URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 03/26

www.uodo.gov.pl

SPIS TREŚCI

SPIS TREŚCI

Szanowni Państwo,

jedną z istotnych kwestii, którą zajmował się Urząd Ochrony Danych Osobowych w marcu, jest sprawa retencji danych osobowych przez polskie firmy telekomunikacyjne. Prawo telekomunikacji elektronicznej nakłada na operatorów obowiązek przechowywania ogromnej ilości danych na potrzeby policji i służb. Operatorzy muszą przechowywać je przez 12 miesięcy – niezależnie od tego czy użytkownicy są o cokolwiek podejrzewani. Takie rozwiązanie stoi w sprzeczności ze standardami UE, zgodnie z którymi dane można zbierać i przechowywać tylko w uzasadnionych konkretną sytuacją przypadkach.

Trybunał Sprawiedliwości UE wielokrotnie podkreślał, że gromadzenie danych przez operatorów telekomunikacyjnych może być dopuszczalne jedynie w zakresie ściśle niezbędnym i proporcjonalnym – np. w celu zwalczania poważnej przestępczości lub ochrony bezpieczeństwa państwa. Z kolei Europejski Trybunał Praw Człowieka w wyroku z 28 czerwca 2024 r. stwierdził, że polskie przepisy dotyczące kontroli operacyjnej i dostępu do danych komunikacyjnych nie zapewniają wystarczających gwarancji ochrony prawa do prywatności. Z uwagi na orzeczenia TSUE i ETPC dotyczące tego zagadnienia skierowałem już wcześniej do rządu wystąpienia wskazujące na konieczność zmiany polskich przepisów.

W marcu przedstawiłem Sądowi Okręgowemu, zgodnie z ustawą o ochronie danych osobowych, istotny pogląd w sprawie dotyczącej obywateli, którzy wnieśli, by ich dane były przetwarzane przez firmy telekomunikacyjne zgodnie z prawem. Istotne poglądy Prezesa UODO to ekspertyzy, które mogą sądom pomóc rozstrzygnąć te sprawy. W stanowisku skierowanym do sądu zwróciłem szczególną uwagę na brak zgodności krajowych regulacji dotyczących retencji danych telekomunikacyjnych z Konstytucją RP, Europejską Konwencją Praw Człowieka oraz prawem UE.

Sądy administracyjne w sprawie decyzji Prezesa UODO

W marcu sądy administracyjne potwierdziły decyzje Prezesa UODO w kilku ważnych sprawach, w jednej – decyzja została uchylona. Ta ostatnia to bardzo poważna sprawa – dotycząca tzw. wyborów korespondencyjnych, które miały odbyć się w 2020 r. Prezes UODO nałożył na Pocztę Polską karę za to, że przetwarzała dane 30 mln polskich wyborców pobrane z bazy PESEL bez podstawy prawnej. Ustawa, która by na to zezwoliła, nie weszła wtedy w życie, a Poczta działała tylko na podstawie decyzji premiera, która nie miała podstawy ustawowej. Potwierdził to potem NSA uznając tę decyzję za nieważną.

Badając sprawę Poczty WSA uznał jednak, że spółka była zobowiązana wykonać decyzję premiera, gdyż w owym czasie (w kwietniu 2020 r.) nie została ona jeszcze zakwestionowana, a Poczta nie mogła oceniać ważności decyzji premiera. W sprawie tej rozważamy złożenie skargi kasacyjnej do NSA. W grę wchodzi bezpieczeństwo danych 30 mln polskich obywateli.

Inaczej wygląda sprawa ujawnienia przez Ministra Zdrowia danych lekarzy. Tu WSA nakazał Prezesowi UODO ponownie zająć się tą sprawą, a to dlatego, że toczy się tu także sprawa karna i należy uwzględnić wyrok karny zapadły dwa lata po wydaniu decyzji organu nadzorczego.

Sprawa miała swój początek w grudniu 2023 r., gdy Prezes UODO nałożył karę na Ministra Zdrowia za ujawnienie danych lekarza, w tym dotyczących zdrowia. Po przeprowadzeniu postępowania administracyjnego Prezes UODO stwierdził, że dane zostały ujawnione bez podstawy prawnej. WSA wskazał jednak w marcu, że pełniący wówczas funkcję Ministra Zdrowia Adam Niedzielski został prawomocnie skazany we wrześniu 2025 r. za przekroczenie uprawnień właśnie poprzez ujawnienie danych lekarza. Zdaniem WSA wyrok w sprawie karnej wpływa na postrzeganie stanu faktycznego opisanego w decyzji Prezesa UODO z grudnia 2023 r. Trzeba więc ją uchylić, by sprawę jeszcze raz ocenić.

WSA podtrzymał decyzję Prezesa UODO w sprawie kary dla Radia Szczecin. Sąd oddalił skargę radia. Nałożyłem na stację karę za to, że nie miała procedur chroniących bohaterów materiałów prasowych przed naruszeniem ich prywatności. To uchybienie mogło przyczynić się w 2022 r. do ujawnienia danych młodej osoby będącej ofiarą bardzo poważnego przestępstwa. Niestety dane osobowe zawarte w materiale prasowym w sposób jednoznaczny pozwalały na jej zidentyfikowanie. Następstwem całej sytuacji było samobójstwo nastolatka.

NSA podtrzymał z kolei decyzję Prezesa UODO o karze na Santander Bank Polska S.A. Sąd przyznał rację Prezesowi UODO, że przez zaniechanie właściwego powiadomienia osób o naruszeniu ochrony ich danych osobowych bank naruszył przepisy RODO. Incydent, który Santander Bank Polska S.A. zgłosił do UODO, polegał na tym, iż byłemu pracownikowi nie odebrano dostępu do Platformy Usług Elektronicznych ZUS. W efekcie, nawet po zakończeniu pracy w banku, miał on dostęp do danych innych pracowników z PUE ZUS na profilu płatnika firmy. Co więcej, pięciokrotnie logował się on do platformy po wygaśnięciu umowy o pracę. Bank tymczasem uznał, że ryzyko incydentu nie było wysokie i nie powiadomił o tym osób, których dane dotyczyły.

NSA podzielił też stanowisko Prezesa UODO uchylając decyzję WSA sprawie naruszenia przepisów o ochronie danych osobowych przez Fortum Marketing and Sales S.A. i Pika Sp. z o.o. NSA zgodził się z PUODO, że za proces przetwarzania danych osobowych odpowiada administrator oraz podmiot przetwarzający.

Sprawa sięga kwietnia 2020 r., kiedy Fortum zgłosiło organowi nadzorczemu naruszenie ochrony danych osobowych. Naruszenie było związane z wprowadzeniem zmian w cyfrowym archiwum.

W odpowiedzi na sygnalizowane przez Fortum problemy z wydajnością systemu podmiot przetwarzający – spółka Pika –utworzyła dodatkową bazę danych i zasiliła je danymi klientów administratora. Jednak nowo utworzoną bazę udostępniono w sposób nieprawidłowy, co umożliwiło osobom nieuprawnionym dostęp do danych klientów oraz ich kopiowanie. Sprawa trafiła do ponownego rozpatrzenia.

W marcu wydałem też kilka istotnych decyzji administracyjnych

Ukarałem Komitet wyborczy Karola Nawrockiego za naruszenie przepisów RODO przez publiczne udostępnienie danych osobowych. Przedstawiciele Komitetu Wyborczego pokazali niezanonimizowane dokumenty dotyczące transakcji nabycia nieruchomości. Ujawnili w ten sposób dane nie tylko właściciela mieszkania, ale i członków jego rodziny oraz małżonki kandydata na prezydenta. Tymczasem dokumenty można było pokazać nie naruszając prawa do prywatności osób nie pełniących funkcji publicznych.

Nałożyłem administracyjną karę pieniężną na Glovo w wysokości blisko 6 mln złotych za kopiowanie dokumentów bez podstawy prawnej. Spółka pozyskiwała skany oraz zdjęcia dowodów tożsamości użytkowników aplikacji mobilnej, służącej m.in. do zamawiania posiłków. Sprawa była następstwem kontroli obejmującej sposób przetwarzania danych użytkowników aplikacji mobilnej „Glovo – dostawa jedzenie i inne". W decyzji wskazałem, że kopiowanie lub utrwalanie dokumentów tożsamości powinno być stosowane wyłącznie w wyjątkowych przypadkach przez konkretne i upoważnione ustawowo podmioty oraz w sytuacjach wyraźnie przewidzianych przepisami prawa.

W tym miesiącu podjęliśmy też kilka ważnych kwestii prawnych:

- Sprawę kamer nasobnych kontrolorów biletów. Zwróciłem się do Ministra Infrastruktury o doprowadzenie do skutecznego stosowania przepisów o ochronie danych osobowych, bo monitoring za pomocą urządzeń rejestrujących dźwięk lub obraz jest inwazyjną formą przetwarzania danych osobowych i stwarza zagrożenie w zakresie praw i wolności osób fizycznych.
- Sprawę badań przesiewowych. RODO daje podstawę prawną do kierowania zaproszeń na badania przesiewowe – takie wyjaśnienie przekazałem prof. Mariuszowi Bidzińskiemu z Narodowego Instytutu Onkologii im. Marii Skłodowskiej-Curie. Dane szczególnych kategorii mogą być przetwarzane bez zgody pacjenta, jeśli jest to niezbędne do celów profilaktyki, diagnozy lub organizacji systemu opieki zdrowotnej. Przetwarzanie takich danych musi jednak odbywać się pod nadzorem osób zobowiązanych do zachowania tajemnicy zawodowej. UODO stale wzmacnia poziom ochrona danych osobowych poprzez edukację i wzrost świadomości społecznej.

Przedstawiciele Urzędu biorą udział z licznych spotkaniach i konferencjach, na który omawiają zagadnienia związane z tą dziedziną. Oto przykłady:

- Przetwarzaniem danych na potrzeby targetowania reklamy politycznej omawialiśmy na spotkaniu w IAB Polska
- O tym, jak chronić dzieci na platformach cyfrowych mówiłem podczas Forum Cyfrowego Obywatelstwa
- O ochronie danych osobowych w epoce deepfake'ów, sztucznej inteligencji i , rozpowszechnianie wizerunku małoletnich mówiłem w ramach wydarzenia „Dzień Ochrony Danych Osobowych z Vizją".
- Problem bezpieczeństwa seniorów w kontekście danych wrażliwych poruszyliśmy na posiedzeniu sejmowej Komisji Polityki Senioralnej.
- Praktycznym interakcjom między RODO a Aktem w usługach cyfrowych (DSA) poświęcone było moje wystąpienie na konferencji w Brukseli „Międzyregulacyjne oddziaływanie i współpraca w UE: perspektywa ochrony danych osobowych" (ang. „cross-regulatory cooperation in the EU")
- Zorganizowaliśmy szkolenie dla medyków z warszawskiej Okręgowej Izby Lekarskiej pt. „Sektor medyczny – współczesne wyzwania dla ochrony danych osobowych".
- W Monasterze Zwiastowania Najświętszej Maryi Panny w Supraślu odbyło się szkolenie dotyczące ochrony danych osobowych oraz bezpieczeństwa dzieci i młodzieży w internecie.
- Zorganizowaliśmy, wspólnie z Wydziałem Prawa i Administracji Uniwersytetu Warszawskiego oraz Instytutem Nauk Prawnych Polskiej Akademii Nauk, międzynarodową konferencję „Europejska przestrzeń danych dotyczących zdrowia – wtórne przetwarzanie danych osobowych oraz prawa osób fizycznych".

Jak zwykle braliśmy udział w pracach Europejskiej Rady Ochrony Danych (EROD), która m.in. zaczyna koordynować egzekwowanie prawa w zakresie przejrzystości i informacji wynikających z RODO. Rozporządzenie gwarantuje, że osoby fizyczne są informowane o przetwarzaniu ich danych (zgodnie z art. 12, 13 i 14). Prawo do informacji jest podstawowym elementem przejrzystości oraz zapewnia osobom fizycznym większą kontrolę nad ich danymi.

Warto też zauważyć, że EROD przyjęła sprawozdanie dotyczące działań w ramach Skoordynowanego Egzekwowania Prawa (CEF) dotyczących prawa do usunięcia danych (art. 17 RODO). Jest to jedno z najczęściej wykorzystywanych praw wynikających z RODO, na które organy nadzorcze często otrzymują skargi od osób prywatnych.

Do zapisana w kalendarzu:

Serdecznie zapraszam 17 kwietnia na konferencję pt. „Projektowanie ochrony danych w zamówieniach publicznych. Wyzwania w świetle rozwoju nowych technologii”.

Polecam też gorąco udział w webinarium poświęconym analizie ryzyka. Podczas spotkania online omówione zostaną punkty analizy opisane w styczniowym numerze Biuletynu UODO w materiale „Jak przeprowadzić analizę ryzyka zgodnie z zasadą rozliczalności?”. Wydarzenie odbędzie się 9 kwietnia 2026 r.

Polecam śledzenie strony internetowej UODO, gdzie dokładnie opisujemy na bieżąco nasze działania.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W tym numerze Biuletynu chcieliśmy przede wszystkim zająć się tematem ochrony wizerunku, danych osobowych i bezpieczeństwa dzieci w internecie. Poruszamy go w wywiadzie z członkiem Społecznego Zespołu Ekspertów przy Prezesie UODO – Tomaszem Izydorczykiem. W rozmowie przeczytacie m.in. o zagadnieniu weryfikacji wieku i tym, jak ją pogodzić z ochroną prywatności internautów. Rozmawialiśmy też o konieczności ochrony małoletnich podczas ich korzystania z gier on-line. Nie zdradzę zbyt dużo z rozmowy, ujawniając, że mój rozmówca bardziej niż na kolejne regulacje kładzie akcent na edukację – zarówno dzieci, jak i rodziców.

Kwestii ochrony wizerunku najmłodszych w internecie – w kontekście coraz częstszego używania go do promocji przez szkoły, przedszkola i podobne placówki – poświęciliśmy także obszerny tekst w dziale „Działalność UODO". Również tam przeczytacie komentarze dwojga innych członków Społecznego Zespołu Ekspertów przy Prezesie UODO.

Ochrony danych dzieci dotyczy też jeden z tekstów z działu poświęconego nowym technologiom – tym razem chodzi o konieczność zmiany przepisów tak, by możliwa była aktualizacja dokumentacji medycznej dziecka po pełnej adopcji (co wiąże się także ze zmianą numeru PESEL). W dziale tym poruszono również kwestię przekazywania danych medycznych przez NFZ w ramach programów pilotażowych oraz informacji o mandatach wystawionych przez straż gminną – do komisji przeciwdziałania problemom alkoholowym.

W dziale „Naruszenia i kontrole" także poruszamy temat związany po części z nowymi technologiami: omawiamy naruszenia ochrony danych osobowych w świetle ustawy o Krajowym Systemie Cyberbezpieczeństwa.

Jak zwykle dużo się dzieje w Europejskiej Radzie Ochrony Danych. Przede wszystkim EROD przedstawiła swój program prac na ten i następny rok, a także opinię dotyczącą zmian prawnych planowanych w ramach tzw. Digital Omnibus. Rada zwróciła też uwagę na problemy związane z pełną realizacją prawa do usunięcia danych. Niezmiennie w polu zainteresowań EROD pozostaje przetwarzanie danych przez systemy AI – czy to w kontekście generowania obrazów, czy regulacji prawnych dotyczących sztucznej inteligencji (kwestię omówiono podczas konferencji Bird and Bird w Budapeszcie).

W dziale współpracy międzynarodowej przedstawiamy relację z wizyty delegacji UODO w Helsinkach. Kilkudniowa wymiana doświadczeń z fińskimi urzędami dotyczyła przede wszystkim kwestii wdrażania Aktu o zarządzaniu danymi oraz praktycznych aspektów działania systemu pośrednictwa danych. Wiedza ta będzie bardzo przydatna przy implementacji DGA w Polsce, jako że Finlandia to pierwszy kraj Unii, który wdrożył u siebie tę dyrektywę. W dziale dotyczącym strefy Schengen prezentujemy zaś pierwszą część tekstu dotyczącego systemowych problemów z interpretacją Dyrektywy 2016/680 – jego kontynuację planujemy w numerze kwietniowym.

Wątek międzynarodowy pojawia się też w dziale „Pracownicy UODO", który dotyczy kodeksów postępowania. Polska znajduje się pod tym względem w unijnej czołówce i jest jedynym krajem w regionie, w którym w ogóle takie kodeksy zaakceptowano. W tekście wskazujemy również, jakie problemy wiążą się z przygotowywaniem i zatwierdzaniem takich kodeksów.

Gorąco polecam dział Edukacja, w którym wracamy do ochrony dzieci przed szkodliwymi i uzależniającymi mechanizmami w grach internetowych – tym razem w kontekście webinarium dla nauczycieli i dyrektorów w ramach programu „Twoje dane – Twoja sprawa".

Zapraszamy do lektury!

Karol Witowski
Dyrektor Departamentu Komunikacji Społecznej
Rzecznik Prasowy UODO

NIE MA CZEGOŚ TAKIEGO JAK ANONIMOWOŚĆ W SIECI – MÓWI TOMASZ IZYDORCZYK

Jeśli ktoś korzysta z internetu, zawsze zostawia za sobą cyfrowe ślady. Od pełnych danych osobowych np. w trakcie zakupów on-line, po pliki cookies, profile użytkownika czy metadane związane z urządzeniami, które ten dostęp do sieci i usług zapewniły – mówi Tomasz Izydorczyk, członek Społecznego Zespołu Ekspertów przy Prezesie UODO.

Jak w ostatnich latach zmieniło się podejście administratorów do ochrony danych?

Podejście to zmieniło się przez ostatnie lata i nadal ewoluuje. W początkowej fazie, w latach 2016–2020, polegało ono na organizacji projektu, wdrożeniu i przygotowaniu do stosowania przepisów. Z czasem administratorzy musieli zrozumieć, że RODO to nie zestaw polityk do odłożenia na półkę, tylko procesy – tak samo jak księgowość, płace, sprzedaż czy zamówienia. Ochrona danych musiała wejść w normalne procesy operacyjno-administracyjne każdej organizacji. Oczywiście, wiele podmiotów ma jeszcze dużo elementów do wdrożenia czy udoskonalenia, jednak są i tacy administratorzy, którzy zintegrowali swoje procesy ochrony danych w normalnej codziennej pracy operacyjnej.

Nie mam żadnych statystyk, aby podeprzeć swoje twierdzenia, ale aktualnie obserwuję kilkadziesiąt dużych i średnich podmiotów, w których funkcjonujący system ochrony danych naturalnie się rozwija, łączy i przeplata z innymi działaniami, których celem jest zapewnienie zgodności z przepisami dotyczącymi nowych technologii. Mam tu na myśli (w zależności od sektora i branży) wymagania m.in. dotyczące cyberbezpieczeństwa czy sztucznej inteligencji.

Skoro RODO jest silnie związane z technologią, to jej rozwój i pojawiające się nowe technologiczne akty prawne naturalnie łączą się z przepisami o ochronie danych. Uważam też, że postawienie przez UODO wyraźnych granic działalności inspektorów ochrony danych oraz mnogość nowych regulacji w dziedzinie gospodarki cyfrowej opartej na wiedzy sprawiła, że administratorzy zaczynają dostrzegać i rozumieć potrzebę oddzielenia funkcji inspektora ochrony danych od funkcji wykonawczych, decyzyjnych i wdrożeniowych, które zapewnią szeroko rozumianą zgodność z takimi przepisami jak RODO, DSA, DGA, NIS2/KSC, AIA. Nawet jeśli przyjąć, że inspektor ochrony danych posiada wszechstronne i interdyscyplinarne kompetencje, to jednak samodzielnie nie udźwignie takiej liczby regulacji i wdrożeń. Administratorzy chyba zaczynają to rozumieć i budować swoje komórki, działy, departamenty i piony zgodności regulacyjnej.

1 ROZMOWA Z EKSPERTEM

Jakie znaczenie dla ochrony danych osobowych ma przyjęcie ustawy implementującej NIS2 w Polsce (ustawa o KSC)?

Tu także nie dysponuję statystykami, ale dzięki obserwacjom własnym oraz wielu koleżanek i kolegów – inspektorów ochrony danych – mogę przewidywać pewne zjawiska w ochronie danych i prywatności. Uważam, że NIS2 (znowelizowane przepisy Ustawy KSC) będzie miało dwa główne efekty z punktu widzenia ochrony danych. Po pierwsze, nastąpi pewnego rodzaju „odkurzenie" lub udoskonalenie procesów oceny ryzyka. Nic tak nie wymusza na organizacji przeglądu i aktualizacji polityk, procedur, analiz, jak zmiany w przepisach.

Medialna i branżowa dyskusja pomaga nam w zdobywaniu budżetów na wewnętrzne projekty, szkolenia, edukację czy zakup profesjonalnych usług lub systemów wsparcia zarządzania bezpieczeństwem informacji. Świadomość najwyższego kierownictwa z pewnością się poprawi, a co za tym idzie, większość personelu administratorów także będzie bardziej odpowiedzialnie podchodziła do szeroko rozumianego bezpieczeństwa danych. Po drugie, NIS2 może realnie wesprzeć ochronę danych osobowych w istotnym aspekcie – zachowania poufności, integralności i dostępności tych danych. Nic tak nie skupia uwagi na tej triadzie, jak właśnie systemy zarządzania bezpieczeństwem informacji, które są najistotniejszym elementem przepisów KSC.

W jednym z postów na LinkedIn pisał Pan o „końcu pseudo-anonimowości" w internecie. Czy faktycznie nowe regulacje, jak NIS2 czy DSA, sprawią, że platformy internetowe będą powszechnie weryfikować tożsamość użytkowników?

Może zacznę od wyjaśnienia, dlaczego w ogóle użyłem pojęcia „pseudo-anonimowość". Otóż uważam, że nie ma czegoś takiego jak anonimowość w sieci. Jeśli ktoś korzysta z internetu, zawsze zostawia za sobą cyfrowe ślady. Od pełnych danych osobowych np. w trakcie zakupów on-line, po pliki cookies, profile użytkownika czy metadane związane z urządzeniami, które ten dostęp do internetu i usług zapewniły.

To, co pozwala zidentyfikować konkretną osobę fizyczną, to czasami „okruchy" informacji, które przy odpowiednich umiejętnościach, chęciach, ale i zasobach czasowych czy finansowych dają możliwość wskazania konkretnego człowieka. Nie bez powodu w samej definicji danych osobowych w RODO zostało użyte pojęcie „możliwości identyfikacji" osoby fizycznej, a katalog informacji, które identyfikują konkretną osobę, pozostaje otwarty.

Internet staje się coraz bardziej niebezpieczną domeną funkcjonowania człowieka. Chyba wszyscy możemy się zgodzić z takim twierdzeniem. A skoro jakaś przestrzeń działań jednych ludzi staje się niebezpieczna dla innych, politycy, eksperci, a na końcu prawodawcy wprowadzają prawo, które ma chronić ludzi i określone wartości. Skoro tak łatwo można skrzywdzić drugiego człowieka on-line, społeczeństwa wprowadzają rozwiązania pomagające nie tylko zapobiegać, ale też wykrywać i karać sprawców tych niepożądanych działań.

1 ROZMOWA Z EKSPERTEM

Organy regulacyjne i organy ścigania nie mogą działać wobec „użytkownika cyfrowego”, tylko muszą ustalić personalia osoby fizycznej lub prawnej stojącej za konkretną aktywnością w internecie. Skoro jako społeczeństwo żądamy, aby platformy były bardziej bezpieczne dla nas, naszych transakcji, naszych pieniędzy czy naszych danych osobowych, a przede wszystkim dla słabszych grup społecznych, jak dzieci czy osoby starsze, administratorzy muszą zaostrzyć swoje działania wobec użytkowników platform.

I na czym ma polegać to zaostrzenie?

Jednym z wielu środków bezpieczeństwa, jakie serwisy internetowe mogą wdrożyć, to obniżenie anonimowości kont internetowych. To prowadzi wprost do zbierania większej ilości danych, aż po weryfikację wieku użytkowników. Skoro media społecznościowe mają być bezpieczne dla dzieci, platformy muszą wprowadzić weryfikację wieku. A skoro platformy sprzedaży on-line mają być bardziej bezpieczne dla osób kupujących w internecie, muszą prowadzić polityki KYC, KYB (Know Your Customer) i KYB (Know Your Business).

Dostawcy platform społecznościowych chyba także są zainteresowani samą weryfikacją wieku, bo to daje im jeszcze większy wgląd do tego, kim jesteśmy my – ich użytkownicy. Źródła OSINT, na podstawie danych publicznych dotyczących lobbingu i zeznań podatkowych, donoszą, że Meta tylko w USA wydała ponad 2 mld dolarów na lobbowanie przepisów wprowadzających obowiązek weryfikacji wieku w internecie. Oczywiście wszystkie te działania mają szczytny cel: bezpieczeństwo dzieci i innych użytkowników w sieci.

Czy można to pogodzić z prywatnością i bezpieczeństwem danych użytkowników? W zeszłym roku doszło do dużego wycieku danych z Discorda, wysłanych przy okazji weryfikacji tożsamości. Wówczas wielu komentatorów mówiło, że takich danych nie da się całkowicie zabezpieczyć i jest tylko kwestią czasu, aż wyciekną. Rzeczywiście tak jest?

Uważam, że można pogodzić prywatność i bezpieczeństwo danych użytkowników w internecie. Aby to nastąpiło, musimy zrobić tylko i aż trzy rzeczy. Każdy z nas powinien sam wyznaczyć swoją granicę prywatności – czyli jako świadomy użytkownik udostępniać tyle danych, ile uważa za właściwe, i wybierać takich dostawców usług cyfrowych, którym ufa. Druga sprawa – administratorzy muszą ustawić odpowiedni, a słowami RODO – adekwatny – poziom bezpieczeństwa klientów (użytkowników), który będzie odpowiadał temu społecznemu i indywidualnemu poczuciu prywatności.

I żeby te dwie rzeczy się wydarzyły, czyli: „świadomy użytkownik” i „bezpieczny administrator”, musi zaistnieć trzeci, równie ważny element: masowa edukacja zarówno w ramach systemu oświaty, jak i innych działań uświadamiających wszystkich zainteresowanych bezpieczną cyberprzestrzenią. W tak idealnie zbudowanym świecie tak głośne i duże wycieki danych nie będę miały większego wpływu na nas jako użytkowników sieci.

1 ROZMOWA Z EKSPERTEM

Każdy internauta będzie świadomie udostępniał informacje o sobie, a administratorzy będą wdrażać odpowiednie środki, aby nasze dane i prywatność odpowiednio zabezpieczyć.

Jak więc weryfikować tożsamość, by rodziło to jak najmniejsze zagrożenia dla prywatności? Jakie dane zbierać w tym celu i jak je zabezpieczać?

Istnieją przynajmniej cztery techniki weryfikowania tożsamości w taki sposób, aby rodziło to jak najmniejsze zagrożenia dla prywatności. Pierwszą z nich są dowody z wiedzą zerową (Zero-Knowledge Proofs). To metoda pozwalająca udowodnić, że dana informacja jest prawdziwa (np. użytkownik ma ukończone 18 lat) bez ujawniania konkretnych danych, np. daty urodzenia czy numeru PESEL.

Inną techniką jest weryfikacja atrybutowa (w odróżnieniu od „tożsamościowej"). Przykładowo, zamiast prosić użytkownika o skan dowodu osobistego, system pyta jedynie o konkretną cechę potrzebną – adekwatną do usługi (np. prawo jazdy, czyli uprawnienie, a nie adres zamieszkania).

Kolejnym sposobem jest zdecentralizowana identyfikacja (Decentralized Identity Self-Sovereign Identity). To technika, w której użytkownik przechowuje swoje dane w cyfrowym portfelu (np. mObywatel w polskim kontekście) i udostępnia tylko niezbędne klucze do ich potwierdzenia, zamiast kopiować dane na serwer firmy.

A ostania metoda weryfikacji, jaką polecam administratorom, to weryfikacja lokalna (Edge Verification). Biometria (odcisk palca, Face ID) powinna być przetwarzana wyłącznie na urządzeniu użytkownika, np. naszym smartfonie. Serwer usługodawcy otrzymuje jedynie informację „TAK/NIE", a nie wzorzec biometryczny. To nie są nowe techniki, ale wymagają przemyślanego wdrożenia. Co mamy w zamian? Checkbox potwierdzający, że użytkownik ma 18 lat albo zbieranie ogromnego zakresu danych na tak zwany „zapas", czyli z naruszeniem zarazy minimalizacji danych.

Wspomniany Discord ogłosił wprowadzenie podejścia „Teen-by-Design". Jeśli dobrze rozumiem, zakłada ono, że treści na platformie dostępne domyślnie będą odpowiednie dla nastolatków. A jeśli ktoś chce mieć dostęp do tych „nieodpowiednich", to musi sam się zweryfikować jako dorosły. Może tą drogą powinny iść wszystkie platformy, zamiast starać się wyłapać konta niepełnoletnich?

Trudno mi ocenić, w którym kierunku rozwiną się proponowane rozwiązania. Z jednej stromy mamy ogromne lobby powiązane z mediami społecznościowymi, które chce jak najwięcej zbierania danych – bo właśnie na naszych danych zarabiają największe pieniądze. Z drugiej strony mamy mniejszych administratorów, którzy nie chcą wdrażać skomplikowanych rozwiązań, które tylko utrudniają szybki i łatwy dostęp do ich usług. Jeszcze kilka lat temu zrozumiałbym wdrożenie podejścia „Teen-by-Design" na takiej platformie jak Discord.

1 ROZMOWA Z EKSPERTEM

Dziś Discord nie jest już tylko usługą dla dzieci i nie służy wyłącznie rozrywce. Stał się narzędziem budowania ogromnych społeczności internetowych także dla dorosłych. Jest jeszcze jedna sprawa z podejściem „Teen-by-Design" lub szeroko rozumianym bezpieczeństwem w internecie: a mianowicie cenzura i monitorowanie absolutnie wszystkiego. Pod płaszczykiem bezpieczeństwa zawsze były pokusy wprowadzania narzędzi inwigilacji. Tutaj musimy nieustannie poszukiwać złotego środka pomiędzy bezpieczeństwem jednych a prawami i wolnością innych.

Branża gier, zwłaszcza mobilnych i on-line, wydaje się rodzić zagrożenia dla małoletnich – korzysta z niej wiele dzieci i to często miejsce polowań dla przestępców seksualnych. Jak można walczyć z tymi zagrożeniami?

Znowu mam tylko jedną odpowiedź: edukacja zarówno dzieci, jak i rodziców. To przede wszystkim rodzice powinni wziąć pełną odpowiedzialność za to, co ich dzieci robią w internecie i jak z niego korzystają. Jeśli edukacja nic nie da, a rodzice nie będę odpowiednio nadzorować i edukować swoje dzieci, zostanie nam wprowadzenie prawa przerzucającego całą odpowiedzialność na platformy internetowe i dostawców usług. Jak wiemy z lektur George'a Orwella, może to się skończyć permanentną inwigilacją i monitorowaniem wszystkiego, co robimy w internecie.

Wiele gier ma mechaniki, które mają uzależniać użytkowników, wymuszać działania, zachęcać do wnoszenia opłat (mikropłatności) czy proponować mechanizmy hazardowe, dark patterns. Jednak gry to nie tylko samo zło. Jak można bronić się przed tymi mechanizmami i co mogą nam dać gry, poza rozrywką?

W tym miejscu chciałbym bardzo mocno podkreślić, że gry internetowe czy mobilne nie są złe same w sobie. Wręcz przeciwnie, mogą być nie tylko rozrywką, ale i wspaniałym uzupełnieniem podstawowej edukacji matematyki, geografii czy historii, a zaawansowane gry dla dorosłych uczą zarządzania logistyką, sterowania samolotem, pociągiem, dronem czy nawet strategii wojennej osadzonej w realnych zdarzeniach współczesnych czasów. W tym miejscu chciałbym się odwołać do wykładów i manifestów dr. Krzysztofa M. Maja z Akademii Górniczo-Hutniczej w Krakowie, polonisty uczącego młode pokolenie inżynierów, przyszłych twórców gier. To on właśnie piętnuje to, co jest złego w grach, czyli uzależniające i niebezpieczne mechaniki, oraz uczy, jak należy projektować gry.

O ile jest dużo gier dobrych i wspierających edukację oraz przyszłe kompetencje młodych ludzi, o tyle będą i te, które mają negatywny lub niebezpieczny wpływ na użytkowników. Jak walczyć z zagrożeniami w grach? Ponownie odpowiem: edukacja, edukacja i jeszcze raz edukacja. Jeśli nie zainwestujemy we właściwą edukację, w tym nie zaplanujemy odpowiednich budżetów dla organów regulacyjnych, przemysł gier z mechanikami uzależniającymi będzie niszczył kolejne pokolenia użytkowników.

1 ROZMOWA Z EKSPERTEM

A co z weryfikacją wieku? W grach i nie tylko. Wszyscy mamy świadomość, że to ważna i konieczna sprawa. Czy jest to realne, jak należy to zrobić, kto powinien być za to odpowiedzialny? Ostatnio pojawiły się głosy sugerujące, że powinno się to odbywać na poziomie systemu operacyjnego. Czy to dobry pomysł? No i co z ogromną ilością danych o użytkownikach? To dane osobowe, ale też dane o preferencjach i gustach, łakomy kąsek dla platform.

Zacznijmy od tego, że nie każda gra wymaga założenia konta użytkownika czy weryfikacji wieku. Projektanci i producenci mają swoje cele, które chce osiągnąć poprzez publikację konkretnego tytułu. Zazwyczaj platformy z grami dbają o odpowiednie oznaczenia wieku i opis gry. Uważam jednak, że to my – społeczeństwo i użytkownicy, powinnyśmy wymuszać poprzez nasze decyzje konsumencie, które gry są wartościowe, a które powinny być napiętnowane, aby zniknęły z rynku. Zachęcam rodziców do wspólnego grania ze swoimi dziećmi właśnie po to, aby lepiej zrozumieli i poznali gry, z których korzystają ich pociechy, oraz aby świadomie decydowali, w jakie powinny grać, a w jakie nie.

Uważam, że jeśli jako społeczeństwo zgodzimy się na weryfikację wieku na poziomie systemu operacyjnego komputera, przekroczymy pewną granicę, która będzie miała wpływ na naszą prywatność. Weźmy pod uwagę, że system operacyjny to nie tylko komputer osobisty czy telefon. W telewizorach czy samochodzie też są komputery z systemem operacyjnym. Wiemy z raportów Fundacji Mozilla, jak bardzo producenci IoT (Internetu Rzeczy, w tym samochodów) łakną naszych danych osobowych. Skoro telewizory i samochody mające systemy operacyjne też będą weryfikować wiek, to w jaki sposób powstrzymamy innych producentów urządzeń, jak lodówka, kuchenka, pralka, zmywarka, przed dostępem do informacji o nas i weryfikacji wieku użytkowników?

Przecież te urządzenia także są przeznaczone dla użytkowników w odpowiednim wieku. Jak daleko będziemy przesuwać granicę zbierania dużej ilości danych o nas – użytkownikach, żebyśmy odważyli się nazwać to inwigilacją? Ja nie twierdzę, że mamy nic nie robić, ale uważam, że rozwiązywania problemów wąskiej grupy użytkowników nie można wdrażać kosztem całej społeczności. Tym bardziej że, jak wskazałem wcześniej, istnieją techniki potwierdzania wieku bez zbędnego zbierania danych osobowych.

Na koniec chciałbym zapytać o mObywatela, potężne narzędzie cyfrowego państwa, z którego korzysta ponad 11 mln użytkowników. Jeszcze w tym roku do ekosystemu ma dołączyć Europejski Portfel Tożsamości Cyfrowej (EUDI Wallet), który umożliwi obywatelom bezpieczne potwierdzanie tożsamości oraz korzystanie z usług w całej Unii Europejskiej. Jak Pan to ocenia?

Brałem udział w projektach Komisji Europejskiej związanych z budową i testowaniem rozwiązań cyfrowych portfeli i rozproszonych rejestrów cyfrowych. Zdaję sobie sprawę z tego, że jednym z kluczowych czynników tego typu rozwiązań jest prostota interfejsu i łatwość korzystania.

1 ROZMOWA Z EKSPERTEM

Jako aktywny użytkownik mObywatela jestem bardzo zadowolony z jego funkcjonalności, w szczególności potwierdzania swojej tożsamości w załatwianiu codziennych spraw.

Jednak jako gorący zwolennik transparentności mam duże obawy o bezpieczeństwo i prywatność usługi mObywatel. Wielu ekspertów badających bezpieczeństwo tego typu aplikacji uważa, że nadal nie mamy dostępu do wszystkich informacji i całości dokumentacji, na podstawie których można byłoby zweryfikować działanie tej aplikacji pod kątem zabezpieczenia danych. Uważam, że nic tak nie poprawia jakości i bezpieczeństwa systemów jak możliwość transparentnej weryfikacji przez społeczeństwo i ekspertów niezależnych.

Pełna transparentność i rozwiązania typu open source, rozwijane przez społeczność internetową, dają gwarancję, które nie zawsze otrzymujemy od komercyjnych dostawców. Jakby nie było, cały internet jest zbudowany wyłącznie na standardach RFC - Request for Comments, publikowanych od 1969 r. przez internetową społeczność ekspertów bez nadzoru i własności jakiejkolwiek korporacji czy państwa. Darzę ogromnym zaufaniem społeczeństwo internetowe jako całość i mechanizmy w nim drzemiące. Dlatego zachęcam twórców wszelkich aplikacji, aby poddawali swoje rozwiązania krytyce społecznej użytkowników, a co za tym idzie również ocenie niezależnych ekspertów.

Dziękuję za rozmowę!

PUBLIKOWANIE ZDJĘĆ DZIECI W INTERNECIE RODZI WIELE RYZYK – ZARÓWNO DLA DZIECKA, JAK I PUBLIKUJĄCEGO

Nadmierne rozpowszechnianie wizerunku małoletnich w sieci nie tylko narusza ich prywatność, ale też może powodować realne zagrożenie dla ich bezpieczeństwa. Powinni pamiętać o tym zarówno rodzice i dziadkowie, którzy bezrefleksyjnie wrzucają do sieci zdjęcia swoich pociech, jak i instytucje zajmujące się edukacją i wychowaniem nieletnich, jak szkoły czy przedszkola.

Media coraz częściej informują o placówkach edukacyjnych publikujących filmy z udziałem swoich podopiecznych, w których dzieci zachęcają do zapisania się do danej szkoły albo przedszkola. Zdjęcia z rozmaitych ciekawych aktywności, które również mają przyciągnąć nowych chętnych, są na porządku dziennym. Do sprawy odniosła się też Magdalena Bigaj w wywiadzie dla lutowego Biuletynu UODO, wskazując, że w związku z pogłębiającym się niżem demograficznym szkoły i przedszkola stają przed realnym problemem zabiegania o to, by dzieci zostały zapisane właśnie do nich – działania promocyjne będą się więc tylko nasilać.

Wizerunek dziecka podlega szczególnej ochronie

Prowadząc je, nie można jednak zapominać o przepisach o chroniących dane osobowe oraz wizerunek. Zgodnie z wypracowaną w orzecznictwie i doktrynie definicją to ostatnie pojęcie oznacza obraz danej osoby (nie tylko twarz, ale też np. charakterystyczną sylwetkę), utrwalony w jakiś sposób (najczęściej na zdjęciu lub filmie). Jest on dobrem osobistym w świetle Kodeksu cywilnego, a także podlega ochronie na podstawie prawa autorskiego. Wizerunek stanowi również daną osobową, gdyż pozwala na zidentyfikowanie konkretnego człowieka.

Rozpowszechnianie wizerunku wymaga zgody danej osoby. Choć prawo autorskie dopuszcza możliwość publikacji bez takiej zgody, jeśli wizerunek konkretnej osoby stanowi tylko szczegółów większej całości, tej podstawy nie można stosować bezrefleksyjnie. Kluczową kwestią jest zawsze ustalenie, czy w danym przypadku faktycznie niezbędne jest, by relacjonować wydarzenie, imprezę czy sprawozdawać przebieg wycieczki z wykorzystaniem wizerunku dzieci. To, że w przepisach mamy do czynienia z potencjalnym zwolnieniem z konieczności pozyskania zezwolenia na rozpowszechnienie, nie oznacza, że w każdych okolicznościach jest to niezbędnie konieczne.

Oddzielną sprawą są regulacje dotyczące danych osobowych. Znajdują one zastosowanie zawsze, gdy na podstawie zdjęcia można rozpoznać konkretną osobę. Nawet więc, jeśli stanowi ona szczegół całości (co pozwala na publikację bez zezwolenia w świetle prawa autorskiego), ale można ją zidentyfikować, w grę wchodzą przepisy RODO. Warto też podkreślić, że w motywie 38 tego Rozporządzenia wskazano, iż dane osobowe dzieci wymagają szczególnej ochrony, zaś motyw 58 zawiera wytyczną nakazującą stosowanie jasnych i prostych komunikatów w przypadku przetwarzania danych dziecka – tak, by mogło ono zrozumieć swoje prawa.

Przetwarzanie wizerunku musi mieć podstawę prawną

Przede wszystkim więc przetwarzanie wizerunku (a więc zarówno jego publikacja w internecie, jak i samo utrwalenie poprzez np. zrobienie zdjęcia) wymaga wskazania jednej z podstaw wymienionych w art. 6 ust. 1 RODO. W grę nie wejdzie lit. b tego przepisu, gdyż publikacja zdjęć nie wydaje się konieczna dla celów wykonania umowy.

Ta przesłanka jest nieadekwatna w przypadku publikacji wizerunku w celach marketingowych placówki oświatowej także wówczas, gdy zdjęcia na zamówienie szkoły zostaną odpłatnie przygotowane przez profesjonalnego fotografa. Okoliczność ta nie ma żadnego znaczenia dla rozpowszechniania wizerunku dzieci. Nawet jeśli świadczenie placówki oświatowej chcielibyśmy potraktować jako usługę edukacyjną, placówka ta jest w stanie w pełni realizować program nauczania i zapewniać opiekę nad uczniem bez upubliczniania jego wizerunku w internecie. Publikacja zdjęć jest jedynie działaniem akcesoryjnym, niemającym wpływu na istotę świadczonej usługi (edukacji) – mówi dr hab. Marlena Sakowska-Baryła, prof. Uniwersytetu Łódzkiego, radczyni prawna i partnerka w Sakowska-Baryła, Czaplińska Kancelarii Radców Prawnych, należąca do Społecznego Zespołu Ekspertów przy Prezesie UODO.

Tym bardziej trudno się powołać na przesłankę konieczności przetwarzania dla ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (lit. d). W tym miejscu znów warto odwołać się do wywiadu z Magdaleną Bigaj, która zwróciła uwagę, że w przypadku placówek publicznych żaden przepis nie nakłada na nie obowiązku promocji. Także dr hab. Sakowska-Baryła wskazuje, że w świetle obecnie obowiązującego prawa publikacji wizerunku dziecka przez placówkę oświatową nie można postrzegać w kategoriach obowiązku prawnego.

A co za tym idzie, tego rodzaju przetwarzanie danych osobowych nie ma i nie może mieć podstaw w przesłance określonej w art. 6 ust. 1 lit. c RODO. Zwykle publikowanie wizerunków dzieci przez różnego rodzaju placówki odbywa się w celach informacyjno-promocyjnych, a realizowanie takich potrzeb w żadnym razie nie stanowi wypełnienia obowiązku prawnego ciążącego na administratorze, ponieważ taki obowiązek po prostu nie istnieje – tłumaczy ekspertka.

Przypomina też, że przetwarzanie danych osobowych na podstawie wspomnianej przesłanki wymaga istnienia konkretnego przepisu prawa krajowego lub unijnego. Co prawda Prawo oświatowe nakłada na szkoły obowiązki w zakresie dokumentowania przebiegu procesu nauczania, ale żaden przepis nie obliguje placówki do prowadzenia publicznej galerii zdjęć czy profilu w mediach społecznościowych.

Działania takie wykraczają poza sferę imperium (władczych działań państwa) i przechodzą w sferę promocji, która nie ma nic wspólnego z obowiązkiem prawnym, choć trzeba zauważyć, że szkoły faktycznie prowadzą swoistą politykę informacyjną, z jednej strony promując swoje działania edukacyjne, z drugiej zabiegając o zainteresowanie potencjalnych kandydatów – mówi prof. Sakowska-Baryła.

Publikowanie zdjęć dzieci nie stanowi uzasadnionego interesu administratora

Ekspertka wskazuje też, iż rozpowszechnianie przez placówkę oświatową wizerunków dzieci na podstawie art. 6 ust. 1 lit. f RODO także jest wysoce ryzykowne i – wbrew utartej praktyce – zazwyczaj prawnie bezpodstawne. Przepis ten stanowi bowiem, że przetwarzanie danych osobowych – w tym ich pozyskiwanie i rozpowszechnianie – jest zgodne z prawem, o ile jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, w szczególności gdy jest ona dzieckiem.

Choć przez lata obserwowaliśmy rozwój działalności placówek oświatowych prowadzonej w mediach społecznościowych obejmującej głównie szeroką dystrybucję zdjęć i filmów, co bardzo często odbywa się równolegle z umieszczaniem ich także na stronach internetowych placówek, uzasadniona jest analiza tego, czy praktyka ta rzeczywiście znajduje podstawę w prawie, a także, czy faktycznie niezbędne jest realizowanie celów informacyjnych i promocyjnych głównie na bazie rozpowszechniania wizerunków dzieci. Teoretycznie szkoły mogą się powołać na „interes promocyjny" jako uzasadniony prawnie cel przetwarzania, ale przecież musi on przejść tzw. test równowagi i w kolizji między interesem promocyjnym szkoły a prawem do prywatności i ochrony wizerunku dziecka ten ostatni niemal zawsze należy uznać za nadrzędny. Dzieci korzystają ze szczególnej ochrony danych (motyw 38 RODO), co sprawia, że ich interesy przeważają nad chęcią autopromocji placówki – tłumaczy prof. Sakowska-Baryła.

Oczywiście należy tu zachować zdrowy rozsądek i nie chodzi o to, aby przestać informować o działalności szkoły, osiągnięciach uczniów, relacjonować wydarzenia czy promować godne pochwały zachowania. Każdorazowo trzeba jednak rozważyć, czy w tym przypadku niezbędne jest okraszanie

przekazywanej informacji zdjęciem lub filmem z udziałem uczniów. Dzieci w szkole zwykle pozostają w sytuacji, w której ograniczona jest ich swoboda i autonomia, a ich pozycja, sposób percepcji rzeczywistości i postrzegania świata zwykle nie sprzyja świadomemu decydowaniu o tym, czy chcą, czy nie chcą być bohaterem filmu, zdjęcia, fotorelacji czy rolki w socialmediach.

Czym się kierować, wyrażając zgodę na publikację zdjęcia dziecka?

W przypadku osób niepełnoletnich zgody na przetwarzanie danych udzielają w ich imieniu rodzice lub opiekunowie prawni. Jest to element wykonywania władzy rodzicielskiej, a więc – zgodnie z Kodeksem rodzinnym i opiekuńczym – musi on uwzględniać najlepszy interes dziecka, a także szanować jego godność i prawa. KRO, podobnie jak Konwencja ONZ o prawach dziecka, przewiduje też, że przed podjęciem ważnych decyzji dotyczącej podopiecznego rodzice powinni wysłuchać ich zdania. Oczywiście należy tu uwzględnić wiek i stopień dojrzałości dziecka – nie zawsze bowiem zdaje sobie ono sprawę z konsekwencji wyrażenia takiej zgody. W przypadku starszych dzieci jednak powinno się skonsultować z nimi przed wyrażeniem takiej zgody.

Należałoby przyjąć, że człowiek w ogóle – nawet ten jeszcze niepełnoletni – powinien mieć wpływ na to czy, jego wizerunek będzie pozyskany i czy będzie rozpowszechniony. Nie chodzi oczywiście o to, by zabieganie o zgodę na utrwalanie i rozpowszechnianie wizerunku doprowadzić do absurdu poprzez pytanie o nią dzieci w każdym wieku, nawet tych, które nie są w stanie jej wyrazić. Ale przymuszanie do pozowania do zdjęć, szykany z powodu braku zgody na rozpowszechnianie wizerunku, szydzenie z niechęci do pozowania należy uznać za praktyki w wysokim stopniu naganne – wyjaśnia prof. Sakowska-Baryła.

Ekspertka wskazuje, że właśnie zgoda w tym przypadku wydaje się najlepszą podstawą prawną. Musi być ona jednak całkowicie dobrowolna (podobnie jest w przypadku pełnoletnich uczniów).

Jeśli zatem dziecko nie może wziąć udziału w teatrzyku szkolnym tylko dlatego, że rodzic nie chce, by zdjęcie z tego wydarzenia trafiło na Facebooka, mamy do czynienia z wymuszeniem zgody. Podobnie nie można uzależniać wzięcia przez ucznia udziału w zawodach sportowych czy zajęciach dodatkowych od przymusowego wyrażenia zgody na pozyskanie i rozpowszechnianie wizerunku. Właściwym rozwiązaniem jest zapewnienie dziecku udziału w aktywności przy jednoczesnym zadbaniu, by nie znalazło się ono w kadrze publikowanych zdjęć – zaznacza badaczka.

Zgoda musi też mieć charakter uprzedni, być precyzyjna i przejrzysta (m.in. na rzecz jakiego podmiotu jest udzielana i na jaki czas), wyraźnie wskazywać cel i sposób wykorzystania wizerunku oraz jego warunki (np. w jakich serwisach zdjęcie będzie publikowane, z jakim podpisem, czy zostanie poddane jakiejś edycji). Wszystkie powyższe informacje muszą być przekazane zrozumiałym językiem.

Niebezpieczeństwa związane z publikacją wizerunku dziecka w sieci

Kluczowym argumentem przeciwko dzieleniu się zdjęciami dziecka jest jego godność i autonomia. Udostępniając zdjęcia dziecka, odbieramy mu prawo do samodzielnego kształtowania swojej obecności w internecie i podejmowania decyzji o swoim wizerunku. Decyzje podjęte dziś przez rodziców będą z dzieckiem przez całe jego życie – mówi Wojciech Klicki, wiceprezes Fundacji Panoptykon i członek Społecznego Zespołu Ekspertów przy Prezesie UODO.

Jak wskazano w broszurze „Wizerunek dziecka w internecie" (opracowanej z udziałem UODO), udostępnianie wizerunku w sieci rodzi poważne zagrożenia. Są one szczególnie poważne w przypadku osób niepełnoletnich. Przede wszystkim publikując wizerunek, tracimy nad nim kontrole – nie wiemy, kto skopiuje to zdjęcie ani do czego go użyje. A użyte może być zarówno w celu dokonania oszustwa (np. fałszywa zbiórka na rzekomo chore dziecko, z wykorzystaniem skradzionego zdjęcia), jak i do cyberprzemocy (np. przerabianie zdjęć, by pognębić ofiarę, lub rozpowszechnianie jej kompromitującego zdjęcia z przeszłości).

Bardzo istotne jest to, jak komponowane są zdjęcia lub filmy, co faktycznie prezentują, jak są kadrowane. To, co dla niektórych może być urocze, śmieszne i warte pokazania, dla innych – zwłaszcza dla dzieci – bywa przyczyną znacznego dyskomfortu nie tylko w chwili publikacji, ale także długo po niej. Jak wiemy – w internecie nic nie ginie i właściwie nie jesteśmy w stanie przewidzieć, jak z pozoru niewinne ujęcie, nawet w pewnych okolicznościach uzasadnione interesem edukacyjnym (promocyjnym, informacyjnym), zostanie wykorzystane w przyszłości – zaznacza prof. Sakowska-Baryła.

Zdjęcia dzieci mogą być bowiem używane także przez osoby o skłonnościach pedofilskich – w celu wymieniania się na różnych forach dla takich osób, a nawet – zlokalizowania dziecka i nawiązania z nim kontaktu. Szczególnie zdjęcia na profilach czy stronach szkół i przedszkoli mogą pozwolić przestępcy ustalić, gdzie dziecko znajduje się w danych godzinach itp. Ze względu na to ostatnie zagrożenie należy w szczególności unikać publikacji zdjęć małoletnich nie w pełni ubranych (np. na basenie). Niestety technologia deepfake pozwala dziś przerobić w kontekście seksualnym praktycznie każde zdjęcie.

Pod koniec roku 2025 wielkie poruszenie wywołała nowa funkcja Groga (modelu sztucznej inteligencji na portalu X), która pozwalała na błyskawiczne „rozbieranie" osób na zdjęciach – tj. generowanie nagich fotografii z ich twarzami. Potencjalnie mogło to dotyczyć także zdjęć dzieci. Co prawda X zablokował już tę funkcję, ale wciąż istnieje wiele podobnych aplikacji. Tylko w styczniu 2026 r. Apple zablokował ich w swoim sklepie 28, lecz wciąż pojawiają się nowe.

Dobrze, że sprawa ta odbiła się szerokim echem, bo trudno o bardziej wyrazisty przykład negatywnych konsekwencji publicznego udostępniania wizerunku dzieci. Mam nadzieję, że przemówi on do wyobraźni rodziców – podkreśla Wojciech Klicki.

Jak usunąć z internetu zdjęcia nasze lub naszych dzieci?

Art. 17 RODO przyznaje nam tzw. prawo do bycia zapomnianym, czyli do usunięcia naszych danych. Dotyczy to również zdjęć zawierających nasz wizerunek. Usunięcia danych możemy domagać się, gdy są już one nieaktualne (np. dziecko dorosło i zmieniło wygląd), nadmiarowe, przetwarzane niezgodnie z prawem lub gdy zgoda na ich przetwarzanie została cofnięta. Po osiągnięciu pełnoletniości dziecko może cofnąć zgodę na publikację, wyrażoną wcześniej przez rodziców. Jak zwróciła uwagę Magdalena Bigaj, w przytaczanym wywiadzie, pojawiły się już pierwsze przypadki młodych ludzi domagających się od szkół usunięcia swoich zdjęć sprzed lat.

Prócz skargi na podstawie RODO można domagać się usunięcia zdjęcia z naszym wizerunkiem na podstawie przepisów o ochronie dóbr osobistych. Najpierw należy wezwać podmiot, który te zdjęcia opublikował, do ich bezzwłocznego usunięcia. Jeśli tego nie zrobi, można rozważyć dalsze kroki, np. pozew cywilny, a w pewnych okolicznościach nawet postępowanie karne. Art. 202 par. 4b KK penalizuje bowiem produkcję, rozpowszechnianie, prezentowanie, przechowywanie lub posiadanie pornografii z wykorzystaniem wytworzonego (np. rysunek) lub przetworzonego (np. fotomontaż, deepfake) wizerunku małoletniego uczestniczącego w czynności seksualnej. Dotyczy to więc także zdjęć przerobionych przez wspomniane wyżej aplikacje „rozbierające".

Jeśli zdjęcia publikowane są na wielkich platformach społecznościowych, można też domagać się ich usunięcia bezpośrednio od administratorów tych platform – na podstawie Aktu o usługach cyfrowych (DSA). Wojciech Klicki wskazuje, że im dłużej materiał jest dostępny w sieci, tym większe ryzyko jego szerokiego rozpowszechnienia i szkodliwych konsekwencji.

Platformy nie mogą lekceważyć wniosków o usunięcie zdjęcia

Dlatego najpierw zawsze warto zgłosić taką nielegalną treść platformie z żądaniem jej usunięcia. Art. 16 umożliwia bowiem każdej osobie domaganie się usunięcia bezprawnej treści, którą inny użytkownik opublikował na platformie. W tym zakresie DSA obowiązuje bezpośrednio, nie wymaga wdrożenia). Platformy mają co do zasady obowiązek niezwłocznie reagować na takie zgłoszenia. Jeśli tego nie zrobią, same narażają się na to, że mogą za taką treść ponieść odpowiedzialność – tłumaczy ekspert.

Art. 6 wspomnianego Aktu o usługach cyfrowych przewiduje bowiem, że hostingodawca (w tym np. portal społecznościowy) nie odpowiada za bezprawne materiały tak długo, jak nie ma wiedzy o ich nielegalnym charakterze. Kiedy jednak zostanie o nim poinformowany, aby uniknąć odpowiedzialności, musi niezwłocznie taką treść usunąć.

Ten mechanizm ma skłaniać m.in. platformy do szybkiego reagowania na nielegalne treści. DSA nakłada też na platformy pewne obowiązki proceduralne ws. zgłoszeń na postawie art. 16. Platforma ma obowiązek stworzyć do tego odpowiednią ścieżkę, potwierdzić otrzymanie zgłoszenia (jeśli ma dane kontaktowe użytkownika/użytkowniczki), a następnie rozpatrzyć je „w sposób terminowy, niearbitralny i obiektywny oraz z zachowaniem należytej staranności" (nie może go więc po prostu zignorować, co czasem zdarzało się w przeszłości). Jeśli odmówi usunięcia, musi stworzyć odpowiedni wewnętrzny mechanizm odwoławczy, który umożliwi osobie zgłaszającej zakwestionowanie pierwotnej decyzji – zauważa Wojciech Klicki.

Jeśli ta procedura odwoławcza zawiedzie, można także złożyć skargę do sądu lub organu pozasądowego rozwiązywania sporów. Niestety przez brak ustawy implementującej DSA w Polsce wciąż nie wyznaczono wprost Koordynatora Usług Cyfrowych, do którego można by odwoływać się w kwestiach naruszeń proceduralnych przy rozpatrywaniu odwołania przez platformę.

STRAŻ GMINNA MOŻE PRZEKAZAĆ DANE GMINNEJ KOMISJI ROZWIĄZYWANIA PROBLEMÓW ALKOHOLOWYCH

Prowadząc działania związane ze zobowiązaniem określonej osoby do poddania się leczeniu odwykowemu, gminna komisja rozwiązywania problemów alkoholowych może wnioskować do straży miejskiej o udostępnienie informacji np. o mandatach karnych czy orzeczeniach o ukaraniu przez straż miejską takiej osoby w związku z nadużywaniem przez nią alkoholu. Podstawą uprawniającą do takiego działania są przepisy ustawy z 26 października 1982 r. o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi.

Przepisy przywołanej ustawy stanowią, że osoby, które w związku z nadużywaniem alkoholu powodują rozkład życia rodzinnego, demoralizację małoletnich, uchylają się od obowiązku zaspokajania potrzeb rodziny albo systematycznie zakłócają spokój lub porządek publiczny, gminna komisja rozwiązywania problemów alkoholowych kieruje na badanie przez biegłego w celu **wydania opinii dotyczącej uzależnienia od alkoholu i wskazania rodzaju zakładu leczniczego** (art. 25 w związku z art. 24).

Komisja ta ma również prawo **wnioskować do sądu o nałożeniu na takie osoby obowiązku poddania się leczeniu w stacjonarnym lub niestacjonarnym zakładzie lecznictwa odwykowego** (art. 26 ust. 1). Do takiego wniosku należy **dołączyć zebraną dokumentację wraz z opinią biegłego**, jeżeli badanie przez biegłego zostało przeprowadzone (art. 26 ust. 3 zdanie drugie).

Jakie dane mogą przetwarzać gminne komisje?

Jednocześnie (stosownie do art. 25a ust. 1) członkowie gminnej komisji rozwiązywania problemów alkoholowych, **w zakresie niezbędnym do realizacji zadań związanych z procedurą zobowiązania do poddania się leczeniu odwykowemu**, mogą przetwarzać informacje o osobach, o których mowa w art. 24, bez ich zgody i wiedzy, dotyczące stanu zdrowia, nałogów, skazań, mandatów karnych, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, z uwzględnieniem następujących danych:

1) imienia (imion) i nazwiska;
2) daty i miejsca urodzenia;
3) płci;

4) numeru PESEL, a w przypadku gdy dana osoba nie posiada numeru PESEL – serii i numeru dokumentu potwierdzającego tożsamość;

5) stanu cywilnego;

6) daty zawarcia małżeństwa, jeżeli dotyczy;

7) daty ustania małżeństwa, jeżeli dotyczy;

8) wykształcenia;

9) zawodu;

10) miejsca pracy lub nauki;

11) stopnia niezdolności do pracy, posiadania orzeczenia o niepełnosprawności i stopnia niepełnosprawności;

12) adresu miejsca zamieszkania lub miejsca pobytu;

13) adresu do korespondencji;

14) adresu poczty elektronicznej;

15) numeru telefonu.

Członkowie gminnej komisji rozwiązywania problemów alkoholowych (zgodnie z art. 25a ust. 2), w zakresie niezbędnym do realizacji zadań związanych z procedurą zobowiązania do poddania się leczeniu odwykowemu osób, o których mowa w art. 24, mogą przetwarzać dane o członkach rodzin tych osób, w następującym zakresie:

1) imienia (imion) i nazwiska;

2) daty i miejsca urodzenia;

3) płci;

4) stopnia pokrewieństwa lub powinowactwa;

5) adresu do korespondencji lub numeru telefonu, lub adresu poczty elektronicznej.

Wniosek do straży miejskiej o informacje ws. mandatów – uprawniony

Zatem uznać należy, **że gminne komisje rozwiązywania problemów alkoholowych mogą** – na podstawie art. 25a ustawy o wychowaniu w trzeźwości i przeciwdziałaniu alkoholizmowi – **występować do straży gminnej o udostępnienie informacji dotyczących m.in. stanu zdrowia, nałogów, skazań, mandatów karnych, orzeczeń o ukaraniu, a także innych orzeczeń wydanych w**

postępowaniu sądowym lub administracyjnym w odniesieniu do osób, o których mowa w art. 24 ww. ustawy. I to te przepisy będą podstawą uprawniającą straż gminną do udostępnienia danych.

Jednocześnie w przedstawionej sytuacji **zastosowania nie będą miały przepisy ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i ze zwalczaniem przestępczości**. Ustawa ta odnosi się bowiem do przetwarzania danych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności.

DOKUMENTACJA MEDYCZNA ADOPTOWANEGO DZIECKA – WYSTĄPIENIE PREZESA UODO DO MINISTER ZDROWIA

Prezes UODO zabiega o dokonanie takich zmian w przepisach regulujących postępowanie z dokumentacją medyczną, by możliwa była aktualizacja zawartych w niej danych osobowych adoptowanych dzieci.

Wystąpienie w sprawie braku regulacji prawnych dotyczących zasad i sposobu wprowadzania zmian w dokumentacji medycznej dziecka, które zostało przysposobione całkowicie, Prezes UODO skierował do minister zdrowia. Wskazał w nim, że **problem ten ujawnił się w związku z rozpatrywaną przez Prezesa UODO skargą matki dziecka w pełni przysposobionego, którego dane osobowe nie zostały zaktualizowane przez placówkę medyczną**. W skardze podniesiono, że **po adopcji skarżąca poinformowała podmiot medyczny o nowym numerze PESEL dziecka i złożyła nową deklarację wyboru lekarza i pielęgniarki POZ**. Tymczasem w dokumentacji medycznej, w tym w zaświadczeniu lekarskim, nadal widniał stary numer, co skutkowało ujawnieniem informacji o procedurze adopcji.

Z dokumentacji medycznej nie można usuwać danych

Obecnie dokumentacja medyczna, stosownie do przepisów **ustawy z 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta (art. 23 ust. 2 i art. 24 ust. 1)** podlega ochronie prawnej, a podmiot udzielający świadczeń zdrowotnych ma obowiązek zapewnić ochronę danych gromadzonych w dokumentacji medycznej. Szczegółowe regulacje związane z zakresem dokumentacji medycznej oraz sposobem jej prowadzenia i przetwarzania zawartych w niej danych osobowych zawierają **natomiast przepisy wykonawcze wydane na podstawie art. 30 wymienionej ustawy.**

Przesądzają one (§ 4 ust. 6 rozporządzenia Ministra Zdrowia z 6 kwietnia 2020 r. w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania), że wpis w dokumentacji w postaci papierowej nie może być z niej usunięty, a jeżeli został dokonany błędnie, skreśla się go i zamieszcza adnotację o przyczynie błędu oraz datę i oznaczenie osoby dokonującej adnotacji, zgodnie z § 10 pkt 3. **Brak jest natomiast jakichkolwiek przepisów, które umożliwiałyby zmianę danych osobowych dziecka zawartych w dokumentacji medycznej w związku z koniecznością uwzględnienia takich okoliczności, jak dokonanie jego przysposobienia pełnego.**

Nowy akt urodzenia i nowy numer PESEL dla przysposobionego

Tymczasem **przysposobienie pełne** (zgodnie z art. 121 § 1 i § 2. Kodeksu rodzinnego i opiekuńczego) **prowadzi do powstania między przysposabiającym a przysposobiobionym takiego stosunku, jak między rodzicami a dziećmi**, w tym przysposobiony nabywa prawa i obowiązki wynikające z pokrewieństwa w stosunku do krewnych przysposabiającego. Zmianie ulega nazwisko przysposabianego, a dodatkowo zmianie może ulec również jego imię (stosownie do art. 122 Kodeksu rodzinnego i opiekuńczego).

Ponadto **sąd opiekuńczy, orzekając przysposobienie pełne małoletniego może** – w myśl art. 72 ustawy z 28 listopada 2014 r. – Prawo o aktach stanu cywilnego – **postanowić o sporządzeniu dla niego nowego aktu urodzenia**. Dotychczasowy akt urodzenia, stosownie do brzmienia art. 73 ust. 1 ustawy – Prawo o aktach stanu cywilnego, nie podlega ujawnieniu. **Sporządzenie nowego aktu skutkuje nadaniem nowego numeru PESEL.** Zgodnie bowiem z art. 20 ust. 1 ustawy – Prawo o aktach stanu cywilnego, kierownik urzędu stanu cywilnego, który sporządził akt urodzenia, występuje, za pośrednictwem systemu teleinformatycznego, o nadanie numeru PESEL, który po nadaniu jest zamieszczany w rejestrze stanu cywilnego.

Sporządzenie nowego aktu urodzenia w wyniku przysposobienia albo obalenia domniemania ojcostwa męża matki skutkuje nadaniem nowego numeru PESEL i **usunięciem z rejestru PESEL oraz z rejestrów mieszkańców prowadzonych przez organy gmin** właściwe ze względu na aktualne lub poprzednie miejsca zameldowania na pobyt stały lub czasowy **danych przysposobionego** albo osoby, której dotyczy obalenie domniemania ojcostwa męża matki, **zamieszczonych w tych rejestrach przed przysposobieniem** albo przed obaleniem domniemania ojcostwa męża matki (stosownie do § 5 ust. 1 rozporządzenia Ministra Spraw Wewnętrznych z 4 stycznia 2012 r. w sprawie nadania lub zmiany numeru PESEL).

Niezgodność z RODO

Biorąc pod uwagę przedstawiony stan prawny i problem, jaki został opisany w skardze, Prezes UODO uznał, iż niezbędne jest podjęcie możliwie pilnych działań legislacyjnych w celu zapewnienia skutecznej ochrony danych osobowych dzieci przysposobionych, które zawarte są w dokumentacji medycznej. **Brak kompleksowych regulacji, które umożliwiałyby zmianę takich danych i realizację prawa dostępu do aktualnych danych, budzi poważne zastrzeżenia z punktu widzenia określonych w RODO zasad ochrony danych osobowych, w tym m.in. zgodności z prawem, rzetelności i przejrzystości czy prawidłowości.**

Prezes UODO podkreślił, że **podstawa przetwarzania danych osobowych**, które są niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze lub wykonania zadania realizowanego

w interesie publicznym lub w ramach sprawowania władzy publicznej – właściwa dla podmiotów prawa publicznego – **musi być określona w sposób jasny i precyzyjny w prawie Unii lub w prawie państwa członkowskiego**, któremu podlega administrator. Wymóg taki wynika **także z przepisów Konstytucji RP.**

Dodatkowo wskazał, że **utrzymywanie w obrocie dokumentów zawierających uprzednie dane identyfikacyjne**, które utraciły aktualność na skutek sporządzenia nowego aktu urodzenia, **budzi też wątpliwości z perspektywy określonej w RODO zasady minimalizacji danych**, a także w związku z konstytucyjnym nakazem, **by władze publiczne pozyskiwały, gromadziły i udostępniały jedynie takie informacje o obywatelach, które są niezbędne** dla demokratycznego państwa prawa.

Interwencja RPD i pierwsze działania

Na problem z zapewnieniem ciągłości dokumentacji medycznej dzieci przysposobionych **zwróciła uwagę również Rzeczniczka Praw Dziecka**, która o korektę przepisów w tym zakresie wystąpiła do: Ministra Zdrowia, Ministra Spraw Wewnętrznych i Administracji, Ministra Sprawiedliwości oraz Ministra Obrony Narodowej, a więc podmiotów, które wydają przepisy wykonawcze dotyczące dokumentacji medycznej. Jej inicjatywa została przychylnie przyjęta przez **resorty sprawiedliwości, obrony narodowej oraz spraw wewnętrznych i administracji, które już podjęły lub zapowiedziały rozpoczęcie stosownych inicjatyw legislacyjnych.**

Potrzeba kompleksowych regulacji

Zwrócono jednak uwagę na potrzebę **podjęcia spójnych rozwiązań prawnych w odniesieniu do wszystkich rozporządzeń wykonawczych wydanych na podstawie art. 30 ustawy o Rzeczniku Praw Pacjenta. Ma to istotne znaczenie ze względu na konieczność stosowania przez podmioty lecznicze** (niezależnie od podmiotu tworzącego) **jednolitej dokumentacji medycznej**. Jeden z resortów zaznaczył, że podejmie prace nad zmianą rozporządzenia niezwłocznie po zainicjowaniu podobnych prac przez Ministerstwo Zdrowia.

Biorąc powyższe pod uwagę oraz fakt, że **resort zdrowia prowadził zaawansowane prace nad nowelizacją rozporządzenia Ministra Zdrowia w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania**, **Prezes UODO** postanowił **wystąpić do tego resortu o podjęcie możliwie pilnych kompleksowych działań legislacyjnych** w opisanej sprawie, tak by zapewnić właściwe gwarancje w zakresie prawa dostępu do aktualnych i prawidłowych danych osobowych zawartych dokumentacji medycznej przy zachowaniu prawa do prywatności i prawa do ochrony danych osobowych.

REALIZACJA PILOTAŻOWYCH PROGRAMÓW ZDROWOTNYCH – UDOSTĘPNIANIE DANYCH PACJENTÓW PRZEZ NFZ

Pismo Narodowego Funduszu Zdrowia (NFZ), które ostatnio wpłynęło do Prezesa UODO, po raz kolejny potwierdza, że istnieje potrzeba stworzenia właściwej podstawy prawnej do przetwarzania danych osobowych świadczeniobiorców w związku z realizacją programów pilotażowych w opiece zdrowotnej.

NFZ działając jako administrator danych osobowych świadczeniobiorców, po wnikliwej analizie obowiązujących przepisów prawa **powziął wątpliwości, czy podmiot zaangażowany w jeden z programów pilotażowych, wykonujący czynności koordynacyjno-organizacyjno-analityczne, ma prawo domagać się udostępnienia danych pacjentów** z rejestrów NFZ. Są to bowiem **dane szczególnej kategorii w rozumieniu RODO** i mogą być przetwarzane po spełnieniu rygorystycznych warunków i zapewnieniu odpowiednich gwarancji.

W opinii NFZ **podstawą legalizującą ich udostępnienie nie mogą być przepisy rangi rozporządzenia** regulującego kwestie związane z realizacją programu pilotażowego. **Nie stanowią jej także przepisy ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych** – zwłaszcza jej art. 188 ust. 1 pkt 4b, wskazywany przez Ministerstwo Zdrowia jako podstawa prawna żądania danych osobowych od NFZ. Dotyczy on bowiem wyłącznie przekazywania danych w celu terapeutycznym świadczeniodawcom prowadzącym aktualnie leczenie.

Narodowy Fundusz Zdrowia prosi Prezesa UODO o opinię

NFZ w swoim piśmie przedstawia obszerną analizę sytuacji, prosząc Prezesa UODO o stanowisko odnośnie do przesłanki, która legalizowałaby udostępnienie przez NFZ szczególnej kategorii danych osobowych pacjentów owemu wskazanemu wyżej podmiotowi wykonującemu czynności koordynacyjno-organizacyjno-analityczne.

Abstrahując od szczegółów sprawy, która zainicjowała korespondencję ze strony NFZ, wskazać należy, że stanowi ona **kolejny dowód na to, że wciąż aktualne pozostają generalne zastrzeżenia Prezesa UODO odnośnie do przetwarzania danych osobowych w związku z realizacją programów pilotażowych** formułowane zarówno w wystąpieniach, jak i opiniach legislacyjnych przedstawianych w odniesieniu do aktów wykonawczych wydawanych przez Ministra Zdrowia.

Wskazują one m.in. na:

- **niedopuszczalność określania podstawowych kwestii** dotyczących przetwarzania danych osobowych na potrzeby realizacji programów pilotażowych **w formie aktu podstawowego**,
- **konieczność zainicjowania przez resort zdrowia zmian legislacyjnych** w ustawie o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, **mających na celu stworzenie jasnych i precyzyjnych regulacji ustawowych** stanowiących podstawę dla przetwarzania danych osobowych w celu programów pilotażowych, w tym **określenie w normach ustawowych: zakresu danych** gromadzonych w czasie trwania programu pilotażowego**, okresu ich przetwarzania, roli poszczególnych podmiotów** przetwarzających dane, **rozwiązań dotyczących wzajemnego przepływu danych** (warunków udostępniania danych i dalszego ich przetwarzania),
- potrzebę takiego **konstruowania przez Ministerstwo Zdrowia przepisów rozporządzeń** dotyczących realizacji programów pilotażowych, by **zapewniona została ich zgodność z RODO,**
- niezbędność **wyeliminowania zgody pacjenta jako podstawy przetwarzania** danych osobowych.

NARUSZENIA OCHRONY DANYCH OSOBOWYCH W ŚWIETLE USTAWY O KSC

Nowelizacja ustawy o Krajowym Systemie Cyberbezpieczeństwa, wdrażająca dyrektywę NIS 2, wprowadza mechanizm, na którego podstawie organy właściwe ds. cyberbezpieczeństwa będą informować Prezesa UODO o podejrzeniach naruszeń ochrony danych osobowych stwierdzanych w toku nadzoru. Kształtuje to nowy kanał pozyskiwania przez Prezesa UODO informacji o potencjalnych naruszeniach, niezależny od zgłoszeń dokonywanych przez samych administratorów w trybie art. 33 RODO. Co to oznacza w praktyce?

Ustawa z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (ustawa o KSC), której nowelizacja wejdzie w życie 3 kwietnia br., reguluje przede wszystkim kwestie związane z bezpieczeństwem systemów informacyjnych. Jej adresatami są tzw. **podmioty kluczowe i ważne**, działające w sektorach takich **jak energetyka, transport, ochrona zdrowia, infrastruktura cyfrowa czy sektor publiczny**.

Nowy punkt styku ochrony danych osobowych i cyberbezpieczeństwa

Choć ustawa o KSC i RODO stanowią odrębne reżimy prawne, służące odmiennym celom, ich zakresy w praktyce częściowo się pokrywają – incydent zagrażający bezpieczeństwu systemu informacyjnego często wiąże się z naruszeniem ochrony przetwarzanych w tym systemie danych osobowych.

Przykładem krzyżowania się tych systemów jest art. 59a znowelizowanej ustawy o KSC, zgodnie z którym, **w przypadku stwierdzenia podczas sprawowania nadzoru podejrzenia naruszenia ochrony danych osobowych organ właściwy ds. cyberbezpizeństwa w terminie 7 dni informuje o tym Prezesa UODO** (lub ewentualnie inny właściwy organ nadzorczy – np. odpowiedni organ prokuratury).

Nadzór na gruncie ustawy o KSC

Rozdział 11 ustawy o KSC reguluje **nadzór nad podmiotami kluczowymi i ważnymi,** sprawowany przez organy właściwe ds. cyberbezpieczeństwa, którego **celem jest weryfikacja, czy podmioty te prawidłowo wykonują obowiązki** wynikające z ustawy.

Przewiduje ona **szeroki wachlarz narzędzi nadzorczych:** organ może prowadzić kontrole w siedzibie podmiotu lub zdalnie, nakazać przeprowadzenie audytu bezpieczeństwa, zlecić odpowiedniemu CSIRT-owi ocenę bezpieczeństwa systemu informacyjnego, żądać przekazania dokumentów i informacji, a nawet okresowo wyznaczyć urzędnika monitorującego (art. 53 ust. 2 i 5 ustawy o KSC). Osoba prowadząca czynności kontrolne ma przy tym **prawo wglądu do dokumentów, przetwarzania danych osobowych w zakresie niezbędnym do realizacji celu kontroli, żądania wyjaśnień oraz przeprowadzania oględzin urządzeń, nośników i systemów informacyjnych** (art. 55 ustawy o KSC).

Dlaczego to istotne? Zakres tych uprawnień sprawia, że **organy ds. cyberbezpieczeństwa,** badając np. konfigurację zabezpieczeń baz danych, logi systemu czy rejestr incydentów lub analizując składane wyjaśnienia, **mogą natrafić na okoliczności wskazujące na naruszenie ochrony danych osobowych,** takie jak np. przypadkowa utrata lub nieuprawniony dostęp do danych osobowych. Oznacza to, że **źródłem informacji o naruszeniach może być potencjalnie kilkanaście różnych organów,** takich jak np. KNF, Prezes UKE czy właściwi ministrowie wskazani w ustawie – każdy w ramach nadzorowanego przez siebie sektora (art. 41 i 41a ustawy o KSC).

Informowanie o podejrzeniu naruszenia ochrony danych osobowych

Warto zwrócić uwagę, **że art. 59a ustawy o KSC kreuje obowiązek, a nie uprawnienie.** Sformułowanie „organ właściwy do spraw cyberbezpieczeństwa informuje" nie pozostawia pola do uznaniowości. **Jeżeli taki organ stwierdzi podejrzenie naruszenia ochrony danych osobowych**, co do zasady **powinien przekazać informację Prezesowi UODO**.

Próg aktualizacji obowiązku jest zaś stosunkowo niski. Przepis posługuje się określeniem „stwierdzenie podejrzenia naruszenia", a nie „stwierdzenie naruszenia", znane z art. 33 ust. 1 RODO. **Organ ds. cyberbezpieczeństwa nie musi zatem mieć pewności, że doszło do naruszenia w rozumieniu art. 4 pkt 12 RODO** ani dokonywać jego kwalifikacji prawnej. Wystarczy, że okoliczności stwierdzone w toku czynności nadzorczych wskażą na **samo podejrzenie jego wystąpienia**.

Co ciekawe, mechanizm ten będzie funkcjonować niezależnie od obowiązku zgłoszenia naruszenia przez samego administratora w trybie art. 33 RODO. Terminy będą biec odrębnie i rozpoczynać się w innym momencie: w przypadku administratora – w ciągu 72 godzin od stwierdzenia naruszenia; w przypadku organu ds. cyberbezpieczeństwa – **w ciągu 7 dni od stwierdzenia jego podejrzenia**. Prezes UODO może więc otrzymywać informacje o tych samych zdarzeniach z co najmniej dwóch niezależnych źródeł, w różnym czasie i o różnym stopniu szczegółowości.

4 NARUSZENIA I KONTROLE

Praktyczne znaczenie dla ochrony danych osobowych

Art. 59a ustawy o KSC stworzy więc nowy, nieistniejący dotychczas kanał pozyskiwania przez Prezesa UODO (i inne właściwe organy) informacji o potencjalnych naruszeniach ochrony danych osobowych. Do tej pory głównym źródłem wiedzy na ten temat były zgłoszenia dokonywane przez samych administratorów na podstawie art. 33 RODO. **Nadchodzące wejście w życie nowelizacji wdrażającej NIS 2 spowoduje, że obowiązek notyfikacyjny – choć o innym charakterze – będzie spoczywał także na organach prowadzących nadzór w zakresie cyberbezpieczeństwa.**

Z perspektywy podmiotów, które będą podlegać jednocześnie ustawie o KSC, jako podmioty kluczowe lub ważne, oraz RODO, jako administratorzy danych, oznacza to, że **wzrośnie prawdopodobieństwo wykrycia w ich organizacjach ewentualnych zaniedbań**, w tym np. niezgłoszonych naruszeń ochrony danych osobowych. Nadzór nad cyberbezpieczeństwem, prowadzony na podstawie ustawy o KSC, będzie mógł więc ujawnić nie tylko uchybienia w zakresie zarządzania bezpieczeństwem systemów informacyjnych, ale także okoliczności istotne w świetle potencjalnego naruszenia przepisów RODO.

Praktyczne stosowanie art. 59a ustawy o KSC będzie wymagało **wypracowania standardów współpracy pomiędzy organami właściwymi ds. cyberbezpieczeństwa a organami nadzorczymi na gruncie RODO.** Zagospodarowanie informacji napływających z wielu różnych organów sektorowych będzie stanowić wyzwanie operacyjne, ale jednocześnie **szansę na pełniejszy obraz stanu ochrony danych osobowych w podmiotach objętych ustawą o KSC.**

DIGITAL OMNIBUS: EROD I EIOD POPIERAJĄ UPROSZCZENIA I WZMACNIANIE KONKURENCYJNOŚCI, JEDNOCZEŚNIE WSKAZUJĄC KLUCZOWE ZASTRZEŻENIA

Europejska Rada Ochrony Danych oraz Europejski Inspektor Ochrony Danych przyjęli wspólną opinię dotyczącą projektu rozporządzenia *Digital Omnibus*. Celem tego projektu jest uproszczenie unijnego cyfrowego otoczenia regulacyjnego, zmniejszenie obciążeń administracyjnych oraz zwiększenie konkurencyjności europejskich organizacji.

EROD i EIOD koncentrują się na aspektach dotyczących RODO, rozporządzenia EUDPR, dyrektywy ePrivacy oraz tzw. *Data Acquis*. W szczególności oceniają, czy projekt:

1) prowadzi do rzeczywistego uproszczenia i ułatwia zgodność z przepisami,

2) zwiększa pewność prawa oraz

3) wpływa na prawa podstawowe osób.

Zmiany w RODO i EUDPR budzą poważne obawy

Na początku tego roku EROD rozpoczęła skoordynowaną akcję dotyczącą prawa do usunięcia danych, czyli „prawa do bycia zapomnianym" (art. 17 RODO). Raport z wynikami tej akcji zostanie przyjęty w nadchodzących miesiącach. **Niektóre proponowane zmiany** budzą istotne zastrzeżenia, ponieważ **mogą negatywnie wpłynąć na poziom ochrony** przysługujący osobom, tworzyć niepewność prawną oraz utrudniać stosowanie przepisów o ochronie danych.

– *Zdecydowanie apelujemy, aby nie przyjmować proponowanych zmian definicji danych osobowych. Zmiany te nie są zgodne z orzecznictwem Trybunału i prowadziłyby do znaczącego zawężenia pojęcia danych osobowych. Musimy mieć pewność, że wszelkie zmiany RODO i EUDPR rzeczywiście doprecyzowują obowiązki i zwiększają pewność prawa, jednocześnie utrzymując zaufanie i wysoki poziom ochrony praw i wolności jednostki* – podkreślił **Europejski Inspektor Ochrony Danych, prof. Wojciech Wiewiórowski.**

EROD i EIOD apelują do współprawodawców, aby **nie przyjmowali proponowanych zmian definicji danych osobowych**, ponieważ wykraczają one daleko poza zakres technicznej lub ukierunkowanej nowelizacji RODO. Ponadto **nie odzwierciedlają one orzecznictwa TSUE** i prowadziłyby do **znaczącego**

zawężenia pojęcia danych osobowych. Komisja Europejska nie powinna otrzymać uprawnienia do określania, w drodze aktu wykonawczego, jakie dane po pseudonimizacji nie są już danymi osobowymi, gdyż **wpływa to bezpośrednio na zakres stosowania unijnego prawa ochrony danych.**

– *Uproszczenia są niezbędne, aby ograniczyć biurokrację i wzmocnić konkurencyjność UE, ale nie kosztem praw podstawowych. Z zadowoleniem przyjmujemy działania Komisji na rzecz większej harmonizacji, spójności i pewności prawa. Jednak zdecydowanie apelujemy, aby nie przyjmować proponowanych zmian definicji danych osobowych, ponieważ mogą one znacząco osłabić ochronę danych jednostek* – powiedziała **przewodnicząca EROD, Anu Talus.**

Kroki w dobrym kierunku

EROD i EIOD **popierają podniesienie progu ryzyka**, **od którego powstaje obowiązek zgłoszenia naruszeni**a ochrony danych do właściwego organu nadzorczego, oraz **wydłużenie terminu na dokonanie takiego zgłoszenia**. Zmiany te mogłyby **znacząco zmniejszyć obciążenia administracyjne organizacji, nie obniżając poziomu ochrony** danych osobowych. Pozytywnie oceniono również propozycję **wprowadzenia wspólnych wzorów zgłoszeń naruszeń oraz list kontrolnych** dla ocen skutków dla ochrony danych.

EROD i EIOD z zadowoleniem przyjmują także propozycję wprowadzenia **nowego wyjątku umożliwiającego przetwarzanie szczególnych kategorii danych na potrzeby uwierzytelniania biometrycznego**, gdy środki weryfikacji znajdują się pod wyłączną kontrolą osoby. Popierają również **harmonizację pojęcia „badań naukowych"** oraz powiązanych zmian, ponieważ zwiększają one **pewność prawa i wspierają spójność** regulacyjną.

Zmiany wymagające dopracowania

Jak wskazano w opinii EROD 28/2024 dotyczącej modeli AI, prawnie uzasadniony interes może w niektórych przypadkach stanowić podstawę prawną przetwarzania w kontekście rozwoju i wdrażania modeli lub systemów AI. Dlatego EROD i EIOD nie uważają za konieczne wprowadzania do RODO szczególnego przepisu w tym zakresie. **EROD i EIOD pozytywnie oceniają zamiar wprowadzenia szczególnego wyjątku od zakazu przetwarzania danych wrażliwych, pod pewnymi warunkami, obejmującego incydentalne i szczątkowe przetwarzanie takich danych w kontekście rozwoju i działania systemów lub modeli AI.** Zalecają jednak doprecyzowanie zakresu wyjątku oraz zapewnienie odpowiednich zabezpieczeń na każdym etapie cyklu życia danych.

EROD i EIOD zgadzają się z celem Komisji, jakim jest zapewnienie administratorom większej jasności prawnej w sytuacjach nadużywania praw przez osoby, których dane dotyczą. Uważają jednak, że **wyko-**

nywanie prawa dostępu w celach innych niż ochrona danych osobowych nie powinno być elementem definiującym nadużycie. W odniesieniu do nowego wyjątku dotyczącego obowiązków informacyjnych, EROD i EIOD popierają **uproszczenie wymogów i zmniejszenie obciążeń administracyjnych, zwłaszcza dla MŚP,** ale sugerują doprecyzowania, aby zapewnić pewność prawa i **zagwarantować, że osoby fizyczne nadal będą mogły otrzymać istotne informacje o swoich danych**, gdy będzie to konieczne.

Ostatnia grupa zmian dotyczy zautomatyzowanego podejmowania decyzji indywidualnych – EROD i EIOD wskazują, że przepisy te wymagają doprecyzowania, aby były znaczące i prawnie spójne.

Zmiany w dyrektywie ePrivacy

EROD i EIOD popierają cel polegający na znalezieniu rozwiązania regulacyjnego dla problemu „zmęczenia zgodami" oraz nadmiaru banerów cookie. Dotyczy to m.in. **proponowanych wymogów dotyczących stosowania zautomatyzowanych i możliwych do odczytu maszynowego sygnałów wyrażających wybory użytkowników dotyczące przetwarzania ich danych**. Wykorzystanie środków technicznych może ułatwić administratorom zgodność z przepisami oraz pomóc osobom w skutecznym egzekwowaniu ich wyborów on-line.

EROD i EIOD pozytywnie oceniają również ograniczone dodatkowe wyjątki od ogólnego zakazu przechowywania lub uzyskiwania dostępu do danych w urządzeniach końcowych. Zachęcają współprawodawców **do promowania reklamy kontekstowej zamiast behawioralnej** poprzez **dodanie szczególnego wyjątku otoczonego odpowiednimi zabezpieczeniami**.

Obie instytucje z zadowoleniem przyjmują także fakt, że nadzór nad tymi kwestiami zostanie powierzony organom ochrony danych. Jednocześnie **podkreślają trudności prawne i techniczne wynikające z współistnienia dwóch różnych reżimów dla danych osobowych i nieosobowych**. Przedstawiają także dodatkowe rekomendacje mające na celu **zwiększenie pewności prawa, minimalizację ryzyka oraz wspieranie odpowiedzialnej innowacji.**

Zmiany w *Data Acquis*

EROD i EIOD popierają uproszczenie *Data Acquis* poprzez **włączenie do Data Act przepisów Data Governance Act oraz dyrektywy Open Data** dotyczących **ponownego wykorzystywania danych i dokumentów będących w posiadaniu podmiotów sektora publicznego.** W odniesieniu do dostępu przyznawanego przez podmioty publiczne na potrzeby ponownego wykorzystywania danych zalecają utrzymanie jasności obecnych przepisów – w szczególności tego, że **nie nakładają one obowiązku umożliwienia ponownego wykorzystywania danych ani nie stanowią podstawy prawnej do udzielania takiego dostępu**.

5 SPRAWY MIĘDZYNARODOWE

W kontekście sytuacji nadzwyczajnych EROD i EIOD zalecają **potwierdzenie, że dane osobowe mogą być udostępniane podmiotom sektora publicznego wyłącznie w formie pseudonimizowanej**, jeśli dane anonimowe są niewystarczające do reagowania na sytuację kryzysową. W odniesieniu do usług pośrednictwa danych i organizacji altruizmu danych EROD i EIOD **podkreślają znaczenie odpowiedzialnego i godnego zaufania udostępniania danych**. Zalecają **utrzymanie szczególnych zabezpieczeń, promowanie przejrzystości i nadzoru.**

EROD i EIOD rekomendują dalsze **uspójnienie przepisów dotyczących egzekwowania prawa** (np. poprzez **umożliwienie wymiany informacji między organami regulacyjnymi**, w tym organami ochrony danych, oraz doprecyzowanie roli organów ochrony danych w egzekwowaniu Data Act). Z zadowoleniem przyjmują też potwierdzenie roli Europejskiej Rady ds. Innowacji w Dziedzinie Danych (EDIB) we wspieraniu spójnego stosowania Data Act. W odniesieniu do wytycznych zalecają **umożliwienie Komisji wydawania wytycznych dotyczących dowolnego aspektu Data Act oraz doprecyzowanie roli EDIB jako organu wspierającego Komisję** w tym procesie. Pozwoliłoby to Komisji opracowywać wspólne wytyczne z EROD, a EDIB – doradzać i wspierać Komisję w ich przygotowaniu.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych:

Digital Omnibus: EDPB and EDPS support simplification and competitiveness while raising key concerns | European Data Protection Board

PROGRAM PRAC EROD NA LATA 2026–2027: UŁATWIANIE ZGODNOŚCI I WZMACNIANIE WSPÓŁPRACY W ZMIENIAJĄCYM SIĘ ŚRODOWISKU CYFROWYM

Podczas ostatniego posiedzenia plenarnego Europejska Rada Ochrony Danych przyjęła program prac na lata 2026–2027. Jest to drugi program wspierający realizację strategii EROD na lata 2024–2027. Przewiduje w nim ściślejsze współdziałanie między organami regulacyjnymi, wydanie nowych wytycznych oraz wspieranie dialogu ze wszystkimi interesariuszami.

Dokument opiera się na priorytetach określonych w strategii oraz na potrzebach uznanych za najistotniejsze dla administratorów, podmiotów przetwarzających i innych interesariuszy. Uwzględnia również **zobowiązania wynikające z Deklaracji Helsińskiej,** której celem jest zwiększenie przejrzystości, wsparcia i zaangażowania, a także ułatwienie zgodności z RODO, wzmocnienie spójności oraz rozwój współpracy między organami regulacyjnymi. Program prac opiera się na czterech filarach strategii EROD i koncentruje się na:

1. zwiększaniu harmonizacji i promowaniu zgodności,
2. wzmacnianiu wspólnej kultury egzekwowania przepisów i skutecznej współpracy,
3. ochronie danych w rozwijającym się, wieloregulatorowym środowisku cyfrowym,
4. wspieraniu globalnego dialogu na temat ochrony danych.

Przedłużenie ważności decyzji umożliwi organizacjom i właściwym organom z siedzibą w Europie dalsze przekazywanie danych do podmiotów i organów z siedzibą w Wielkiej Brytanii bez konieczności wdrażania dodatkowych zabezpieczeń.

Zwiększanie harmonizacji i promowanie zgodności

EROD **będzie kontynuować opracowywanie terminowych i jasnych wytycznych dotyczących kluczowych zagadnień prawa ochrony danych** w UE, aby ułatwić zgodność z RODO. Wśród prac znajdują się m.in. **wytyczne dotyczące modeli „zgoda lub zapłać", anonimizacji, pseudonimizacji oraz danych dzieci.** Ważnym elementem programu jest rozwój narzędzi skierowanych do szerokiego grona odbiorców, w tym osób niebędących ekspertami. EROD zapowiedziała **przygotowanie zestawu praktycznych materiałów,** takich jak:

- szablony,
- przykłady,
- listy kontrolne,
- FAQ,
- przewodniki „how-to”.

W ramach inicjatywy ułatwiania zgodności z RODO **Rada zdecydowała o opracowaniu nowych, gotowych do użycia szablonów**, które mają wspierać administratorów w codziennej pracy. Po konsultacjach publicznych EROD zapowiedziała przygotowanie szablonów:

- **oceny prawnie uzasadnionego interesu** (LIA),
- rejestru czynności przetwarzania,
- klauzul informacyjnych i polityk prywatności,
- a także wcześniej zapowiedzianych **szablonów zgłoszeń naruszeń i ocen skutków dla ochrony danych** (DPIA).

Działania te są **zgodne z celami Deklaracji Helsińskiej**, która podkreśla konieczność wzmacniania dialogu z interesariuszami i ułatwiania zgodności z RODO. Rada będzie również **doradzać unijnym prawodawcom w kwestiach związanych z ochroną danych osobowych**, w tym **opiniować projekty aktów prawnych** – wspólnie z EIOD, m.in. w ramach **opinii dotyczących Digital Omnibus** – w odpowiedzi na wnioski KE.

Wzmacnianie wspólnej kultury egzekwowania przepisów i skutecznej współpracy

– *Będziemy nadal współpracować, aby zapewnić większą spójność w całej Europie i wzmocnić współpracę między organami ochrony danych. Zobowiązania, które podjęliśmy w ubiegłym roku w Deklaracji Helsińskiej, będą naszym drogowskazem. Wykorzystamy także możliwości wynikające z niedawno przyjętego rozporządzenia w sprawie przepisów proceduralnych RODO* – zaznacza Przewodnicząca EROD, Anu Talus.

EROD pozostanie **forum regularnej wymiany informacji o toczących się sprawach, wiedzy eksperckiej i dobrych praktyk między organami ochrony danych**. Rada będzie kontynuować **rozwój narzędzi wspierających egzekwowanie przepisów i współpracę** oraz dbać o sprawne **funkcjonowanie mechanizmu spójności**. W programie przewidziano również **ocenę i rozwój narzędzi oraz systemów IT wykorzystywanych przez Radę**, aby usprawnić współpracę transgraniczną i procesy decyzyjne.

5 SPRAWY MIĘDZYNARODOWE

Ochrona danych w rozwijającym się środowisku cyfrowym i z wieloma regulatorami

EROD będzie promować **podejście zorientowane na człowieka w odniesieniu do nowych technologii**, m.in. poprzez przyjęcie **wytycznych dotyczących generatywnej sztucznej inteligencji oraz pozyskiwania danych** (data scraping). Rada będzie **aktywnie współpracować z innymi organami regulacyjnymi,** wspierając nowe środowisko wieloregulatorowe. EROD będzie kontynuować udział w istotnych gremiach, takich jak:

- Grupa Wysokiego Szczebla ds. Aktu o Rynkach Cyfrowych (DMA),
- Europejska Rada ds. Usług Cyfrowych,
- Europejska Rada ds. Innowacji w Dziedzinie Danych.

Rada będzie **opracowywać wspólne stanowiska i wytyczne dotyczące współistnienia różnych reżimów regulacyjnych**, dbając o **spójne i skuteczne zabezpieczenia ochrony danych**. Wśród planowanych dokumentów znajdują się m.in. wspólne wytyczne dotyczące relacji między Aktem o Sztucznej Inteligencji a RODO oraz **wytyczne dotyczące reklamy politycznej**.

Wspieranie globalnego dialogu na temat ochrony danych

EROD zobowiązuje się do **promowania globalnego dialogu na temat prywatności i ochrony danych**, ze szczególnym uwzględnieniem współpracy międzynarodowej w zakresie egzekwowania przepisów – zarówno między członkami Rady, jak i z organami państw trzecich. Rada będzie kontynuować **inicjatywy ścisłej współpracy z organami z krajów lub organizacji**, wobec których obowiązuje decyzja stwierdzająca odpowiedni poziom ochrony.

EROD będzie też kontynuować **prace nad mechanizmami transferu danych wynikającymi z** RODO i dyrektywy LED oraz udzielać dalszych **wskazówek dotyczących ich praktycznego stosowania**. Rada pozostanie aktywna na arenie międzynarodowej, dbając o wymianę informacji i współpracę między członkami EROD uczestniczącymi w globalnych forach.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

EDPB work programme 2026-2027: easing compliance and strengthening cooperation across the evolving digital landscape | European Data Protection Board

Making GDPR compliance easier through new initiatives: a key focus of the EDPB work programme 2026-2027 | European Data Protection Board

EROD IDENTYFIKUJE WYZWANIA UTRUDNIAJĄCE PEŁNĄ REALIZACJĘ PRAWA DO USUNIĘCIA DANYCH

Europejska Rada Ochrony Danych przyjęła raport dotyczący działań prowadzonych w ramach Skoncentrowanego Wspólnego Egzekwowania (CEF) w obszarze prawa do bycia zapomnianym (art. 17 RODO). Prawo do usunięcia danych jest jednym z najczęściej wykonywanych praw wynikających z RODO, a organy nadzorcze regularnie otrzymują skargi dotyczące jego realizacji. Głównym celem tej skoordynowanej akcji było zapewnienie, aby prawo do usunięcia danych było skutecznie wykonywane przez osoby w całej Europie, oraz zrozumienie, w jaki sposób administratorzy realizują je w praktyce. Ponadto EROD zidentyfikowała dobre praktyki oraz najważniejsze wyzwania związane z tym prawem, aby móc opracować dalsze wytyczne.

W 2025 r. w inicjatywie wzięły udział **32 organy ochrony danych w Europie**. W szczególności **9 organów wszczęło nowe postępowania formalne** lub kontynuowało już trwające, natomiast **23 organy przeprowadziły działania o charakterze informacyjnym i analitycznym**. Łącznie **odpowiedzi udzieliło 764 administratorów** z całej Europy, od małych i średnich przedsiębiorstw po duże firmy działające w wielu sektorach, a także różne podmioty publiczne. Wyniki działań krajowych zostały zagregowane i przeanalizowane, co umożliwiło ukierunkowane działania następcze tak na poziomie krajowym, jak i unijnym.

Obszary wymagające poprawy i główne wyzwania

Raport przedstawia problemy zidentyfikowane przez organy nadzorcze oraz zawiera **rekomendacje dla administratorów, które mają pomóc im w prawidłowej realizacji prawa do usunięcia danych.** Organy nadzorcze wskazały **siedem powtarzających się głównych wyzwań.** Wyniki potwierdziły część ustaleń z koordynowanej akcji z 2024 r. dotyczącej prawa dostępu – m.in**. brak odpowiednich procedur wewnętrznych do obsługi wniosków i niewystarczające informowanie osób o sposobie realizacji ich praw.** Dodatkowo organy zgłosiły problemy specyficzne dla prawa do usunięcia danych, takie jak:

- stosowanie przez niektórych administratorów nieskutecznych technik anonimizacji jako alternatywy dla faktycznego usunięcia danych,
- niespójne praktyki w zakresie realizacji prawa do usunięcia,
- trudności w ustalaniu okresów przechowywania danych,
- problemy z usuwaniem danych w kontekście kopii zapasowych.

5 SPRAWY MIĘDZYNARODOWE:

Ponieważ **prawo do usunięcia nie ma charakteru absolutnego**, część administratorów ma trudności z oceną i ze stosowaniem przesłanek umożliwiających jego realizację, w tym z **przeprowadzaniem testów równowagi między prawem do usunięcia a innymi prawami i wolnościami.**

Działania następcze wspierające zgodność

Na poziomie krajowym istnieje **już szeroki zestaw wytycznych, dokumentów i szablonów,** które pomagają administratorom w realizacji prawa do usunięcia danych oraz wspierają osoby w korzystaniu z tego prawa. Zgodnie z **celami Deklaracji Helsińskie**j – ułatwienia zgodności z RODO oraz zapewnienia spójnej interpretacji i egzekwowania przepisów w całej Europie – **EROD planuje wykorzystać te istniejące materiały na poziomie unijnym** tam, gdzie będzie to właściwe.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

EDPB identifies challenges hindering the full implementation of the right to erasure | European Data Protection Board

OBRAZY GENEROWANE PRZEZ AI A OCHRONA PRYWATNOŚCI: EROD POPIERA WSPÓLNE OŚWIADCZENIE GLOBAL PRIVACY ASSEMBLY

Przewodnicząca Europejskiej Rady Ochrony Danych, Anu Talus, podpisała w imieniu Rady wspólne oświadczenie dotyczące obrazów generowanych przez sztuczną inteligencję i ochrony prywatności.

Oświadczenie zostało przygotowane przez Grupę Roboczą ds. Międzynarodowej Współpracy w Egzekwowaniu Przepisów (IEWG) działającą w ramach Global Privacy Assembly (GPA) i reprezentuje wspólne stanowisko **61 organów ochrony danych z całego świata**. Dokument ten odzwierciedla zaangażowanie EROD w globalny dialog na temat ochrony danych, zgodnie z **czwartym filarem programu prac Rady na lata 2026–2027.**

Rosnące zagrożenia związane z generowaniem realistycznych obrazów i nagrań

Oświadczenie odnosi się do poważnych obaw dotyczących systemów AI, które generują realistyczne obrazy i nagrania przedstawiające możliwe do zidentyfikowania osoby, bez ich wiedzy lub zgody. Choć sztuczna inteligencja może przynieść liczne korzyści dla społeczeństwa, jej szybki rozwój, zwłaszcza integracja generatorów obrazów i wideo z powszechnie dostępnymi platformami społecznościowymi, umożliwi tworzenie:

- niezamówionych, intymnych materiałów przedstawiających prawdziwe osoby,
- treści zniesławiających,
- innych szkodliwych materiałów wykorzystujących wizerunek jednostek.

Szczególny niepokój budzą potencjalne szkody wobec dzieci i innych grup wrażliwych, w tym ryzyko cyberprzemocy i wykorzystywania.

Oczekiwania wobec organizacji

Sygnatariusze przypominają, że organizacje tworzące i wykorzystujące systemy generowania treści za pomocą AI muszą działać zgodnie z obowiązującymi przepisami, w tym dotyczącymi ochrony danych i prywatności. Niezależnie od różnic w przepisach poszczególnych państw wszystkie organizacje powinny kierować się wspólnymi zasadami:

- **wdrażanie solidnych zabezpieczeń**,
- **zapewnienie rzeczywistej przejrzystości**,
- **zapewnienie skutecznych i dostępnych mechanizmów ochrony osób**,
- **uwzględnianie szczególnych zagrożeń dla dzieci**.

Wspólne działania wobec globalnego ryzyka

Szkody wynikające z niezamierzonego generowania intymnych, zniesławiających lub innych szkodliwych treści przedstawiających prawdziwe osoby są poważne i wymagają pilnej reakcji regulacyjnej. **Sygnatariusze zobowiązują się do wspólnego działania i wymiany informacji na temat stosowanych podejść i środków zaradczych**. W oświadczeniu wezwano organizacje do:

- aktywnego dialogu z regulatorami,
- wdrażania odpowiednich zabezpieczeń już na etapie projektowania systemów,
- zapewnienia, że rozwój technologiczny nie będzie odbywał się kosztem prywatności, godności, bezpieczeństwa i innych praw podstawowych — zwłaszcza osób najbardziej narażonych.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

AI-generated imagery and protection of privacy: EDPB supports joint Global Privacy Assembly's statement | European Data Protection Board

SPOTKANIE EKSPERTÓW W BIRD & BIRD BUDAPEST: O PRZYSZŁOŚCI REGULACJI DANYCH I SZTUCZNEJ INTELIGENCJI W EUROPIE

25 lutego w siedzibie Bird & Bird w Budapeszcie odbyło się spotkanie poświęcone najnowszym europejskim inicjatywom regulacyjnym w obszarze ochrony danych oraz AI. W wydarzeniu uczestniczyli przedstawiciele organów nadzorczych, środowiska akademickiego oraz sektora prywatnego z Węgier i Polski. UODO reprezentował Krzysztof Król, zastępca Dyrektorki Departamentu Współpracy Międzynarodowej.

Gospodarzem wydarzenia był Bálint Halász, partner w Bird & Bird Budapest, który poprowadził zarówno część wprowadzającą, jak i późniejszą dyskusję panelową. Spotkanie otworzyła sesja networkingowa, po której uczestnicy wysłuchali wykładu Pétera Báldyego dotyczącego najnowszych europejskich prac nad tzw. Digital Omnibus Package.

Krytyczna analiza założeń Omnibusa

W swoim wystąpieniu Péter Báldy zwrócił uwagę na szereg wyzwań związanych z propozycjami Komisji Europejskiej. Podkreślił, że cele wskazane w Omnibusie są, jego zdaniem, **nierealistyczne i obarczone ryzykiem nadmiernego obciążenia administratorów**. Wskazał, że:

- **trzy główne cele KE, EROD i EIOD mogą się okazać nieosiągalne w praktyce,**
- wprowadzanie przepisów dotyczących ochrony danych w ramach Omnibusa AI, a nie Omnibusa RODO**, budzi poważne wątpliwości systemowe**,
- nadmierne skupienie na tworzeniu nowych standardów **może być nieefektywne**, skoro istnieją już narzędzia RODO, takie jak art. 22 czy art. 35,
- obecne podejście **koncentruje się bardziej na bezpieczeństwie danych niż na ochronie praw osób**, co rozmywa pierwotny cel RODO, jakim, zgodnie z motywem 4, jest służenie ludzkości.

Wskazał również, że studenci prawa często nie dostrzegają tego fundamentalnego celu RODO, co według niego odzwierciedla szerszy problem w debacie publicznej.

Perspektywa organów nadzorczych

Julia Sziklay, wiceprzewodnicząca NAIH, przedstawiła główne wątki wspólnej opinii EROD i EIOD dotyczącej Omnibusa. Podkreśliła:

- **wysoki poziom zgodności między członkami EROD,**
- **duże zaangażowanie w prace** grup roboczych i posiedzeń plenarnych,
- potrzebę **spójnego podejścia do nowych regulacji**, zwłaszcza w kontekście dynamicznego rozwoju technologii AI.

Dyskusja panelowa: praktyczne wyzwania dla administratorów

W panelu, obok przedstawicieli organów nadzorczych, udział wzięli reprezentanci sektora prywatnego: Meta oraz Yettel Hungary. Rozmowa koncentrowała się na praktycznych skutkach projektowanych regulacji. Oto jej najważniejsze wątki:

- **Zgłaszanie naruszeń** – przedstawiciele biznesu wyrazili potrzebę doprecyzowania kryteriów identyfikacji naruszeń oraz ich poziomów.
- **Cookie walls** – wskazano, że obserwacja praktyk rynkowych może pomóc w ocenie, które podmioty już stosują takie rozwiązania; Meta postulowała większą aktywność KE w tym obszarze.
- **Realizacja praw osób** – administratorzy podkreślali, że jest to obszar trudny operacyjnie, a propozycje Omnibusa mogą stanowić krok w dobrym kierunku, o ile zostaną odpowiednio doprecyzowane.

Znaczenie dialogu między regulatorami a rynkiem

Spotkanie w Bird & Bird Budapest pokazało, jak ważna jest **wymiana doświadczeń między regulatorami, praktykami i przedstawicielami biznesu**. Dynamiczny rozwój sztucznej inteligencji oraz równoległe prace nad nowymi ramami regulacyjnymi wymagają stałego dialogu, aby zapewnić spójność i skuteczność systemu ochrony danych w Europie. Organizatorzy podkreślili, że planowane są kolejne spotkania tego typu, które mają wspierać wspólne zrozumienie wyzwań i wypracowywanie praktycznych rozwiązań.

5 SPRAWY MIĘDZYNARODOWE:

PRZEDSTAWICIELE UODO Z WIZYTĄ W HELSINKACH – WYMIANA DOŚWIADCZEŃ W ZAKRESIE WDRAŻANIA DGA

W dniach 9–13 marca delegacja Urzędu Ochrony Danych Osobowych wzięła udział w wizycie studyjnej w Helsinkach, zorganizowanej w ramach inicjatywy flagowej PACE Instrumentu Wsparcia Technicznego (TSI), programu Komisji Europejskiej. Celem wizyty jest wymiana doświadczeń między organami administracji odpowiedzialnymi za wdrażanie Aktu w sprawie zarządzania danymi. Dlatego wizyta była szczególnie istotne w kontekście trwających w polskim Parlamencie prac nad ustawą implementującą te przepisy.

W wyjeździe uczestniczyli przedstawiciele Departamentu Innowacyjności i Zarządzania Danymi: Agata Czekaj, Aleksandra Grabowska-Kral, Aleksandra Spyra i Artur Kalinowski, a także Iwona Piórkowska-Kapica z Departamentu Inicjatyw Edukacyjnych. Pierwszego dnia delegacja odwiedziła Traficom, czyli Fińską Agencję Transportu i Komunikacji.

Dzień pierwszy – wymiana informacji o strukturze i działaniu urzędów

Przedstawiciele UODO przedstawili prezentację dotyczącą takich kwestii jak: **konstytucyjne podstawy ochrony prywatności** (art. 47, art. 49 i art. 51 ustawy zasadniczej), tła historycznego działalności Urzędu i jej **podstaw prawnych** (ustawy z 1997 r. i z 2018 r.), **a także statutu UODO**. Przedstawiono też **sylwetki Prezesa oraz wiceprezesów UODO**, działalność Departamentu Innowacyjności i Zarządzania danymi, (w tym statystyki), a także **omówiono proces implementacji DGA w Polsce**.

Z kolei pracownicy Traficomu przybliżyli działalność **„Data Economy Unit”** (Jednostka ds. Ekonomii Danych) która działa **od stycznia 2023 r.** Powstała ona ze względu na, planowane wówczas, rozpoczęcie obowiązywania DGA. Jednak oprócz tego aktu, DEU pracuje także nad Aktem o usługach cyfrowych (DSA), Aktem w sprawie sztucznej inteligencji (AI Act), Aktem w sprawie danych (DA), oraz Rozporządzeniami ws. przeciwdziałania rozpowszechnianiu w internecie treści o charakterze terrorystycznym i ws. ram swobodnego przepływu danych nieosobowych w Unii Europejskiej. Do zadań jednostki należą też: **wspieranie i kooperacja w przygotowaniu implementacji aktów prawnych UE, informowanie interesariuszy o regulacjach, udział w pracach EU Board i doradzanie ws. zobowiązań operatorów i prawa użytkowników**.

Podczas drugiej sesji tego dnia wizyty przedstawiono natomiast strukturę organizacyjną Traficomu, w tym liczbę pracowników (1160) oraz budżet agencji, a także jego perspektywach i spostrzeżeniach dla UE czy spraw międzynarodowych. **Zadaniem Trafikomu jest zapewnienie bezpieczeństwa zarówno w ruchu powietrznym, jak i procesie cyfryzacji.** Podejmuje on również działania prewencyjne, prowadzi rejestry

i statystyki a nawet - wykonuje prace związane z programami kosmicznymi. **Traficom jest instytucją niezależną w swojej działalności.**

W części przeznaczonej na pytania polscy delegaci chcieli dowiedzieć się przede wszystkim, **w jaki sposób fińskie instytucje osiągnęły tak wysoki wskaźnik zaufania społecznego.**

Fińskie doświadczenia mogą być pomocne przy wdrażaniu DGA

Trzecia sesja poświęcona była ustawie implementującej w Finlandii DGA. Państwo to jako **pierwsze w UE dokonało wdrożenia DGA, obowiązującego już od 24 września 2023 r.** Ustawa implementująca **obejmuje swoim zakresem również Akt o danych (DA).** Pierwsza fińska organizacja pośrednictwa danych **została zarejestrowana już w styczniu 2024 r.** Z kolei pierwszą taką **organizację spoza UE zarejestrowano zaś w czerwcu 2024 r.** – pochodziła ona z Wielkiej Brytanii.

Traficom ma prawo do **udzielania ostrzeżeń oraz upomnień** podmiotom, które naruszą DGA. Urząd wyznacza im też **czas na naprawienie błędu**. Jeśli nie zrobią tego w terminie, może **nałożyć kary pieniężne od 1 tys. do 100 tys. euro**. Ich względnie niska wysokość (np. w porównaniu z tymi przewidzianymi w RODO) wynika z faktu, że większość organizacji pośrednictwa danych to start-upy, nie dysponujące wielkimi budżetami. Traficom, w ramach priorytetyzowania swoich zadań, może jednak odmówić wszczęcia postępowania w niektórych przypadkach.

Wnioski po pierwszym dniu:

- Traficom, w odróżnieniu od UODO, zajmuje się także sprawami transportu (obok kwestii ochrony danych osobowych).
- **W Finlandii ustawa wdrażająca DGA obowiązuje od stycznia 2024 r.**, w Polsce trwają prace legislacyjne w parlamencie.
- **Zakres kar za nieprzestrzeganie DGA w Finlandii jest znacznie niższy** niż w polskim projekcie ustawy implementującej.
- Organ fiński ma **możliwość prioretyzacji zadań, a nawet odstąpienie od podjęcia postępowania** w niektórych przypadkach.
- **Digitalizacja w Finlandii jest bardziej rozwinięta**, niż w Polsce.

5 SPRAWY MIĘDZYNARODOWE:

Dzień drugi: jak działa fiński system pośrednictwa danych

10 marca 2026 r. w siedzibie Traficom w Helsinkach odbyło się kolejne spotkanie, tym razem poświęcone **praktycznym aspektom wdrażania przepisów Data Governance Act oraz funkcjonowania systemu pośrednictwa danych**. Kwestie te omówiono w panelu pt. DGA in practice continues and Traficom's views on Digital Omnibus". Drugi blok tematyczny, przygotowany przez Data Space Europe Oy, nosił nazwę: „Experiences from the first registered data intermediary".

Prezentację w tej sprawie przedstawiła Jaana Sinipuro, CEO DataSpace Europe Oy, która posiada wieloletnie doświadczenie w obszarze analityki danych i od trzech lat jest związana z firmą. W wystąpieniu pokazano całą genezę powstania tej spółki – od koncepcji w 2016 r. gdy utworzono projekt Cinia. Następnie w 2018 r. rozwinięto go do postaci pierwszej wersji platformy ValueNet. Jej celem było m.in. stworzenie cyfrowego paszportu dla rolników. System ten został następnie zmodernizowany w 2022 r. do rozwiązania Tritom tj. infrastruktury służącej do pośrednictwa danych. W tym samym roku powstała spółka Data Space Europe Oy, która w styczniu 2024 r. została zarejestrowana jako organizacja pośrednictwa danych.

Data Space Europe Oy – model i zasady działania

Podkreślono, że **główną rolą DSE, jako należącej do kategorii tzw. „data flows", jest ułatwianie przepływu danych pomiędzy przedsiębiorstwami,** opartymi na zgodzie oraz odpowiednich uprawnieniach („permission flows"). Aspekt komercyjny działalności pozostaje drugorzędny, bowiem **kluczowe znaczenie ma budowanie standardów umożliwiających bezpieczne i zgodne z prawem ponowne wykorzystanie danych** oraz tworzenie zaufania między uczestnikami rynku.

Ten model działania określany jest jako „Data Sharing Pool". Obejmuje on **współpracę w modelu B2B**, **weryfikację zgód i pozwoleń** obu stron, zarządzanie udostępnianiem danych oraz **reprezentowanie interesów podmiotów należących do ekosystemu**. Kluczowe elementy modelu to: **interoperacyjność oparta na otwartych standardach, przejrzystość prawna oraz budowanie realnego rynku danych**.

Na czym polega międzynarodowa przestrzeń wymiany danych?

W dalszej części umówione zostały **podstawowe zasady funkcjonowania międzynarodowych przes-**

trzeni danych, takie jak: „Twoje dane — Twój wybór", „ufaj, ale sprawdzaj", zdecentralizowana i **neutralna infrastruktura, interoperacyjność** poprzez otwarte standardy oraz **bezpieczne, oparte na zgodzie przepływy danych**.

Usługi pośrednictwa danych mogą przyjmować różne formy organizacyjne, m.in. **systemów zarządzania informacją osobową (PIMS), spółdzielni danych, trustów danych, unii danych, rynków danych czy właśnie „data sharing pools".** Zastosowania tego typu rozwiązań obejmują wiele sektorów gospodarki, w szczególności **zdrowie i zdrowie publiczne, transport i mobilność, platformy internetowe i systemy IT, finanse i ubezpieczenia, rolnictwo i żywność, edukację i badania, a także działania związane ze środowiskiem i klimatem**. Jak podkreślono w prezentacji, rozwój usług pośrednictwa **danych wymaga wsparcia ze strony sektora publicznego**, a model ten, mimo że wciąż się rozwija, ma potencjał, aby w przyszłości funkcjonować jako samowystarczalny i trwały model biznesowy.

Wdrażanie DGA w praktyce – pytania i odpowiedzi

Polska delegacja aktywnie uczestniczyła w dyskusji, zadając **szereg pytań o praktyczne aspekty wdrażania DGA**, w tym **formularza do zgłaszania organizacji pośrednictwa danych**. Eksperci z Traficom, Päivi Karkkola oraz Jussi Kataja – szczegółowo omówili fińskie doświadczenia w implementacji tych przepisów oraz odpowiedzieli na pytania naszych przedstawicieli.

1. *Jak wyglądały Wasze przygotowania do wdrożenia procedury rejestracji organizacji pośrednictwa danych i jak długo trwały? Jaki był Wasz pierwszy krok?*

W pierwszej kolejności skoncentrowano się na **analizie wymagań ustawowych** oraz ustaleniu, w jaki sposób zorganizować **proces rejestracyjny, aby był możliwie prosty oraz efektywny** dla urzędu, a jednocześnie **spełniał wszystkie wynikające z DGA wymogi** dotyczące procesu rejestracyjnego.

2. *Które z kryteriów zawartych w art. 12 DGA sprawiły najwięcej trudności interpretacyjnych?*

Największe trudności wynikały z nieprecyzyjnych sformułowań użytych w rozporządzeniu. W szczególności problematyczne były kwestie wskazane w obszernym, (ok. 85 stron) dokumencie interpretacyjnym dotyczącym zagadnień, które mogły potencjalnie sprawiać kłopoty. **Wątpliwości dotyczyły m.in. przepisów odnoszących się do cyberbezpieczeństwa oraz pojęć takich jak „odpowiednie zasoby techniczne"**, których zakres jest trudny do jednoznacznego określenia.

5 SPRAWY MIĘDZYNARODOWE:

3. *Jakich dokumentów wymagacie od organizacji na potwierdzenie spełniania wymagań określonych w art. 12 DGA?*

Zakres wymaganej dokumentacji zależy m.in. od tego, czy organizacja zamierza korzystać z oznaczenia przewidzianego w ramach systemu. W przypadku ubiegania się o takie oznaczenie **proces weryfikacji jest bardziej złożony i wymaga dokładniejszej analizy dokumentów**. W praktyce jednak agencja stara się **ograniczać wymagania formalne do niezbędnego minimum** – organizacje przekazują głównie informacje umożliwiające ocenę spełnienia wymogów ustawowych, natomiast **szczegółowe dokumenty mogą być wymagane na późniejszym etapie w celu potwierdzenia przekazanych informacji.**

4. Czy i jakie wyzwania pojawiły się w związku z rejestracją pierwszych organizacji pośrednictwa danych?

W toku pierwszych postępowań pojawiły się m.in. **problemy związane z zakresem informacji publikowanych w rejestrze** oraz **koniecznością uzupełniania braków formalnych** przez wnioskodawców. Inne trudności dotyczyły też **reprezentacji podmiotów i braku przekazania przez Komisję Europejską danych kontaktowych** do zarejestrowanych organizacji (Finlandia musiała sama się o nie zwrócić). Część tych zagadnień została następnie wyjaśniona w materiałach typu Q&A. W odpowiedz podkreślono, że **pomocne jest analizowanie praktycznych przykładów funkcjonowania pośrednictwa danych**, bo pozwala lepiej zrozumieć sposób przepływu i wykorzystywania danych w rzeczywistych procesach.

5. Jaki był podział kompetencji w departamentach, aby skutecznie wdrożyć DGA?

Istotną rolę w procesie odegrał **dział IT,** który **odpowiada za przygotowanie narzędzi technicznych i systemów obsługujących proces rejestracji.** Realizuje on rozwiązanie od początku do końca, w oparciu o wymagania określone przez jednostki merytoryczne, a w trakcie prac wprowadzane są niezbędne konsultacje i korekty.

6. Ile trwa procedura rejestracyjna organizacji pośrednictwa danych?

Procedura rejestracyjna trwa zazwyczaj **ok. tygodnia**, jej **długość zależy od tego, czy w toku postępowania pojawią się dodatkowe pytania lub konieczność uzupełnienia informacji** przez wnioskodawcę.

7. Jak wygląda nadzór nad zarejestrowanymi organizacjami pośrednictwa danych?

Nadzór ten **nie ma charakteru ciągłego**. W praktyce opiera się on przede wszystkim na spotkaniach organizowanych w formie zdalnej, podczas których **urząd wspiera organizacje w ich działalności oraz wyjaśnia ewentualne wątpliwości.** W przypadku określonych obowiązków sprawozdawczych **możliwe jest przeprowadzenie kontroli.**

8. Jakie wskazówki możecie przekazać Polsce przy wdrażaniu przepisów?

Podkreślono znaczenie prostoty procedur**. Rekomendowano przygotowanie formularzy rejestracyjnych w sposób przejrzysty i zrozumiały** dla użytkowników oraz zapewnienie ich szerokiej dostępno-ści. Podkreślono również **rolę wsparcia doradczego ze strony urzędu** oraz udzielania praktycznych wskazówek zainteresowanym podmiotom.

9. Czy macie jakieś toczące się obecnie procedury rejestracyjne?

Obecnie w **toku są dwa postępowania dotyczące rejestracji** organizacji pośrednictwa danych. Jednocześnie, **zainteresowanie rejestracją organizacji altruizmu danych jest niewielkie** - do tej pory nie zarejestrowano żadnej takiej organizacji ani nie prowadzi się obecnie postępowań w tym zakresie. **Potencjalną zachętą do rejestracji mogłoby być potwierdzanie przez organ publiczny bezpieczeństwa przetwarzania danych poprzez system certyfikacji**.

Wnioski po drugim dniu:

- **Departament**, który będzie rejestrował i nadzorował organizacje pośrednictwa danych, **powinien doszkolić się w zakresie ich form organizacyjnych**.
- **Formularze**, z którymi polska delegacja się zapoznała, mogą być **przydatne w procesie przygotowania formularzy, po wejściu w życie polskiej ustawy**.

W trakcie spotkania zwrócono też uwagę na praktyczne przykłady wykorzystania pośrednictwa danych. Wskazano m.in**. rozwiązanie stosowane przez Traficom, w którym po wprowadzeniu numeru rejestracyjnego pojazdu odpowiednia aplikacja umożliwia przekazanie warsztatowi samochodowemu danych technicznych pojazdu.** Podkreślono także, że w celu zwiększenia świadomości dotyczącej pośrednictwa danych oraz altruizmu danych organizowane są warsztaty i inne działania informacyjne. Jednocześnie, ze względu na ograniczone zasoby administracyjne prowadzenie szeroko zakrojonych działań promocyjnych w tym obszarze pozostaje wyzwaniem. Wskazano również na **potrzebę lepszego komunikowania potencjalnych korzyści biznesowych wynikających z wykorzystywania danych udostępnianych na podstawie przepisów DGA.**

5 SPRAWY MIĘDZYNARODOWE:

Dzień trzeci – spotkanie z Ministerstwem Transportu i Komunikacji

11 marca 2026 r. polska delegacja wzięła udział w spotkaniu z przedstawicielami Ministerstwa Transportu i Komunikacji Finlandii, które było poświęcone Strategii łączenia danych i Pakietowi Cyfrowemu.

Na wstępie przedstawione zostały zagadnienia łańcucha wartości danych i suwerenności danych. Analiza przeprowadzona w oparciu o łańcuch pozwala odpowiedzieć na pytania: **kto jest właścicielem źródła danych, kto ujednolica standardy i zarządza nimi, a kto infrastrukturą**, a także **kto kontroluje decyzje i ustalanie cen**. Z kolei suwerenność danych obejmuje następujące obszary: **otwarty rynek wewnętrzn**y i **uczciwa konkurencja**, **interoperacyjność i standaryzacja**, **potencjał i technologie kluczowe, zaufanie, bezpieczeństwo i regulacje** – podczas spotkania przedstawiono działania resorty w każdej z tych sfer.

W dalszej części zaprezentowano **również Strategia Danych 2020 oraz Strategia Unii Danych 2025**. Fińskie Ministerstwo przedstawiło też swoje stanowisko w kwestii Cyfrowego Omnibusa oraz działania, jakie w związku z nim podjęło. Wśród nich znalazły się: **aktywny dialog z fińskimi interesariuszami, szerokie poparcie dla podjętych działań oraz ambicji Komisji**. W kwestii sztucznej inteligencji, Finlandia popiera zaproponowaną oś czasu i podtrzymuje konieczność ochrony danych.

Wnioski po trzecim dniu:

- Potrzebna jest *lepsza koordynacja wymiany informacji* między UODO a Ministerstwem Cyfryzacji.
- Należy **pracować u podsta**w, w celu uzyskania zaufania społeczeństwa.
- Trzeba **edukować społeczeństwo w jego prawach**.

Dzień czwarty – spotkanie z Rzecznikiem ds. ochrony danych

12 marca delegacja zaczęła od wizyty w **Fińskim urzędzie Rzecznika ds. ochrony danych** (Office of the Data Protection Ombudsman). Na czele tego urzędu stoi **Anu Talus, która jest jednocześnie przewodniczącą EROD.** W DPO obecnie pracuje 60 pracowników, jednak dzięki uzyskaniu środków budżetowych, organizacja planuje zatrudnienie około 20 kolejnych osób. Interesujący jest model zarządzania w urzędzie **– nie ma w nim podziału na departamenty, ale na zespoły specjalistów i ich liderów**. Pracę zorganizowano sektorowo, co pozwala ekspertom na głęboką specjalizację w konkretnych dziedzinach, co jest niezbędne przy rozbudowanym fińskim prawie sektorowym. Podobnie jak w przypadku UODO, **liczba skarg do instytucji od obywateli rośnie od 2018 r.** Uwzględniając różnice w populacji obu krajów, **jest ich stosunkowo więcej niż w Polsce**. Wynika to z uproszczonej procedury administracyjnej, która umożliwia **złożenie skargi w formie e-mailowej lub przez formularz na stronie internetowej.**

5 SPRAWY MIĘDZYNARODOWE:

Delegacja miała też **możliwość przedyskutowania kompetencji urzędu, w związku z DGA.** Akt ten wprowadza szeroką kategorię „danych" dzieląc je na osobowe i nieosobowe. Urząd Rzecznika ds. ochrony danych zajmuje się jedynie danymi osobowymi. Instytucja ta nie nadzoruje więc żadnych przepisów DGA – jego obowiązki wynikają natomiast z RODO. Na chwilę obecną **urząd nie prowadzi także żadnego postępowania ani nie otrzymał skarg związanych z DGA**. Kluczowa jest jednak współpraca organu z Traficomem, w ramach której dochodzi do wymiany informacji, regularnych spotkań i konsultacji.

Cyfrowy Omnibus – co się zmieni w DGA?

Po wizycie u Rzecznika ds. ochrony danych, delegacja miała spotkanie w Traficomie. Została przedstawiona prezentacja na temat **zmian w DGA wprowadzonych przez Cyfrowy Omnibus**, z punktu widzenia Traficom. Urząd ten popiera dobrowolną rejestrację organizacji pośrednictwa danych. Jak zauważają przedstawiciele Traficom, **przeniesienie odpowiedzialności za utrzymanie rejestru na Komisję, nie zmieni obłożenia pracą urzędu.**

Traficom stoi na stanowisku, że **poluzowanie wymagań związanych z organizacją pośrednictwa danych jest akceptowalne,** ale powinny zostać w dalszym ciągu egzaminowane, żeby **upewnić się, że wiarygodność i neutralność są zachowane.** Co do Europejskiej Rady ds. Innowacji w zakresie Danych, przejście w kierunku pełnienia bardziej strategicznej roli jest pożądane, **jednakże należy zadbać o to, żeby mechanizmy współpracy między właściwymi organami pozostawały** wystarczające.

Wnioski po czwartym dniu:

- Potrzebna jest **współpraca między organami państwowymi w Polsce** zajmującymi się ochroną danych.
- W Finlandii ochrona danych jest bardziej rozproszona niż w Polsce.
- Mogłoby być **więcej skarg do UODO, gdyby procedura administracyjna była uproszczona, na model fiński.**

Wizyta studyjna w Helsinkach zakończyła się 13 marca. Podczas ostatniego spotkania w siedzibie Traficomu, delegacja dokonała pełnego podsumowania zebranej wiedzy. Kluczowym elementem było **zweryfikowanie poprawności pozyskanych danych**, aby zapewnić pełną zgodność materiału ze stanem faktycznym. Obie delegacje skupiły się na **wstępnym opracowaniu planu działania dotyczącego wdrożenia DGA w Polsce w oparciu o zdobyte w Traficom doświadczenia** a także na określeniu obszarów dalszej współpracy między instytucją przyjmującą a UODO.

DYREKTYWA 2016/680 W PRAKTYCE KRAJOWEJ: GDZIE KOŃCZY SIĘ IMPLEMENTACJA, A ZACZYNAJĄ PROBLEMY SYSTEMOWE? (CZ. I)

W lutowym numerze Biuletynu UODO omówiliśmy wkład Europejskiej Rady Ochrony Danych do ewaluacji dyrektywy 2016/680 (DODO), wskazując najważniejsze wyzwania związane z jej stosowaniem na poziomie unijnym. Niniejszy artykuł koncentruje się na poziomie krajowym – przedstawia doświadczenia Polski związane z wdrażaniem i ze stosowaniem dyrektywy, ze szczególnym uwzględnieniem obszaru sądowego.

Dyrektywa 2016/680 reguluje przetwarzanie danych osobowych przez właściwe organy w obszarze zapobiegania i zwalczania przestępczości, ustanawiając wspólne ramy ochrony danych w sektorze egzekwowania prawa. Została ona wdrożona w Polsce ustawą z 10 maja 2018 r. o ochronie danych osobowych oraz ustawą z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i ze zwalczaniem przestępczości. W zakresie nadzoru nad przetwarzaniem danych przez sądy i prokuraturę zastosowanie znajdują przepisy ustaw ustrojowych.

Wkład Polski do ewaluacji stosowania dyrektywy za okres 2022–2025 został przygotowany na bazie doświadczenia Prezesa UODO oraz organów nadzorczych właściwych dla sądów i prokuratur. Poniżej przedstawiono kluczowe problemy zidentyfikowane na etapie wdrażania i stosowania dyrektywy w Polsce, ze szczególnym uwzględnieniem wymiaru sprawiedliwości oraz krajowego modelu nadzoru nad przetwarzaniem danych osobowych przez właściwe organy. Na styku tych zagadnień ujawnia się **szersze napięcie między zapewnieniem niezależności wymiaru sprawiedliwości a koniecznością zagwarantowania skutecznego i niezależnego nadzoru nad przetwarzaniem danych osobowych**.

Wyłączenia w wymiarze sprawiedliwości

Zgodnie z art. 1 pkt 3 ustawy z 14 grudnia 2018 r. nie określa ona sposobu prowadzenia nadzoru nad ochroną danych osobowych przetwarzanych przez sądy i prokuraturę oraz nie stosuje się do dokumentacji znajdującej się w aktach spraw prowadzonych na podstawie kodeksów postępowania i ustaw szczególnych. W praktyce oznacza to, że **przetwarzanie danych osobowych przez sądy i prokuraturę w ramach zadań związanych z zapobieganiem i ze zwalczaniem przestępczości podlega przede wszystkim regulacjom szczególnym,** w tym przepisom proceduralnym.

Część organów ochrony danych właściwych dla sądów wskazuje, że **mechanizmy służące zapewnieniu poufności akt sądowych są wystarczające** dla ochrony danych osobowych, a dalsze zmiany nie są konieczne. **Odmienne stanowisko prezentują Prezes UODO oraz część sądowych organów nadzorczych**, podkreślając, że **obowiązujące regulacje** proceduralne, w szczególności przepisy postępowania karnego, **nie odzwierciedlają w pełni standardów wynikających z dyrektywy 2016/680.** W szczególności wskazuje się na brak skutecznych i praktycznie wykonalnych gwarancji realizacji praw osób, których dane dotyczą, takich jak prawo do informacji, dostępu do danych, ich sprostowania, usunięcia lub ograniczenia przetwarzania.

Niejasny zakres wyłączenia – problem interpretacyjny

Dodatkowym problemem pozostaje **brak ustawowej definicji pojęcia „sprawowania wymiaru sprawiedliwości”**, które wyznacza zakres wyłączeń spod niezależnego nadzoru organu ochrony danych. W praktyce prowadzi to do sytuacji, w których czynności o charakterze techniczno-administracyjnym, takie jak wysyłka korespondencji, przechowywanie dokumentów czy transport akt, są kwalifikowane jako element sprawowania wymiaru sprawiedliwości, a w konsekwencji wyłączane spod nadzoru. **Prezes UODO wielokrotnie wskazywał, że tego rodzaju czynności nie mieszczą się w istocie sprawowania wymiaru sprawiedliwości** i powinny podlegać niezależnemu nadzorowi.

Jednocześnie obserwuje się zróżnicowaną praktykę interpretacyjną pomiędzy sądami różnych instancji. Sądy apelacyjne częściej przyjmują szerokie rozumienie wyłączenia, podczas gdy sądy okręgowe i rejonowe niekiedy stosują wykładnię bardziej zawężającą. Prowadzi to do **rozbieżności w stosowaniu prawa, osłabienia spójności systemu nadzoru oraz zmniejszenia pewności prawnej.**

Na tym tle szczególnego znaczenia nabiera **praktyczne stosowanie ustawy z 14 grudnia 2018 r. w strukturach sądów**. Choć przepisy ustrojowe przypisują sądom określone zadania i uprawnienia organu nadzorczego wynikające z ustawy grudniowej, w praktyce większość organów właściwych dla sądów nie identyfikuje obszarów, w których ustawa ta powinna znajdować zastosowanie. Odmiennie kształtuje się praktyka w prokuraturze, gdzie – przy analogicznym modelu nadzoru – właściwe organy przyjmują, że są uprawnione do sprawowania nadzoru w trybie dyrektywy 2016/680. Stan ten wskazuje na **systemowy problem interpretacyjny**, w którym formalne przypisanie kompetencji nadzorczych nie przekłada się na ich realne i konsekwentne wykonywanie.

Sprawowanie nadzoru nad przetwarzaniem danych – problemy systemowe

Model nadzoru nad przetwarzaniem danych w sądach i prokuraturze ma **charakter kaskadowy** –

organy wyższego szczebla sprawują kontrolę nad jednostkami niższego rzędu. W przypadku sądów funkcjonowanie tego modelu jest równoważone przez konstytucyjne gwarancje niezależności sędziowskiej. Odmiennie przedstawia się **sytuacja w prokuraturze**, gdzie **silna struktura hierarchiczna rodzi poważne wątpliwości** co do spełnienia wymogu niezależności organu nadzorczego w rozumieniu dyrektywy 2016/680.

Znaczenie ma również status prokuratury w systemie konstytucyjnym. **Prokuratura nie sprawuje wymiaru sprawiedliwości *sensu stricto***, co prowadzi do wniosku, że **wyłączenia przewidziane dla sądów nie powinny mieć do niej zastosowania**. W konsekwencji przetwarzanie danych przez prokuraturę powinno podlegać pełnemu reżimowi niezależnego nadzoru.

Niezależnie od powyższych kwestii strukturalnych problematyczne pozostaje **zapewnienie skutecznego wykonywania kompetencji nadzorczych.** Choć dyrektywa 2016/680 przewiduje szeroki katalog zadań organów nadzorczych, w praktyce ich realizacja napotyka istotne ograniczenia wynikające z niejednoznacznego zakresu kompetencji oraz przyjmowanych interpretacji przepisów krajowych. W Polsce **część zadań została skoncentrowana w rękach Prezesa UODO,** podczas gdy organy funkcjonujące w strukturach sądów i prokuratury nie posiadają pełni zakresu kompetencji przewidzianych w dyrektywie, co prowadzi do **fragmentacji systemu nadzoru i utrudnia zapewnienie jednolitego standardu ochrony danych.**

Doświadczenia innych państw członkowskich wskazują, że **podobne trudności interpretacyjne występują jedynie w ograniczonej grupie państw**, podczas gdy w większości system nadzoru w tym obszarze funkcjonuje bez istotnych problemów.

Wnioski

Doświadczenia Polski pokazują, że kluczowym wyzwaniem nie jest już sama implementacja przepisów, lecz zapewnienie ich skutecznego i spójnego stosowania. Najpoważniejsze problemy mają charakter systemowy i dotyczą w szczególności zakresu wyłączeń w wymiarze sprawiedliwości, modelu nadzoru oraz braku jednolitych standardów interpretacyjnych.

W następnym numerze Biuletynu zostaną przedstawione kolejne aspekty stosowania dyrektywy 2016/680 w Polsce, w tym uprawnienia organów nadzorczych, model sankcyjny oraz przede wszystkim problemy związane z realizacją praw osób, których dane dotyczą.

POLSKA W CZOŁÓWCE EUROPY POD WZGLĘDEM LICZBY ZATWIERDZONYCH KODEKSÓW POSTĘPOWANIA

Prezes Urzędu Ochrony Danych Osobowych zatwierdził już trzy branżowe kodeksy postępowania. To tyle samo, ile organy nadzorcze w Niemczech i Hiszpanii, a więcej niż np. we Francji. Ogólnie liczba zatwierdzonych kodeksów postępowania w UE nie jest duża, a wiele krajów nie ma żadnego. Z czego to wynika i jakie problemy towarzyszą przygotowywaniu tego typu dokumentów?

Kodeksy przewidziane w RODO to dobrowolne narzędzia w zakresie rozliczalności, zawierające szczegółowe postanowienia o ochronie danych. Mogą one stanowić użyteczne i skuteczne narzędzie w zakresie rozliczalności, zawierające **dokładny opis najodpowiedniejszych, zgodnych z prawem i etycznych zbiorów zachowań w sektorze**. Z punktu widzenia ochrony danych osobowych kodeksy mogą zatem funkcjonować jako **zbiór instrukcji dla administratorów danych i podmiotów przetwarzających,** którzy projektują i wdrażają zgodne z RODO czynności przetwarzania danych, nadających znaczenie operacyjne zasadom ochrony danych określonym w prawie europejskim i krajowym. Kodeksy **zapewniają możliwość ustanowienia zbioru reguł, które przyczyniają się do właściwego stosowania RODO w sposób praktyczny, przejrzysty i potencjalnie opłacalny**, a przy tym **uwzględniający specyfikę danego sektora** lub prowadzonych w nim czynności przetwarzania.

– Kodeksy muszą zwiększać bezpieczeństwo tych danych względem przepisów ogólnych. Mają gwarantować wyższy standard ochrony – tłumaczy **dr Roman Sobotka, główny specjalista w Departamencie Prawa i Nowych Technologii UODO**.

Przykładem zwiększania poziomu ochrony może być uznanie numeru telefonu za daną osobową w kodeksie dla prywatnych agencji badania opinii i rynku. Twórcy kodeksu uznali, że takie podejście lepiej zabezpieczy prywatność osób, do których wykonywane są połączenia telefoniczne w ramach badania opinii, i przyczyni się do zapewnienia większej jednolitości orzecznictwa sądowego. W tym kodeksie nałożono też na członków kodeksu obowiązek powołania Inspektora Ochrony Danych, mimo że nie wynika on z przepisów prawa.

7 PRACOWNICY UODO

Zatwierdzanie kodeksu

Organ nadzorczy zatwierdzając kodeks postępowania, opiera się głównie na Wytycznych EROD nr 1/2019 –wiążą o ne krajowe organy nadzorcze (zob. Grzelak A., *Charakter prawny zaleceń i wytycznych Europejskiej Rady Ochrony Danych*, dodatek Monitor Prawniczy 23/2021). Najpierw sprawdza się, **czy wniosek o zatwierdzenie kodeksu złożył podmiot uprawniony tj. taki, który wykaże, że jest reprezentatywny dla administratorów lub podmiotów przetwarzających w pewnej branży.** Kodeks musi zawierać szereg elementów, m.in.: **zakres podmiotowy i przedmiotowy, raport z przeprowadzonych konsultacji, odpowiednie mechanizmy monitorowania**.

Przed złożeniem projektu kodeksu do zatwierdzenia należy **sprawdzić listę kontrolną** (załącznik 3 do wspomnianych wytycznych). Ocena formalna wniosku o zatwierdzenie kodeksu postępowania jest przeprowadzona z uwzględnieniem **kryteriów dopuszczalności określonych przez EROD w ww. wytycznych i przepisów Kpa.** Następnie podczas oceny merytorycznej treści kodeksu analizowana jest jego treść w kontekście spełnienia kryteriów dopuszczalności, wskazanych w Wytycznych 1/2019.

Najważniejsze jest ustalenie zakresu obowiązywania kodeksu

Jak podkreśla dr Sobotka, **główna trudność przy tworzeniu takich kodeksów**, jak również późniejszego zatwierdzania ich przez UODO, **polega na właściwym wyznaczeniu zakresu, jaki on obejmie.** Może być on bardzo wąski, ale za to dokładnie określony. Dr Sobotka podkreśla, iż ciężko wyobrazić sobie stworzenie kodeksu obejmującego wszystkie czynności przetwarzania danych osobowych w konkretnej branży. Możliwe wydaje się natomiast przygotowanie kodeksu obejmującego np. zasady przetwarzania danych w procesie rekrutacyjnym, do którego mogłyby dołączać firmy z różnych branż.

W kodeksie trzeba **dokładnie wskazać, do jakich czynności przetwarzania ma on zastosowanie i jakie podmioty** (administratorzy lub podmioty przetwarzające) mogą do niego przystąpić. Jest to bardzo ważne również z perspektywy kontroli prowadzonych przez organ nadzorczy, który później ocenia, czy kodeks ten jest przestrzegany. Przykładowo – **jak wskazuje Agnieszka Kociełkiewicz, naczelniczka Wydziału Kodeksów i Analiz w Departamencie Prawa i Nowych Technologii UODO** – kodeks może się odnosić do przetwarzania danych klientów, ale już nie do danych pracowników.

Uprawniony podmiot i utrwalona praktyka

Kolejny problem, jaki zauważają pracownicy Wydziału Kodeksów i Analiz, polega na tym, że o **zatwierdzenie kodeksu wnioskują często podmioty, które nie mają do tego uprawnień**. Zgodnie z

przepisami musi to bowiem być **podmiot reprezentatywny dla danej branży**, **zrzeszający administratorów lub podmioty przetwarzające dane** (ich bowiem obejmują kodeksy). Z tego względu niemożliwe było zatwierdzenie kodeksu postępowania zgłoszonego przez stowarzyszenie zrzeszające pracowników czy inspektorów ochrony danych danego sektora. Podobnie w innej branży: firma posiadająca ponad połowę udziału w rynku sama stworzyła kodeks i wnioskowała o jego zatwierdzenie. UODO musiał odmówić, gdyż nie wykazała ona reprezentatywności dla całej branży.

Gdy w postępowaniu o zatwierdzenie kodeksu pojawiają się problemy interpretacyjne, istnieje **możliwość ustalenia, jak organy nadzorcze innych krajów rozumieją konkretne zagadnienie**. Takie konsultacje wpływają na jednolitość stosowania RODO. Nieraz problematyczne są same zapisy w kodeksie. Zgodnie z wytycznymi EROD powinny one **uwzględniać krajowe przepisy i orzecznictwo**. Niestety, twórcy kodeksów rzadko odwołują się do wytycznych EROD dotyczących zgody, przejrzystości, prawnie uzasadnionego interesu, zgłaszania naruszeń itd. **Wytyczne EROD zawierają szereg praktycznych przykładów i mogą stanowić wzór dla rozwiązań kodeksowych.**

– Poważne trudności sprawia także przedstawienie w kodeksie rozwiązań charakterystycznych dla konkretnej branży. Mają one bowiem **doprecyzowywać RODO i dostosowywać sposób działania z zakresu ochrony danych.** Wprowadzać pewien **standard postępowania dla wszystkich podmiotów z branży, które zdecydują się przystąpić do stosowania kodeksu**. I tu pojawi się największy problem, bo często okazuje się, że trudno znaleźć jakiś wspólny mianownik, by przedstawić go w kodeksie – wyjaśnia Agnieszka Kociełkiewicz.

Ważne jest również, by **kodeks napisany był językiem precyzyjnym, prawniczym, ale też zrozumiałym dla osób, których dane będą przetwarzane na podstawie jego postanowień**. W przypadku danych dzieci przyjmuje się, że tekst musi być zrozumiały dla ich rodziców lub opiekunów, gdyż to oni będą ewentualnie składać skargi w imieniu podopiecznych.

Kluczowe znaczenie ma podmiot monitorujący wykonywanie kodeksu

Jak wskazuje naczelniczka Agnieszka Kociełkiewicz, **trudności powoduje także stworzenie systemu monitorowania przestrzegania kodeksu**. Przepisy wymagają bowiem, by każdy kodeks ustanawiał odpowiednie mechanizmy monitorowania, a **kodeksy dla podmiotów niepublicznych muszą dodatkowo wskazać podmiot monitorujący lub sposób, w jaki zostanie on powołany**. Ponieważ nie można wyznaczyć podmiotu monitorującego dla podmiotów publicznych (w Polsce definiowanych zgodnie z ustawa o finansach publicznych), kodeks dla sektora publicznego musi zawierać szczegółowe mechanizmy monitorowania oparte na przepisach powszechnie obowiązujących. **Aby podmiot monitorujący mógł wypełniać swoją rolę, musi uzyskać akredytację Prezesa UODO** – jest ona przyznawana w ramach odrębnego postępowania przed Prezesem UODO.

Podmiot monitorujący sprawdza, czy potencjalny członek kodeksu spełnia warunki, by do niego przystąpić (audyt wstępny). Później **pilnuje także, czy postanowienia kodeksu są przestrzegane**. Osoba, która czuje, że jej prawa zostały naruszone, może więc **wnieść skargę zarówno do UODO, jak i do podmiotu monitorującego** (w zakresie objętym postanowieniami kodeksu). W związku z tym, że w ramach jednego działania członka kodeksu skargi mogą trafić i do urzędu, i do podmiotu monitorującego, niezbędne jest współdziałanie obu podmiotów. Należy zwrócić uwagę, że postępowania mogą być prowadzone niezależnie.

– Inny jest też zakres kar, którymi może posłużyć się UODO oraz podmiot monitorujący. Ten ostatni może np. zalecić wprowadzenie pewnych konkretnych zmian w procedurze przetwarzania danych (które mogą być inne niż te, które zaleca Urząd), albo **wykluczyć dany podmiot z grona członków kodeksu** – zwraca uwagę dr Sobotka.

Ekspert wskazuje, że w przypadku prowadzonych postępowań **organ nadzorczy zawsze weryfikuje, czy administrator jest członkiem kodeksu** (informację o tym też można uzyskać od podmiotu monitorującego).

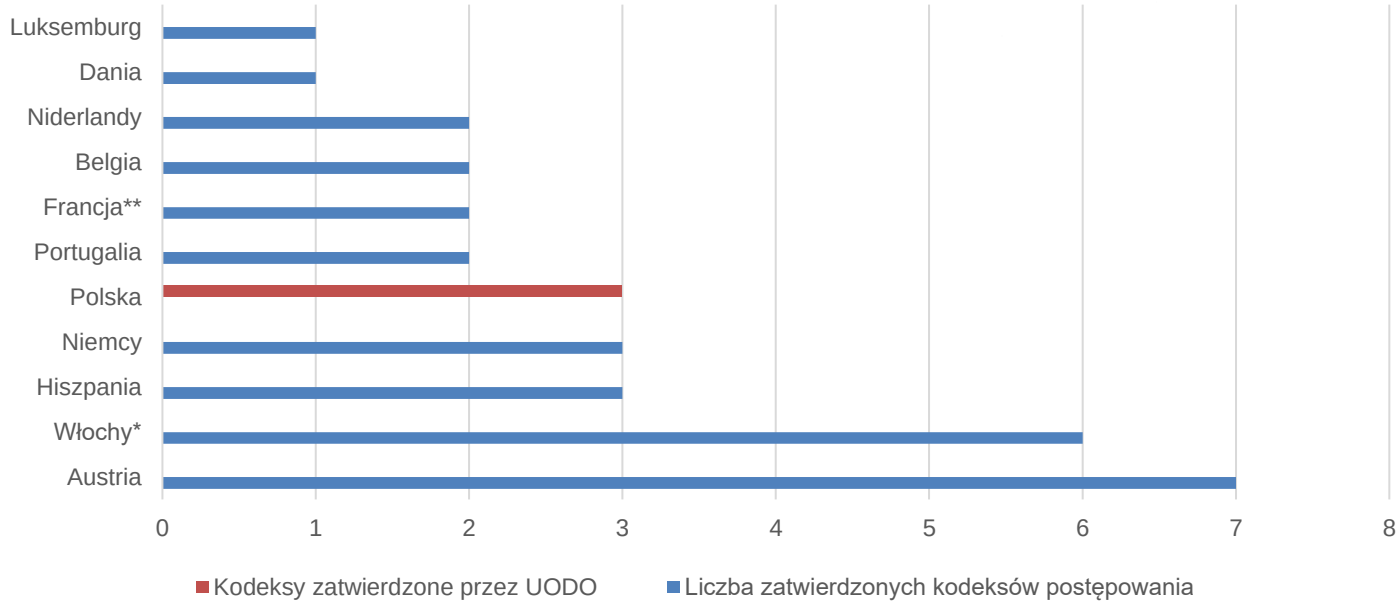
– Jeśli dany podmiot przystąpił do kodeksu, ale go nie przestrzega, UODO może zaostrzyć wymierzoną mu karę. Wprowadza on bowiem w błąd osoby, których dane dotyczą, sugerując, iż stosuje wyższy stopień ochrony danych, podczas gdy faktycznie tego nie robi – podkreśla dr Sobotka.

Obecnie UODO proceduje wnioski o zatwierdzenie kodeksów podstępowań m.in. dla jednego z samorządów zawodów zaufania publicznego, a także pewnej dużej branży biznesowej – prace są już na zaawansowanym etapie. W kilku innych branżach trwają rozmowy z zainteresowanymi organizacjami. W minionych latach parę innych wniosków o zatwierdzenie zostało zaś wycofanych po uwagach Urzędu. **UODO aktywnie zachęca kolejne sektory do tworzenia własnych kodeksów postępowania** – od niektórych z nich spodziewa się szybkiego wniosku o zatwierdzenie, w wielu innych przypadkach jednak po wyrażeniu wstępnego zainteresowania sprawa nie nabiera dalszego biegu.

Kodeksy postępowania w różnych państwach UE

Po kliku latach obowiązywania RODO kodeksy postępowań wciąż sprawiają liczne problemy i mało podmiotów je tworzy lub dołącza do nich. **W całej Unii Europejskiej jest nieco ponad 30 zatwierdzonych kodeksów** (przynajmniej tych zgłoszonych do EROD), przy czym oprócz Polski występują one jedynie w krajach tzw. starej Unii, czyli tych które dołączyły przed 2004 r. Jak wskazano na wstępie, **w Polsce zatwierdzono trzy kodeksy postępowania, co stawia nasz kraj na europejskim podium. Trzecie miejsce dzielimy z Niemcami i Hiszpanią.**

7 PRACOWNICY UODO



Jak wskazuje powyższy wykres, **liderem w kwestii zatwierdzonych kodeksów postępowania jest Austria,** w której obowiązuje ich aż siedem. **Na drugim miejscu uplasowały się Włochy,** które zatwierdziły sześć kodeksów postępowań (w tym dwa nie znajdują się jeszcze na stronie EROD). Kilka krajów ma też po dwa kodeksy: Francja, Belgia, Niderlandy i Portugalia. W Danii i Luksemburgu zatwierdzono po jednym kodeksie.

Kodeksy zatwierdzone **w Austrii** obejmują następujące branże: pracodawców prywatnych instytucji oświatowych, księgowych, brokerów i doradców ubezpieczeniowych dostawców inteligentnych urządzeń do pomiaru zużycia prądu, stowarzyszenia na rzecz integracji zawodowej i społecznej, dostawców urządzeń mierzących zużycie wody i energii cieplnej, podmioty prowadzące marketing bezpośredni.

Z kolei **we Włoszech** funkcjonują kodeksy dotyczące informacji handlowej, telemarketingu i telesprzedaży, a także agencji zatrudnienia. Osobny kodeks mają firmy ubezpieczeniowe (reguluje on dostęp do wspólnych baz danych), a także twórcy programowania i podmioty wykorzystujące wtórnie dane pacjentów do badań klinicznych. Ten ostatni kodeks obejmuje tylko region Veneto.

Również **w Niemczech** istnieje kodeks postępowania dla dostawców urządzeń pomiarowych do zużycia wody i ciepła. Swój kodeks mają tam też notariusze (ma on charakter publiczny) oraz agencje kredytowe (reguluje kwestię retencji danych). Z kolei **w Hiszpanii** zatwierdzono kodeks dotyczący przetwarzania danych w badaniach klinicznych, w branży reklamowej i ubezpieczeniowej.

Francja posiada dwa zatwierdzone kodeksy, przyjęcie trzeciego planowane jest wkrótce. Oba mają charakter transgraniczny, pierwszy dotyczy dostawców usług w chmurze, drugi zaś – podwykonawców w badaniach klinicznych, działających na zlecenie sponsora (CRO). Belgia również posiada transgraniczny kodeks dla dostawców usług chmurowych oraz publiczny kodeks postępowania dla notariuszy.

7 PRACOWNICY UODO

W Portugalii zatwierdzono dwa kodeksy o bardzo wąskim charakterze – jeden dotyczy wymiany danych między dwiema gminami, drugi – zarządzania danymi przez administrację kilku wskazanych portów. Z kolei w Niderlandach istnieje ogólny kodeks dla podmiotów przetwarzających, a także dla dostawców inteligentnych urządzeń do zarządzania siecią energetyczną. **Kodeks duński** dotyczy przetwarzania danych przez rady parafialne, a ten **w Luksemburgu** obejmuje agencje pracy tymczasowej.

Wymienione kodeksy najczęściej liczą od kilkunastu do kilkudziesięciu stron, choć najkrótszy z nich ma sześć stron, a najdłuższy – 140. Również tutaj Polska znajduje się w czołówce, gdyż wszystkie kodeksy zatwierdzone w naszym kraju liczą ok. 100 stron.

Agnieszka Kociełkiewicz,

naczelniczka Wydziału Kodeksów i Analiz

Departament Prawa i Nowych Technologii

Urząd Ochrony Dany Osobowych

dr Roman Sobotka,

główny specjalista

Departament Prawa i Nowych Technologii

Urząd Ochrony Dany Osobowych

Przydatne linki i dokumenty:

Najczęstsze błędy podczas przygotowywania kodeksów postępowania

Najważniejsze informacje dotyczące kodeksów postępowania

Wytyczne CNIL (francuski organ nadzorczy) ws. kodeksów postępowania

Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679

Wymogi akredytacji podmiotów monitorujących kodeksy

Rejestr zatwierdzonych kodeksów postępowania w UE

WARTO WIEDZIEĆ…
NIE KAŻDA GRA TO TYLKO ZABAWA. GRY ON-LINE, HAZARD, TWOJE DANE – DLACZEGO TO WAŻNE?

Współczesny świat cyfrowy pozornie stwarza możliwości rozwoju, komunikacji i rozrywki. Niestety niesie z sobą szereg poważnych zagrożeń związanych z ochroną prywatności i bezpieczeństwem danych osobowych. W odpowiedzi na te wyzwania, w ramach XVI edycji programu edukacyjnego „Twoje dane – Twoja sprawa" przeprowadzono webinarium dla nauczycieli i dyrektorów szkół biorących udział w programie. Celem było pogłębienie wiedzy na temat ochrony danych dzieci w środowisku cyfrowym. Webinarium poprowadzili: Katarzyna Staciwa, Koordynatorka ds. badań i rozwoju w UPKDP i Krzysztof Król, zastępca Dyrektorki Departamentu Współpracy Międzynarodowej w UODO

Internet i aplikacje mobilne stały się naturalną przestrzenią funkcjonowania młodych ludzi. To właśnie tam dzieci nawiązują kontakty społeczne, korzystają z rozrywki czy budują swoją tożsamość. Niestety, cyfrowe środowisko bywa miejscem manipulacji, przemocy i ryzykownych zachowań. Coraz częściej małoletni mają kontakt z osobami nieznajomymi, mechanizmami hazardu czy zwodniczymi rozwiązaniami projektowymi, które skłaniają użytkowników do bezrefleksyjnego udostępniania danych.

Dodatkowym wyzwaniem jest dynamiczny rozwój technologii umożliwiających łatwą modyfikację wizerunku lub głosu. W połączeniu z ograniczonym nadzorem dorosłych i niewystarczającą świadomością zagrożeń sprawia to, że dane osobowe dzieci są coraz częściej wykorzystywane lub udostępniane w sieci w sposób szkodliwy. Takie zjawiska mogą prowadzić do poważnych konsekwencji dla prywatności, bezpieczeństwa i dobrostanu najmłodszych.

Jak reagować na zagrożenia dla prywatności dzieci?

Podczas zorganizowanego w marcu webinarium eksperci przyjrzeli się tym zagrożeniom z dwóch perspektyw. Z jednej strony omówione zostały mechanizmy funkcjonowania współczesnych usług cyfrowych i ich wpływ na zachowania użytkowników, w tym dzieci i młodzieży. Z drugiej – uczestnicy poznali praktyczne sposoby reagowania na zagrożenia oraz zasady przydatne podczas korzystania z dostępnych obecnie technologii, w tym sztucznej inteligencji, a także otrzymali informacje o tym, gdzie

szukać pomocy, kiedy staniemy się ofiarą takich zagrożeń. Pani Katarzyna Staciwa omówiła, czym jest i czemu służy „Internet dzieci", oraz przedstawiła skalę przestępstw min. na tle seksualnym wobec małoletnich w sieci.

Należy pamiętać, że szkoła odgrywa ważną rolę w kształtowaniu odpowiedzialnych postaw w sieci, dlatego wspieranie nauczycieli w tym obszarze jest jednym z kluczowych celów programu „Twoje dane – Twoja sprawa". Ponieważ tylko wysoki poziom świadomości dorosłych odpowiedzialnych za zapewnienie bezpieczeństwa dzieci i młodzieży może prowadzić do realnych zmian.

Niebezpieczne mechanizmy i „dark patterns" w grach on-line

Gry on-line są często postrzegane jako atrakcyjna i niewinna forma rozrywki dla dzieci i młodzieży. Warto jednak pamiętać, że poza funkcją rozrywkową mogą one się wiązać z różnymi zagrożeniami. Platformy i aplikacje gamingowe wykorzystują zaawansowane mechanizmy analizy zachowań użytkowników, które pozwalają profilować graczy i wpływać na ich decyzje – m.in. poprzez kierowanie reklam, zachęcanie do dodatkowych zakupów czy projektowanie rozgrywki w sposób utrudniający jej przerwanie. W wielu grach pojawiają się także elementy przypominające mechanizmy hazardowe, takie jak losowe nagrody czy tzw. lootboxy.

Dodatkowym wyzwaniem są tzw. dark patterns, czyli rozwiązania projektowe w interfejsie, które mogą w sposób manipulacyjny skłaniać użytkowników do pozostania w grze lub wydawania pieniędzy. Z tego względu istotne jest, aby dorośli byli świadomi tych mechanizmów i potrafili rozmawiać z dziećmi o bezpiecznym oraz odpowiedzialnym korzystaniu z gier on-line. Często wzbudzają one wrażenie niewinnej zabawy. Można dzięki nim budować „światy", ścigać się samochodami, rozwiązywać zagadki czy grać z kolegami z klasy. Co może się wydawać atrakcyjne. Jednak oprócz zabawy w grach mogą się pojawić zagrożenia. Warto je znać.

Profilowanie zachowań użytkowników

Platformy internetowe analizują, ile czasu spędzasz w grze, kiedy grasz, na co wydajesz pieniądze, a nawet jak reagujesz na nagrody. Na tej podstawie tworzą profil użytkownika, aby:

- podsuwać Ci reklamy,
- zachęcać do kolejnych zakupów,
- utrudniać przerwanie gry.

Niebezpieczeństwo gier hazardowych

Niektóre gry lub aplikacje posiadają mechanizmy hazardowe, co oznacza, że można:

- kupować „lootboxy” (tajemnicze paczki z nagrodami),
- losować skórki lub przedmioty,
- obstawiać wyniki meczów.

Takie elementy działają podobnie jak automaty do gier czy ruletka. Gracz nigdy nie wie, co wylosuje – to czysty przypadek. Twój mózg bardzo lubi takie mechanizmy, więc chcesz próbować jeszcze raz i kolejny. A to może prowadzić do uzależnienia.

Uzależnienie od gier

Gry są tak zaprojektowane, aby były wciągające. Zdobywanie punktów, nowych poziomów czy wirtualnych nagród sprawia, że chce się grać coraz dłużej. Jeśli:

- grasz kilka godzin dziennie,
- zaniedbujesz lekcje lub obowiązki,
- denerwujesz się, gdy nie możesz grać,

to może być sygnał, że tracisz kontrolę. Zbyt długie granie może powodować zmęczenie, problemy z koncentracją i gorsze wyniki w szkole.

„Dark patterns” – czyli manipulacja w interfejsie

To sztuczki, które mają Cię zatrzymać w grze lub skłonić do wydania pieniędzy. Przykłady:

- komunikaty typu „ostatnia szansa!”,
- trudny do znalezienia przycisk „anuluj”,
- automatycznie zaznaczona zgoda na przetwarzanie danych,
- ukrywanie rzeczywistych kosztów.

Deepfake i fałszywe reklamy

Technologia deepfake potrafi podrobić czyjąś twarz i głos tak, że wygląda jak prawdziwe nagranie. Czasem oszuści tworzą fałszywe reklamy, w których znane osoby zachęcają do zagrania w gry hazardowe. Na co zwrócić uwagę:

- nie klikaj w podejrzane linki,
- nie podawaj swoich danych w internecie,
- zawsze pokaż taką reklamę dorosłemu.

Jeśli coś wydaje się podejrzane – zatrzymaj się i sprawdź, zanim uwierzysz.

Nieznajomi w internecie

W grach on-line często można rozmawiać z innymi graczami. Niestety nie każdy w sieci mówi prawdę o sobie. Uważaj, gdy ktoś:

- prosi o twoje dane osobowe (nazwisko, adres),
- proponuje tylko sobie znane sposoby na zdobycie darmowych nagród w grze, np. w zamian za przesłanie zdjęcia lub udostępnienie numer telefonu,
- próbuje nawiązać z Tobą bliższy kontakt, nigdy nie wiesz, kto jest po drugiej stronie.

Nigdy nie podawaj swoich danych osobowych nieznanym osobom. Jeśli coś cię zaniepokoi – powiedz o tym rodzicom lub nauczycielowi.

PAMIĘTAJ!

Gry mogą być rozrywką, ale tylko wtedy, gdy korzystamy z nich rozsądnie i z umiarem. **Pamiętaj o nauce, sporcie i spotkaniach z przyjaciółmi w realnym świecie**.

Gry projektowane są tak, aby przejmować kontrolę nad czasem i zachowaniem gracza. Zdecyduj, czy się na to godzisz. Jeśli w grze coś cię niepokoi – nie zostawaj z tym sam. **Zawsze możesz poprosić o pomoc dorosłych.**

Hejt i negatywne zachowania

W grach on-line można spotkać osoby, które obrażają innych, wyśmiewają lub celowo przeszkadzają w grze. Nie odpowiadaj agresją. Skorzystaj z opcji „zablokuj” lub „zgłoś” użytkownika. **Zanim zagrasz w grę on-line, warto:**

- ustalić z rodzicami limit czasu przeznaczonego na grę,
- porozmawiać z rodzicami o tym, w co chcesz zagrać,
- pamiętać, aby nie podawać danych osobowych.

Trudne słowa – proste wyjaśnienia

Co oznaczają słowa, które pojawiają się w poradzie?

- **Gry on-line z mechanizmami hazardu** – to gry, które imitują mechanizmy tradycyjnego hazardu, wykorzystując **elementy losowości**. Nie oferują wygranej pieniężnej, „wygrane" zazwyczaj mają **charakter wirtualny** (wirtualna waluta, skórki/skiny, przedmioty w grze). Jednak często posiadają **opcję zwiększenia szans na zdobycie nagrody poprzez wydanie prawdziwych pieniędzy**. Gry wykorzystują dźwięki, wizualizacje i mechanizmy wygranej, które przypominają prawdziwe automaty do gier. **Mechanizmy te mogą prowadzić do uzależnienia.**

- **Profilowanie w grach on-line** – to proces **zbierania, analizy i modelowania danych behawioralnych, czyli zachowań graczy** w celu stworzenia **ich cyfrowych profili** poprzez wykorzystanie telemetrii, czyli **automatycznego zapisu działań użytkownika podczas rozgrywki** (np. ruchy, czas reakcji, wybory, częstotliwość logowania). Ma to na celu m.in. zrozumienie, jak gracze grają, aby ulepszyć grę lub naprawić błędy, ale również przewidywanie momentu, w którym gracz może zrezygnować z gry, aby zaoferować mu np. specjalny bonus, który spowoduje zatrzymanie gracza w grze.

- **Dane osobowe** – to **informacje, które mogą pomóc kogoś zidentyfikować,** np. imię i nazwisko, adres, numer telefonu, e-mail, głos czy wizerunek. **Takich danych nie powinno się udostępniać nieznanym osobom i aplikacjom bez potrzeby**. Dane osobowe w grach są zbierane m.in. w celu profilowania graczy.

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

- **„Dark patterns"** – to **techniki stosowane w projektowaniu interfejsów** (np. gier, aplikacji, stron), które **mają na celu manipulowanie decyzjami użytkownika**. Są to subtelne, ale celowe zabiegi, które mogą **prowadzić do niezamierzonych zakupów, subskrypcji czy udostępnienia danych osobowych**.

WEBINARIUM

Analiza ryzyka

w sposób zgodny z zasadą rozliczalności

18 dobrych praktyk*

URZĄD OCHRONY DANYCH OSOBOWYCH

UODO RUSZA W KRAJ

Czwartek, 9 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

Prezes UODO zaprasza na wydarzenia

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 „Administrator danych osobowych nieposiadający osobowości prawnej”

Termin: **27 kwietnia 2026 r.,** godz. **10:00 - 13:30**

Organizatorzy: **Prezes Urzędu Ochrony Danych Osobowych, Społeczny Zespół Ekspertów przy Prezesie UODO oraz Uniwersytet Jagielloński w Krakowie**

Miejsce: **Urząd Ochrony Danych Osobowych, ul. Stanisława Moniuszki 1A w Warszawie**

Formuła: **hybrydowa z transmisją online za pośrednictwem strony internetowej www.uodo.gov.pl**

Konferencja poświęcona jest analizie sytuacji prawnej podmiotów nieposiadających osobowości prawnej, które w ramach swojej działalności podejmują decyzje dotyczące przetwarzania danych osobowych w organizacji.
Sytuacja ta dotyczy np. organów administracyjnych, zakładów administracyjnych (np. niektórych jednostek samorządu terytorialnego), przedsiębiorstw, grup przedsiębiorstw, oddziałów i zakładów przedsiębiorstw czy spółek cywilnych. Osobowość prawna rozumiana jako możliwość samodzielnego decydowania i działania we własnym imieniu, dotyczy podmiotów wyraźnie wskazanych przepisami kodeksu cywilnego.
Ale zarówno podmioty posiadające osobowość prawną, jak i te nieposiadające osobowości prawnej, mogą mieć status administratora danych osobowych i ponosić odpowiedzialność majątkową / niemajątkową w wyniku naruszenia. **Jak więc interpretować przepis art. 82 RODO w kontekście odpowiedzialności cywilnej administratora danych nieposiadającego osobowości prawnej, a także w świetle art. 83 RODO w zakresie nakładania na niego administracyjnych kar pieniężnych?** – o tym m.in. będziemy rozmawiać podczas tej konferencji.

Omówione zostaną również inne zagadnienia, jak:

- **wielość podmiotów podejmujących decyzje dotyczące przetwarzania danych w imieniu jednego administratora,**
- **rola prawa zakładowego w przedmiocie realizacji zadań wynikających z RODO,**
- **zdolność sądowa i odpowiedzialność cywilna administratorów nieposiadających osobowości prawnej,**
- **zdolność egzekucyjna roszczeń oraz kar administracyjnych.**

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 oraz 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