:

- uprzednie uzgodnienie z organem prowadzącym szkołę lub placówkę,
- przeprowadzenie konsultacji z radą pedagogiczną, radą rodziców i samorządem uczniowskim,
- wprowadzenie zabezpieczeń przed stosowaniem monitoringu w celu kontroli jakości pracy pracowników lub zachowania uczniów,
- odpowiednie informowanie i oznaczanie miejsc objętych obserwacją.

Dodatkowo analiza powinna obejmować przepisy Kodeksu pracy w zakresie dotyczącym zasad stosowania monitoringu wizyjnego wobec pracowników.

3 PRAWO I NOWE TECHNOLOGIE

Środki organizacyjne i techniczne zapewniające zgodność z RODO

W przypadku instalacji kamer w sali dydaktycznej na administratorze ciąży obowiązek zapewnienia, że monitoring stosowany jest **wyłącznie** w celu zapewnienia bezpieczeństwa lub ochrony mienia, a jednocześnie w taki sposób, który **gwarantuje poszanowanie godności i innych dóbr osobistych** osób nim objętych.

Powyższe realizować należy poprzez wdrożenie konkretnych, adekwatnych środków organizacyjnych i technicznych zapewniających zgodność z prawem i zasadami przetwarzania określonymi w art. 5 RODO. Zapewniona musi być również **proporcjonalność** stosowanego monitoringu w stosunku do praw osób, których dane dotyczą.

Jako przykłady takich środków wskazać można:

- **ścisłe ograniczenie dostępu do zapisów nagrań lub bieżącego wglądu na żywo** jedynie do osób, których udział jest niezbędny i które dają rękojmię niezależności i stosowania monitoringu zgodnie z jego przeznaczeniem,
- **przejrzysty regulamin wykorzystywania monitoringu** oraz prawidłowe informowanie osób nim objętych o zasadach stosowania wideonadzoru,
- **objęcie monitoringiem jedynie koniecznych przestrzeni** (nie całych sal lekcyjnych, ale jedynie konkretnych miejsc wzmożonego ryzyka**, np. przy stanowiskach z urządzeniami, takimi jak: piły, obcinarki, palniki**),
- instalowanie kamer o **parametrach dobranych do celu monitoringu** (ewentualnie **wyłączenie funkcji nadmiarowych**, takich jak np. inteligentna analiza obrazu, nagrywanie dźwięku),
- **stosowanie masek prywatności lub innych form zautomatyzowanej anonimizacji**, które w sposób skuteczny uniemożliwiają rozpoznanie tożsamości poszczególnych osób (o ile nie jest to konieczne do realizacji celów stosowania wideonadzoru),
- możliwie **ograniczona retencja danych,**
- stosowanie skutecznych **środków gwarantujących poufność, bezpieczeństwo i cyberbezpieczeństwo.**

Pomocne materiały

Powyższe zagadnienia zostały szerzej omówione w Wytycznych Europejskiej Rady Ochrony Danych 3/2019, przyjętych 29 stycznia 2020 r. w sprawie przetwarzania danych osobowych przez urządzenia wideo. Ponadto warto wziąć pod uwagę dotychczasowe stanowiska dotyczące omawianej materii, wyrażane przez Prezesa Urzędu Ochrony Danych Osobowych oraz Rzecznika Praw Obywatelskich.

NOWE SPOJRZENIE NA ZARZĄDZANIE DANYMI – DGA W PIGUŁCE

W drugiej części nowego cyklu poświęconego rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/868 z 30 maja 2022 r. w sprawie europejskiego zarządzania danymi (Akt w sprawie zarządzania danymi), określanego jako DGA, omówimy przepisy dotyczące usług pośrednictwa danych[1].

Usługi pośrednictwa danych są nowym rodzajem działalności gospodarczej, które – jak wyjaśnia motyw 27 DGA – mają pełnić kluczową funkcję w gospodarce danych. Ich celem jest przede wszystkim wspieranie i promowanie dobrowolnego dzielenia się danymi między przedsiębiorstwami, jak również ułatwianie takiego dzielenia się, jeśli wynika to z obowiązków ustanowionych w prawie Unii lub prawie krajowym. Zakłada się, że takie usługi mogą ułatwiać powstawanie nowych ekosystemów opartych na danych, które będą niezależne od podmiotów o znaczącej pozycji rynkowej i umożliwią niedyskryminacyjny dostęp do gospodarki danych przedsiębiorstwom o dowolnej wielkości, w szczególności MŚP i start-upom o ograniczonych środkach finansowych, prawnych lub administracyjnych. Usługi pośrednictwa danych mogą również wspierać osoby, których dane dotyczą, w realizacji przez nie swoich praw przyznanych przez RODO.

1. Usługa pośrednictwa danych

DGA definiuje usługę pośrednictwa danych w art. 2 pkt 11 jako 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 posiadaczami 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.

DGA reguluje następujące rodzaje usług pośrednictwa danych (Art. 10):

1. Dz. Urz. UE L 152 z 3.6.2022, s. 1–44.
2. Posiadacza danych zdefiniowano w art. 2 pkt 8 DGA jako osobę prawną, w tym podmiot sektora publicznego lub organizację międzynarodową, lub osobę fizyczną niebędącą w odniesieniu do przedmiotowych konkretnych danych osobą, której dane dotyczą, która ma – zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym – prawo do udzielania dostępu do niektórych danych osobowych lub danych nieosobowych lub do dzielenia się nimi; zgodnie zaś z art. 2 pkt 9 DGA użytkownik danych oznacza osobę fizyczną lub osobę prawną, która ma zgodny z prawem dostęp do niektórych danych osobowych lub nieosobowych i prawo, w tym – w przypadku danych osobowych – na podstawie rozporządzenia (UE) 2016/679, do wykorzystywania tych danych w celach komercyjnych lub niekomercyjnych.

a) usługi pośrednictwa między posiadaczami danych a potencjalnymi użytkownikami danych. Do takich usług w szczególności należy udostępnianie środków technicznych lub innych umożliwiających ich świadczenie takich usług. Mogą one obejmować:
   - dwustronną lub wielostronną wymianę danych;
   - tworzenie platform lub baz danych umożliwiających wymianę wspólne wykorzystywanie danych;
   - tworzenie innej specjalnej infrastruktury do stworzenia powiązań między posiadaczami danych a użytkownikami danych.

b) 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 rozporządzeniu (UE) 2016/679 praw osób, których dane dotyczą. Dostawcy takich usług pośrednictwa danych w swojej działalności mają dążyć do zwiększenia sprawczości osób, których dane dotyczą, w zakresie kontroli nad przetwarzaniem ich danych osobowych[3], pomagając im w wykonywaniu swoich praw wynikających z RODO[4], a w szczególności prawa do wyrażenia i wycofania zgody na przetwarzanie danych, prawa dostępu do danych czy też prawa do przenoszenia danych[5].

W tym kontekście ważne jest, aby model biznesowy takich dostawców zapewniał, że nie stosują oni niewłaściwych zachęt do korzystania ze swoich usług w celu skłonienia osób fizycznych do przekazania im większej ilości danych, niż leży to w interesie tych osób. Gwarancje takie mogą obejmować doradzanie osobom fizycznym w zakresie możliwego wykorzystywania ich danych oraz przeprowadzanie kontroli należytej staranności użytkowników danych przed umożliwieniem im kontaktu z osobami, których dane dotyczą. Ma to na celu unikanie oszukańczych praktyk.[6] Takie usługi mogą przybrać postać systemów zarządzania danymi osobowymi (ang. PIMS). Jak wskazuje Europejski Inspektor Ochrony Danych, takie systemy są nowymi produktami i usługami, które pomagają osobom fizycznym mieć więk-

3. I. Małobęcka-Szwast [w:] A. Piskorz-Ryń, M. Sakowska-Baryła, Rozporządzenie w sprawie europejskiego zarządzania danymi (DGA), Warszawa 2025, Komentarz do art. 10, s. 273.
4. Por. P. Drobek, Pomoc pośredników danych w wykonywaniu przez osoby, których dane dotyczą, swoich praw. Zagadnienia wybrane (dodatek MoP 11/2023), Monitor Prawniczy 2023, nr 11, s. 72-78.
5. Motyw 30 DGA.
6. tamże.

szą kontrolę nad swoimi danymi, umożliwiając im zarządzanie własną tożsamością cyfrową[7]. usługi świadczone przez spółdzielnie danych, które zgodnie z art. 2 pkt 15 DGA oznaczają usługi pośrednictwa danych oferowane przez strukturę organizacyjną utworzoną przez osoby, których dane dotyczą, przedsiębiorstwa jednoosobowe lub MŚP będące członkami tej struktury. Głównymi celami spółdzielni danych jest wspieranie swoich członków w wykonywaniu ich praw w odniesieniu do niektórych danych, w tym dokonywanie świadomego wyboru przed wyrażeniem przez nich zgody na przetwarzanie danych, wymienianie poglądów na temat celów przetwarzania danych i warunków, które najlepiej będą odzwierciedlać interesy jej członków w odniesieniu do ich danych, oraz negocjowanie w imieniu członków warunków i zasad przetwarzania danych przed udzieleniem pozwolenia na przetwarzanie danych nieosobowych lub przed zgodą na przetwarzanie danych osobowych.

Komisja Europejska wyjaśniła, że uregulowane w DGA usługi pośrednictwa danych są inspirowane następującymi istniejącymi lub powstającymi modelami[8]:

1) „rynki danych, które dopasowują podaż i popyt w jakimkolwiek zorganizowanym ekosystemie, a nawet poza nim;
2) orkiestratorów ekosystemów, np. (wspólnych europejskich) przestrzeni danych, w których uczestnicy akceptują określone zasady (prawne lub techniczne) uczestnictwa w ekosystemie;
3) pule danych utworzone przez przedsiębiorstwa lub osoby fizyczne, w przypadku gdy korzyści płynące z wykorzystania puli są przekazywane bezpośrednio podmiotom przekazującym dane do puli;
4) „spółdzielnie” lub „związki” danych posiadające mechanizm zbiorowych obrad lub podejmowania decyzji w sprawie wykorzystania danych, którymi dysponują członkowie spółdzielni lub związku;
5) usługi „portalu danych osobowych lub chmury obliczeniowej”, tj. usługi oferowane osobom fizycznym, które mogą przechowywać dotyczące ich dane osobowe będące obecnie w posiadaniu innych przedsiębiorstw i umożliwiać przetwarzanie takich danych przez osoby trzecie w ramach ich „chmury danych osobowych” („wprowadzanie algorytmu do danych” w celu maksymalizacji prywatności danych) albo poprzez przekazanie takich danych tej osobie trzeciej”.

7. Europejski Inspektor Ochrony Danych, TechDispatch #3/2020 – Personal Information Management Systems, https://www.edps.europa.eu/sites/default/files/publication/21-01-06_techdispatch-pims_en_0.pdf

8. Wdrażanie aktu w sprawie zarządzania danymi – wytyczne, s. 10, opublikowane na stronie internetowej: https://digital-strategy.ec.europa.eu/pl/library/new-practical-guide-data-governance-act

4 ZARZĄDZANIE DANYMI

Art. 2 pkt 11 DGA zawiera otwarty katalog usług, które nie są zaliczane do usług pośrednictwa danych:

a) usługi, 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. Tym samym poza zakresem „usług pośrednictwa danych" znajdą się brokerzy danych, którzy nie ustanawiają stosunku handlowego między posiadaczami danych a ich użytkownikami;

b) usługi skoncentrowane na pośrednictwie treści chronionych prawem autorskim;

c) usługi, 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, klientami lub współpracy nawiązanej na podstawie umowy. Chodzi tu w szczególności o usługi, których głównym celem jest zapewnienie funkcjonalności przedmiotów i urządzeń podłączonych do Internetu rzeczy;

d) usługi dzielenia się danymi oferowane przez podmioty sektora publicznego, które to usługi nie mają na celu ustanowienia stosunków handlowych.

Zgodnie z motywem 28 DGA świadczenie usług przechowywania w chmurze, usług analitycznych, dostarczanie oprogramowania na potrzeby dzielenia się danymi, przeglądarek internetowych, wtyczek do przeglądarek lub świadczenie usług poczty elektronicznej, nie powinno być uznawane za usługę pośrednictwa danych w rozumieniu tego rozporządzenia. Warunkiem jest jednak, że usługi takie jedynie dostarczają osobom, których dane dotyczą, lub posiadaczom danych, narzędzia techniczne służące do dzielenia się z innymi danymi. Celem dostarczania takich narzędzi nie może być jednak nawiązywanie stosunków handlowych między posiadaczami a użytkownikami ani umożliwienie dostawcy usług pośrednictwa danych uzyskiwania informacji o nawiązywaniu stosunków handlowych do celów dzielenia się danymi.

Określone w DGA obowiązki nałożone na dostawców usługi pośrednictwa danych nie mają zastosowania do uznanych organizacji altruizmu danych ani do innych podmiotów o charakterze niekomercyjnym – choć jedynie w pewnym zakresie. Chodzi tu o działalność polegającą na gromadzeniu danych w interesie ogólnym, udostępnianych przez osoby fizyczne lub prawne w myśl altruizmu danych.

Przy czym przepisy dotyczące usług pośrednictwa danych będzie się stosowało do tych podmiotów i organizacji, jeśli mają one na celu ustanowienie stosunków handlowych między nieokreśloną liczbą osób, których dane dotyczą, i posiadaczy danych z jednej strony oraz użytkownikami danych z drugiej.

2. Obowiązek zgłoszenia przez dostawców usług pośrednictwa danych

Zgodnie z art. 11 ust. 1 DGA każdy dostawca usług pośrednictwa danych, który zamierza świadczyć swoje usługi, ma obowiązek zgłoszenia do organu właściwego do spraw usług pośrednictwa danych.

Art. 19 projektu ustawy o zarządzaniu danymi przewiduje, że w Polsce będzie nim Prezes UODO.

DGA określa, że w takim zgłoszeniu muszą się znaleźć następujące informacje:

- nazwa dostawcy usług pośrednictwa danych;
- status i forma prawna, struktura własności oraz wskazanie odpowiednich jednostek zależnych dostawcy usług pośrednictwa danych, a w przypadku gdy figuruje on w rejestrze handlowym lub innym podobnym rejestrze publicznym – jego numer rejestracyjny;
- adres głównej jednostki organizacyjnej dostawcy usług pośrednictwa danych w Unii, o ile takowy istnieje, oraz, jeżeli ma to zastosowanie, drugorzędnego oddziału w innym państwie członkowskim lub adres przedstawiciela prawnego;
- adres ogólnodostępnej strony internetowej, na której można znaleźć kompletne i aktualne informacje na temat dostawcy usług pośrednictwa danych oraz jego działalności[9];
- dane kontaktowe osób wyznaczonych do kontaktów przez dostawcę usług pośrednictwa danych;
- opis usługi pośrednictwa danych, którą dostawca zamierza świadczyć, oraz wskazanie kategorii wymienionych w art. 10, do których należą takie usługi pośrednictwa danych;
- planowaną datę rozpoczęcia działalności, jeżeli jest inna od daty zgłoszenia[10];
- jeżeli zaszły jakiekolwiek zmiany informacji przekazanych w zgłoszeniu, dostawcy usług pośrednictwa danych zobowiązani są do powiadomienia o tym organu właściwego w terminie 14 dni od dnia, kiedy zmiana nastąpiła[11].

9. Na stronie internetowej powinny także zostać opublikowane co najmniej następujące informacje: nazwa dostawcy usług pośrednictwa danych, status prawny, forma prawna, struktura własności oraz odpowiednie jednostki zależne dostawcy usług pośrednictwa danych, a w przypadku gdy dostawca usług pośrednictwa danych jest zarejestrowany w rejestrze handlowym lub innym podobnym rejestrze publicznym – jego numer rejestracyjny, adres głównej jednostki organizacyjnej dostawcy usług pośrednictwa danych w Unii, o ile takowa istnieje, oraz, jeżeli ma to zastosowanie, drugorzędnego oddziału w innym państwie członkowskim lub adres przedstawiciela prawnego, opis usługi pośrednictwa danych, którą dostawca usług pośrednictwa danych zamierza świadczyć;
10. Art. 11 ust. 6 DGA
11. Art. 11 ust. 12 DGA

Dostawca usług pośrednictwa danych po dokonaniu zgłoszenia do organu właściwego do spraw usług pośrednictwa danych w jednym z państw członkowskich UE może rozpocząć działalność z zastrzeżeniem warunków określonych w rozdziale III DGA[12]. Takie zgłoszenie uprawnia dostawcę usług pośrednictwa danych do świadczenia swoich usług we wszystkich państwach członkowskich UE[13].

3. Uznany w Unii dostawca usług pośrednictwa danych

Zgodnie z art. 11 ust. 9 DGA na wniosek dostawcy usług pośrednictwa danych organ właściwy do spraw usług pośrednictwa danych potwierdza, że dostawca usług pośrednictwa danych przestrzega art. 11 oraz art. 12 DGA. Po otrzymaniu takiego potwierdzenia dostawca usług pośrednictwa danych może w swojej komunikacji pisemnej i ustnej posługiwać się oznakowaniem „uznany w Unii dostawca usług pośrednictwa danych" i używać wspólnego logo, które zostało ustanowione przez Komisję Europejską [14].

12. Art. 11 ust. 4 DGA.

13.Art. 11 ust. 5 DGA.

14. Rozporządzenie wykonawcze Komisji (UE) 2023/1622 z 9 sierpnia 2023 r. w sprawie wzoru wspólnych logo służących identyfikacji uznanych w Unii dostawców usług pośrednictwa danych i organizacji altruizmu danych , Dz. Urz. UE L 200 z 10.8.2023, s. 1–4.

4. Warunki świadczenia usług pośrednictwa danych

Warunki, które muszą spełnić dostawcy usług pośrednictwa danych, zostały określone w art. 12 DGA:

- dostawca usług pośrednictwa danych nie może wykorzystywać danych będących przedmiotem świadczonych przez niego usług pośrednictwa danych do celów innych niż oddanie ich do dyspozycji użytkownikom danych, a usługi pośrednictwa danych świadczy poprzez odrębną osobę prawną (lit. a);
- warunki handlowe, w tym ceny, świadczenia usług pośrednictwa danych posiadaczowi lub użytkownikowi danych nie mogą być uzależnione od tego, czy posiadacz lub użytkownik danych korzysta z innych usług świadczonych przez tego samego dostawcę usług pośrednictwa danych, powiązany z nim podmiot, ani od tego w jakim zakresie posiadacz lub użytkownik danych korzysta z takich innych usług (lit. b);
- dane zebrane w odniesieniu do działalności osoby fizycznej lub prawnej w celu świadczenia usługi pośrednictwa danych, w tym dane dotyczące daty, godziny i geolokalizacji, czasu trwania działalności; połączeń ustanowionych przez osobę korzystającą z usługi pośrednictwa danych z innymi osobami fizycznymi lub prawnymi, mogą być wykorzystywane tylko do celów rozwoju tej usługi pośrednictwa danych. Może to obejmować wykorzystywanie danych do wykrywania oszustw lub na potrzeby cyberbezpieczeństwa; udostępnia się je na żądanie posiadaczom danych (lit. c);
- dostawca usług pośrednictwa danych ułatwia wymianę danych w formacie, w jakim otrzymuje je od osoby, której dane dotyczą, lub od posiadacza danych. Konwertowanie tych danych do określonych formatów jest dopuszczalne wyłącznie w celu zwiększenia interoperacyjności w obrębie sektorów i między sektorami, zapewnienia harmonizacji z międzynarodowymi lub europejskimi standardami danych albo też na wniosek użytkownika danych lub wtedy, gdy jest to wymagane przez prawo Unii. Dostawca usług musi też oferować osobom, których dane dotyczą, lub posiadaczom danych możliwość rezygnacji z tych konwersji, chyba że taka konwersja jest wymagana przez prawo Unii (lit. d);
- usługi pośrednictwa danych mogą obejmować oferowanie posiadaczom danych lub osobom, których dane dotyczą, dodatkowych specjalnych narzędzi i usług ułatwiających wymianę danych. Chodzi tu o takie usługi jak: tymczasowe przechowywanie, kuratorstwo, konwersja, anonimizacja i pseudonimizacja. Z tych narzędzi korzysta się wyłącznie na wyraźny wniosek lub za zgodą posiada-

cza danych lub osoby, której dane dotyczą, a narzędzia osób trzecich oferowane w tym kontekście nie mogą wykorzystywać danych do innych celów (lit. e);

- dostawca usług pośrednictwa danych zapewnia, aby procedura dostępu do usługi była sprawiedliwa, przejrzysta i niedyskryminująca zarówno dla osób, których dane dotyczą, jak i posiadaczy danych, a także użytkowników danych, w tym w odniesieniu do cen i warunków świadczenia usługi (lit. f);
- dostawca usług pośrednictwa danych wprowadza procedury mające na celu zapobieganie oszustwom lub nadużyciom w odniesieniu do podmiotów ubiegających się o dostęp za pośrednictwem jego usług (lit. g);
- dostawca usług pośrednictwa danych zapewnia w przypadku niewypłacalności odpowiednią ciągłość świadczenia swoich usług pośrednictwa danych, a w przypadku gdy te usługi zapewniają przechowywanie danych, wprowadza mechanizmy umożliwiające posiadaczom i użytkownikom danych uzyskanie dostępu do swoich danych, ich przekazywanie lub pobieranie. Natomiast w przypadku świadczenia usług pośrednictwa danych między osobami, których dane dotyczą, a użytkownikami danych, dostawca zapewnia środki umożliwiające osobom, których dane dotyczą, wykonywanie przysługujących im praw (lit. h);
- dostawca usług pośrednictwa danych podejmuje odpowiednie środki w celu zapewnienia interoperacyjności z innymi usługami pośrednictwa danych, m.in. za pomocą standardów otwartych, które są powszechnie stosowane w sektorze działalności danego dostawcy usług pośrednictwa danych (lit. i);
- dostawca usług pośrednictwa danych wprowadza odpowiednie środki techniczne, prawne i organizacyjne w celu zapobiegania niezgodnemu z prawem Unii lub z prawem krajowym danego państwa członkowskiego przekazywaniu danych nieosobowych lub dostępowi do tych danych (lit. j);
- dostawca usług pośrednictwa danych informuje niezwłocznie posiadaczy danych, w przypadku gdy nastąpiły niedozwolone przekazanie, dostęp lub wykorzystanie danych nieosobowych, którymi się podzielił (lit. k);
- dostawca usług pośrednictwa danych podejmuje niezbędne środki w celu zapewnienia odpowiedniego poziomu bezpieczeństwa w zakresie przechowywania, przetwarzania i przesyłania danych nieosobowych. Dostawca usług pośrednictwa danych zapewnia również najwyższy poziom bezpieczeństwa przy przechowywaniu i przesyłaniu istotnych dla konkurencji, szczególnie chronio-

nych informacji (lit. l);

- dostawca usług pośrednictwa danych oferujący usługi osobom, których dane dotyczą, działa w najlepszym interesie tych osób, w przypadku gdy ułatwia wykonywanie przysługujących im praw. W szczególności zapewnia on – zanim osoby, których dane dotyczą, wyrażą zgodę – informacje oraz, w stosownych przypadkach, doradztwo w zwięzły, przejrzysty, zrozumiały i łatwo dostępny sposób co do zamierzonego wykorzystywania danych przez użytkowników danych oraz co do standardowych warunków związanych z takim wykorzystywaniem (lit. m);
- w przypadku gdy dostawca usług pośrednictwa danych zapewnia narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub pozwoleń na przetwarzanie danych udostępnionych przez posiadaczy danych, określa on – w stosownych przypadkach – jurysdykcję państwa trzeciego, w których ma się odbywać wykorzystywanie danych. Musi też dostarczyć osobom, których dane dotyczą, narzędzia umożliwiające zarówno wyrażenie, jak i wycofanie zgody, a posiadaczom danych – narzędzia umożliwiające zarówno udzielenie, jak i wycofanie pozwolenia na przetwarzanie danych (lit. n);
- dostawca usług pośrednictwa danych prowadzi rejestr zdarzeń dotyczących działalności w zakresie pośrednictwa danych (lit. o).

5. Rejestr uznanych w Unii dostawców usług pośrednictwa danych

Komisja Europejska prowadzi publiczny rejestr uznanych w Unii dostawców usług pośrednictwa danych. Dziś zarejestrowanych jest w nim 27 dostawców pośrednictwa danych z 7 państw członkowskich UE:

Austria: DID Daten-Intermediär-Dienste FlexCo

Belgia: Athumi, Datajoy

Finlandia: Dataspace Europe OY, Inteligentniejsze umowy

Francja: AGDATAHUB, Health DataTrust, Hub One DataTrust, M-ITRUST, NOTO, THEMIS-X, Real Data 4 Real Estate, Space Data Marketplace, VISIONS

Węgry: NIDHAS Adatközvetítő Korlátolt Felelelősségű Társaság

Niderlandy: Datakeeper B.V, Dexes, Fairsfair.io, Luminis Technologies, Stichting Health-RI, Stichting Ontwikkeling Schluss, Poort8, WeCity, Yivi.

Szwecja: iGrant.io, Gortanore Data Brokerage AB, Nilsson International AB

KONTROLE PLANOWE PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH W 2026 ROKU – JAK SIĘ DO NICH PRZYGOTOWAĆ?

W planie kontroli sektorowych UODO na rok 2026 (opublikowanym w styczniu) znalazły się m.in. te obszary, w których odnotowywano incydenty związane z ochroną danych osobowych, oraz te, które – z uwagi w szczególności na napływające do Urzędu skargi i zgłaszane naruszenia – Prezes UODO uznał za szczególnie problematyczne.

Zgodnie z tym planem kontrole sektorowe będą obejmowały pięć głównych obszarów:

- **podmioty lecznicze** – w zakresie przetwarzania danych osobowych przy wykorzystaniu monitoringu wizyjnego, w szczególności dotyczących dzieci;
- **podmioty prowadzące Biuletyn Informacji Publicznej** – w szczególności w zakresie anonimizacji danych oraz udostępniania przebiegu sesji rad gminy;
- **podmioty marketingowe** – w szczególności w zakresie podstaw prawnych przetwarzania danych osobowych w celach marketingowych;
- **internetowe platformy dostaw** – w zakresie przetwarzania danych osobowych w związku ze świadczeniem usług pośrednictwa w sprzedaży towarów i usług za pomocą aplikacji internetowych;
- organy, które przetwarzają dane osobowe w Wielkoskalowych Systemach Unii Europejskiej, w tym przetwarzanie danych osobowych SIS/VIS.

Kontrolę przeprowadzają upoważnieni przez Prezesa Urzędu pracownicy UODO (art. 79 ust. 1 ustawy).

Prawa i obowiązki kontrolowanego

Czynności kontrolne dokonywane są **w obecności kontrolowanego lub osoby przez niego upoważnionej**. Kontrolowany jest obowiązany do pisemnego wskazania osoby upoważnionej do reprezentowania go w trakcie kontroli.

5 NARUSZENIA I KONTROLE

Kontrolujący w ramach prowadzonych czynności kontrolnych mają prawo (art. 84 ust. 1 ustawy):

• **wstępu w godzinach od 6:00 do 22:00** na grunt oraz do budynków, lokali lub innych pomieszczeń;

• **wglądu do dokumentów** i informacji mających bezpośredni związek z zakresem przedmiotowym kontroli;

• przeprowadzania **oględzin miejsc, przedmiotów, urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych** służących do przetwarzania danych;

• żądania **złożenia pisemnych lub ustnych wyjaśnień** oraz **przesłuchiwania w charakterze świadka** osoby w zakresie niezbędnym do ustalenia stanu faktycznego;

• zlecania **sporządzania ekspertyz i opinii**.

Powyższym uprawnieniom kontrolujących towarzyszą obowiązki nałożone na kontrolowanych. Kontrolowany ma **obowiązek zapewnić kontrolującemu warunki i środki niezbędne do sprawnego przeprowadzenia kontroli**, a w szczególności sporządza we własnym zakresie kopie lub wydruki dokumentów oraz informacji zgromadzonych na nośnikach, w urządzeniach lub systemach informatycznych. Kontrolowany ma także obowiązek potwierdzenia za zgodność z oryginałem sporządzonych kopii lub wydruków (art. 84 ust. 2 i ust. 3 ustawy).

W trakcie kontroli **kontrolowany i jego pracownicy mają obowiązek składania wyjaśnień i zeznań.**

Uwaga: Ustawa o ochronie danych osobowych (art. 108 ust. 1) przewiduje odpowiedzialność karną za czyn polegający na udaremnieniu lub utrudnianiu kontrolującemu prowadzenia kontroli przestrzegania przepisów o ochronie danych osobowych.

Jak przygotować się do kontroli, by przebiegła ona sprawnie?

W celu umożliwienia sprawnego przeprowadzenia czynności kontrolnych kontrolowany powinien m.in.:

• **zgromadzić** i posiadać przygotowane **dokumenty mające bezpośredni związek z zakresem przedmiotowym kontroli,** wskazane podczas zawiadamiania o kontroli, oraz dokumenty **tłumaczone na język polski** (w przypadku, gdy dokumentacja jest sporządzona w języku obcym);

• zapewnić **obecność osób posiadających szczegółową wiedzę dotyczącą procesów przetwarzania danych osobowych**, w tym wykorzystywanych do tego celu nośników i systemów informatycznych, zarówno w kwestiach dotyczących ich funkcjonalności, jak i sposobu zapewnienia poufności, rozliczalności oraz integralności danych osobowych przetwarzanych w tych systemach;

• **sprawdzić procedury uaktualniania oprogramowania** (zarówno systemów operacyjnych, oprogramowania użytkowego, systemów antywirusowych, jak i firmware urządzeń sieciowych), czy też procedury **wykonywania i testowania kopii zapasowych;**

• **zweryfikować, czy zalecenia** powstałe w wyniku przeprowadzenia uprzedniego audytu/sprawdzenia **zostały wdrożone**;

• **zapewnić kontrolującym warunki i środki niezbędne do sprawnego przeprowadzenia kontroli**, w tym przygotować dla kontrolujących miejsce do pracy (pomieszczenie o charakterze biurowym, w którym będą mogły być dokonywane czynności kontrolne);

5 NARUSZENIA I KONTROLE

Rekomendowane jest także **dokonanie przed kontrolą przeglądu procesów przetwarzania danych osobowych oraz przeanalizowanie dokumentacji związanej z przetwarzaniem danych osobowych** (takiej jak m.in.: rejestr czynności przetwarzania danych osobowych, rejestr kategorii czynności – jeśli podmiot działa jako podmiot przetwarzający, wewnętrzne polityki i procedury ochrony danych osobowych, np. procedura dotycząca realizacji obowiązku dokumentowania wszelkich naruszeń ochrony danych osobowych, umowy powierzenia przetwarzania danych osobowych, analiza ryzyka, ocena skutków dla ochrony danych – jeśli jest wymagana).

Ważne: Należy pamiętać, że dokumentacja ochrony danych osobowych musi być aktualna i zgodna z rzeczywistymi procesami przetwarzania danych osobowych w podmiocie.

NSA POTWIERDZIŁ ARGUMENTACJĘ PREZESA UODO W SPRAWIE INSTALOWANIA MONITORINGU W ALTANACH ŚMIETNIKOWYCH

Egzekwowanie prawidłowej segregacji śmieci przez mieszkańców domów wielorodzinnych nie może stanowić podstawy do montowania kamer przy śmietniku przez spółdzielnie – wskazał NSA. Sąd podzielił w ten sposób interpretację przyjętą przez Prezesa UODO, wskazując jednocześnie, że istnieją mniej ingerujące w prywatność sposoby osiągnięcia tego celu – np. wydawanie worków na śmieci przypisanych do danego lokalu.

Prezes Urzędu w wydanej decyzji nakazał Spółdzielni usunięcie danych osobowych Skarżącego w zakresie jego wizerunku zarejestrowanego przez system monitoringu wizyjnego, zainstalowanego w altanie śmietnikowej, znajdujących się w zasobach Spółdzielni, a także zaprzestania pozyskiwania danych osobowych Skarżącego za pomocą systemu monitoringu zainstalowanego w altanie śmietnikowej. Uzasadniając tak wydane rozstrzygnięcie, organ uznał, że art. 6 ust. 1 lit. f RODO ani żadna z pozostałych przesłanek z art. 6 ust. 1 RODO nie może stanowić podstawy prawnej do legalnego przetwarzania danych za pomocą urządzeń monitorujących w takich miejscach.

Według Prezesa UODO nie można uznać, aby potrzeba wyegzekwowania poprawnej segregacji odpadów, w tym w szczególności względy finansowe, które stały się główną przyczyną montażu monitoringu wizyjnego w altanach śmietnikowych, miały charakter nadrzędny wobec podstawowych praw i wolności osób, których dane dotyczą, jakim niewątpliwie jest prawo do prywatności i ochrona wizerunku.

Spółdzielnia złożyła na decyzję Prezesa UODO skargę do Wojewódzkiego Sądu Administracyjnego w Warszawie. Wniosła w niej o uchylenie decyzji w zaskarżonej części oraz o umorzenie postępowania w tym zakresie.

WSA w Warszawie podzielił stanowisko zawarte w skardze. Zdaniem sądu pierwszej instancji spółdzielnia wykazała, że wystąpiły przesłanki pozwalające na przetwarzanie danych osobowych poprzez rejestrowanie wizerunku Skarżącego za pomocą monitoringu wizyjnego, zainstalowanego

w altanie śmietnikowej zgodnie z art. 6 ust. 1 lit. f RODO, oraz że przetwarzanie danych osobowych w ww. sposób było niezbędne do realizacji celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora

NSA popiera zdanie Prezesa UODO wyrażone w decyzji

Prezes UODO złożył skargę kasacyjną do Naczelnego Sądu Administracyjnego. Ten nie podzielił stanowiska sądu pierwszej instancji. NSA orzekł, że dla osiągnięcia celu w postaci egzekwowania segregacji odpadów nie jest niezbędne przetwarzanie danych osobowych w drodze rejestracji obrazu z altan śmietnikowych. Uznał ponadto, że w tej sytuacji „prawnie uzasadnione interesy" realizowane przez administratora danych osobowych nie mają charakteru nadrzędnego wobec interesów lub podstawowych praw i wolności osoby, której dotyczy ich przetwarzanie.

Zdaniem NSA przetwarzanie danych osobowych jednostki, polegające na rejestracji obrazu w przestrzeni wspólnej dla mieszkańców budynków wielorodzinnych, która nie jest przestrzenią ani stricte prywatną, ani stricte publiczną, nie może się odbywać na podstawie podstawy legalizującej przetwarzanie danych osobowych wyrażonej w art. 6 ust. 1 lit. f RODO, nawet jeśli jest to niezbędne, czyli nieodzowne dla realizacji celów w postaci prawidłowej segregacji odpadów komunalnych, gdyż wolność jednostki i jej prawo do prywatności są nadrzędne względem prawnie uzasadnionych interesów administratora danych osobowych. Tym samym NSA zgodził się ze stanowiskiem zawartym w decyzji Prezesa UODO.

NSA podkreślił, że obecnie istnieją alternatywne, względem rejestracji obrazu z altan śmietnikowych, sposoby egzekwowania i ustalania, którzy mieszkańcy dokonują segregacji opadów, a którzy ten obowiązek naruszają. Jako przykład takiego sposobu NSA wskazał wydawanie zindywidualizowanych worków na śmieci przypisanych do konkretnego lokalu mieszkalnego, co umożliwia następczą kontrolę realizacji zadeklarowanego obowiązku segregacji śmieci przez każdego z właścicieli.

Sygnatury:

III OSK 147/23

DS.523.3031.2020

EROD PRZEDSTAWIA WKŁAD DO RAPORTU Z EWALUACJI DYREKTYWY POLICYJNEJ ORAZ WYTYCZNE WS. WDRAŻANIA WIĄŻĄCYCH REGUŁ KORPORACYJNYCH

Europejska Rada Ochrony Danych wskazuje, że Dyrektywa policyjna ma kluczowe znaczenie dla ochrony danych osobowych w kontekście działań organów ścigania. Na posiedzeniu plenarnym 19 stycznia EROD przyjęła także zalecenia dotyczące wniosku o zatwierdzenie oraz elementów i zasad, które powinny się znaleźć w wiążących regułach korporacyjnych dla podmiotów przetwarzających (BCR-P).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680, zwana **Dyrektywą policyjną** lub **LED** (Law Enforcement Directive), ustanawia gwarancje i zasady ochrony danych osobowych przez organy ścigania i egzekucji prawa w związku wykrywaniem, ściganiem czy zapobieganiem przestępstwom. Jej art. 62 zakłada sporządzanie przeglądu i oceny stosowania jej przepisów co 4 lata. Komisja Europejska ma przedstawić najbliższy taki raport Parlamentowi Europejskiemu i Radzie do 6 maja 2026 r.

– *Z zadowoleniem przyjmujemy regularne oceny stosowania dyrektywy LED prowadzone przez Komisję Europejską i jesteśmy gotowi dzielić się naszą wiedzą ekspercką, aby zapewnić, że LED nadal będzie gwarantować wysoki poziom ochrony danych w kontekście działań organów ścigania* – powiedziała **Przewodnicząca EROD, Anu Talus.**

EROD pyta organy krajowe o ocenę i stosowanie Dyrektywy policyjnej

W sporządzeniu wspomnianego przeglądu pomocy KE udziela EROD, do której zadań należy **m.in. ułatwianie współpracy i koordynacji między organami ochrony danych podczas nadzorowania przetwarzania danych w sektorze egzekwowania prawa.** Ponadto sekretariat EROD pełni funkcję sekretariatu **Komitetu ds. Skoordynowanego Nadzoru (CSC), który zapewnia skoordynowany nadzór nad dużymi systemami teleinformatycznymi oraz organami i agencjami UE w obszarze egzekwowania prawa** i wymiaru sprawiedliwości w sprawach karnych. Dlatego w ramach przygotowań do przeglądu Komisja za pośrednictwem EROD zebrała opinie europejskich organów ochrony danych na temat stosowania i funkcjonowania Dyrektywy policyjnej w okresie od stycznia 2022 do 31 sierpnia 2025 r.

7 SPRAWY MIĘDZYNARODOWE

W swoim raporcie EROD podkreśla **kluczową rolę dyrektywy LED** w ochronie danych osobowych w działalności organów ścigania. Jednocześnie zwraca uwagę, że w świetle orzecznictwa, które rozwinęło się od czasu ostatniej oceny dyrektywy (tj. od 2022 r.), kluczowa jest silniejsza implementacja przepisów dyrektywy w prawie krajowym państw członkowskich. Aby zaś zwiększyć spójność i skuteczność stosowania jej przepisów, należy wzmocnić pozycję IOD w tym sektorze.

Organy ochrony danych potrzebują więcej zasobów w związku z nowymi zadaniami

Z raportu EROD wynika ponadto, że organy ochrony danych coraz częściej doradzają właściwym organom krajowym w zakresie ograniczania skutków naruszeń ochrony danych, a wiele z nich prowadzi również działania edukacyjne i wydaje wytyczne. Jednocześnie organy nadzorcze same zgłaszają potrzebę większej jasności co do zakresu stosowania LED oraz tego, gdzie przebiega granica między nią a RODO. Wnioskują także o bardziej szczegółowe zajęcie się wyzwaniami wynikającymi z rosnącego wykorzystania nowych technologii, takich jak **sztuczna inteligencja**, w kontekście działań organów ścigania. EROD podkreśla konieczność stosowania tych narzędzi przez organy ścigania w **ścisłej zgodności z dyrektywą policyjną**, by zapewnić, że ich użycie jest niezbędne, proporcjonalne i objęte odpowiednimi zabezpieczeniami.

Raport wskazuje również na potrzebę **poprawy współpracy** – zarówno między właściwymi organami odpowiedzialnymi za stosowanie LED, jak i szerzej między organami ścigania. Wreszcie EROD podkreśla, że zarówno organy ochrony danych, jak i sam EROD potrzebują **dodatkowych zasobów finansowych i kadrowych**, aby realizować nowe zadania wynikające z ostatnich aktów prawnych, w tym obowiązki związane z CSC, którego działalność obejmuje obecnie również nadzór nad systemami takimi jak **System Informacyjny Schengen (VIS), Prüm II oraz System Wjazdu/Wyjścia (EES).**

Wytyczne dla podmiotów przetwarzających ws. Wiążących Reguł Korporacyjnych

Przyjęte w styczniu przez EROD wytyczne stanowią aktualizację istniejącego referencyjnego zestawu wymogów BCR-P, który zawiera kryteria zatwierdzania BCR-P, oraz łączą go ze standardowym formularzem wniosku o BCR-P. **BCR-P są narzędziem transferowym**, które może być stosowane przez grupę przedsiębiorstw do przekazywania danych osobowych poza Europejski Obszar Gospodarczy do podmiotów przetwarzających w ramach tej samej grupy. BCR tworzą **możliwe do egzekwowania**

zasady oraz określają zobowiązania mające zapewnić poziom ochrony danych zasadniczo równoważny temu, który gwarantuje RODO.

Aktualne wytyczne ws. BCR-P: jasne kryteria i brak osobnych umów powierzenia

Nowe zalecenia opierają się na uzgodnieniach i doświadczeniach zdobytych przez organy ochrony danych w trakcie procedur zatwierdzania konkretnych wniosków BCR-P od czasu wejścia w życie RODO, a także na pracach prowadzonych w ramach zaktualizowanych zaleceń dotyczących **wiążących reguł korporacyjnych dla administratorów (BCR-C).**

Zalecenia zawierają **jasne kryteria i wyjaśnienia**, aby zapewnić, że BCR-P opracowywane przez grupy przedsiębiorstw są zgodne z RODO. Wyjaśniają również, kiedy BCR-P mogą być stosowane – mianowicie **wyłącznie do transferów wewnątrzgrupowych między podmiotami przetwarzającymi**, gdy administrator nie należy do grupy.

Ponadto zalecenia precyzują, że BCR-P są zaprojektowane tak, aby spełniać wymogi **art. 28 ust. 4 RODO**. Oznacza to, że każdy podmiot przetwarzający w grupie korzystający z BCR-P **nie musi podpisywać odrębnej umowy powierzenia** z każdym podwykonawcą przetwarzania w grupie.

Zalecenia będą poddane **konsultacjom publicznym do 2 marca 2026 r.** Członkowie EROD przeprowadzili także wymianę poglądów na temat nadchodzącej **wspólnej opinii dotyczącej pakietu Digital Omnibus**, której przyjęcie zaplanowano na lutowe posiedzenie plenarne.

Więcej informacji na temat wiążących reguł korporacyjnych (WRK) można znaleźć na stronie UODO: https://uodo.gov.pl/pl/638

Więcej informacji o Dyrektywie policyjnej dostępne na stronie UODO: https://uodo.gov.pl/pl/405

Źródło:

Komunikat Europejskiej Rady Ochrony Danyc: EDPB contributes to the LED evaluation and adopts recommendations on the application for Processor BCR | European Data Protection Board

PREZES UODO UCZESTNICZYŁ W WEBINARIUM MIĘDZYNARODOWYM (CIPL) POŚWIĘCONYM OPINII EROD NA TEMAT SZTUCZNEJ INTELIGENCJI

Mimo postępów w interpretacji zasad RODO w kontekście AI nadal istnieją obszary wymagające doprecyzowania – to główny wniosek z webinarium organizowanego przez CIPL. W dyskusji wskazano też m.in. na potrzebę dalszej współpracy między organami nadzorczymi a sektorem technologicznym, aby zapewnić odpowiedzialny rozwój sztucznej inteligencji przy poszanowaniu praw osób, których dane dotyczą.

13 stycznia 2026 r. odbyło się międzynarodowe webinarium pt. **„The EDPB's Opinion on AI: One Year On",** zorganizowane przez Centre for Information Policy Leadership (CIPL). Poświęcone ono było zmianom w podejściu regulatorów do sztucznej inteligencji rok po publikacji opinii Europejskiej Rady Ochrony Danych. W wydarzeniu wzięli udział przedstawiciele organów nadzorczych, instytucji europejskich oraz eksperci branżowi. Jednym z zaproszonych uczestników był **Prezes Urzędu Ochrony Danych Osobowych, Mirosław Wróblewski.**

W dyskusji uczestniczyli również przedstawiciele organów nadzorczych z Łotwy, a także reprezentanci branży – OpenAI i Microsoft – co pozwoliło na zestawienie perspektyw regulatorów i praktyków. W pierwszej części spotkania omówiono najważniejsze zmiany w europejskiej debacie regulacyjnej dotyczącej sztucznej inteligencji. Przedstawiciele EROD, organów nadzorczych z Irlandii i Hamburga wskazywali na rosnącą potrzebę spójności interpretacyjnej, zwłaszcza w obszarach takich jak minimalizacja danych czy stosowanie prawnie uzasadnionego interesu w kontekście systemów AI. Dyskusja udowodniła, że dynamiczny rozwój technologii wymaga od organów nadzorczych ciągłego dostosowywania metod oceny ryzyka i adekwatności zabezpieczeń.

Prezes UODO – zasad ochrony danych trzeba pilnować na każdym etapie rozwoju AI

W drugiej części webinarium odbyła się moderowana debata dotycząca praktycznego stosowania zasad **minimalizacji danych** oraz **prawnie uzasadnionego interesu** w cyklu życia systemów AI. Prezes UODO, jako jeden z głównych uczestników panelu, przedstawił perspektywę polskiego organu nadzorczego.

Podkreślił znaczenie **rzetelnych i udokumentowanych ocen** stosowania tych zasad na każdym etapie tworzenia i wdrażania systemów AI – od projektowania modeli, przez trenowanie, aż po ich eksploatację. Zwrócił uwagę, że kluczowe jest nie tylko ograniczanie zakresu danych, ale także zapewnienie przejrzystości procesów oraz adekwatnych środków technicznych i organizacyjnych.

UODO NA WEBINARIUM IAPP POŚWIĘCONYM PAKIETOWI DIGITAL OMNIBUS

Digital Ombnibus może się przyczynić do zwiększenia przejrzystości i dostępności regulacji, jednak nie może to odbywać się kosztem praw osób, których dane dotyczą – zgodzili się uczestnicy webinarium zorganizowanego przez IAPP.

W dyskusji, w której brał udział przedstawiciel UODO, wskazano również na potrzebę dalszych wyjaśnień i praktycznych wskazówek, które są już przygotowywane w następstwie **Helsinki Statement** przyjętego przez Europejską Radę Ochrony Danych. 15 stycznia 2026 r. odbyło się webinarium zorganizowane przez oddziały IAPP z Polski, Słowacji i Litwy, poświęcone projektowi **Digital Omnibus** oraz planowanym uproszczeniom wynikającym z RODO. W wydarzeniu uczestniczyli przedstawiciele administracji publicznej, eksperci prawa ochrony danych oraz praktycy z regionu Europy Środkowo-Wschodniej. **Urząd Ochrony Danych Osobowych reprezentował Krzysztof Król, zastępca dyrektorki Departamentu Współpracy Międzynarodowej.**

Digital Omnibus – szansa na uproszczenia, ale z poszanowaniem praw obywateli

Dyskusja koncentrowała się na propozycjach Komisji Europejskiej dotyczących uproszczenia i ujednolicenia przepisów w ramach pakietu Digital Omnibus. W trakcie webinarium Krzysztof Król podzielił się doświadczeniami UODO w zakresie stosowania przepisów RODO w praktyce oraz oceny wpływu planowanych zmian na funkcjonowanie administratorów i podmiotów przetwarzających. Podkreślił znaczenie zachowania równowagi między upraszczaniem regulacji a zapewnieniem wysokiego poziomu ochrony danych osobowych.

Dialog ws. regulowania sztucznej inteligencji wciąż trwa

Webinarium IAPP było okazją do wymiany doświadczeń między ekspertami z regionu. W dyskusji udział wzięli m.in. Migle Dewsbury, Lukas A. Mrazik oraz dr Urszula Góral, a całość moderował Szymon Sieniewicz. Uczestnicy podkreślali, że współpraca między państwami Europy Środkowo-Wschodniej jest kluczowa dla spójnego wdrażania nowych regulacji i wypracowywania wspólnych standardów.

Spotkanie odbyło się wkrótce po seminarium **„AI Omnibus”** zorganizowanym przez Centre for Information Policy Leadership (CIPL), w którym uczestniczył prezes UODO Mirosław Wróblewski. Prezes zwrócił wówczas uwagę na priorytety organów nadzorczych w obszarze sztucznej inteligencji – bezpieczeństwo, przejrzystość i zgodność operacji przetwarzania danych. Przedstawił również wnioski z badania dotyczącego potrzeb organizacji w zakresie AI, wskazując na rosnącą rolę edukacji i szkoleń zarówno w sektorze publicznym, jak i prywatnym.

UODO NA KLUCZOWYCH WYDARZENIACH EUROPEJSKICH Z OKAZJI DNIA OCHRONY DANYCH 2026

27–28 stycznia 2026 r. przedstawiciele Urzędu Ochrony Danych Osobowych, zastępca Prezesa UODO Konrad Komornicki oraz dyrektorka Departamentu Współpracy Międzynarodowej Maria Owczarek wzięli udział w trzech ważnych wydarzeniach poświęconych przyszłości ochrony danych osobowych, współpracy między regulatorami oraz wyzwaniom związanym z nowymi technologiami.

Digital Clearinghouse 2.0 – współpraca regulatorów w erze nowych regulacji

Pierwszym z tych wydarzeń była konferencja **„Towards a Digital Clearinghouse 2.0”**, zorganizowana przez Europejskiego Inspektora Ochrony Danych **27 stycznia 2026 r. w Brukseli**. Jej celem było omówienie przyszłości współpracy między organami nadzorczymi w kontekście gwałtownego rozwoju regulacji cyfrowych. Udział przedstawicieli UODO pozwolił na przedstawienie polskiej perspektywy dotyczącej potrzeby spójności regulacyjnej i praktycznych rozwiązań wspierających współdziałanie organów.

Nowe akty prawne – takie jak **Akt o zarządzaniu danymi**, **Akt o rynkach cyfrowych**, **Akt o usługach cyfrowych**, **Akt o danych** czy **Akt o sztucznej inteligencji** – coraz silniej przenikają się z ochroną danych osobowych. Wspólne wyzwania wymagają więc skutecznych mechanizmów koordynacji między regulatorami odpowiedzialnymi za konkurencję, konsumentów, cyberbezpieczeństwo i prywatność.
Podczas spotkania analizowano doświadczenia istniejących forów współpracy w różnych państwach oraz identyfikowano bariery utrudniające wymianę informacji między instytucjami. Dyskutowano również o tym, jakie funkcje powinno pełnić **Digital Clearinghouse 2.0**, aby stać się efektywną platformą współpracy na poziomie UE.

Data Protection Day Celebration w Stałym Przedstawicielstwie RP przy UE

Z okazji **Dnia Ochrony Danych Osobowych, 28 stycznia 2026 r.,** Stałe Przedstawicielstwo RP przy UE zorganizowało również w Brukseli coroczne spotkanie, w którym uczestniczyli przedstawiciele administracji, instytucji europejskich oraz eksperci.

7 SPRAWY MIĘDZYNARODOWE

Dyrektor generalny Ministerstwa Cyfryzacji, **Bartosz Dominiak**, podkreślił potrzebę przejścia od „labiryntu regulacji" do **cyfrowej synergii**. Wskazał, że Unia Europejska powinna być miejscem, w którym ochrona danych jest standardem, a zgodność z przepisami – wartością, a nie obciążeniem.
Wśród kluczowych postulatów Polski znalazły się: **cyfrowy omnibus** - uproszczenie regulacji przy zachowaniu wysokiego poziomu ochrony, oraz **pojedynczy punkt zgłaszania incydentów** – jedno miejsce raportowania zamiast wielu równoległych obowiązków wobec różnych instytucji.

Wydarzeniu towarzyszyła debata **„One entry to rule them all"**, z udziałem ekspertów z Komisji Europejskiej, ENISA, ECSO oraz UODO, a także prezentacja aplikacji **mObywatel** jako przykładu praktycznej cyfryzacji usług publicznych.

Data Protection Day 2026: Reset or refine? – konferencja EIOD i Rady Europy

Tego samego dnia i również w Brukseli odbyła się konferencja **„Data Protection Day 2026: Reset or refine?"**, współorganizowana przez EIOD i Radę Europy. Jej tematem przewodnim była przyszłość europejskiego systemu ochrony danych w obliczu dynamicznych zmian technologicznych. Konferencja zgromadziła decydentów, regulatorów, naukowców i praktyków, tworząc przestrzeń do wymiany doświadczeń i wskazania kierunków dalszego rozwoju europejskiej ochrony danych.

Głównymi tematami dyskusji było znaczenie modernizacji Konwencji 108 (przez Konwencję 108+), refleksja nad prawie dekadą doświadczeń z RODO i dalszym kierunkiem rozwoju przepisów i praktyki ochrony danych osobowych, a także rola Europy jako globalnego lidera w kształtowaniu cyfrowej przeszłości nastawionej na człowieka (**human-centric digital future). Padły też ważne pytania, np. o to, jak pogodzić uproszczenia regulacyjne z utrzymaniem silnych gwarancji dla obywateli.**

DZIEŃ OCHRONY DANYCH 2026: JAK CHRONIĆ DANE OSOBOWE DZIECI W INTERNECIE

Wkrótce zostanie uruchomiona specjalna platforma „Privacy for Kids", na której rodzice, nauczyciele i edukatorzy znajdą wszystko, czego potrzebują, aby pomóc dzieciom zrozumieć i chronić ich prywatność w internecie. Hub będzie gromadził materiały edukacyjne dostarczane przez organy ochrony danych z całej Europy. Treści będą dostępne w różnych językach.

Każdego dnia europejskie organy ochrony danych, tworzące Europejską Radę Ochrony Danych, współpracują, aby zapewnić ochronę danych osobowych obywateli. W przypadku danych dzieci konieczna jest szczególna czujność, zwłaszcza w dzisiejszym szybko zmieniającym się środowisku cyfrowym, w którym nieustannie pojawiają się nowe zagrożenia.

Dzieci są bardziej narażone w internecie niż dorośli, ponieważ trudniej rozpoznają niebezpieczeństwa, mają skłonność do nadmiernego zaufania obcym i mogą udostępniać dane osobowe, nie zdając sobie z tego sprawy. Aplikacje, z których korzystają, często zbierają ich dane, a bez odpowiednich zabezpieczeń dzieci mogą być narażone na szkodliwe treści. Rodzi to ryzyko pozostawienia trwałych, cyfrowych śladków które trudno usunąć, oraz naruszeń prywatności, których skutki towarzyszyć im mogą przez całe życie.

Zaangażowanie EROD w praktyce – potrzeba skutecznej weryfikacji wieku

Ochrona danych dzieci jest strategicznym priorytetem EROD, a Rada poczyniła ważne postępy w zakresie wzmacniania cyfrowych praw najmłodszych. W lutym 2024 r. przyjęła oświadczenie dotyczące rozwoju prac legislacyjnych nad projektem rozporządzenia mającego na celu zapobieganie i zwalczanie wykorzystywania seksualnego dzieci. Oświadczenie to nawiązuje do wspólnej opinii EROD–EIOD w sprawie tego samego projektu. Ponadto, zgodnie ze strategią EROD na lata 2024–2027, Rada pracuje obecnie nad wytycznymi dotyczącymi przetwarzania danych dzieci.

W lutym 2025 r. EROD przyjęła również oświadczenie dotyczące weryfikacji wieku, mające pomóc organizacjom w ocenie wieku użytkowników w sposób zgodny z RODO. Weryfikacja wieku jest kluczowa, aby dzieci nie miały dostępu do treści dla nich nieodpowiednich. Jednocześnie metoda weryfikacji musi być możliwie najmniej ingerująca, a dane osobowe dzieci – odpowiednio chronione.

7 SPRAWY MIĘDZYNARODOWE

W swoim oświadczeniu dotyczącym weryfikacji wieku EROD przedstawia dziesięć zasad zgodnego z prawem przetwarzania danych osobowych w celu ustalenia wieku lub przedziału wiekowego danej osoby. EROD popiera środki pozwalające ustalić, czy dana osoba przekroczyła określony próg wiekowy, ale tylko wtedy, gdy są one proporcjonalne i zgodne z kluczowymi zasadami ochrony danych UE, takimi jak domyślna ochrona prywatności.

EROD sprawia, że ochrona danych staje się dziecinnie prosta

28 stycznia, w duchu Dnia Ochrony Danych, EROD zapowiedziała uruchomienie nowej platformy, „Prywatność dla dzieci", oraz zaprezentowała zapowiedź tego projektu w formie animowanego filmu. W ten sposób EROD zwraca się bezpośrednio do dzieci w kwestii prywatności on-line. Upraszczając złożone zagadnienia do przystępnych, zrozumiałych treści i wykorzystując kolorowe, interaktywne materiały, pomoże najmłodszym zrozumieć ich prawa cyfrowe oraz znaczenie ochrony danych osobowych. Film pozwala także rodzicom dowiedzieć się, dlaczego tak ważne jest, aby dzieci były świadome zagrożeń związanych z ochroną danych w internecie. Wspólne obejrzenie materiału to doskonały sposób, by rozpocząć rozmowę z dziećmi o prywatności i odpowiedzialnym zachowaniu w sieci. EROD zachęca też do udostępniania filmu, by dotarł do jak największej liczby młodych odbiorców.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych (pod którym znaleźć można też wspomniany film)

Data Protection Day 2026: keeping children's personal data safe online | European Data Protection Board

CZESKI SN: NIE WOLNO POBIERAĆ PREWENCYJNIE DANYCH O AKTYWNOŚCI I LOKALIZACJI KAŻDEGO INTERNAUTY

Zbiorcze pobieranie i przechowywanie danych w zakresie telefonicznej i elektronicznej aktywności użytkownika pozostaje w sprzeczności z prawem Unii Europejskiej – orzekł czeski Sąd Najwyższy w grudniu 2025 r. Wskazał również na potrzebę zmian legislacyjnych, ponieważ w obecnym kształcie przepisy prawa krajowego pozwalają „na prewencyjne przechowywanie danych praktycznie wszystkich użytkowników usług elektronicznych, praktycznie zawsze, i to w takim zakresie, z którego można wywodzić jednoznaczne ustalenia o życiu prywatnym".

Omawiany wyrok jest rezultatem postępowania cywilnego, które zostało wszczęte pozwem dziennikarza Czeskiego Radia przeciwko Republice Czeskiej. Powód zażądał w nim jako zadośćuczynienia przeprosin dla siebie i innych obywateli tego państwa za naruszenie ich praw oraz niewłaściwe transponowanie dyrektywy unijnej do prawa krajowego.

Skarga na masowe zbieranie danych użytkowników sieci

Powód wniósł o zadośćuczynienie w zw. z przepisami ustawy o komunikacji elektronicznej regulującymi pobieranie oraz przechowywanie danych o aktywności i lokalizacji użytkownika. Na ich podstawie dostawcy usług telekomunikacyjnych są uprawnieni do przechowywania danych przez pół roku. O dostęp do nich mogą następnie wystąpić organy ścigania, służby bezpieczeństwa państwa i w niektórych przypadkach **–** Czeski Bank Narodowy.

Złożenie pozwu poprzedziło żądanie dziennikarza skierowane do operatora telekomunikacyjnego o usunięcie dotyczących go danych osobowych (art. 17 RODO). W związku z niepowodzeniem skorzystania ze swojego uprawnienia wniósł skargę do czeskiego organu nadzorczego, który stwierdził, że czeskie prawo krajowe pozostaje w sporze z orzecznictwem europejskim. Konfliktu tego organ nie może rozwiązać w drodze wykładni. To stanowiło impuls dla dziennikarza do domagania się zadośćuczynienia od państwa za brak właściwej implementacji prawa.

Natomiast w 2019 r. czeski Sąd Konstytucyjny orzekł, że instytucja retencji danych nie pozostaje w sprzeczności z porządkiem konstytucyjnym państwa. Sąd ten wskazał jednocześnie, że po stronie ustawodawcy leży zapewnienie sprawiedliwej równowagi między interesem publicznym a ingerencją w prawa jednostki. Odnośnie do zakresu czasowego zbierania i przechowywania danych Sąd Konstytucyjny orzekł, iż nie może dublować roli ustawodawcy i wskazać, jaki okres byłby właściwy. Wcześniej jednak dwukrotnie (w roku 2010 oraz 2011) orzekał on w sprawie poprzednich nowelizacji przepisów – wskazując na niedopuszczalność dwuletniego okresu przechowywania danych oraz na obowiązek jasnego wskazania celu ich przetwarzania.

8 ORZECZNICTWO ZAGRANICZNE

SN: państwo musi przeprosić za naruszenie prywatności dziennikarza

Prawomocne orzeczenie Sądu Najwyższego zobowiązało czeskie Ministerstwo Przemysłu i Handlu do wystosowania przeprosin dla dziennikarza za naruszenie jego prawa do prywatności i ochrony danych osobowych. Sąd Najwyższy ponadto stwierdził, że czeskie normy regulujące pobieranie i przechowywanie danych o aktywności użytkownika i jego danych lokalizacyjnych naruszają prawo do prywatności każdego, kto korzysta z usług komunikacji elektronicznej. Uznał także za niezgodne z prawem prewencyjne przechowywanie danych potencjalnie wszystkich korzystających z usług świadczonych drogą elektroniczną. Potwierdził również, że państwo ponosi odpowiedzialność za majątkową i niemajątkową szkodę będącą rezultatem braku implementacji dyrektyw (lub ich niewłaściwej implementacji).

Źródła:

30 Cdo 2556/2025-335 z 30 grudnia 2025 r.

54 Co 89/2025-276 z 22 kwietnia 2025 r.

N 76/94 SbNU 19 z dnia 14 maja 2019 r.

N 217/63 SbNU 483 z dnia 20 grudnia 2011 r.

TSUE UZNAŁ, ŻE WHATSAPP MOŻE ZASKARŻYĆ WIĄŻĄCĄ DECYZJĘ EUROPEJSKIEJ RADY OCHRONY DANYCH

Trybunał w Luksemburgu orzekł, że wiążąca decyzja EROD nr 1/2021 dotyczy WhatsAppa bezpośrednio, a więc może być zaskarżona. Uchylił wcześniejszy wyrok Sądu UE w tej sprawie i przekazał ją do ponownego rozpoznania. Stwierdził przy tym, że skarga została wniesiona w terminie, więc powinna zostać rozpatrzona.

Korzenie sprawy sięgają 2018 r., kiedy to irlandzki organ ochrony danych osobowych (Data Protection Commission – DPC) po otrzymaniu licznych skarg dotyczących aplikacji WhatsApp (zarówno od jej użytkowników, jak i osób, które z niej nie korzystały) wszczął z urzędu postępowanie w sprawie przestrzegania przez tę firmę obowiązków informacyjnych i zasad przejrzystości. Był on organem wiodącym, gdyż europejska siedziba grupy Facebook (obecnie Meta), do której należy WhatsApp, znajduje się właśnie w Irlandii. Skargi na aplikację wpływały jednak również do organów nadzorczych w innych krajach, m.in. W Niemczech.

Dlatego po przeprowadzeniu dochodzenia i uzyskaniu wyjaśnień od spółki DPC przedstawiła w grudniu 2020 r. projekt decyzji pozostałym organom nadzorczym, których sprawa dotyczyła. W styczniu następnego roku osiem z nich wniosło sprzeciwy wobec niektórych elementów tego projektu. Ponieważ nie udało się osiągnąć kompromisu, organ irlandzki zwrócił się do EROD o rozstrzygnięcie sporu. Ta w lipcu 2021 r. wydała – stosownie do art. 65 ust. 2 RODO – decyzję wiążącą wszystkie organy nadzorcze, których sprawa dotyczy, w której stwierdziła m.in. naruszenie niektórych przepisów RODO i zobowiązała irlandzki organ nadzorczy do zmiany planowanych środków naprawczych, w tym wysokości grzywien. Na tej podstawie DPC wydało ostateczną decyzję wobec WhatsAppa.

Stanowisko EROD i kara za naruszenie zasad ochrony danych

W decyzji tej irlandzki organ nadzorczy uznał, iż WhatsApp naruszył zasadę przejrzystości oraz wynikające z niej obowiązki określone w art. 5 ust. 1 lit. a), w art. 12 ust. 1, w art. 13 ust. 1 lit. c)–f), w art. 13 ust. 2 lit. a), c) oraz e), a także w art. 14 RODO. W owej decyzji organ ten stwierdził natomiast, że WhatsApp wypełnił obowiązki określone w art. 13 ust. 1 lit. a) oraz b), a także w art. 13 ust. 2 lit. b) oraz d) RODO. W ramach środków zaradczych DPC udzieliło WhatsAppowi upomnienia, nakładając przy tym na niego obowiązek wdrożenia szeregu działań mających na celu doprowadzenie – w terminie trzech miesięcy – do przestrzegania przepisów RODO, które zostały naruszone. Organ nałożył też na firmę cztery grzywny administracyjne związane z naruszeniami, o których mowa w art. 5 ust. 1 lit. a) oraz w art. 12–14 RODO, na łączną kwotę 225 mln EUR.

Jednocześnie w swojej decyzji wskazał aspekty, w odniesieniu do których decyzja EROD nałożyła nań obowiązek zmiany oceny zawartej w projekcie decyzji. Decyzja EROD rozstrzygnęła bowiem kwestie będące przedmiotem sprzeciwów, takie jak m.in.: naruszenia obowiązków informacyjnych z art. 13 i 14 RODO, uznania za dane osobowe informacji pochodzących z kompresji ze stratą (tzw. haszowanie stratne) w odniesieniu do kontaktów niebędących użytkownikami WhatsAppa, naruszenia zasad przejrzystości i minimalizacji danych. EROD poleciła też skrócić termin na wprowadzenie środków zaradczych z planowanych 6 do 3 miesięcy, a także podwyższenie grzywien w stosunku do projektu.

Ukarana spółka wnosi skargę do Luksemburga

WhatsApp zaskarżył decyzję DPC przed sądem irlandzkim, a w odniesieniu do decyzji EROD odwołał się do Sądu UE. Ten jednak odrzucił skargę jako niedopuszczalną, uznając, że zaskarżony dokument stanowi jedynie akt przygotowawczy lub pośredni, a dopiero decyzja organu krajowego jest ostateczna. Decyzja EROD, zdaniem Sądu, nie wywołuje więc niezależnych skutków prawnych i nie podlega zaskarżeniu, nie dotyczy też WhatsAppa bezpośrednio. Skuteczną ochronę spółce zapewnia zaś wniesienie odwołania do sądu krajowego, który w razie wątpliwości może wystąpić z pytaniem prejudycjalnym. Uznanie dopuszczalności skargi spowodowałoby zaś konieczność prowadzenia dwóch równoległych postępowań – przed sądem krajowym i unijnym.

WhatsApp zaskarżył decyzję Sądu do Trybunału Sprawiedliwości, zarzucając naruszenie prawa przez uznanie, że decyzja EROD nie jest aktem zaskarżalnym.

Europejska Rada Ochrony Danych wskazywała, że skarga została wniesiona po terminie. TSUE uznał jednak, że w tym wypadku termin liczy się od ogłoszenia (publikacji) decyzji EROD, a nie od poinformowania o niej WhatsAppa (co nastąpiło nieco wcześniej). Termin na wniesienie skargi został więc zdaniem Trybunału zachowany.

Spór przed TSUE – czy decyzja EROD była ostateczna i dotyczyła firmy bezpośrednio?

Osią sporu przed TSUE była kwestia tego, czy wiążąca decyzja EROD jest zaskarżalna. Zdaniem spółki nie jest w tym celu konieczne wykazanie, że decyzja EROD dotyczyła jej bezpośrednio, ale jedynie że wywołała skutki prawne wobec niej lub osób trzecich (w niniejszej sprawie, wobec irlandzkiego organu nadzorczego i wszystkich innych organów nadzorczych, których sprawa dotyczy). W tym wypadku zaś wywoływała takie skutki w szczególności poprzez uznanie, że dane poddane kompresji stratnej stanowią dane osobowe. Skarżąca spółka zwróciła też uwagę, iż decyzja EROD była wiążąca dla organu irlandzkiego.

EROD argumentowała zaś, że choć decyzja zwiera jej ostateczne stanowisko, to sama w sobie nie powoduje zmiany sytuacji prawnej WhatsAppa – czyni to dopiero decyzja ostateczna DPC. Nie nakłada też na spółkę nowych obowiązków – gdyż te wynikają z samego RODO i są egzekwowane przez organ krajowy. EROD podnosiła m.in., że jej decyzja i decyzja DPC zostały wydane w ramach jednolitej procedury administracyjnej składającej się z wzajemnie od siebie zależnych etapów na szczeblach: krajowym i europejskim i dotyczącej tego samego przedmiotu, nie zaś – w następstwie przeprowadzenia dwóch niezależnych postępowań, które dotyczyłyby odrębnych kwestii. Za to EROD

podnosiła, że celem procedury rozstrzygania sporów jest zapewnienie spójnego wdrażania RODO przez organy krajowe.

Zdaniem TSUE nie ma też w tym wypadku znaczenia, że na decyzję EROD nie można się powołać bezpośrednio wobec skarżącej spółki – dopuszczalność zaskarżenia należy bowiem oceniać obiektywnie. Skargę wnieść może nie tylko podmiot, który jest adresatem decyzji, ale także ten, którego dotyczy ona bezpośrednio. Tak jest w sytuacji, gdy wpływa ona na sytuację prawną tego podmiotu oraz gdy organ, który ma ją wykonać, nie ma żadnego zakresu uznania, a wykonanie odbywa się w sposób automatyczny. TSUE badał więc, czy wymogi te zostały spełnione w odniesieniu do WhatsAppa w tym przypadku.

Trybunał Sprawiedliwości: skarga WhatsAppa zasługuje na rozpatrzenie

Wbrew wcześniejszemu rozstrzygnięciu Sądu UE Trybunał uznał, że decyzja EROD dotyczy spółki bezpośrednio. Choć nie jest decyzją kończącą postępowanie, to zawiera ostateczne stanowisko organu UE i nie może być uznana za akt pośredni. Wpływa ona także na jej sytuację prawną spółki – choćby przez uznanie danych pozyskanych w wyniku haszowania stratnego za dane osobowe, co rodzi konieczność zmiany w umowach z użytkownikami.

Po drugie zaś, decyzja EROD jest wiążąca dla organu irlandzkiego i innych zainteresowanych organów w kwestii interpretacji RODO. Bez znaczenia jest tu – zdaniem TSUE – fakt, że ostateczne ustalenie wysokości kary należy do DPC oraz że organ ten ma pewną swobodę w kwestiach nieobjętych sprzeciwami innych organów i co za tym idzie – decyzją EROD.

W związku z powyższym Trybunał w Luksemburgu orzekł, iż decyzja EROD nie jest aktem pośrednim i dotyczy WhatsAppa bezpośrednio, a zatem jest zaskarżalna. Ponieważ zaś skarga została wniesiona w terminie i nie ma powodów, by uznać ją za niedopuszczalną, powinna zostać rozpatrzona. Dlatego TSUE przekazał sprawę do ponownego rozpoznania Sądowi UE. Zwrócił przy tym uwagę, iż nie stanowi problemu toczenie równoległego postępowania przed sądem irlandzkim – zgodnie bowiem z zasadą lojalnej współpracy sąd ten powinien zawiesić postępowanie do czasu wydania orzeczenia przez Sąd UE lub też skierować do TSUE pytanie prejudycjalne ws. tego rozstrzygnięcia.

SYGNATURA:

C-97/23 P WhatsApp Ireland/Europejska Rada Ochrony Danych

WKŁAD EROD DO EWALUACJI DYREKTYWY POLICYJNEJ – GŁÓWNE WNIOSKI I WYZWANIA DLA ORGANÓW NADZORCZYCH

Europejska Rada Ochrony Danych przyjęła ogólne stanowisko oraz syntetyczne podsumowanie odpowiedzi krajowych organów nadzorczych na potrzeby drugiej ewaluacji stosowania Dyrektywy 2016/680 (DODO). Komisja Europejska planuje opublikowanie raportu z ewaluacji w maju 2026 r., obejmującego okres od stycznia 2022 do 31 sierpnia 2025 r.

EROD podkreśliła, że Dyrektywa policyjna – obok RODO oraz rozporządzenia (UE) 2018/1725 – stanowi kluczowy element europejskiego systemu ochrony danych osobowych. DODO wprowadziła jednolite, wysokie standardy ochrony danych w sektorze organów ścigania, zapewniając wspólne ramy dla organów odpowiedzialnych za zapobieganie i zwalczanie przestępczości.

EROD pozytywnie oceniła fakt, że prawodawca unijny przewidział cykliczną ocenę stosowania dyrektywy, co umożliwia identyfikację problemów praktycznych i dostosowywanie ram prawnych do dynamicznie zmieniającego się środowiska operacyjnego organów ścigania.

Coraz bogatsze orzecznictwo i potrzeba dalszych wyjaśnień

Od poprzedniej ewaluacji (w 2022 r.) wzrosła liczba orzeczeń sądów krajowych i Trybunału Sprawiedliwości UE dotyczących przetwarzania danych w kontekście ścigania przestępstw. Orzecznictwo to stopniowo doprecyzowuje kwestie interpretacyjne, jednak – zdaniem EROD – proces ten dopiero się rozpoczyna. **Większa liczba pytań prejudycjalnych kierowanych do TSUE mogłaby przyczynić się do dalszego ujednolicenia praktyki stosowania DODO w państwach członkowskich.**

Granice stosowania DODO i relacja z RODO

W odpowiedziach organów nadzorczych wyraźnie wybrzmiała potrzeba doprecyzowania:

- zakresu zastosowania DODO (w szczególności pojęcia „zapobiegania zagrożeniom dla bezpieczeństwa publicznego”);
- **granicy między DODO a RODO**, zwłaszcza w kontekście **działalności sądów i organów administracji** poza sprawowaniem wymiaru sprawiedliwości;
- **relacji między DODO a przepisami sektorowymi** oraz nowymi regulacjami, w tym **dotyczącymi sztucznej inteligencji**.

9 SPRAWY MIĘDZYNARODOWE/SCHENGEN

Wraz z rosnącą rolą narzędzi takich jak AI i analityka big data w postępowaniach karnych, **EROD podkreśla konieczność ich stosowania w ścisłej zgodności z zasadami DODO** – w szczególności zasadą niezbędności, proporcjonalności i odpowiednich zabezpieczeń praw osób, których dane dotyczą.

Systemy wielkoskalowe i współpraca transgraniczna

Rosnąca liczba unijnych systemów informacyjnych oraz interoperacyjność baz danych zwiększają stopień złożoności przetwarzania danych w sektorze ścigania. Organy nadzorcze wskazują, że **współpraca transgraniczna wiąże się z częstymi transferami danych** – zarówno wewnątrz UE, jak i poza EOG, przez co **wykonywanie praw osób, których dane dotyczą, staje się coraz bardziej skomplikowane**. Dlatego konieczne jest zapewnienie odpowiednich narzędzi technicznych i bezpiecznych platform wymiany informacji.

Rola inspektorów ochrony danych w sektorze operacyjnym

EROD zwraca uwagę na **kluczową rolę inspektorów ochrony danych** w organach ścigania i wymiarze sprawiedliwości. W praktyce ich skuteczność bywa jednak ograniczona przez **brak dostępu do informacji operacyjnych, niewystarczające szkolenia i niedostateczne umocowanie instytucjonalne**.

Wzmocnienie pozycji i kompetencji IOD – w tym poprzez rozwój dedykowanych narzędzi oceny ryzyka i wzorów DPIA dostosowanych do specyfiki działań operacyjnych – zostało wskazane jako **jeden z kluczowych kierunków działań**.

Wyzwania w implementacji krajowej

Choć większość organów nadzorczych nie zgłosiła nowych, istotnych problemów w zakresie transpozycji DODO, część państw członkowskich wskazała m.in. na:

- **brak pełnych narzędzi egzekucyjnych** (np. brak możliwości nakładania kar administracyjnych);
- **niejasności dotyczące kompetencji organów nadzorczych** wobec sądów w toku sprawowania przez nich wymiaru sprawiedliwości;
- problemy związane z tzw. systemem dostępu pośredniego do danych przetwarzanych przez organy ścigania;
- **rozbieżności w zakresie uprawnień naprawczych i sankcyjnych** w porównaniu z reżimem RODO.

W niektórych państwach wskazano także na **trudności w jednoznacznym rozróżnieniu administratora i podmiotu przetwarzającego w strukturach sądownictwa**.

9 SPRAWY MIĘDZYNARODOWE/SCHENGEN

Zasoby organów nadzorczych – warunek skutecznego nadzoru

Jednym z najczęściej powtarzających się wyzwań **była kwestia niewystarczających zasobów finansowych i kadrowych** organów nadzorczych. Skuteczny nadzór nad przetwarzaniem danych w sektorze ścigania wymaga bowiem specjalistycznej wiedzy z zakresu ochrony danych i współpracy międzynarodowej w sprawach karnych, zrozumienia technicznego i operacyjnego funkcjonowania systemów informatycznych oraz odpowiedniego wsparcia analitycznego i szkoleniowego.

Znaczenie ewaluacji dla przyszłości DODO

Druga ewaluacja stosowania Dyrektywy policyjnej stanowi istotny moment refleksji nad funkcjonowaniem systemu ochrony danych w obszarze ścigania przestępstw. Zebrane doświadczenia pokazują, że **choć DODO stworzyła solidne podstawy prawne, jej skuteczne stosowanie wymaga dalszego doprecyzowania przepisów i ich wykładni, wzmocnienia zasobów i kompetencji organów nadzorczych,** rozwoju praktycznych narzędzi wspierających ocenę ryzyka i zgodność operacyjną, stałego dialogu między organami nadzorczymi, ustawodawcą i praktykami sektora bezpieczeństwa.

Wkład EROD do raportu Komisji Europejskiej będzie stanowił **ważny punkt odniesienia do dalszego rozwoju unijnych standardów ochrony danych** w kontekście działań organów ścigania – w warunkach rosnącej cyfryzacji, interoperacyjności systemów i wykorzystania nowych technologii.

Pełna treść przyjętego stanowiska oraz syntetyczne opracowanie odpowiedzi organów nadzorczych są dostępne na stronie internetowej Europejskiej Rady Ochrony Danych. W kolejnych numerach biuletynu przedstawimy Państwu, jak wdrożenie dyrektywy w Polsce prezentuje się na tle innych państw UE.

CSC PRZEDSTAWIA RAPORT Z DZIAŁANIA SYSTEMU INFORMACYJNEGO SCHENGEN ZA ROK 2024

System Informacyjny Schengen zajmuje szczególne miejsce wśród wielkoskalowych systemów informatycznych Unii Europejskiej – nie tylko ze względu na zakres przetwarzanych danych i znaczenie operacyjne dla obszaru wolności, bezpieczeństwa i sprawiedliwości, lecz również z uwagi na odrębny, szczególny reżim prawny w zakresie sprawozdawczości.

Rozporządzenia (UE) 2018/1861 oraz 2018/1862 ustanawiają obowiązek corocznej sprawozdawczości skoncentrowanej na praktyce wykonywania praw osób, których dane dotyczą, w państwach członkowskich. W przekształconej wersji SIS ustawodawca unijny wprowadził obowiązek przekazywania do EROD danych statystycznych dotyczących wykonywania prawa dostępu, sprostowania i usunięcia danych.

Dane te są przekazywane przez państwa członkowskie, a zadaniem CSC jest ich zebranie, analiza oraz opracowanie rocznego sprawozdania dla EROD, obejmującego również informacje o postępowaniach sądowych. Sprawozdania państw członkowskich obejmują trzy poziomy wykonywania praw:

- działania administratorów danych;
- środki odwoławcze realizowane przez organy ochrony danych;
- środki ochrony sądowej.

Rok 2024 był drugim rokiem publikacji sprawozdania CSC dotyczącego statystyk wykonywania praw osób, których dane dotyczą w SIS. Doświadczenia zebrane w tym cyklu potwierdzają jednak, że jakość, kompletność i terminowość przekazywanych danych pozostają zróżnicowane. W wielu przypadkach dane nie były raportowane w pełnym zakresie, część sprawozdań została złożona po terminie, a niektóre państwa członkowskie nie przekazały sprawozdań w ogóle. Wskazywane przyczyny obejmowały m.in. brak jasno przypisanych kompetencji w zakresie gromadzenia statystyk SIS, brak scentralizowanych narzędzi do agregowania danych z systemów sądowych czy niepełne wdrożenie przepisów szczególnych. Dlatego też raport z działalności za 2024 r. został opublikowany dopiero na początku lutego 2026 r.

Realizacja prawa dostępu w SIS

W 2024 r. w skali europejskiej dominowały wnioski o dostęp do danych przetwarzanych w dziedzinie odpraw granicznych – 29 151 wniosków, z czego w 89% przypadków udzielono dostępu do danych. Na drugim miejscu znajdują się wnioski osób, których dane nie są przetwarzane w SIS – 28 121 przypadków, przy czym w 60% udzielono informacji potwierdzającej brak wpisu.

9 SPRAWY MIĘDZYNARODOWE/SCHENGEN

Trzecią kategorię stanowią wnioski dotyczące wpisów dokonywanych do celów powrotu nielegalnie przebywających obywateli państw trzecich – 4 501 wniosków, z czego w 95% przypadków udzielono dostępu. W odniesieniu do wpisów w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości odnotowano łącznie 800 wniosków o dostęp, przy wskaźniku udzielenia dostępu na poziomie 86%.

Na tym tle wyniki Polski przedstawiają się zróżnicowanie. W przypadku wpisów dotyczących powrotu nielegalnie przebywających obywateli państw trzecich dostęp do danych został udzielony w 100% przypadków. W odniesieniu do wpisów z zakresu współpracy policyjnej i współpracy wymiarów sprawiedliwości wskaźnik ten wyniósł 94%.

W przypadku wniosków osób, których dane nie są przetwarzane w SIS, Polska udzieliła informacji w 36% przypadków, natomiast w odniesieniu do danych przetwarzanych w dziedzinie odpraw granicznych – w 20% przypadków.

Ograniczenia prawa dostępu i rola organów nadzorczych

Zgodnie z rozporządzeniami SIS państwo członkowskie może – w określonych sytuacjach – podjąć decyzję o nieprzekazywaniu w całości lub części informacji osobie, której dane dotyczą. Ograniczenie to musi być zgodne z prawem krajowym oraz stanowić niezbędny i proporcjonalny środek w społeczeństwie demokratycznym, w szczególności w celu:

- zapobieżenia utrudnianiu urzędowych lub sądowych dochodzeń, postępowań przygotowawczych lub procedur;
- zapobieżenia utrudnianiu zapobiegania przestępstwom, ich wykrywania, ścigania lub wykonywania kar;
- ochrony bezpieczeństwa publicznego;
- ochrony bezpieczeństwa narodowego;
- ochrony praw i wolności innych osób.

W takich przypadkach osoba, której dane dotyczą, może wykonywać swoje prawa za pośrednictwem właściwego organu nadzorczego (tzw. dostęp pośredni).

Dane za 2024 r. pokazują, że mechanizm ten jest wykorzystywany w praktyce, jednak odsetek przypadków zakończonych przyznaniem pośredniego dostępu jest zróżnicowany. Najwięcej wniosków skierowanych do organów nadzorczych dotyczyło wpisów w dziedzinie odpraw granicznych – 603 przypadki, z czego jedynie w 12% zrealizowano pośredni dostęp do danych.

W 312 przypadkach zwrócono się do organów nadzorczych w sytuacji, w której osoba nie figurowała w SIS – w tej kategorii potwierdzono podmiotom danych brak wpisu w 18% spraw. W odniesieniu do wpisów w dziedzinie współpracy policyjnej i wymiarów sprawiedliwości odnotowano 111 wniosków, przy czym pośredni dostęp został udzielony jedynie w 2% przypadków. Najwyższy odsetek przyznanego dostępu pośredniego dotyczył wpisów dokonywanych do celów powrotu nielegalnie przebywających obywateli państw trzecich – spośród 25 wniosków dostęp przyznano w 80% spraw.

Dane te pokazują, że w szczególności w obszarze współpracy policyjnej i sądowej poziom ujawniania informacji jest bardzo niski, co może wynikać z częstszego powoływania się na przesłanki związane z bezpieczeństwem publicznym lub skutecznością postępowań karnych. Jednocześnie mechanizm dostępu pośredniego pozostaje istotnym gwarantem kontroli nad legalnością przetwarzania danych w sytuacjach, gdy bezpośrednie przekazanie informacji jest ograniczone.

Jednakże w przypadku Polski obowiązujące przepisy krajowe nie przewidują mechanizmu dostępu pośredniego w rozumieniu rozporządzeń SIS. Osoby, których dane dotyczą, mogą dochodzić swoich praw bezpośrednio wobec administratora oraz wnieść skargę do Prezesa UODO, jednak nie mają możliwości wykonywania swoich praw za pośrednictwem organu nadzorczego w razie odmowy dostępu, sprostowania lub usunięcia danych. W toku ewaluacji Schengen, której Polska podlegała w 2024 r., wskazano, że obecne rozwiązanie nie zapewnia pełnej realizacji art. 53 ust. 3 rozporządzenia (UE) 2018/1861, art. 67 ust. 3 rozporządzenia (UE) 2018/1862 oraz art. 19 rozporządzenia (UE) 2018/1860, i sformułowano wobec Polski zalecenie wdrożenia mechanizmu dostępu pośredniego.

Nadzór, statystyki i działania koordynacyjne

W 2024 r. Komitet Skoordynowanego Nadzoru (CSC) prowadził szereg działań o charakterze systemowym, skoncentrowanych na długofalowym kształtowaniu ram nadzoru nad funkcjonowaniem Systemu Informacyjnego Schengen (SIS). Jednym z kluczowych obszarów była kontynuacja prac nad wykładnią przepisów dotyczących cyklu audytu SIS. Dyskusje prowadzone na forum CSC dotyczyły zakresu audytu, jego kompleksowości, częstotliwości oraz stosowania międzynarodowych standardów audytu przez krajowe organy ochrony danych i Europejskiego Inspektora Ochrony Danych. Prace te, zapoczątkowane jeszcze przed 2024 r., były w omawianym roku dalej rozwijane i ukierunkowane na wypracowanie wspólnego, spójnego podejścia nadzorczego.

Równolegle CSC prowadził wymianę informacji z Komisją Europejską w kontekście nowych ram Ewaluacji Schengen (SCHEVAL). W 2024 r. omawiano m.in. doświadczenia z pierwszych ocen przeprowadzanych według nowej metodyki, rolę ekspertów ds. ochrony danych w zespołach oceniających, planowanie przyszłych inspekcji oraz stopień integracji systemów EES i ETIAS z mechanizmem oceny Schengen.

Istotnym elementem działalności CSC była również współpraca z Agencją eu-LISA. Regularne kontakty z inspektorem ochrony danych Agencji umożliwiały bieżącą wymianę informacji dotyczących funkcjonowania nowego SIS, w tym doświadczeń z pierwszego roku jego operacyjnego działania. Informacje te stanowiły ważny kontekst dla dalszych działań nadzorczych i pozwalały identyfikować potencjalne wyzwania o charakterze technicznym i organizacyjnym.

Działania tematyczne CSC – artykuły 36 i 40 SIS

Istotnym obszarem aktywności CSC w 2024 r. były działania tematyczne dotyczące szczególnie wrażliwych kategorii wpisów w SIS.

9 SPRAWY MIĘDZYNARODOWE – SCHENGEN

W odniesieniu do wpisów opartych na art. 36 rozporządzenia (UE) 2018/1862, dotyczących niejawnego nadzoru, CSC kontynuował działania zapoczątkowane jeszcze przez Grupę ds. Koordynacji Nadzoru nad SIS II. Po wznowieniu prac po okresie pandemii COVID-19 krajowe organy ochrony danych przekazały informacje z przeprowadzonych działań nadzorczych, które zostały poddane analizie na forum CSC. Efektem było opublikowanie w październiku 2024 r. sprawozdania zawierającego wnioski dotyczące poziomu zgodności i zalecenia odnośnie do jakości dokumentacji, okresów przechowywania danych oraz aspektów merytorycznych i technicznych wpisów.

W odniesieniu do art. 40 rozporządzenia 2018/1862, umożliwiającego wprowadzanie do SIS danych biometrycznych nieznanych osób poszukiwanych, CSC od początku monitoruje statystyki dotyczące tych wpisów. Niewielka liczba wpisów i ograniczona liczba państw członkowskich korzystających z tej możliwości wskazują, że na obecnym etapie nie zachodzi potrzeba podejmowania skoordynowanych działań, przy jednoczesnym utrzymaniu bieżącego monitoringu i wymiany informacji.

Znaczenie sprawozdawczości SIS dla systemu nadzoru

Szczególny reżim sprawozdawczy SIS pokazuje, że ochrona praw osób, których dane dotyczą, została wpisana w architekturę systemu i nie ogranicza się wyłącznie do reaktywnego nadzoru. Coroczne sprawozdania, oparte na danych krajowych, pozwalają EROD i CSC identyfikować problemy systemowe oraz wspierać państwa członkowskie w doskonaleniu swoich procedur.

Dla krajowych organów ochrony danych oznacza to konieczność dalszego wzmacniania współpracy z właściwymi organami, tak aby sprawozdawczość SIS była kompletna, porównywalna i terminowa. W dłuższej perspektywie doświadczenia te będą miały znaczenie również dla innych wielkoskalowych systemów informatycznych UE, w których podobne mechanizmy sprawozdawcze dopiero się kształtują.

Pełna treść raportu CSC za 2024 r. dotyczącego działań nadzorczych oraz wykonywania praw osób, których dane dotyczą w SIS, jest dostępna na stronie Europejskiej Rady Ochrony Danych (EROD) w sekcji poświęconej CSC.

KLUCZOWE JEST ROZDZIELENIE FUNKCJI IOD I ADMINISTRATORA

Inspektorzy ochrony danych stanowią ważny element systemu ochrony danych osobowych wprowadzonego przez RODO. Aby właściwie pełnili swoje zadania, administratorzy muszą im zapewnić niezależność, odpowiednie wsparcie, oraz zapobiegać konfliktom interesów. Monika Kurzajewska, główny specjalista w Wydziale Współpracy z IOD, przypomniała najważniejsze elementy roli i pozycji IOD podczas spotkania z inspektorami w ramach akcji „UODO rusza w kraj".

23 stycznia Prezes Urzędu Ochrony Danych Osobowych **Mirosław Wróblewski** wraz z innymi pracownikami Urzędu odwiedzili **Suwałki**. Było to kolejne wydarzenie **w ramach akcji „UODO rusza w kraj",** której celem jest **przybliżenie działalności UODO mieszkańcom różnych regionów Polski**. Prócz debaty na temat zagrożeń i wyzwań dla ochrony danych osobowych oraz otwartego punktu porad dla mieszkańców odbyło się spotkanie z inspektorami ochrony danych oraz administratorami.

Rola i pozycja inspektora

Podczas tego spotkania **Monika Kurzajewska, główny specjalista w Wydziale Współpracy z IOD,** wygłosiła referat pt**. „Rola i pozycja IOD w sektorze publicznym"**. Na wstępie ekspertka wskazała, że **kompetentny, właściwie usytuowany i niezależny – a przez to skuteczny IOD** – to fundament przestrzegania przepisów o ochronie danych osobowych. Podkreśliła również, że od początku obowiązywania przepisów RODO Urząd wypracował wiele wytycznych i wskazówek dotyczących zapewnienia IOD warunków do prawidłowego funkcjonowania i wykonywania zadań.

Były one sukcesywnie publikowane na stronie internetowej UODO, przede wszystkim w zakładce Inspektor Ochrony Danych czy w Newsletterze UODO dla IOD (Biuletynie UODO), ale również w sprawozdaniu krajowym polskiego organu nadzorczego przygotowanym w związku z udziałem w działaniu CEF DPO oraz w podsumowaniu spotkania w UODO pt. Niezależność IOD musi być standardem.

W publikowanych na stronie internetowej UODO materiałach i odpowiedziach na pytania inspektorów i administratorów Urząd w działaniach na rzecz zwiększania świadomości, co do roli i statusu IOD, zwłaszcza co do przewidzianych w RODO gwarancji niezależnego wykonywania tej funkcji wskazywał, np.:

Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?

Czy możliwe jest łączenie funkcji IOD z obowiązkami administratora systemu informatycznego (ASI)?

Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji?

Czy IOD może jednocześnie pełnić funkcję pełnomocnika do spraw ochrony informacji niejawnych?

10 PRACOWNICY UODO

Czy funkcję IOD można łączyć z wykonywaniem zawodu adwokata lub radcy prawnego?

Czy z zewnętrznym IOD należy zawrzeć umowę powierzenia?

Czy administrator jest zobowiązany na podstawie RODO do zapewnienia inspektorowi zespołu IOD?

Czy obowiązek z art. 38 ust. 2 RODO dotyczy administratora korzystającego z usług zewnętrznego IOD?

Czy zastępca IOD powinien być wyznaczony na stałe?

i wiele innych, z których część nadal jest dostępna pod linkiem: https://uodo.gov.pl/pl/506/2579).

UODO w poprzednich latach wielokrotnie odnosił się również do kwestii wykonywania zadań przez IOD, wyjaśniając, np.:

– Czy administrator może przerzucać swoje obowiązki na IOD?

– Czy prowadzenie rejestru czynności powinno być zaliczane do zadań IOD?

– Czy IOD może nadawać upoważnienia?

– Czy IOD może w imieniu administratora zawierać umowy powierzenia?

– Kto powinien opracować wewnętrzną politykę ochrony danych osobowych? Administrator czy IOD?

Pytania wraz z odpowiedziami udostępnione były na poprzedniej stronie internetowej naszego Urzędu w zakładce Inspektor Ochrony Danych (https://archiwum.uodo.gov.pl/p/zadania-iod), obecnie znajdują się w Numerze specjalnym Biuletynu UODO.

Kompetencje IOD, wsparcie i niezależność

Aby wykonywać swoje obowiązki, inspektor musi nie tylko **znać krajowe i europejskie przepisy** o ochronie danych osobowych, ale też **rozumieć przeprowadzane procesy przetwarzania danych** oraz posiadać **wiedzę z zakresu IT i bezpieczeństwa danych**. Niezbędna jest także znajomość organizacji i sektora, w którym działa. IOD odgrywa bowiem kluczową rolę w promowaniu kultury ochrony danych w organizacji i przypilnowaniu przestrzegania RODO. Znacznie mają również osobiste cechy IOD – **rzetelność i wysoki poziom etyki zawodowej.**

Wybór inspektora spełniającego te wymogi należy do administratora. Powinien dokonać starannej analizy i mieć pewność, że osoba wyznaczona przez niego do pełnienia funkcji IOD będzie miała zapewnione właściwe warunki dla prawidłowego wykonywania zadań IOD. Oznacza to, że administrator ma obowiązek **właściwego i niezwłocznego włączania IOD we wszystkie sprawy związane z ochroną danych osobowych, wspierania go w wykonywaniu przez niego zadań oraz zagwarantowania niezależności dla prawidłowego i efektywnego realizowania jego zadań.**

W praktyce oznacza to, że inspektor powinien być angażowany w najkrótszym możliwym czasie we wszystkie kwestie związane z ochroną danych osobowych, w szczególności brać udział w spotkaniach kierownictwa organizacji oraz mieć możliwość wyrażenia swojej opinii przy podejmowaniu decyzji z zakresu ochrony danych.

– *Stanowisko inspektora powinno być zawsze brane pod uwagę. Grupa Robocza art. 29, zaleca w ramach dobrych praktyk* ***dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem inspektora*** – wskazała ekspertka.

Z kolei wsparcie działań inspektora sprowadza się **do zapewnienia mu odpowiednich zasobów zarówno do wykonywania zadań** (w przypadku większych organizacji, np. zapewnienie jego zastępcy lub nawet całego zespołu, a także pomieszczeń i infrastruktury dla jego działania), **jak i utrzymania fachowej wiedzy** (udział w szkoleniach). IOD musi mieć także dostęp do danych osobowych i **wystarczający czas umożliwiający mu wykonywanie jego zadań.**

Gwarancja niezależności podstawą pozycji IOD w organizacji

Kluczowe dla prawidłowego wykonywania funkcji IOD jest zagwarantowanie inspektorowi niezależności w pełnieniu obowiązków. Oznacza to w szczególności, że powinien on podlegać bezpośrednio najwyższemu kierownictwu organizacji.

– *Celem tej bezpośredniej podległości jest skrócenie drogi raportowania. Zapewnienie IOD możliwości bezpośredniego kontaktu, bez pośrednictwa kierownictwa niższego szczebla, daje gwarancję najpełniejszej i najszybszej informacji w kwestii procesów przetwarzania i umożliwia szybką reakcję w sprawach przedstawianych przez inspektora.* ***Inspektor nie może też otrzymywać poleceń dotyczących sposobu załatwienia danej sprawy*** – tłumaczyła Monika Kurzajewska.

Ponadto IOD nie może być odwoływany lub karany za pełnienie swojej funkcji, np. za wydanie zaleceń sprzecznych ze stanowiskiem administratora. Kary należy tu rozumieć szeroko, także jako utrudnianie IOD awansu lub rozwoju zawodowego czy też ograniczanie dostępu do korzyści przysługujących innym pracownikom.

Bardzo ważne jest również unikanie konfliktu interesów w związku z wykonywaniem zadań IOD. Przede wszystkim **nie można powierzać inspektorowi wykonywania obowiązków administratora** – gdyż rolą inspektora jest ocena realizacji tych obowiązków pod kątem ich zgodności z przepisami powszechnie obowiązującymi oraz regulacjami wewnętrznymi administratora. W takim przypadku więc IOD kontrolowałby sam siebie. Warto przy tym podkreślić, że IOD **nie może określać celów i sposobów przetwarzania danych** – decyzja w tych kwestiach należy do administratora. **IOD nie może być też pełnomocnikiem administratora przed organem nadzorczym lub sądem.**

W wyroku z 9 lutego 2023 r. w sprawie C-453/21 X-FAB Dresden (pkt 41)
TSUE wskazał, że w świetle znaczenia wyrażenia „konflikt interesów" w języku potocznym, należy uznać, że zgodnie z celem realizowanym przez art. 38 ust. 6 RODO nie można powierzyć osobie będącej IOD wykonywania zadań lub obowiązków, które mogłyby zaszkodzić pełnieniu funkcji, które wykonuje jako IOD, a tym samym negatywnie wpłynąć na zapewnienie skuteczności przepisów RODO.

– ***Ocena zaistnienia konfliktu interesów*** *powinna być dokonywania indywidualnie i z uwzględnieniem konkretnych okoliczności. Należy to badać* ***zarówno przed wyznaczeniem Inspektora, jak i w trakcie pełnienia przez niego funkcji***, ***ponieważ przyczyny zaistnienia takiego konfliktu mogą następować w późniejszym czasie*** *(np. nałożenie dodatkowego zadania). Sam inspektor też powinien odpowiednio wcześniej sygnalizować administratorowi ryzyko wystąpienia takiego konfliktu, by możliwe było odpowiednio wczesne jemu zapobieganie. Gdy inspektor jest niezależny i wyposażony w odpowiednie uprawnienia, jest w stanie skutecznie realizować swoje obowiązki w zakresie monitorowania przestrzegania przepisów przez administratora i wspierania go doradztwem i opiniami w sytuacjach problemowych wymagających fachowej oceny* – podkreśliła Monika Kurzajewska.

Art. 57 ust. 1 lit. a RODO zobowiązuje Prezesa UODO do monitorowania i egzekwowania przepisów RODO, w tym tych dotyczących IOD i jego niezależności. Prezes UODO może więc np**. nakazać wyznaczenie inspektora**, bądź też **skorzystać z innych swoich uprawień**, gdy **gwarancje dotyczące IOD nie są przestrzegane** (np. nie podlega on bezpośrednio najwyższemu kierownictwu). Prezes UODO w swoich decyzjach reagował na naruszenia niezależności IOD, m.in. kiedy administrator:
1. nie zapewnił bezpośredniej podległości IOD pod najwyższe kierownictwo (decyzja z 18 grudnia 2024 r DKN.5112.14.2022);
2. zobowiązywał IOD do nadawania upoważnień personelowi w zakresie przetwarzania danych osobowych (decyzja z 22 września 2020 r. ZWAD.405.31.331.2019);
3. nie zapewnił, aby IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (decyzje z: 2 kwietnia 2025 r. DKN.5110.14.2022, 23 czerwca 2025 r. DKN.5130.4179.2020);
4. nie zapewnił zasobów niezbędnych do utrzymania jego wiedzy fachowej (decyzja z 2 kwietnia 2025 r.DKN.5110.14.2022);
5. nie zapewnił, aby w związku z wykonywaniem swoich zadań IOD nie otrzymywał instrukcji dotyczących ich wykonywania oraz nie był odwoływany i karany za wykonywanie tych zadań, (decyzja z 2 kwietnia 2025 r. DKN.5110.14.2022);
6. nie zapewnił, że na IOD nie będą nakładane zadania mogące powodować konflikt interesów: decyzje z: 2 kwietnia 2025 r. DKN.5110.14.2022; 2 kwietnia 2025 r. DKN.5110.16.2022, 12 września 2025 r. DKN.5131.7.2025, 2 stycznia 2026 r. DKN.5131.4.2025);
7. pełnienie funkcji IOD powierzył osobie zajmującej stanowisko prezesa zarządu w strukturze organizacyjnej podmiotu (decyzja z 12 września 2025 r. DKN.5131.7.2025).

Zadania Inspektora – audyt, edukacja i pośrednictwo

Zadania IOD polegają na monitorowaniu działań i decyzji podejmowanych przez administratorów i podmioty przetwarzające dane (**rola audytorska**), informowaniu, szkoleniu, oraz doradzaniu, w tym w zakresie oceny skutków dla ochrony danych (**rola edukacyjno-doradcza**) oraz **pośredniczeniu w kontaktach między administratorem a organem nadzorczym lub osobami, których dane dotyczą**.

IOD odgrywa ważną rolę w przypadku naruszenia ochrony danych osobowych. Powinien być o nich **niezwłocznie informowany, by móc monitorować obsługę przez administratora takich incydentów**. Pamiętać jednak należy, że **nie może działać w imieniu administratora,** np. zgłaszając naruszenie do UODO czy zawiadamiając o naruszeniu osoby, których dane dotyczą. Nie może również w imieniu administratora podejmować zobowiązań co do bezpieczeństwa przetwarzania, ani dokumentować naruszeń ochrony danych.

Sposoby na zapewnienie przestrzegania przepisów UODO w odniesieniu do IOD

Administrator lub podmiot przetwarzający musi zapewnić i móc wykazać, że przetwarzanie danych osobowych jest wykonywane zgodnie z przepisami określonymi w RODO. Zgodnie zaś z art. 83 ust. 4 RODO administrator i podmiot przetwarzający odpowiadają za naruszenie obowiązków określonych w art. 37–39 RODO (wyznaczenia IOD, w tym dokonania wyboru IOD o odpowiednich kwalifikacjach zawodowych, zapewnienia IOD gwarancji niezależności i udzielania mu wsparcia oraz zapewnienie prawidłowego wykonania zadań IOD).

Administrator lub podmiot przetwarzający powinien zatem przyjąć odpowiednie rozwiązania mające na celu zapewnienia IOD warunków do prawidłowego funkcjonowania i wykonywania zadań (np. odpowiednie regulacje w polityce ochrony danych, opracowanie polityki zarządzania konfliktem interesów zgodnie ze wskazówkami zawartymi w Wytycznych GR Art. 29 dot. IOD, opracowanie procedury dot. przypadków wymagających konsultacji z IOD konsultacji z IOD czy też lista 27 pytań jako lista kontrolna odnosząca się do zagwarantowania IOD prawidłowego statusu i wykonywania zadań).

Inspektorzy mogą liczyć na wsparcie Prezesa UODO

Ponadto IOD ma prawo zwrócić się do organu nadzorczego o indywidulne konsultacje odnoszące się do problematycznych zagadnień związanych z przetwarzaniem danych osobowych oraz z wykonywaniem swojej funkcji. Ta forma wsparcia IOD przez UODO jest szczególnie istotna dla ciągłego i systematycznego doskonalenia systemu ochrony danych osobowych.

Z kolei administrator powinien konsultować problematyczne zagadnienia dotyczące ochrony danych przede wszystkim ze swoim IOD. Doświadczenia UODO w tym względzie pokazują, że czasami jest jednak inaczej.

– *Często bowiem dostajemy pytania od administratorów, którzy – mimo że posiadają wyznaczonego inspektora – nie konsultowali z nim swoich wątpliwości czy możliwych rozwiązań danego problemu. Jest to wbrew obowiązkowi włączania IOD w sprawy przetwarzania danych* – wskazała ekspertka.

Monika Kurzajewska, główny specjalista w Wydziale Współpracy z IOD. Na podstawie wystąpienia podczas spotkania z IOD w ramach akcji „UODO rusza w kraj" w Suwałkach.

10 PRACOWNICY UODO

PRZYDATNE LINKI:

– na stronie internetowej UODO: – zamieszczone są materiały dotyczące wyznaczenia i statusu IOD,

– Podsumowanie spotkania w UODO „Niezależność IOD musi być standardem”,

– 27 pytań pozwalających zweryfikować przestrzeganie przepisów dotyczących IOD,

– Sprawozdanie EROD z badań CEF,

– Portal orzeczeń UODO.

URZĄD OCHRONY DANYCH OSOBOWYCH

Decydując się na przetwarzanie danych osobowych stajesz się administratorem. Oznacza to, że musisz znać i respektować prawa osoby, której dane dotyczą.

Osoba, której dane dotyczą:

MA PRAWO wiedzieć, co będzie się działo z jej danymi

Realizując obowiązek informacyjny, musisz wskazać na jakiej podstawie i po co przetwarzane będą jej dane osobowe, jak długo będziesz je przechowywał, oraz podać dane kontaktowe inspektora ochrony danych (IOD), jeśli go wyznaczyłeś. Wszelkie przekazywane przez Ciebie informacje związane z przetwarzaniem danych powinny być sformułowane jasnym, prostym i zrozumiałym językiem, dla osoby, której dane przetwarzasz.

MA PRAWO wiedzieć, jakie prawa daje jej RODO

Jako administrator masz obowiązek wskazać osobie, której dane dotyczą, jakie prawa daje jej RODO. A ma prawo m.in. do: dostępu do swoich danych, ich sprostowania, usunięcia, ograniczenia przetwarzania, przenoszenia, wniesienia sprzeciwu oraz do tego, by być poinformowanym o zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu.

MA PRAWO wycofać zgodę

Jeśli podstawą przetwarzania danych była wyrażona – świadomie i dobrowolnie – zgoda, osoba, która jej udzieliła ma prawo w dowolnym momencie ją wycofać i nie może to rodzić dla niej żadnych negatywnych konsekwencji (np. podwyższenia opłaty za usługi).

Pamiętaj, że cofnięcie zgody powinno być równie łatwe jak jej udzielenie.

MA PRAWO do informacji o naruszeniu ochrony jej danych

Wyciek danych, ich zagubienie czy udostępnienie osobom niepowołanym – to się zdarza. Jeżeli jednak naruszenie ochrony danych osobowych skutkuje ryzykiem naruszenia praw lub wolności osoby, której dane dotyczą, masz obowiązek ją o tym poinformować. Niezmiernie istotną kwestią w tym przypadku jest czas reakcji, tj. jak najszybsze zawiadomienie o naruszeniu osób, których dane dotyczą.

MA PRAWO do wniesienia sprzeciwu wobec marketingu

Osoba, której dane są wykorzystywane w celach marketingowych, a więc do przedstawiania jej oferty towarów czy usług, w dowolnym momencie może się temu sprzeciwić. Jeżeli to zrobi, nie wolno już wykorzystywać jej danych do takich celów.

PAMIĘTAJ!

Praw tych nie można ograniczyć zapisami regulaminu ani umowy.
Jako administrator masz obowiązek je znać, respektować i umożliwiać ich realizację.

URZĄD OCHRONY DANYCH OSOBOWYCH

Prezes UODO zaprasza na wydarzenie

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”.

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

Termin: **24 marca 2026 r.**

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

Formuła: **online**

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.

WEBINARIUM

Analiza ryzyka

w sposób zgodny z zasadą rozliczalności

18 dobrych praktyk*

Wtorek, 14 kwietnia 2026r.
10.00 - 14.00
Przerwy przewidziane o godz.:
11.15-11.30
12.45-13.00

SŁOWO WSTĘPU
Mirosław Wróblewski, *Prezes Urzędu Ochrony Danych Osobowych*

WEBINARIUM POPROWADZĄ:

dr Mirosław Gumularz
Przewodniczący Społecznego Zespołu Ekspertów przy Prezesie UODO

Bartłomiej Kowalski
Starszy Specjalista, Departament Kontroli i Naruszeń w UODO

Tomasz Izydorczyk
Społeczny Zespół Ekspertów przy Prezesie UODO

*Lista dobrych praktyk

1. Stawiaj prawa i wolności człowieka w centrum analizy ryzyka
2. Odwołuj się do wymogów i wskazówek zawartych w RODO
3. Opieraj analizę ryzyka na faktach i dowodach, a nie na intuicji
4. Dokumentuj źródła ocen i przyjętych założeń
5. Traktuj analizę ryzyka jako proces ciągły, a nie jednorazowe działanie
6. Wersjonuj analizy ryzyka i dokumentuj istotne zmiany w ich treści
7. Opisuj przetwarzanie w sposób kompletny, konkretny i zgodny z realiami
8. Analizuj cały cykl życia danych – od pozyskania do usunięcia
9. Uwzględniaj wszystkie zasoby wspierające proces, którego dotyczy analiza ryzyka
10. Nie ograniczaj analizy ryzyka do obszaru bezpieczeństwa danych (poufności, integralności i dostępności)
11. Zwróć uwagę na mniej oczywiste, pośrednie i długofalowe skutki przetwarzania dla osób fizycznych
12. Uwzględniaj „stan wiedzy technicznej" oraz „koszt wdrażania" przy doborze środków ochrony danych
13. Monitoruj wdrażanie zaplanowanych środków ochrony danych
14. Dokumentuj regularne testowanie skuteczności stosowanych zabezpieczeń
15. Jasno określ role i odpowiedzialność w procesie analizy ryzyka
16. Zapewnij realny udział inspektora ochrony danych w procesie oceny ryzyka
17. Traktuj zatwierdzenie analizy ryzyka jako świadomą i udokumentowaną decyzję zarządczą
18. Dokumentuj i uzasadniaj decyzje o odstąpieniu od dalszych działań związanych z zarządzaniem ryzykiem

URZĄD OCHRONY DANYCH OSOBOWYCH

Konferencja „Projektowanie ochrony danych w zamówieniach publicznych. Wyzwania w świetle rozwoju nowych technologii”

Termin: **17 kwietnia 2026 r.**

Organizatorzy: **Prezes Urzędu Ochrony Danych Osobowych, Prezes Urzędu Zamówień Publicznych**

Formuła: **online**

Celem wydarzenia będzie omówienie kluczowych wyzwań związanych z przetwarzaniem danych osobowych oraz informacji objętych innymi tajemnicami ustawowo chronionymi w obszarze zamówień publicznych, ze szczególnym uwzględnieniem zasad odpowiedzialności w obliczu rozwoju technologii XXI wieku. Zamówienia publiczne stanowią jeden z najważniejszych instrumentów realizacji polityk publicznych. Jednocześnie wiążą się z przetwarzaniem ogromnej liczby danych, co nakłada na zamawiających i wykonawców szczególne obowiązki wynikające z przepisów prawa. Prawidłowe pogodzenie wymogów prawa zamówień publicznych, ochrony danych osobowych oraz ustawy o dostępie do informacji publicznej, jest dziś nie tylko obowiązkiem prawnym, ale także elementem budowania zaufania obywateli i odpowiedzialnego państwa.

Wydarzenie będzie stanowić forum wymiany doświadczeń i dobrych praktyk pomiędzy ekspertami z zakresu prawa zamówień publicznych, ochrony danych osobowych oraz praktykami administracji publicznej, którzy porozmawiają na tematy związane z odpowiedzialnością stron postępowania o udzielenie zamówienia publicznego w świetle obowiązujących przepisów prawa, praktycznymi aspektami zabezpieczania danych w dokumentacji oraz realizacją umów.

URZĄD OCHRONY DANYCH OSOBOWYCH

Konferencja „Europejskie Ramy Cyfrowej Tożsamości (eIDAS2) w praktyce. Cyfrowa tożsamość i weryfikacja wieku w służbie ochrony dzieci i młodzieży”

Termin: **28 maja 2026 r.**

Organizatorzy: **Prezes Urzędu Ochrony Danych Osobowych, Społeczny Zespół Ekspertów przy Prezesie UODO**

Formuła: **hybrydowa**

Celem wydarzenia jest pogłębiona dyskusja na temat roli cyfrowej tożsamości oraz mechanizmów weryfikacji wieku w zwiększaniu bezpieczeństwa dzieci i młodzieży w środowisku cyfrowym. Podczas konferencji zagadnienie zostanie przedstawione z kilku perspektyw: prawnej, technologicznej oraz społecznej, aby kompleksowo pokazać wyzwania i możliwości związane z wdrażaniem tych rozwiązań.

W programie przewidziano wystąpienia ekspertów oraz panelowe dyskusje dotyczące m.in. ram regulacyjnych, dostępnych technologii weryfikacji wieku, praktycznych aspektów implementacji oraz wpływu tych rozwiązań na użytkowników. Istotnym elementem konferencji będzie również prezentacja doświadczeń regulatorów i instytucji publicznych z wybranych państw, które już wdrażają lub testują podobne mechanizmy.
Konferencja ma stworzyć przestrzeń do wymiany wiedzy, doświadczeń i dobrych praktyk pomiędzy przedstawicielami administracji publicznej, regulatorów, sektora technologicznego, środowiska naukowego oraz organizacji społecznych.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl