URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 04/26

www.uodo.gov.pl

SPIS TREŚCI

SPIS TREŚCI

Szanowni Państwo,

w kwietniu Prezes UODO zyskał nowe kompetencje wynikające z unijnego rozporządzenia o zarządzaniu danymi, czyli DGA. Zgodnie z nimi Prezes UODO zajmuje się również sprawami pośrednictwa danych, rejestracją organizacji altruizmu danych oraz przekazywaniem danych nieosobowych do państw trzecich.

Kompetencje Prezesa UODO zmieni też procedowana w parlamencie ustawa o systemach sztucznej inteligencji. Przedstawiliśmy Sejmowi uwagi do projektu tej ustawy. Wykorzystanie danych przez systemy sztucznej inteligencji jest już jednak w zakresie naszych zainteresowań od dłuższego czasu. O naszych pracach w tym zakresie i zasadach związanych z ich wykorzystaniem mówiłem więc m.in. w kwietniu podczas Europejskiego Kongresu Gospodarczego w Katowicach (EEC – European Economic Congress).

Pragnę zwrócić Państwa uwagę, że wejście w życie nowelizacji ustawy o Krajowym Rejestrze Karnym w związku z wdrożeniem rozporządzenia (UE) 2019/816 również rozszerza zakres zadań Prezesa UODO w kontekście uruchamianego systemu ECRIS-TCN (European Criminal Records Information System for Third Country Nationals). Jest to scentralizowany system informatyczny do wymiany informacji o wyrokach skazujących obywateli państw trzecich (spoza UE) oraz bezpaństwowców. Prezes UODO pełni w Polsce funkcję organu nadzorczego odpowiedzialnego za monitorowanie zgodności przetwarzania danych osobowych w ramach ECRIS.

Ważne orzeczenia

NSA potwierdził stanowisko Prezesa UODO, uznając, iż śmierć dłużnika nie oznacza, że jego spadkobiercy automatycznie stają się odpowiedzialnymi za te długi. Tym samym nie uprawnia to wierzycieli do pozyskiwania danych potencjalnych spadkobierców w celu windykacji zobowiązania.

Chciałbym też zwrócić Państwa uwagę na wydaną ostatnio decyzję o nałożeniu na wspólnotę mieszkaniową kary w wysokości 5 tys. zł za to, że nie zgłosiła ona do Prezesa UODO faktu naruszenia danych osobowych. Chodziło o to, że zawiadomienie o opłatach z danymi osobowymi trafiło do nieupoważnionej osoby. Wspólnota zbagatelizowała incydent tłumacząc, że dotyczył on tylko „jednego członka Wspólnoty". Jednak skoro doszło do naruszenia danych, to istotny jest poziom ryzyka dla osoby, której dane dotyczą. Incydentu nie trzeba zgłaszać do Prezesa UODO tylko wtedy, gdy można wykluczyć, że prawa i wolności osoby zostały naruszone. W tym przypadku tak nie było. Zgłaszanie incydentów jest tymczasem jednym z ważniejszych obowiązków administratorów danych osobowych. Pozwala bowiem m.in. minimalizować ryzyko naruszeń i ograniczać konsekwencje zdarzenia, do którego już doszło.

Stanowiska Prezesa UODO

W kwietniu wsparliśmy wprowadzenie obowiązkowej edukacji zdrowotnej w szkołach. Wskazałem, że obejmuje ona też edukację w zakresie bezpieczeństwa cyfrowego, a to wzmacnia ochronę prywatności i praw podstawowych dzieci. Pismo, które skierowałem do ministry edukacji narodowej, publikujemy na naszej stronie – zawiera ono nie tylko argumenty za taką edukacją, ale też przykłady, jak inne kraje rozwiązały ustawowo problem cyfrowej i medialnej edukacji w szkołach.

„Musimy pamiętać, że dzieci w internecie oddają swoje dane, i przez to tracą nad nimi kontrolę, a zatem także kontrolę nad własną prywatnością. A dane te mogą być wykorzystane w najróżniejszy sposób: od nadużyć finansowych po najcięższe przestępstwa o charakterze seksualnym" – mówiłem 20 kwietnia w dyskusji New Education Forum 2026 „Dzieci w sieci. Jak możemy realnie wzmacniać bezpieczeństwo cyfrowe".

Głos zabraliśmy również w sprawie zmian przepisów, które dotyczą zakresu przetwarzania danych przez policję i służby:

- Zwróciliśmy m.in. uwagę, że projekt incydentalnej ustawy o organizowaniu w 2027 roku „XXVI Światowego Jamboree Skautowego w Polsce" zakłada wprowadzenie instytucji „police screening'u" dla wszystkich wydarzeń o statusie wydarzenia specjalnego. Jego organizator (nawet firma prywatna) mógłby wnieść o screening uczestników, a osoby te nie wiedziałyby nawet, że pozostają w zainteresowaniu policji lub służb. Zarówno forma, w jakiej ta zmiana jest wprowadzana, jak i jej zakres budzą poważne wątpliwości.
- Zwróciliśmy także MSWiA uwagę, że przepisy polskiej ustawy wdrażającej tzw. unijną dyrektywę policyjną wymagają zmian legislacyjnych. W obecnym kształcie ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości nie zapewnia pełnych gwarancji ochrony praw osób, których dane są przetwarzane. Wprowadzono bowiem do niej m.in. liczne wyłączenia.

Wskazaliśmy też, że przepisy dotyczące przetwarzania danych osobowych w procedurze budżetu obywatelskiego wymagają poważnych zmian. Chodzi o to z jednej strony, by samorządy organizujące konsultacje społeczne nie domagały się od uczestniczących w nich niepotrzebnych danych. Należałoby również rozważyć wprowadzenie przepisów dotyczących elektronicznego głosowania, gwarantujących bezpieczeństwo stosowania instytucji budżetu obywatelskiego.

Rozmowy o danych osobowych

Jak zwykle sporo czasu poświęciliśmy na działalność edukacyjną i wspieranie wiedzy o ochronie prywatności.

- 2 kwietnia 2026 r. w siedzibie UODO w Warszawie spotkaliśmy się ze społecznością Uniwersytetu im. Adama Mickiewicza w Poznaniu.

- 9 kwietnia zorganizowaliśmy webinarium „Analiza ryzyka w sposób zgodny z zasadą rozliczalności". Nagranie z niego dostępne jest na naszej stronie.

- 10 kwietnia w warszawskiej siedzibie Polskiej Agencji Prasowej debatowałem o danych w systemie ochrony zdrowia przy okazji premiery raportu „Mapa źródeł danych medycznych w Polsce".

- 13 kwietnia w Rzeszowie eksperci UODO ponownie dyżurowali w punkcie konsultacyjnym.

- 14 kwietnia na Europejskim Szczycie e-Commerce przedstawiłem uwagi dotyczące ochrony danych osobowych w kontekście handlu elektronicznego.

- Z przedstawicielami Polskiej Rady Psychoterapii rozmawialiśmy na temat kodeksu postępowania przy przetwarzaniu danych osobowych w związku ze świadczeniem pomocy psychoterapeutycznej oraz o możliwościach opracowania kodeksu postępowania dla tej branży.

- 17 kwietnia wraz z Urzędem Zamówień Publicznych zorganizowaliśmy konferencję „Projektowanie ochrony danych w zamówieniach publicznych".

- 20 kwietnia we współpracy z Kościelnym Inspektorem Ochrony Danych zorganizowaliśmy szkolenie dla kościelnych inspektorów ochrony danych, księży, zakonnic i pracowników oraz wolontariuszy jednostek organizacyjnych Kościoła katolickiego.

- Także 20 kwietnia przedstawiciele IAB Polska oraz IAB TECH LAB przedstawili w siedzibie UODO opracowany przez branżę reklamy internetowej nowy mechanizm postępowania z żądaniami usunięcia danych (Data Deletion Request Framework, DDRF). Ma to być mechanizm o charakterze globalnym, który będzie można wykorzystywać w różnych systemach prawnych.

- 28 kwietnia spotkałem się z prezesem Naczelnej Rady Lekarskiej. Rozmawialiśmy o tajemnicy lekarskiej oraz potrzebie zmian legislacyjnych, które pozwolą skutecznie chronić wrażliwe dane pacjentów.

- 29 kwietnia wziąłem udział w panelu „Europejska konkurencyjność innowacyjna w świetle regulacji danych i AI" („European Innovation Competitiveness under Data and AI Regulation"), w ramach projektu naukowego BRIDGE 2026 (Bilateral Research Initiative on Data and the Governance of Emerging Technologies).

Warto wiedzieć:

Już po raz czternasty Prezes UODO zaprasza studentów kierunków prawa i administracji III–V roku studiów jednolitych oraz I–III roku studiów drugiego stopnia do udziału w konkursie na esej „Korzystanie z treści deepfake jako forma przetwarzania danych osobowych”. Organizatorami konkursu jest UODO oraz Krajowa Izba Radców Prawnych. Partnerem merytorycznym konkursu jest kancelaria Kobylańska Lewoszewski Mednis sp. j.

Zapraszamy, szczegóły znajdą Państwo na naszej stronie.

Drodzy Czytelnicy!

W kwietniowym wydaniu Biuletynu skupiamy się przede wszystkim na temacie Europejskiej przestrzeni danych o zdrowiu (EHDS). Związane jest to przede wszystkim z publikacją raportu dotyczącego źródeł danych o zdrowiu, przygotowanego przez Fundację AI One Health. W jego prezentacji ważną rolę odegrał prezes UODO Mirosław Wróblewski, który zwrócił uwagę na konieczność zabezpieczenia praw i wolności osób, których dane dotyczą, oraz transparentnego ich przetwarzania. Pod koniec marca zorganizowaliśmy konferencję poświęconą tej tematyce.

Wokół tematu danych dotyczących zdrowia jest też skoncentrowany wywiad z członkinią Społecznego Zespołu Ekspertów przy Prezesie UODO, Anetą Sieradzką. Podkreśla ona znaczenie społecznego zaufania w budowie systemu danych o zdrowiu, a także zwraca uwagę na „silosowość" obecnego systemu w Polsce – dane są zbierane oddzielnie przez liczne instytucje, a systemy ich wymiany pozostawiają wiele do życzenia, a czasem nie istnieją. Mamy więc jako kraj jeszcze wiele do zrobienia przy wdrażaniu Rozporządzenia EHDS.

W dziale „Naruszenia i kontrole" wskazujemy na – często pomijany lub lekceważony przez administratorów danych – temat zagrożeń wynikających z korzystania z poczty elektronicznej. W tekście wskazano najczęstsze metody cyberataków tą drogą, najczęściej popełniane błędy oraz dobre praktyki, które pozwolą zabezpieczyć się przed kradzieżą lub utratą danych.

Z kolei dział „Prawo i nowe technologie" tym razem skupia się na kwestiach prawnych – opisując ciekawy przypadek ujawnienia danych osobowych poprzez doręczenie, jednemu z obwinionych w sprawie o wykroczenia, aktu oskarżenia, zawierającego dane pozostałych obwinionych. Administratorów danych z sektora publicznego zainteresować może szczególnie tekst o zasadach publikowania skanów dokumentów w Biuletynie Informacji Publicznej. To ważne w kontekście zapowiedzianych sektorowych kontroli UODO na ten rok, które skupią się m.in. właśnie na BIP-ach.

W dziale o zarządzaniu danymi kontynuujemy cykl „DGA w pigułce", który przybliża regulacje przewidziane w Akcie o zarządzaniu danymi i prezentuje nowe spojrzenie na te przepisy. Tym razem skupiamy się na pojęciu altruizmu danych i związanych z nim organizacji. Tekst jest szczególnie aktualny, bowiem w kwietniu parlament przyjął ustawę wdrażającą DGA, która została podpisana przez Prezydenta RP. Przewiduje ona m.in. nowe zadania dla Prezesa UODO.

W dziale współpracy międzynarodowej prezentujemy wspólne stanowisko Europejskiej Rady Ochrony Danych (EROD), oraz Europejskiego Inspektora Ochrony Danych (EIOD) w sprawie propozycji przedstawionych przez Komisję Europejską. Dotyczą one Europejskiego Aktu Biometechnologicznego, oraz dyrektywy NIS 2 i Drugiego Aktu o Cyberbezpieczeństwie.

Relacjonujemy też udział prezesa UODO Mirosława Wróblewskiego w Cambridge Forum on International Privacy & Data Laws, gdzie dyskutowano o największych obecnie wyzwaniach dla ochrony danych, powodowanych przez rozwój nowych technologii. Z kolei przedstawiciele Urzędu wzięli udział w organizowanym przez EROD wydarzeniu dotyczącym wytycznych w kwestii targetowania reklamy politycznej.

Opisujemy również ciekawą decyzję organu nadzorczego we Włoszech, który nałożył karę na bank za nieprzestrzeganie wewnętrznych procedur, w skutek czego pracownik przez długi czas miał nieuprawniony dostęp do danych wielu klientów. W dziale poświęconym strefie Schengen, zgodnie z zapowiedzią, kontynuujemy temat Dyrektywy 2016/680, dotyczącej przetwarzania danych w wymiarze sprawiedliwości.

Pod koniec numeru wracamy do tematu ochrony danych o zdrowiu w rozmowie z wiceprezesem Naukowej Fundacji Polpharmy Krzysztofem Kurowskim, dotyczącej wspomnianego już raportu o źródłach danych medycznych. Jak co miesiąc zapowiadamy też ciekawe wydarzenia organizowane lub współorganizowane przez UODO.

Zapraszamy do lektury!

Karol Witowski
Dyrektor Departamentu Komunikacji Społecznej
Rzecznik Prasowy UODO

NAJWIĘKSZYM WYZWANIEM NIE JEST TECHNOLOGIA, LECZ ZAUFANIE – MÓWI ANETA SIERADZKA

Ludzie są gotowi dzielić się danymi, jeśli widzą sens i mają poczucie kontroli. Dlatego kluczowe jest zapewnienie pełnej transparentności – kto korzysta z danych, kiedy, w jakim celu i jakie są tego efekty. Równie ważne jest pokazanie wartości zwrotnej, czyli tego, że dzięki tym danym poprawia się jakość leczenia i funkcjonowanie całego systemu – mówi Aneta Sieradzka, członkini Społecznego Zespołu Ekspertów przy Prezesie UODO.

Czym jest altruizm danych i dlaczego ma on kluczowe znaczenie w przypadku Europejskiej przestrzeni danych dotyczących zdrowia?

Altruizm danych to coś znacznie więcej niż techniczna zgoda na przetwarzanie informacji. To nowy wymiar odpowiedzialności społecznej, w którym obywatele świadomie współtworzą przyszłość medycyny. W kontekście Europejskiej przestrzeni danych zdrowotnych to absolutny fundament – bez gotowości ludzi do dzielenia się danymi w imię dobra wspólnego nie zbudujemy systemu zdolnego do realnych przełomów, choćby w medycynie spersonalizowanej czy profilaktyce chorób, a medycyna prewencyjna to fundament longevity (długowieczności). To również potrzeba zmiany kulturowej, w której dane przestają być postrzegane wyłącznie jako zasób prywatny, a zaczynają pełnić funkcję dobra wspólnego. W dłuższej perspektywie może to zdefiniować na nowo relację między jednostką a systemem ochrony zdrowia.

Na jakich filarach opiera się system tworzony przez rozporządzenie EHDS?

EHDS opiera się na bardzo ambitnej architekturze, która łączy cztery kluczowe elementy: kontrolę obywatela nad własnymi danymi, interoperacyjność systemów, możliwość wtórnego wykorzystania danych oraz wysoki poziom bezpieczeństwa. To nie jest zwykła regulacja sektorowa – to próba stworzenia europejskiego modelu zarządzania danymi zdrowotnymi, który może się stać globalnym punktem odniesienia. Każdy z tych elementów musi działać równolegle i w sposób skoordynowany, inaczej system straci swoją spójność. W praktyce oznacza to konieczność ścisłej współpracy między regulatorami, sektorem publicznym i prywatnym. I to muszą teraz zrozumieć polscy decydenci – że nie są to kolejne regulacje, które wystarczy wdrożyć na ostatnią chwilę. EHDS to ogromna szansa dla naszej gospodarki – możemy jako kraj dużo zyskać, lub szansę zmarnować i patrzeć jak inni zrobili to lepiej i szybciej. EHDS to wyzwanie dla wielu resortów, nie tylko MZ, ale np. MF, MS, MNiSW, MRiT, aby systemowo podejść do tej dużej unijnej reformy. Dzięki EHDS rozwój sztucznej inteligencji w Unii Europejskiej znacznie przyspieszy.

Jak przekonać ludzi do dobrowolnego dzielenia się danymi o stanie zdrowia w świecie, w którym te dane są coraz bardziej traktowane jak waluta?

1 ROZMOWA Z EKSPERTEM

Największym wyzwaniem nie jest technologia, lecz zaufanie. Ludzie są gotowi dzielić się danymi, jeśli widzą sens i mają poczucie kontroli. Dlatego kluczowe jest zapewnienie pełnej transparentności – kto korzysta z danych, kiedy, w jakim celu i jakie są tego efekty. Równie ważne jest pokazanie wartości zwrotnej, czyli tego, że dzięki tym danym poprawia się jakość leczenia i funkcjonowanie całego systemu.

Pacjent potrzebuje mieć dostęp do dobrej i szybkiej diagnostyki, bez której nie ma leczenia – bez dostępu do leczenia pacjenci umierają. Trudno oczekiwać długofalowego zaangażowania obywateli, jeśli latami będą czekać na wizytę czy badanie u specjalisty w ramach NFZ, a za rogiem odpłatnie można to zrobić niemalże z dnia na dzień. Warszawa oferuje bardzo szeroki i szybki dostęp do świadczeń komercyjnych, ale stolica to nie kraj, lecz wycinek.

Zaufanie buduje się latami, ale można je stracić w jednej chwili. Po różnych medialnych aferach z ostatnich lat, gdzie wykorzystywano dane medyczne do walk politycznych, jest to trudne wyzwanie. Należy zacząć od wymagania wyjątkowych postaw etycznych od decydentów, przez urzędników i menedżerów na różnych poziomach, aż po rolę samorządów medycznych w budowaniu kultury ochrony danych. Dziś lekarz powinien być pośrednikiem w budowaniu tego zaufania. Tylko jak ma to robić, gdy w praktyce świadomość personelu medycznego wobec ochrony danych jest bardzo różna. Środowiska medyczne same też powinny podejmować działania, aby o zaufanie pacjenta zabiegać.

Jak zabezpieczyć ogromną ilość wrażliwych danych, skoro już teraz specjaliści od cyberbezpieczeństwa mówią, że wyciek jest tylko kwestią czasu i nie da się mu zapobiec?

Musimy realistycznie podejść do kwestii bezpieczeństwa danych. W świecie cyfrowym nie istnieją systemy całkowicie odporne na incydenty. Dlatego zamiast obiecywać pełną szczelność, powinniśmy budować systemy odporne – takie, które minimalizują ryzyko, szybko wykrywają zagrożenia i potrafią skutecznie ograniczać ich skutki. To fundamentalna zmiana myślenia o cyberbezpieczeństwie.

Równie ważna jest edukacja użytkowników i instytucji, bo czynnik ludzki zawsze pozostaje najsłabszym ogniwem. Edukacja rozumiana jako proces, a nie odhaczanie raz na kilka lat szkoleń kiepskiej jakości, aby był „papier” po takim wydarzeniu. Ostatecznie bezpieczeństwo to wspólna odpowiedzialność wszystkich uczestników ekosystemu. Cyberbezpieczeństwa nie można sprowadzać do kupna wyłącznie infrastruktury, potrzebna jest specjalistyczna kadra, wewnętrzna lub zewnętrzna, która zapewnia kompleksowe wsparcie – rynek dziś oferuje wysokospecjalistyczne i komfortowe usługi w tym zakresie.

Jak spojrzymy na głośne medialnie przykłady hakowania szpitali w Polsce, które tygodniami nie mogły powrócić do normalnego funkcjonowania, to jawi nam się obraz rażących, długoletnich zaniedbań. Dziś organizacje muszą sobie odpowiadać na pytanie, czy stać je na to, że linia produkcyjna stanie lub sale operacyjne zostaną wyłączone na dni lub nawet tygodnie. Kiedy prezes o świcie dzwoni do „bezpieczników”, prawników i ludzi od kryzysów medialnych, to oznacza bardzo duży rachunek kosztów, stąd należy zapobiegać, a nie gasić (bardzo drogo) pożary. Bezpieczeństwo to zawsze inwestycja, a nie koszt.

Czy przepisy EHDS da się pogodzić z innymi aktami UE regulującymi przetwarzanie danych (DSA, AI Act, DGA, RODO), czy też pojawiają się tutaj znaczące sprzeczności?

1 ROZMOWA Z EKSPERTEM

EHDS funkcjonuje w bardzo złożonym otoczeniu regulacyjnym. Mamy RODO, AI Act, DGA czy DSA – i one wszystkie dotykają danych w różny sposób. Nie widzę tu sprzeczności systemowych, ale widzę ryzyko niespójności interpretacyjnej. Dlatego kluczowe będzie wypracowanie jasnych wytycznych, które pozwolą instytucjom działać bez obawy o naruszenie prawa. Bez tego istnieje ryzyko tzw. efektu mrożącego, który zahamuje innowacje.

Harmonizacja praktyki stosowania prawa będzie równie ważna jak same przepisy. I tu znów wyzwanie dla ustawodawcy, aby nie popełnić błędów jak w przypadku RODO. Wiele sektorowych przepisów krajowych do dziś nie zostało dostosowanych do możliwości, jakie oferuje RODO. Np. deregulacja przepisów dotyczących anonimizacji w udostępnianiu danych na cele naukowe czeka na ministerialnych biurkach – co jest zresztą inicjatywą i wysiłkiem prezesa UODO Mirosława Wróblewskiego, bo przez dekadę żadnej instytucji nie chciało się nic w tym obszarze skutecznie zrobić. Podkreślam – skutecznie – bo mówić, a robić to nie to samo.

W Europie istnieją już duże zbiory danych medycznych. Czego doświadczenia z nimi uczą nas w kwestii EHDS?

Europa już zgromadziła ogromne ilości danych medycznych, ale ich potencjał pozostaje w dużej mierze niewykorzystany. Powody są trzy: brak interoperacyjności, bariery prawne i niski poziom zaufania. EHDS ma szansę to zmienić, pod warunkiem że nie powieli dotychczasowych błędów i rzeczywiście ujednolici zasady gry. Kluczowe będzie także zapewnienie wysokiej jakości danych, bo ich wartość zależy od wiarygodności. Bez tego nawet największe zbiory nie przełożą się na realne korzyści. Powinniśmy w Polsce zabrać się za wielkie porządkowanie danych medycznych już dziś. I to na wielu poziomach, od instytucji centralnych, które same nie wiedzą, jakie dane posiadają, przez szpitale, po uczelnie medyczne. Żaden lekarz nie jest właścicielem danych pacjentów, choć w praktyce niejeden sobie takie prawo uzurpuje, naruszając przy tym przepisy. Teraz jest dobry czas na audyty EHDS w podmiotach, które przetwarzają dane zdrowotne na dużą skalę.

Jak zapewnić równy podział korzyści ze wspólnej przestrzeni danych dotyczących zdrowia?

Nie możemy budować systemu, w którym dane pochodzą od obywateli, a korzyści trafiają wyłącznie do wąskich grup np. biznesów farmaceutycznych, ubezpieczycieli, fintech, czy niektórych badaczy, którzy uczynią sobie dobry biznes z analizy danych zdrowotnych. Musimy wdrażać sztuczną inteligencję do sektora publicznego, aby ta technologia identyfikowała nieprawidłowości w przepalaniu pieniędzy podatników, aby weryfikowała zasadność, w tym oceny wniosków, albo czy recenzje nie pochodzą z Chata GPT. Sprawiedliwy podział wartości to warunek trwałości całego projektu. Oznacza to m.in. dostęp do wyników badań, wzmacnianie publicznych systemów ochrony zdrowia i realne korzyści dla pacjentów.

W przeciwnym razie pojawi się społeczny opór wobec dzielenia się danymi, co będzie zrozumiałe. A bez społecznej legitymizacji żaden system danych nie będzie funkcjonował efektywnie. Pacjent musi mieć faktyczne prawo do informacji o tym, co się dzieje z jego danymi. Dziś ma to prawo tylko częściowo zapewnione, bo nie wie, kto, kiedy i w jakim celu przegląda jego dane. Dane pacjentów wykorzystywane w badaniach klinicznych powinna cechować pełna transparentność, zaś do tego służy ogrom cyfrowych narzędzi, a nie kartka papieru. Ponadto nie każdy sukces medialny w medycynie jest faktycznym sukcesem medycznym.

1 ROZMOWA Z EKSPERTEM

Jaka jest różnica między pierwotnym a wtórnym wykorzystaniem danych medycznych?

Rozróżnienie między pierwotnym a wtórnym wykorzystaniem danych jest absolutnie kluczowe. Pierwotne dotyczy bezpośredniego leczenia pacjenta, natomiast wtórne obejmuje badania, innowacje i polityki publiczne. To rozróżnienie determinuje zarówno podstawy prawne, jak i sposób zarządzania zgodą pacjenta. W praktyce wymaga to bardzo precyzyjnych mechanizmów zarządzania dostępem do danych. Każde niejasności w tym zakresie mogą prowadzić do utraty zaufania i sporów prawnych.

Niedawno fundacja AI One Health, której jest Pani prezesem, przygotowała raport mapujący źródła danych medycznych. Jakie są te źródła i do czego można je wykorzystać?

Dzisiejszy ekosystem danych zdrowotnych jest znacznie szerszy niż tradycyjna dokumentacja medyczna. Obejmuje dane z urządzeń noszonych, aplikacji mobilnych, badań genomowych czy rejestrów chorób. To ogromna szansa, ale też wyzwanie, bo wymaga integracji bardzo różnych typów informacji. Każde z tych źródeł odznacza się inną jakością i dynamiką aktualizacji danych. Dlatego konieczne jest opracowanie spójnych standardów ich przetwarzania. Bez tego jako kraj nie ruszymy do przodu. Chodzi o rozwój, a nie dreptanie w miejscu.

Dobrym przykładem państwowej platformy jest Internetowe Konto Pacjenta, do którego nie trafia każda dokumentacja, bo nie ma narzędzia do egzekwowania tego obowiązku od szpitali. Kolejny przykład: system P1, gdzie jest obowiązek wpisywania każdej wizyty, ale w praktyce nie ma narzędzia do egzekucji tego obowiązku od lekarzy – dużo danych więc „gubimy" przez dziurawe rozwiązania. Następnie, badanie satysfakcji pacjentów jest u nas symboliczne, a winno być standardem przy każdej zmianie systemowej, gdy wykorzystywane są środki publiczne. Nasz raport można wykorzystać do tworzenia polityk publicznych, identyfikujemy w nim dostępne dane, porządkuje on ekosystem danych, ujawnia luki informacyjne, wspiera decyzje oparte na dowodach (evidence-based policy). Raport ma też walor edukacyjny dla lekarzy oraz pacjentów, aby wiedzieli, jak zarządzanie ich danymi o zdrowiu wpływa na dostęp do diagnostyki i leczenia.

Jak zapewnić równowagę między interoperacyjnością a ochroną prywatności pacjentów?

Nie powinniśmy traktować interoperacyjności i prywatności jako przeciwieństw. Nowoczesne podejście polega na projektowaniu systemów, które łączą oba te elementy – poprzez minimalizację danych, pseudonimizację i kontrolowany dostęp. To kwestia dobrego projektowania, a nie kompromisu. W praktyce oznacza to konieczność stosowania zasady privacy by design na każdym etapie tworzenia systemu. Tylko wtedy można zbudować rozwiązania, które są jednocześnie użyteczne i bezpieczne. To właśnie ochrona prywatności powinna być przewagą konkurencyjności na rynku usług, a audytowanie dostawców przed wdrożeniem powinno być standardem.

Jakie są obecnie problemy z ponownym wykorzystaniem danych i jakich zmian legislacyjnych potrzeba w tym względzie (jak wskazywał Prezes UODO)?

Dziś największym problemem nie jest brak danych, lecz brak możliwości ich ponownego wykorzystania. Instytucje często obawiają się konsekwencji prawnych i wolą nie działać. Z poziomu wielu instytucji, od tych centralnych po lokalne szpitale, obserwuje się uchylanie się od decyzyjności i odpowiedzialności.

Ta niechęć bierze się też z braku kompetencji, wiedzy i doświadczenia w wielu organizacjach, które przetwarzają dane szczególnie wrażliwe. Dochodzą także partykularne interesy, lepiej się nie wychylać, bo można stracić posadę, albo co gorsza, „zrobić komuś dobrze". Nie daj Boże jakiś inny lekarz zrobi świetne badania na danych zebranych w naszej klinice albo wykryje błędy w leczeniu – takich praktyk, gdzie decyduje uznaniowość, a nie wyłącznie podstawy prawne, jest całkiem sporo na rynku. Potrzebujemy jasnych, uproszczonych zasad, które umożliwią bezpieczne i legalne korzystanie z danych w celach badawczych, co nie oznacza, że teraz ta wymiana nie jest możliwa. Trzeba tylko sięgać po narzędzia dostępne na rynku, a prawnicy są od rozwiązywania problemów, a nie generowania kolejnych. Kluczowe jest również skrócenie czasu uzyskiwania zgód i decyzji administracyjnych. Bez tego tempo innowacji pozostanie niewystarczające. Potrzebujemy egzekucji, bo same deklaracje to tylko opowieści.

Co należy zrobić, by odpowiednio korzystać z istniejących już zbiorów danych o zdrowiu?

Europa już poniosła ogromne koszty gromadzenia danych zdrowotnych. Teraz kluczowe jest ich efektywne wykorzystanie. To oznacza inwestycje w jakość danych, ich standaryzację oraz rozwój kompetencji analitycznych – instytucje powinny inwestować w zatrudnianie analityków danych. Inaczej pozostaniemy na etapie niewykorzystanego potencjału. Równie ważne jest tworzenie mechanizmów współpracy między instytucjami. Dane muszą zacząć pracować w ekosystemie, a nie w izolacji. Należy inwestować w kadry, czerpać z know-how, jakie ma biznes. Należy zmieniać także mentalność urzędników, bo nowe regulacje nie sprawią, że nagle system zacznie działać lepiej. I to też od początku robimy w naszej Fundacji AI One Health, budujemy technologiczne mosty, tworzymy merytoryczny dialog, działając interdyscyplinarnie.

Dlaczego nie jesteśmy na tak zaawansowanym etapie wdrażania systemu jak Dania, Finlandia czy Wielka Brytania?

Kraje takie jak Dania czy Finlandia osiągnęły sukces, ponieważ konsekwentnie budowały swoje systemy przez lata, opierając je na zaufaniu i spójnej strategii państwa. W wielu innych krajach zabrakło tej ciągłości i koordynacji. Kluczowa była także stabilność regulacyjna i jasna wizja rozwoju. W Polsce tego stanowczo brakuje, brak przewidywalności prawa znacznie hamuje rozwój gospodarczy, a to z kolei nie są dobre warunki do rozwoju innowacji. To pokazuje, że transformacja cyfrowa w ochronie zdrowia to maraton, a nie sprint jednej kadencji sejmu czy zmieniających się ministrów.

Ponadto Polska pomimo rozwoju e-zdrowia w ostatnich latach ma dekady zaniedbań w obszarze kultury ochrony danych medycznych, którą właściwie zaczęliśmy budować od wejścia w życie RODO, pomimo świętości, jaką jest tajemnica lekarska. Zmiana nawyków, przyzwyczajeń to nie działania jednorazowe, to proces rozłożony w czasie. Najtrudniejsza jest zmiana mentalności. Potrzebujemy wizjonerów, przywództwa i charyzmy, prawdziwego partnerstwa i transparentności, a nie uprawiania niskich lotów marketingu, że jest dobrze, kiedy liczby mówią, że nie jest.

Co można zrobić, by zachęcić instytucje do wymiany danych i ograniczyć zamknięcie ich w systemie silosowym?

1 ROZMOWA Z EKSPERTEM

Silosy danych to nie problem technologiczny, lecz instytucjonalny, mentalny i kompetencyjny. Wynikają z braku zaufania, jasnych zasad i odpowiednich bodźców. Jeśli stworzymy środowisko, w którym dzielenie się danymi jest bezpieczne i opłacalne, instytucje zaczną współpracować. Potrzebna jest też instytucja lider, która chwyciłaby lejce i nadała temu procesowi prędkość, a dziś takiej nie ma. Obecnie transfery danych medycznych odbywają się w różnych hermetycznych gremiach, wytworzono jakąś hierarchiczność i poczucie, że dane są dostępne dla niektórych badaczy. Po prostu mamy uznaniowość udostępniania danych, co jest niegodną praktyką. Niezbędne są również mechanizmy odpowiedzialności i jasne reguły zarządzania ryzykiem.

Dopiero wtedy wymiana danych stanie się standardem, a nie wyjątkiem. I tu ważna rola organu, jakim jest UODO, który już drugi rok z rzędu kontroluje w ramach kontroli sektorowych ochronę zdrowia. Powinien to też robić w kolejnych latach, cyklicznie, z uwagi na rosnące zaniedbania w organizacjach, które ten ekosystem tworzą. Sporo rekomendacji przedstawiliśmy w naszym raporcie „Mapa źródeł danych medycznych w Polsce", w którym eksperci z różnych dziedzin bardzo odważnie mówią o tym, że mają dość systemu, który oferuje warunki nieprzystające do możliwości, zasobów intelektualnych w kraju i współczesnej nauki na światowym poziomie.

Jak możemy skorzystać z tych danych dzięki narzędziom AI, blockchain i nowym technologiom?

Nowe technologie otwierają zupełnie nowe możliwości wykorzystania danych zdrowotnych. Sztuczna inteligencja pozwala na analizę na niespotykaną dotąd skalę, a technologie takie jak blockchain mogą zwiększyć przejrzystość i kontrolę nad danymi. Kluczowe jest jednak to, by technologia była narzędziem, a nie celem samym w sobie. Największą wartość generuje połączenie technologii z wysokiej jakości danymi i odpowiednim zarządzaniem.

To właśnie na tym styku powstają najbardziej przełomowe innowacje. Powinniśmy czerpać dobre wzorce ze świata, ale też finansować te programy, za którymi stoi walidacja, dostęp do publicznych danych pokazujących postęp, skuteczność, skalę. Instytucje publiczne nie mają w swoich kompetencjach przepalania publicznych pieniędzy, choć to niestety także robią. I tu bardzo potrzebujemy sztucznej inteligencji, która może być znakomitym sprzymierzeńcem transparentności i budowania zaufania do systemu ochrony zdrowia.

Dziękuję za rozmowę!

POCZTA ELEKTRONICZNA JAKO ŚRODOWISKO PRZETWARZANIA DANYCH I POTENCJALNE ŹRÓDŁO NARUSZEŃ

Wśród naruszeń ochrony danych osobowych zgłaszanych do Prezesa UODO znaczną część stanowią te związane z niewłaściwym zabezpieczeniem danych przetwarzanych za pośrednictwem poczty elektronicznej. Najczęściej są to incydenty wynikające z włamania na służbowe skrzynki oraz przesyłania niezabezpieczonych dokumentów, co bezpośrednio zagraża ich poufności i integralności.

W związku z tym kluczowe jest, aby organizacje **regularnie dokonywały przeglądu procesów biznesowych opartych na komunikacji elektronicznej**. Pozwoli to na **identyfikację miejsc, w których dane mogą być narażone na nieautoryzowany dostęp** lub **przypadkowe ujawnienie**. Analiza naruszeń ochrony danych osobowych wskazuje na niepokojący trend: **wiele organizacji traktuje skrzynki poczty elektronicznej jako domyślne archiwum dokumentów** oraz bezpieczne **repozytorium do długotrwałego przetwarzania danych**. Często brakuje przy tym refleksji nad fizyczną lokalizacją serwerów przechowujących te tysiące wiadomości, a także nad tym, czy standardowa obsługa codziennej korespondencji zapewnia poziom bezpieczeństwa adekwatny do wagi przesyłanych informacji.

Poczta elektroniczna służy do bieżącej komunikacji, a nie do długoterminowego przechowywania danych — traktowanie jej jako archiwum narusza zarówno zasady bezpieczeństwa, jak i zasady retencji.

Konieczność wprowadzenia i przestrzegania zasad retencji danych

Kluczowe jest, **aby każda organizacja uwzględniła pocztę elektroniczną w swojej analizie ryzyka naruszenia praw lub wolności** osób fizycznych. Wykorzystywanie poczty elektronicznej do przesyłania danych osobowych wiąże się ze specyficznymi zagrożeniami, które administrator musi zidentyfikować, aby skutecznie zminimalizować prawdopodobieństwo ich wystąpienia oraz ograniczyć ich potencjalne skutki. **Dane** przetwarzane za pośrednictwem poczty elektronicznej **muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą,** przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania. W związku z tym **niezbędne jest określenie i wdrożenie polityki retencji danych**, a następnie **regularna weryfikacja jej przestrzegania**. Brak polityki retencji lub jej nieprzestrzeganie prowadzi do przechowywania wiadomości bez podstawy prawnej, co **narusza zasady określone w art. 5 RODO.**

Poza aspektem prawnym istotny jest również wymiar biznesowy: przechowywanie zbędnej korespondencji generuje dodatkowe koszty operacyjne związane z utrzymaniem zasobów serwerowych, które nie przekładają się na żadną wartość dla organizacji.

2 NARUSZENIA I KONTROLE

Główne kategorie naruszeń ochrony danych osobowych dot. poczty elektronicznej

Analiza zgłoszeń naruszeń ochrony danych pozwala na wyodrębnienie dwóch kluczowych kategorii naruszeń ochrony danych osobowych związanych z wykorzystaniem poczty elektronicznej:

1. **NIEUPRAWNIONY DOSTĘP DO SKRZYNEK POCZTOWYCH**
2. **TRANSMISJA DANYCH BEZ ODPOWIEDNICH ZABEZPIECZEŃ**

NIEUPRAWNIONY DOSTĘP DO SKRZYNEK POCZTOWYCH

Przyczyny:

Analiza naruszeń pozwala wskazać **trzy główne źródła sytuacji**, w których dochodzi do przejęcia kontroli nad służbową pocztą elektroniczną:

1. Phishing i brak świadomości zagrożeń

Wielu administratorów danych wciąż nie przywiązuje należytej wagi do budowania świadomości zagrożeń wśród pracowników. Braki te objawiają się szczególnie w obszarze **ataków socjotechnicznych**. W wielu organizacjach:

- Kwestie bezpieczeństwa są pomijane w procesach szkoleniowych.
- Nie przeprowadza się kontrolowanych symulacji ataków, które pozwoliłyby zweryfikować czujność personelu.
- Brakuje rozwiązań technicznych wspierających wykrywanie i blokowanie podejrzanych wiadomości.

2. Niewłaściwa higiena poświadczeń

Znaczna część naruszeń wynika z **błędów w zarządzaniu hasłami**. Do najczęstszych problemów należą:

- **Powtarzalność haseł**: używanie tych samych danych logowania w wielu różnych serwisach (prywatnych i służbowych).
- **Niewłaściwe przechowywanie**: Zapisywanie haseł na fizycznych nośnikach (np. karteczkach) w pobliżu stanowiska pracy.
- **Synchronizacja z kontami prywatnymi**: wykorzystywanie wbudowanych w przeglądarki mechanizmów synchronizacji haseł z prywatnym kontem pracownika. W przypadku włamania na konto prywatne cyberprzestępcy automatycznie uzyskują dostęp do wszystkich poświadczeń służbowych zapamiętanych w przeglądarce.
- **Brak poufności:** przeprowadzanie procesu uwierzytelniania w sposób umożliwiający podejrzenie danych przez osoby postronne.

Złośliwe oprogramowanie typu „info stealer”

Infekcje tym typem malware’u wynikają zazwyczaj z nieświadomego uruchomienia przez użytkownika pliku podszywającego się pod bezpieczny dokument (np. instalator, aktualizacja lub faktura).

- **Mechanizm działania**: Po uruchomieniu złośliwy kod działa w tle, gromadząc dane z przeglądarek i systemów, a następnie przesyła je do atakującego.
- **Manipulacja**: Infekcje info-stealerami są zwykle poprzedzone socjotechniką — np. fałszywymi komunikatami o błędach lub stronami podszywającymi się pod legalne oprogramowanie. Kluczowym momentem jest interakcja użytkownika; system rzadko instaluje takie oprogramowanie samodzielnie bez otwarcia zainfekowanego pliku.
- **Uprawnienia administratora**: Ryzyko potęguje praca na kontach z pełnymi uprawnieniami administracyjnymi bez wyraźnej potrzeby biznesowej. W takim środowisku malware może głębiej infiltrować system, modyfikować ustawienia i skuteczniej omijać zabezpieczenia.

Dobre praktyki:

Mając świadomość zagrożeń**, należy podejmować działania minimalizujące ryzyko** ich materializacji. Kluczowym krokiem jest uwzględnienie tych scenariuszy w **analizie ryzyka** oraz wdrożenie poniższych środków kontrolnych:

1. Budowanie świadomości

Regularna edukacja to pierwsza linia obrony. Oto środki, które warto wdrożyć w tym zakresie.

- **Cykliczne szkolenia:** powinny bazować na aktualnych trendach (np. socjotechnika, vishing) i opisywać rzeczywiste przypadki naruszeń, z którymi pracownik może zetknąć się w codziennej pracy.
- **Symulacje ataków:** warto aktywnie weryfikować wiedzę poprzez kontrolowane kampanie phishingowe. Pozwala to zidentyfikować „słabe punkty” i dopasować program szkoleniowy do realnych potrzeb.

2. Uwierzytelnianie wieloskładnikowe (MFA)

Wdrożenie dodatkowego składnika uwierzytelniającego sprawia, że samo przejęcie loginu i hasła nie wystarczy do włamania.

- **Zasada „coś wiesz i coś masz**”: nawet jeśli hasło wycieknie, cyberprzestępca nie uzyska dostępu bez dodatkowego „sekretu” (np. kodu z aplikacji, klucza sprzętowego czy powiadomienia „push”).
- **Prewencja zamiast reakcji:** MFA powinno być standardem od samego początku, a nie funkcjonalnością włączaną dopiero po wykryciu incydentu.

3. Dostęp warunkowy

Ograniczenie powierzchni ataku poprzez restrykcje lokalizacyjne.

- **Białe listy IP:** tam, gdzie to możliwe, dostęp do systemów pocztowych i administracyjnych powinien być ograniczony do firmowych adresów IP.

- **Ograniczenia geograficzne:** jeśli organizacja nie prowadzi operacji w egzotycznych regionach świata (tj. poza EOG), warto zablokować możliwość logowania z tych lokalizacji. Większość przejętych kont jest wykorzystywana do masowej wysyłki spamu właśnie z serwerów zlokalizowanych w odległych państwach.

4. Ochrona przed atakami siłowymi (Brute Force)

Automatyczne mechanizmy blokujące próby siłowego odgadnięcia hasła. Warto rozważyć wdrożenie m.in. następujących rozwiązań:

- **Limity prób logowania:** System powinien automatycznie blokować konto (tymczasowo lub do interwencji administratora) po określonej liczbie nieudanych prób logowania.
- **Monitorowanie logów:** Analiza nieudanych logowań pozwala na wczesne wykrycie trwającego ataku na infrastrukturę organizacji.

TRANSMISJA DANYCH BEZ ODPOWIEDNICH ZABEZPIECZEŃ

Właściwe zabezpieczenie dostępu do poczty elektronicznej nie zawsze wystarczy do tego, żeby uniknąć naruszenia ochrony danych osobowych. **Duża liczba zgłoszeń wynika z faktu, że procesy biznesowe realizowane organizacji nie uwzględniają potrzeby zabezpieczania dokumentów i danych przesyłanych** za pomocą poczty elektronicznej.

Przyczyny:

Niewłaściwe procesy biznesowe i błędy ludzkie są równie groźne jak ataki hakerskie. Poniżej przedstawiono główne przyczyny naruszeń ochrony danych osobowych związanych z obsługą poczty elektronicznej:

Przesyłanie dokumentów zawierających dane osobowe (np. skany dowodów, umowy, wnioski) w formie otwartych, **niezabezpieczonych plików.**

- **Mechanizm działania:** Poczta elektroniczna nie zapewnia domyślnie szyfrowania „end-to-end”, co oznacza, że treść wiadomości może być dostępna dla podmiotów pośredniczących oraz całkowicie niechroniona w przypadku błędnego adresata. Wiadomość bez zaszyfrowanego załącznika można porównać do **karty pocztowej** – jej treść jest widoczna dla każdego, kto wejdzie w jej posiadanie. Podczas transmisji dane przechodzą przez liczne węzły i serwery pośredniczące, na których mogą zostać odczytane. Co kluczowe, **brak szyfrowania powoduje, że plik nie posiada żadnej „warstwy ochronnej”, która chroniłaby dane w przypadku pomyłki nadawcy.**
- **Skutek:** Wysłanie wiadomości do błędnego adresata skutkuje natychmiastowym ujawnieniem danych, nad którymi administrator traci kontrolę w chwili naciśnięcia „Wyślij”. **Osoba nieuprawniona zyskuje pełny wgląd w treść dokumentów bez konieczności podejmowania jakichkolwiek działań technicznych**. Brak hasła sprawia, że administrator traci jakąkolwiek kontrolę nad zakresem ujawnionych informacji już w sekundzie kliknięcia przycisku „Wyślij”.

2. Nadmierne zaufanie do mechanizmu autouzupełniania adresów

Nadmierne zaufanie do mechanizmu autouzupełniania adresów może prowadzić do wysyłki danych do niewłaściwych osób.

- **Mechanizm działania:** Po wpisaniu pierwszych liter imienia lub nazwiska system sugeruje adresy z książki adresowej lub historii korespondencji. Chwila nieuwagi powoduje wybranie osoby o podobnych danych, ale z zupełnie innego kontekstu biznesowego.
- **Manipulacja/Błąd:** Pośpiech i rutyna sprawiają, że użytkownik nie weryfikuje pełnego adresu przed kliknięciem przycisku „Wyślij", co w połączeniu z brakiem szyfrowania plików prowadzi do utraty poufności**.**

3. Błędy edytorskie w adresach e-mail

Pomyłki powstające na etapie wprowadzania danych do systemów, szczególnie podczas przepisywania ich z formularzy papierowych lub rozmów telefonicznych.

- **Mechanizm działania:** Pojedyncza literówka (tzw. „czeski błąd") lub błąd w domenie może spowodować, że wiadomość trafi do przypadkowego odbiorcy lub na serwer przeznaczony do przejmowania błędnie zaadresowanej poczty.
- **Skutek**: Dane trafiają do zupełnie obcej osoby, co stwarza ryzyko ich nieuprawnionego wykorzystania lub dalszego upublicznienia.

4. Wysyłka masowa bez użycia pola „UDW"

Ujawnienie list adresowych poprzez umieszczenie wielu odbiorców w widocznym polu „Do" lub „DW".

- **Mechanizm działania:** Pracownik wysyła wiadomość do grupy osób (np. pacjentów), nie ukrywając ich tożsamości przed pozostałymi uczestnikami korespondencji.
- **Skutek:** Każdy z odbiorców dowiaduje się o tożsamości pozostałych osób z grupy. Sam fakt przynależności do określonej listy (np. grupy terapeutycznej) jest informacją „wrażliwą", której ujawnienie stanowi naruszenie ochrony danych osobowych.

Dobre praktyki:

Wdrożenie **odpowiednich nawyków oraz standardów technicznych** pozwala niemal całkowicie wyeliminować ryzyko naruszenia ochrony danych, nawet w przypadku pomyłki adresata. Poniższe zasady stanowią fundament kultury bezpieczeństwa w organizacji, łącząc proste rytuały uważności z profesjonalnymi mechanizmami ochrony poufności przesyłanych informacji.

1. Szyfrowanie załączników jako fundament poufności

Szyfrowanie minimalizuje skutki ewentualnego naruszenia, ponieważ uniemożliwia osobom nieuprawnionym dostęp do treści.

- **Szyfrowanie pełni funkcję warstwy ochronnej** — zabezpiecza dane zarówno przed błędnym adresatem, jak i przed dostępem podmiotów pośredniczących**.**

- **Standardy haseł:** Zgodnie z międzynarodowymi normami (np. ISO/IEC 27002) hasła nie mogą zawierać informacji łatwych do powiązania z użytkownikiem. Ponadto numer PESEL nie spełnia kryteriów silnego hasła ze względu **na niską entropię**. Ma stałą długość (11 cyfr) i przewidywalną strukturę — pierwszych sześć cyfr to data urodzenia, a pozostałe są generowane według znanych reguł. To sprawia, że liczba możliwych kombinacji jest ograniczona i podatna na ataki siłowe.
- **Zasada dwóch kanałów:** Hasło do zaszyfrowanego pliku nigdy nie powinno być przesyłane w tej samej wiadomości co załącznik. Prawidłowa procedura zakłada przekazanie hasła innym kanałem komunikacji (np. SMS, telefon, bezpieczny komunikator).

2. Weryfikacja przedwysyłkowa (Rytuały uważności)

Mechanizmy kontrolne mające na celu przełamanie rutyny i automatyzmów, które są najczęstszą przyczyną incydentów typu „błąd ludzki".

- **Reguła 3 sekund:** Tuż przed kliknięciem przycisku „Wyślij" należy zatrzymać się i ponownie zweryfikować pole adresata. To kluczowy moment na sprawdzenie, czy mechanizm autouzupełniania nie zasugerował błędnej osoby o podobnym nazwisku.
- **Test otwartego załącznika:** Dobrym nawykiem jest otwarcie pliku na moment tuż przed jego dołączeniem do wiadomości. Pozwala to na ostateczne upewnienie się, że przesyłamy właściwy dokument z danymi osoby, do której faktycznie kierujemy wiadomość.
- **Odpowiedzialność nadawcy:** Należy przyjąć zasadę ograniczonego zaufania do algorytmów programu pocztowego. System jest jedynie narzędziem wspomagającym, a ostateczna odpowiedzialność za poufność przesyłanych danych spoczywa na pracowniku wysyłającym wiadomość.

3. Ochrona tożsamości zbiorowej (Zasada UDW)

Stosowanie pola UDW przy wysyłkach masowych jest konieczne, ponieważ ujawnienie listy odbiorców może naruszać zasadę poufności wynikającą z RODO.

- **Poufność kontekstowa:** Sam fakt figurowania adresu na określonej liście (np. „Grupa wsparcia X", „Dłużnicy Y") ujawnia wrażliwe informacje o sytuacji życiowej odbiorcy. Stosowanie pola UDW (Ukryta Do Wiadomości) chroni te informacje przed nieuprawnionym wglądem pozostałych uczestników korespondencji.

Podsumowanie

Skuteczna ochrona danych osobowych w komunikacji e-mail wymaga odejścia od traktowania poczty jako „bezpiecznego sejfu" na rzecz świadomego zarządzania dynamicznym kanałem przesyłu informacji. Klucz do minimalizacji ryzyka naruszeń leży w synergii trzech obszarów:

- **Technologii:** Powszechne wdrożenie uwierzytelniania wieloskładnikowego (MFA), szyfrowania załączników oraz mechanizmów ochrony przed atakami siłowymi.

2 NARUSZENIA I KONTROLE

- **Procedur:** Rygorystyczne przestrzeganie polityki retencji danych, stosowanie bezpiecznych standardów haseł oraz bezwzględne wykorzystywanie pola UDW w komunikacji zbiorowej.
- **Świadomości:** Wypracowanie u pracowników „rytuałów uważności” oraz regularne testowanie czujności personelu poprzez symulacje ataków.

Ostatecznie bezpieczeństwo organizacji nie zależy wyłącznie od systemów teleinformatycznych — jego kluczowym elementem jest odpowiedzialność i czujność nadawcy w momencie wysyłania wiadomości.

EKONOMIKA PROCESOWA NIE UZASADNIA KIEROWANIA DO SĄDU JEDNEGO WNIOSKU O UKARANIE KILKU OBWINIONYCH

Przy sporządzaniu wniosku o ukaranie w sprawach o wykroczenia stosować należy wszelkie środki mające na celu minimalizację ryzyk związanych z nieprawidłowym przetwarzaniem danych osobowych. Choć zasada ekonomiki procesowej ma na celu usprawnienie i przyspieszenie procedowania spraw, nie może stanowić podstawy do nieograniczonego ujawniania danych osobowych uczestników postępowania.

Jedna ze straży miejskich zakończyła czynności wyjaśniające w sprawie o wykroczenie w postępowaniu zwyczajnym skierowaniem do sądu wniosku o ukaranie. Wniosek dotyczył pięciu osób obwinionych w podobnych okolicznościach sprawy (działanie w grupie w tym samym miejscu i czasie) i zawierał (stosownie do art. 57 ustawy z dnia 24 sierpnia 2001 r. Kodeks postępowania w sprawach o wykroczenia) następujące dane osobowe:

- imię,
- nazwisko,
- imiona rodziców,
- nazwisko panieńskie matki,
- datę urodzenia,
- numer PESEL,
- adres zamieszkania,
- opis popełnionych czynów i ich kwalifikację prawną (zarzuty),
- imiona i nazwiska świadków zdarzenia.

Wyrok i dane innych osób

Po kilku miesiącach jedna z osób obwinionych, przeciwko której skierowano wniosek o ukaranie, otrzymała z sądu rejonowego wyrok nakazowy wraz z wnioskiem o ukaranie w postępowaniu zwyczajnym. Skoro w jej przypadku **do wyroku dołączony został wniosek o ukaranie zawierający dane osobowe pozostałych obwinionych**, to powzięła przypuszczenie, że **również te osoby otrzymały wyroki nakazowe wraz z wnioskiem o ukaranie**, w którym zostały ujawnione wskazane wyżej dane osobowe.

Zwróciła się więc do straży miejskiej i do sądu rejonowego z wnioskami o wyjaśnienie sprawy. W jej opinii doszło bowiem do bezprawnego ujawnienia danych osobowych.

Opinie straży miejskiej i sądu

Straż miejska uznała, że nie jest właściwym adresatem w tej sprawie, gdyż to nie ona odpowiada za przekazanie kopii wniosku o ukaranie zawierającej dane osobowe współsprawców wykroczenia (kierując wniosek o ukaranie do sądu, nie przesyła jego kopii do obwinionych). Tłumaczyła, **że wniosek o ukaranie jest pismem procesowym skierowanym do sądu**, w którym określonej osobie/osobom przedstawiony jest zarzut/y popełnienia określonego wykroczenia (wykroczeń). Jednocześnie stanowi on żądanie rozpoznania sprawy i ukarania tej osoby/osób.

Jednocześnie zaznaczyła, że **art. 57 Kodeksu postępowania w sprawach o wykroczenia nie precyzuje sposobu formułowania wniosku o ukaranie wobec kilku sprawców** tożsamego wykroczenia, tj. tego, czy każdorazowo wniosek powinien zostać sporządzony wobec każdej z osób indywidualnie, czy może zawierać wskazanie kilku osób łącznie.

Mając na względzie art. 57 § 2 pkt 1 Kodeksu postępowania w sprawach o wykroczenia – jeśli okoliczności sprawy dotyczyły osób sobie postronnych, to można uznać, że wobec każdej z osób mógłby zostać skierowany odrębny wniosek o ukaranie, **lecz praktyka procesowa wskazuje na możliwość łączenia tożsamych spraw i kierowania jednego wniosku** o ukaranie kilku obwinionych.

Z kolei sąd odpowiedział, że **skierowanie do ukaranego wyroku nakazowego wraz z wnioskiem o ukaranie jest jego obowiązkiem i że nie może ingerować** (tj. anonimizować) **w treść otrzymanego od oskarżyciela wniosku** o ukaranie.

Jaka powinna być właściwa praktyka?

Po ponownej analizie sprawy (zainicjowanej kolejnym wnioskiem osoby ukaranej przez sąd) straż miejska uznała, że skoro zgodnie z art. 505 § 1 ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego odpis wyroku nakazowego doręcza się oskarżycielowi i pokrzywdzonemu, a oskarżonemu i jego obrońcy – wraz z odpisem aktu oskarżenia, to rzeczywiście w przypadku sporządzenia wniosku o ukaranie w sposób zbiorowy **oskarżony może wejść w posiadanie danych osobowych osób postronnych w sposób nieuprawnion**y. To zatem przemawiałoby za **sporządzaniem wniosku o ukaranie w sposób indywidualny dla każdej z osób**, wbrew przyjętym przez lata zasadom wyrażonym w doktrynie policyjno-prawnej i praktyce wymiaru sprawiedliwości.

W tej sytuacji Prezes UODO został poproszony o wskazanie prawidłowej praktyki w opisanym zakresie.

Niezależność sądu

W odpowiedzi **Prezes UODO wskazał**, że zarówno **przepisy RODO,** jak i normy określone w przepisach krajowych – ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych i ustawie z dnia 14 grudnia

2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości – **nie mają zastosowania do operacji przetwarzania danych dokonywanych w ramach czynności procesowych** w trybie przewidzianym w kodeksie postępowania w sprawach o wykroczenia (zob. art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości), w tym dokonywania doręczeń zarządzeń, zawiadomień, orzeczeń, wezwań lub innych pism stronom i uczestnikom procesu.

Co stanowią przepisy sektorowe?

Zgodnie z art. 57 kodeksu postępowania w sprawach o wykroczenia wniosek o ukaranie stanowi podstawę wszczęcia postępowania w sprawach o wykroczenia i jest składany przez uprawniony organ występujący w charakterze oskarżyciela publicznego, a wyjątkowo także przez pokrzywdzonego. Powinien on zawierać:

- dane obwinionego umożliwiające ustalenie jego tożsamości,
- opis zarzucanego czynu z uwzględnieniem miejsca, czasu, sposobu i okoliczności jego popełnienia,
- wskazanie dowodów oraz podpis i dane wnioskodawcy,

a w przypadku oskarżyciela publicznego także:

- kwalifikację prawną czynu,
- dane dotyczące sytuacji osobistej i majątkowej obwinionego,
- informacje o pokrzywdzonych,
- informacje o wysokości szkody,
- informacje o właściwości sądu oraz ewentualnej uprzedniej karalności.

Do wniosku **dołącza się materiały postępowania wyjaśniającego, adresy świadków i pokrzywdzonych** oraz **odpisy dla obwinionych**.

Wyrok nakazowy wydaje się bez przeprowadzenia **rozprawy na podstawie przepisów Kodeksu postępowania w sprawach o wykroczenia** z odpowiednim zastosowaniem przepisów kodeksu postępowania karnego (w szczególności art. 504–506 k.p.k.), a **staje się on prawomocny w razie niewniesienia sprzeciwu** lub jego cofnięcia. Odpis wyroku nakazowego **doręcza się oskarżycielowi, pokrzywdzonemu, prokuratorowi oraz oskarżonemu i jego obrońcy,** przy czym oskarżony i jego obrońca otrzymują go wraz z odpisem wniosku o ukaranie, a wszystkim doręcza się również **pouczenie o prawie, terminie i sposobie wniesienia sprzeciwu oraz skutkach jego niewniesienia**, ze wskazaniem, że pokrzywdzony może wnieść sprzeciw jedynie po złożeniu oświadczenia o działaniu w charakterze oskarżyciela posiłkowego.

Dane oskarżonego należy chronić

Prezes UODO podkreślił jednak, że **wyłączenia określonego w art. 3 pkt 1 ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości nie należy interpretować w ten sposób, że dane osobowe oskarżonego nie podlegają żadnej ochronie prawnej**. Rozpatrując konkretną sprawę, **odwoływać należy się do konstytucyjnie chronionych praw do prywatności oraz autonomii informacyjnej jednostki (art. 47, art. 51 ust. 1 i 2 Konstytucji RP) oraz prawa do ochrony danych osobowych określonego w Karcie Praw Podstawowych Unii Europejskiej (art. 8)**. Pomocniczo przy interpretacji przepisów krajowych należy posiłkować się także zasadami określonymi w Dyrektywie Parlamentu Europejskiego i Rady UE 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Tym samym przy sporządzaniu wniosku o ukaranie na podstawie art. 57 kodeksu postępowania w sprawach o wykroczenia należy kierować się zasadami wynikającymi z ww. norm prawnych.

Administrator przy sporządzaniu wniosku o ukaranie powinien podjąć wszelkie środki mające na celu minimalizację ryzyk związanych z nieprawidłowym przetwarzaniem danych osobowych. Ujawnienie danych osobowych innych obwinionych powinno nastąpić jedynie w zakresie niezbędnym do prawidłowego przeprowadzenia postępowania. Zatem dostęp do takich danych powinny mieć tylko takie organy, jak oskarżyciel i sąd.

Jakkolwiek **zasada ekonomiki procesowej** ma na celu usprawnienie i przyspieszenie postępowania, to **nie może ona stanowić podstawy do nieograniczonego ujawniania danych osobowych uczestników postępowania**, w szczególności poprzez przekazywanie jednemu obwinionemu szerokiego zakresu danych dotyczących innego obwinionego. Działanie takie powinno **każdorazowo podlegać ocenie pod kątem niezbędności i proporcjonalności** względem celu procesowego, jakim jest prawidłowe rozpoznanie sprawy, z **uwzględnieniem obowiązku ochrony danych osobowych oraz prawa do prywatności** stron postępowania.

O CZYM NALEŻY PAMIĘTAĆ, PUBLIKUJĄC SKANY DOKUMENTÓW W BIP

Publikacja dokumentów urzędowych w Biuletynie Informacji Publicznej (BIP) musi odbywać się z poszanowaniem prawa do ochrony danych osobowych. Dlatego np. z ich skanów powinien zostać usunięty odręczny podpis.

W ostatnim czasie jednostki samorządu terytorialnego pytają Prezesa UODO, czy publikacja w BIP skanu dokumentu zawierającego graficzny (własnoręczny) wzór podpisu osoby pełniącej funkcję publiczną jest działaniem niezbędnym dla zapewnienia jawności i autentyczności dokumentu, czy też stanowi przetwarzanie danych nadmiarowych w stosunku do celu.

Pytania te są dla organu nadzorczego okazją **do przypomnienia prezentowanych od wielu lat stanowisk** w kwestii stosowania przepisów o ochronie danych osobowych **w kontekście przepisów o dostępie do informacji publicznej**, które są publikowane zarówno na stronie internetowej Urzędu, jak i w „Biuletynie UODO" czy w rocznych sprawozdaniach z działalności Prezesa UODO.

RODO o godzeniu praw

Zgodnie z art. 86 RODO dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny, w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy ww. rozporządzenia.

Również w motywie 154 RODO podkreślono **konieczność pogodzenia tego prawa i ponownego wykorzystywania informacji sektora publicznego**. Motyw ten wskazuje, że przepisy prawa krajowego powinny **godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych**, i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie niniejszego rozporządzenia. Zarówno art. 86 RODO, jak **i motyw 154 RODO odsyłają w tym zakresie do przepisów krajowych.**

Treść i postać dokumentu urzędowego

Przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (art. 6 ust. 1 pkt 4 lit. a) stanowią, że **udostępnieniu podlega informacja publiczna w szczególności o danych publicznych, w tym treść i postać dokumentów urzędowych**. Dokumentem urzędowym w rozumieniu ustawy jest treść oświadczenia woli lub wiedzy, utrwalona i podpisana w dowolnej formie przez funkcjonariusza

publicznego w rozumieniu przepisów Kodeksu karnego, w ramach jego kompetencji, skierowana do innego podmiotu lub złożona do akt sprawy (art. 6 ust. 2 ustawy o dostępie do informacji publicznej).

Jak wskazał Naczelny Sąd Administracyjny (NSA) w wyroku z 28 kwietnia 2020 r. (sygn. akt I OSK 1939/19): „**Odróżnia się pojęcie samej informacji publicznej od nośnika**, na którym została ona utrwalona. Informacja jest pewnym komunikatem, wiedzą o jakimś fakcie. Nośnikiem, na którym taka informacja jest utrwalona, może być papier lub środki elektroniczne przechowujące dokonane na nich zapisy. **Ustawodawca tylko w jednym przypadku**, o którym mowa w art. 6 ust. 4 lit. a u.d.i.p., **zobowiązał do udostępnienia informacji publicznej zarówno co do treści, jak i postaci,** a więc również **do udostępniania nośnika**, który zawiera informację publiczną. **Chodzi tutaj o dokument urzędowy**, którego ustawowa definicja zawarta została w art. 6 ust. 2 u.d.i.p. Ponadto przepis art. 3 ust. 1 pkt 2 określa, że prawo do informacji publicznej obejmuje **uprawnienie do wglądu jedynie do dokumentów urzędowych**".

Trzeba podać, kto wytworzył informację i dokument urzędowy

Podmioty udostępniające informacje publiczne w Biuletynie Informacji Publicznej są – stosownie do art. 8 ust. 6 pkt 2 ustawy o dostępie do informacji publicznej – **obowiązane do podania w informacji danych określających tożsamość osoby**, **która wytworzyła informację** lub odpowiada za treść informacji. Natomiast wymagania, jakie musi spełnić dokument urzędowy, określa art. 76 § 1 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego. Stanowi on, **że dokumenty urzędowe sporządzone w przepisanej formie przez powołane do tego organy państwowe w ich zakresie działania stanowią dowód tego, co zostało w nich urzędowo stwierdzone**.

Dokument urzędowy sporządzony przez organ działający w ramach swojej właściwości **może mieć formę pisemną** (postać papierową) **opatrzoną podpisem** osoby piastującej funkcję organu **lub formę elektroniczną opatrzoną kwalifikowanym podpisem elektronicznym**, **podpisem zaufanym lub kwalifikowaną pieczęcią elektroniczną** organu administracji publicznej ze wskazaniem w treści pisma osoby opatrującej pismo pieczęcią. Wobec powyższego przy publikacji w BIP tego dokumentu **przekazanie informacji o tym, jaka osoba pełniąca funkcję organu go podpisała, nie narusza zasady minimalizacji danych ustanowionej w art. 5 ust. 1 lit. c RODO**.

Do podpisu potrzebna analiza ryzyka

Odrębną sprawą jest dokonanie analizy ryzyka poprzedzającej publikację dokumentów elektronicznych zawierających **numer PESEL w kwalifikowanym certyfikacie podpisu elektronicznego**, którego **rozpowszechnianie nie znajduje** w tym przypadku **podstaw prawnych** (zwłaszcza w kontekście art. 87 RODO).

Także **ze względu na ryzyka związane z kradzieżą tożsamości należy przeanalizować celowość udostępnienia podpisu własnoręcznego** widniejącego na skanach dokumentów wytworzonych w tradycyjnej, papierowej formie (własnoręczny podpis może zostać łatwo podrobiony i wykorzystany do różnego rodzaju fałszerstw czy przestępstw, w tym kradzieży tożsamości, przed czym organ ds. ochrony danych osobowych od dawna przestrzega).

Ocena powyższego powinna być związana z przeprowadzeniem **testu niezbędności i proporcjonalności** (art. 5 RODO) i **analizą ryzyka** (z art. 24 i 32 RODO).

Prawo do bycia zapomnianym

Biorąc pod uwagę fakt, że publikacja dokumentów urzędowych, w tym zawartych w nich danych osobowych, musi się odbywać **z poszanowaniem prawa do ochrony danych osobowych** i uwzględniać stosowanie zasad z art. 5 ust. 1 RODO, w tym **zasady ograniczenia przechowywania** (art. 5 ust. 1 lit. e RODO), podkreślić należy, że **dane osobowe zawarte w dokumentach nie mogą być udostępniane w przestrzeni publicznej przez nieograniczony czas**.

Biuletyn Informacji Publicznej jest miejscem powszechnego udostępniania informacji. **Nie stanowi** on jednak **zasobu archiwalnego, w którym dokumenty, a w nich dane osobowe, mogą być upubliczniane wieczyście**. **Okres ich publikacji** powinien zostać oszacowany i uzależniony od celów publikacji, tj. **nie może być dłuższy, niż jest to niezbędne do celu, w którym są przetwarzane**. Ma to szczególne znaczenie w kontekście zasady rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie przepisów o ochronie danych osobowych i musi być w stanie to wykazać (art. 5 ust. 2 RODO).

Jednocześnie – zgodnie z art. 17 RODO – **każda osoba fizyczna ma prawo do tego, by „być zapomnianym”,** zwłaszcza do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli nie są już one niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane.

Prawo do „bycia zapomnianym” w kontekście prawa do prywatności i konieczność usuwania danych osobowych z przestrzeni publicznej – jeżeli nie istnieje uzasadniona podstawa do ich dalszego upubliczniania – jest przedmiotem orzecznictwa sądowego. Stanowisko w tej kwestii zajął m.in. Trybunał Sprawiedliwości Unii Europejskiej w wyroku z 13 maja 2014 r. C-131/12, Google Spain SL i Google Inc. przeciwko Agencia de Protección de Datos (AEPD) I MARIO COSTEJA GONZÁLEZ.

Opinia IOD

Warto, **by w analizowanej sprawie swoją opinię co do legalności przetwarzania danych osobowych przedstawił inspektor ochrony danych** (IOD), którego powołanie w podmiotach publicznych (zgodnie z art. 37 ust. 1 lit. a RODO) jest obligatoryjne. Inspektor posiada wiedzę nie tylko z zakresu ochrony danych osobowych, ale przede wszystkim zna specyfikę zadań realizowanych przez administratora.

NOWE SPOJRZENIE NA ZARZĄDZANIE DANYMI – DGA W PIGUŁCE

W trzeciej części cyklu poświęconego rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2022/868 z dnia 30 maja 2022 r. w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi)[1] określanego jako DGA – omówimy przepisy dotyczące uznanych organizacji altruizmu danych.

Zgodnie z art. 2 pkt 16 DGA przez altruizm danych należy rozumieć **dobrowolne dzielenie się danymi na podstawie wyrażonej przez osoby, których dane dotyczą, zgody** na przetwarzanie dotyczących ich danych osobowych **lub na podstawie udzielonego przez posiadaczy danych[2] pozwolenia** na wykorzystywanie ich danych nieosobowych, **bez żądania ani otrzymania za to wynagrodzenia** wykraczającego poza zwrot kosztów poniesionych przez te osoby lub posiadaczy w związku z udostępnieniem ich danych **do celów leżących w interesie ogólnym** określonych – w tosownych przypadkach – w prawie krajowym, takich jak **opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk** urzędowych, **poprawa świadczenia usług publicznych, kształtowanie polityki publicznej** lub **do celów badań naukowych** leżących w interesie ogólnym.

Pojęcie altruizmu danych

Przytoczona definicja zakłada konieczność spełnienia następujących przesłanek[3]:

- **dobrowolność dzielenia się danymi** musi wynikać z woli osoby, której dane dotyczą, lub posiadacza danych;
- **wyrażenie zgody[4]** przez osobę, której dane dotyczą, lub udzielenie pozwolenia przez posiadacza danych nieosobowych[5];
- **nieotrzymanie ani nieżądanie wynagrodzenia** wykraczającego poza zwrot kosztów poniesionych w związku z udostępnieniem tych danych;

1. Dz. Urz. UE L 152 z 3.6.2022, s. 1–44.
2. Posiadacz danych oznacza osobę prawną (w tym podmiot sektora publicznego lub organizację międzynarodową), lub osobę fizyczną niebędącą w odniesieniu do przedmiotowych konkretnych danych osobą, której dane dotyczą, która ma – zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym – prawo do udzielania dostępu do niektórych danych osobowych lub danych nieosobowych lub do dzielenia się nimi (art. 2 pkt 8 DGA).
3. Por. A. Michałowicz, Altruizm danych w świetle aktu w sprawie zarządzania danymi – między teorią a praktyką, IKAR 2022/5 s. 48.
4. Pojęcie „zgody" zostało zdefiniowane w art. 2 pkt 4 DGA i oznacza zgodę w rozumieniu art. 4 pkt 11 RODO.
5. Pozwolenie oznacza przyznanie użytkownikom danych prawa do przetwarzania danych nieosobowych (art. 2 pkt 6 DGA).

- **realizacja celów leżących w interesie ogólnym.** Do tych celów należą opieka zdrowotna, zwalczanie zmian klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawa świadczenia usług publicznych, kształtowanie polityki publicznej, a także badania naukowe realizowane w interesie ogólnym. **Katalog ten nie ma charakteru zamkniętego**[6].

Dobrowolna rejestracja uznanych organizacji altruizmu danych

DGA przewiduje dobrowolność rejestracji organizacji altruizmu danych, jednocześnie nie zakazując takiej działalności podmiotom, które nie poddały się takiej rejestracji. Zgodnie z art. 19 ust. 1 DGA **wniosek o rejestrację w publicznym krajowym rejestrze uznanych organizacji altruizmu danych może złożyć podmiot, który spełnia wymogi określone w art. 18 DGA.**

DGA określa właściwość organu, do którego można złożyć wniosek o rejestrację w publicznym krajowym rejestrze uznanych organizacji altruizmu danych, w zależności od tego, czy ta organizacja ma jednostkę organizacyjną w jednym lub więcej państw członkowskich UE, a jeżeli tak, to w którym:

- **jeżeli organizacja altruizmu danych ma jednostkę organizacyjną w jednym państwie członkowskim UE, to składa wniosek do organu właściwego w tym państwie,** np. organizacja mająca jednostkę organizacyjną w Polsce powinna złożyć wniosek do Prezesa UODO;
- jeżeli organizacja altruizmu danych ma swoje **jednostki w więcej niż jednym państwie członkowskim, powinna złożyć wniosek o rejestrację w tym z nich, w którym znajduje się jej główna jednostka organizacyjna**[7], np. fundacja, której zarząd znajduje się w Polsce, a działa poprzez swoje oddziały także na terenie Niemiec i Czech, powinna złożyć wniosek do Prezesa UODO;
- gdy organizacja altruizmu danych **nie ma jednostki organizacyjnej w UE, powinna złożyć wniosek o rejestrację w tym państwie członkowskim UE, w którym znajduje się wyznaczony przez nią przedstawiciel prawny,**[8] np. organizacja mająca jednostkę organizacyjną w Wielkiej Brytanii, która wyznaczyła swojego przedstawiciela prawnego w Polsce ze względu na to, że oferuje tutaj swoje usługi oparte na altruizmie danych, powinna złożyć wniosek do Prezesa UODO.

6. M. Jabłoński, K. Wygoda, (w:) A. Piskorz-Ryń, M. Sakowska-Baryła (red.), Rozporządzenie w sprawie europejskiego zarządzania danymi (DGA). Komentarz, art. 2 pkt 16, s. 128.

7. Gdy organizacja altruizmu danych **nie ma jednostki organizacyjnej w UE, powinna złożyć wniosek o rejestrację w tym państwie członkowskim UE, w którym znajduje się wyznaczony przez nią przedstawiciel prawny**, np. organizacja mająca jednostkę, zgodnie z art. 4 pkt 14 DGA, „główna jednostka organizacyjna" osoby prawnej, oznacza miejsce, w którym znajduje się jej centralna administracja w Unii.

8. Zgodnie z art. 2 pkt 21 DGA „przedstawiciel prawny" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, wyznaczoną w wyraźny sposób do działania w imieniu niemających jednostki organizacyjnej w Unii dostawców usług pośrednictwa danych lub podmiotu gromadzącego dane udostępniane do celów leżących w interesie ogólnym i na zasadzie altruizmu danych przez osoby fizyczne lub prawne; organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych mogą się zwracać jednocześnie do tej osoby oraz dostawcy usług pośrednictwa danych lub podmiotu albo do tej osoby zamiast do dostawcy usług pośrednictwa

4 ZARZĄDZANIE DANYMI

Uznana w Unii organizacja altruizmu danych

Organizacje altruizmu danych będące zarejestrowane jako uznane organizacje są uprawnione do posługiwania się oznaczeniem „uznana w Unii organizacja altruizmu danych" oraz do używania wspólnego logo, które zostało ustanowione przez Komisję Europejską[9].

Uznane organizacje altruizmu danych mają **obowiązek wyraźnego eksponowania wspólnego logo na każdej publikacji w internecie i poza nim**, odnoszącej się do ich działalności w zakresie altruizmu danych. Wspólnemu logo towarzyszy **kod QR z linkiem do publicznego unijnego rejestru** uznanych organizacji altruizmu danych.

Ogólne wymogi dotyczące rejestracji

Art. 18 DGA określa **wymogi, które organizacja altruizmu danych musi spełnić** łącznie, żeby zostać zarejestrowana w publicznym krajowym rejestrze uznanych organizacji altruizmu danych:

- prowadzenie przez nią **działalności w zakresie altruizmu danych,** która spełnia omówione przesłanki;
- podmiot **jest osobą prawną ustanowioną zgodnie z prawem krajowym do realizacji celów leżących w interesie ogólnym,** określonych w prawie krajowym;
- podmiot prowadzi **działalność o charakterze niekomercyjnym i jest prawnie niezależny** od jakiegokolwiek podmiotu nastawionego na zysk;
- podmiot prowadzi działalność w zakresie altruizmu danych, wykorzystując przy tym **strukturę funkcjonalnie odrębną od pozostałej działalności tego podmiotu;**
- **przestrzega zbioru zasad, określonych w art. 22 ust. 1 DGA**, najpóźniej 18 miesięcy po wejściu w życie aktów delegowanych, o których mowa w tym przepisie.

danych lub podmiotu w związku z obowiązkami ustanowionymi na podstawie niniejszego rozporządzenia, w tym w związku ze wszczęciem postępowania egzekucyjnego przeciwko niespełniającym wymogów dostawcy usług pośrednictwa danych lub podmiotowi niemającym jednostki organizacyjnej w Unii.

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

Treść wniosku

Wniosek o rejestrację musi zawierać następujące informacje:

- nazwę podmiotu;
- **status prawny oraz formę prawną** podmiotu, a w przypadku gdy podmiot jest zarejestrowany w publicznym rejestrze krajowym – jego **numer rejestracyjny**;
- **status** podmiotu, stosownie do przypadku;
- **źródła dochodu** podmiotu;
- **adres głównej jednostki organizacyjnej podmiotu w Unii**, jeżeli ma to zastosowanie, oraz drugorzędnego oddziału w innym państwie członkowskim, o ile takowy istnieje, lub adres przedstawiciela prawnego;
- **ogólnodostępną stronę internetową**, na której można znaleźć kompletne i aktualne informacje o podmiocie oraz jego działalności;
- **osoby wyznaczone do kontaktów** przez podmiot i dane kontaktowe tych osób;
- **cele leżące w interesie ogólnym**, które podmiot zamierza wspierać przy gromadzeniu danych;
- **charakter danych, które podmiot zamierza kontrolować lub przetwarzać**, a w przypadku danych osobowych – **wskazanie ich kategorii;**
- wszelkie inne dokumenty, które wykazują, że wymagania z rozporządzenia zostały spełnione.

Po przedłożeniu niezbędnych informacji przez podmiot, który złożył wniosek, organ właściwy do rejestracji organizacji altruizmu danych sprawdza, czy spełnia on wymagania nałożone przez DGA. **Jeżeli wynik weryfikacji będzie pozytywny, organ w ciągu 12 tygodni od dnia otrzymania wniosku dokonuje rejestracji**. **Rejestracja podmiotu** w jednym państwie członkowskim **jest ważna również w innych państwach członkowskich UE**. Organ właściwy do spraw rejestracji organizacji altruizmu danych jest **zobowiązany poinformować o dokonanej rejestracji Komisję Europejską**, która uwzględni tę informację w prowadzonym przez siebie publicznym rejestrze uznanych organizacji altruizmu danych.

Wymogi dotyczące przejrzystości

Artykuł 20 DGA wprowadza obowiązki dotyczące przejrzystości, obejmujące obowiązki dokumentacyjne oraz sprawozdawcze.

Do obowiązków dokumentacyjnych należy prowadzenie pełnej i dokładnej dokumentacji w zakresie:

- **wszystkich osób fizycznych lub prawnych, które otrzymały możliwość przetwarzania danych** będących w posiadaniu tej organizacji altruizmu danych, oraz ich dane kontaktowe;
- **daty lub czasu trwania przetwarzania danych osobowych** lub wykorzystywania danych nieosobowych;

- **celu przetwarzania zadeklarowanego przez osobę** fizyczną lub prawną, która **otrzymała możliwość przetwarzania;**
- **opłat uiszczonych przez osoby** fizyczne lub prawne **przetwarzające dane**.

Z kolei w ramach **obowiązków sprawozdawczych** organizacja altruizmu danych sporządza i przekazuje odpowiedniemu organowi właściwemu do spraw rejestracji (w przypadku Polski będzie to Prezes UODO) organizacji altruizmu danych roczne sprawozdanie z działalności, które zawiera przynajmniej:

- **informację o działalności** uznanej organizacji altruizmu danych;
- **opis sposobu, w jaki** w ciągu danego roku obrotowego **wspierano cele leżące w interesie ogólnym**, dla których dane były gromadzone;
- **wykaz wszystkich osób fizycznych i prawnych, którym zezwolono na przetwarzanie posiadanych danych**, w tym skrócony opis celów leżących w interesie ogólnym, którym służy takie przetwarzanie danych, oraz **opis zastosowanych do tego celu środków technicznych**, wraz z opisem technik stosowanych **w celu zachowania prywatności i ochrony danych**;
- w stosownych przypadkach **podsumowanie wyników przetwarzania danych**, na które zezwoliła uznana organizacja altruizmu danych
- **informacje o źródłach dochodów uznanej organizacji altruizmu danych**, w szczególności o wszystkich dochodach z tytułu zezwolenia na dostęp do danych, oraz o wydatkach.

Gwarancje praw i interesów osób, których dane dotyczą, oraz posiadaczy danych

Art. 21 DGA nakłada na uznane organizacje altruizmu danych następujące wymogi dotyczące zabezpieczenia praw i interesów osób, których dane dotyczą, oraz posiadaczy danych w odniesieniu do ich danych:

- ma ona przekazać osobom, których dane dotyczą, lub posiadaczom danych **w sposób jasny i łatwo zrozumiały informacje o**:

- **celach leżących w interesie ogólnym** oraz o konkretnym, wyraźnym i zgodnym z prawem **celu przetwarzania danych osobowych**, dla którego uznana organizacja altruizmu danych pozwala na przetwarzanie danych osób, których dane dotyczą, lub posiadaczy danych przez użytkowników danych;
- **miejscu przetwarzania oraz celach leżących w interesie ogólnym**, dla których uznana organizacja altruizmu danych pozwala na **przetwarzanie w państwie trzecim**, jeżeli tych operacji przetwarzania dokonuje uznana organizacja altruizmu danych;

- **nie może ona wykorzystywać danych do celów innych niż leżących w interesie ogólnym**, na które wyraziła zgodę osoba, której dane dotyczą, lub udzielił zezwolenia posiadacz danych. Bardzo ważne jest, że **uznana organizacja altruizmu danych nie może stosować wprowadzających w błąd praktyk marketingowych**, by nakłaniać do przekazywania danych;
- musi **zapewnić narzędzia umożliwiające uzyskanie oraz wycofanie zgody** od osób, których dane dotyczą, lub pozwoleń na przetwarzanie danych udostępnionych przez posiadacza danych;

- **ma podjąć środki w celu zapewnienia odpowiedniego poziomu bezpieczeństwa danych nieosobowych**, które zgromadziła w ramach altruizmu danych (obowiązek zapewnienia bezpieczeństwa danych osobowych wynika wprost z RODO).

Dodatkowe zasady altruizmu danych

Komisja Europejska została upoważniona na mocy art. 22 ust. 1 DGA do przyjęcia aktów delegowanych ustanawiających zbiór zasad, który ma na celu uzupełnienie przepisów DGA. Przygotowanie zbioru zasad powinno przebiegać we współpracy z organizacjami altruizmu danych oraz innymi interesariuszami.

Zbiór zasad powinien określać:

- **wymagania informacyjne** w celu zapewnienia, aby osoby których dane dotyczą, i posiadacze danych otrzymali przed wyrażeniem zgody lub udzieleniem pozwolenia na altruizm danych wystarczająco jasne, szczegółowe i przejrzyste informacje dotyczące wykorzystywania danych, narzędzi wyrażania zgody lub udzielania pozwolenia i ich wycofywania oraz **środków podejmowanych w celu uniknięcia nieprawidłowego wykorzystywania danych**, którymi podzielono się organizacją altruizmu danych;
- **odpowiednie wymogi techniczne i wymogi bezpieczeństwa**, by zapewnić adekwatny poziom bezpieczeństwa przy przechowywaniu i przetwarzaniu danych, a także w **odniesieniu do narzędzi wyrażania zgody lub udzielania pozwolenia i ich wycofywania**;
- **plany działania w zakresie komunikacji** zakładające multidyscyplinarne podejście do **budowania wśród odpowiednich interesariuszy** – w szczególności posiadaczy danych i osób, których dane dotyczą, potencjalnie dzielących się swoimi danymi – **świadomości na temat altruizmu danych,** oraz na temat zbioru zasad;
- zalecenia dotyczące **odpowiednich standardów interoperacyjności**.

Komisja Europejska – jak dotąd – **nie wydała takich aktów delegowanych**.

Europejski formularz zgody do celów altruizmu danych

Na podstawie art. 25 DGA Komisja Europejska jest uprawniona do przyjęcia aktu wykonawczego, który ma na **celu ustanowienie europejskiego formularza zgody do celów altruizmu danych**. Komisja Europejska przed przyjęciem takiego aktu jest obowiązana **skonsultować się z Europejską Radą Ochrony Danych**, uwzględnić **stanowisko Europejskiej Rady ds. Innowacji** w zakresie danych, a **także zapewnić udział w tym procesie interesariuszy.** Przyjęcie przez Komisję Europejską takiego formularza ma umożliwiać uzyskiwanie we wszystkich państwach członkowskich UE zgody lub pozwolenia w jednolitym formacie.

Formularz powinien mieć charakter modułowy, który umożliwi **dostosowanie do potrzeb konkretnych sektorów i poszczególnych celów**. Ma on również zapewniać osobom, których dane dotyczą, **możliwość wyrażenia i wycofania zgody** na konkretną operację przetwarzania danych zgodnie z wymogami RODO. Powinien także być **udostępniony w sposób umożliwiający wydruk na papierze,** ale i **w formie elektronicznej,** która nadaje się do odczytu maszynowego, oraz być **łatwy do zrozumienia.**

4 ZARZĄDZANIE DANYMI

Jak dotąd Komisja Europejska nie skorzystała ze swojej kompetencji i nie przyjęła odpowiedniego aktu wykonawczego w tym zakresie.

Rejestr uznanych organizacji altruizmu danych

Zgodnie z art. 17 ust. 1 DGA **organ właściwy do spraw rejestracji organizacji altruizmu danych prowadzi i regularnie aktualizuje publiczny krajowy rejestr** uznanych organizacji altruizmu danych. Z kolei art. 24 ust. 1 ustawy z dnia 27 marca 2026 r. ustawy o zarządzaniu danymi (Dz. U. z 2026 r. poz. 548), która wejdzie w życie 23 lipca 2026 r., **przyznaje kompetencje w tym zakresie Prezesowi UODO.**

Komisja Europejska prowadzi w celach informacyjnych publiczny rejestr uznanych organizacji altruizmu danych.

Obecnie zarejestrowane są 4 organizacje z 3 państw członkowskich UE:

Hiszpania: Associació Dades pel Benestar Planetari - Datalog

Belgia: 101 Genomes, European Brain Data Hub (EBDH)

Irlandia: Elec-tariffs.ie

EROD I EIOD POPIERAJĄ HARMONIZACJĘ BADAŃ KLINICZNYCH W RAMACH EUROPEJSKIEGO AKTU BIOTECHNOLOGICZNEGO, ALE WZYWAJĄ DO WPROWADZENIA SZCZEGÓLNYCH ZABEZPIECZEŃ DLA WRAŻLIWYCH DANYCH ZDROWOTNYCH

Europejska Rada Ochrony Danych (EROD) oraz Europejski Inspektor Ochrony Danych (EIOD) przyjęli wspólną opinię dotyczącą propozycji Komisji Europejskiej w sprawie Europejskiego Aktu Biotechnologicznego. Ma ona na celu wzmocnienie europejskiego sektora biotechnologii i biomanufaktury, w szczególności w obszarze zdrowia, poprzez usprawnienie ram regulacyjnych i aktualizację zasad prowadzenia badań klinicznych.

EROD i EIOD popierają główne założenie propozycji, jakim jest **zwiększenie konkurencyjności UE** oraz **przeciwdziałanie istniejącej fragmentacji w stosowaniu Rozporządzenia w sprawie badań klinicznych** (CTR). W szczególności z zadowoleniem przyjmują dążenie do **ustanowienia jednej podstawy prawnej dla przetwarzania danych osobowych przez sponsorów i badaczy**, co znacząco poprawi przejrzystość prawną w całej Europie. Jednocześnie obie instytucje podkreślają, że wrażliwość danych zdrowotnych i genetycznych przetwarzanych w kontekście badań klinicznych wymaga wysokiego poziomu ochrony. Wspólna opinia **zawiera szereg zaleceń mających zapewnić, że proponowane uproszczenia nie obniżą poziomu ochrony** uczestników badań klinicznych.

–**Konkurencyjny sektor biotechnologiczny w Europie wymaga przewidywalnego i zharmonizowanego środowiska prawnego. Z zadowoleniem przyjmujemy dążenie do ustanowienia jednej podstawy prawnej dla badań klinicznych, co ułatwi zgodność z RODO i wzmocni spójność w całej Unii. Jednak ta harmonizacja musi być uzupełniona silnymi zabezpieczeniami, w tym jasnym określeniem ról i odpowiedzialności wszystkich zaangażowanych podmiotów, aby zapewnić zaufanie i odpowiedzialność w badaniach naukowych."** – skomentował Europejski Inspektor Ochrony Danych, Wojciech Wiewiórowski.

Kluczowe zalecenia obejmują:

- **Doprecyzowanie ról administratorów danych:** propozycja **powinna wskazywać, czy podmioty zaangażowane w finansowanie i prowadzenie badań klinicznych działają jako samodzielni czy wspólni administratorzy danych**, aby zapewnić jasny podział odpowiedzialności.
- **Ograniczenie okresu przechowywania danych:** obowiązkowy **minimalny 25-letni okres przechowywania powinien wyraźnie dotyczyć jedynie głównego pliku badania klinicznego** (clinical trial master file), a nie wszystkich danych osobowych przetwarzanych w trakcie badania.

- **Dalsze przetwarzanie na potrzeby innych badań klinicznych lub badań naukowych:** ponieważ propozycja ma zapewnić podstawę prawną w prawie Unii dla dalszego przetwarzania danych z badań przez tego samego administratora, akt biotechnologiczny powinien **jasno określić cele oraz konkretne zabezpieczenia dla takiego przetwarzania**.

- **Spójność z Aktem o sztucznej inteligencji (AI Act):** promując wykorzystanie AI w biotechnologii, **ustawa powinna zapewnić, że obowiązki sponsorów będą uzupełniać istniejące wymogi wynikające z AI Act,** aby zagwarantować spójne środowisko regulacyjne.

- **Odpowiednie środki techniczne i organizacyjne:** CTR powinno **wprost wymagać stosowania pseudonimizacji** wszędzie tam, gdzie nie jest konieczne przetwarzanie bezpośrednio identyfikowalnych danych osobowych.

Piaskownice regulacyjne: Jeżeli to konieczne, akty wykonawcze Komisji dotyczące piaskownic **w specyficznym kontekście badań klinicznych powinny przewidywać podstawę prawną przetwarzania danych osobowych oraz wyjątek na podstawie art. 9 ust. 2 dla przetwarzania danych wrażliwych**; w przypadku innych piaskownic przetwarzanie danych osobowych powinno zawsze opierać się na podstawie prawnej wynikającej z RODO.

–**Europejskie ambicje w zakresie innowacji medycznych muszą iść w parze z zaufaniem. Nasza opinia zawiera rekomendacje dla współprawodawców, mające zapewnić, że dążenie do opracowywania nowych terapii będzie respektować podstawowe prawa jednostek. Pomoże to stworzyć ramy chroniące uczestników badań klinicznych oraz zapewni większą pewność prawną dla badaczy** – stwierdziła przewodnicząca EROD, Anu Talus.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych:

EDPB and EDPS support harmonisation of clinical trials under European Biotech Act, but call for specific safeguards for sensitive health data | European Data Protection Board

EROD I EIOD POPIERAJĄ WZMOCNIENIE CYBERBEZPIECZEŃSTWA W UE ORAZ UŁATWIENIE ZGODNOŚCI Z PRZEPISAMI, PRZY JEDNOCZESNEJ OCHRONIE DANYCH OSOBOWYCH OSÓB FIZYCZNYCH

Europejska Rada Ochrony Danych (EROD) oraz Europejski Inspektor Ochrony Danych (EIOD) przyjęli wspólną opinię dotyczącą propozycji Komisji Europejskiej w sprawie drugiego aktu o cyberbezpieczeństwie (CSA2) oraz propozycji zmian do dyrektywy NIS2.

20 stycznia 2026 r. Komisja opublikowała pakiet dotyczący cyberbezpieczeństwa, mający na celu dalsze **wzmacnianie cyberbezpieczeństwa w Europie**, a jednocześnie **ułatwienie organizacjom spełniania wymogów wynikających z przepisów w tym obszarze.** W swojej wspólnej opinii, wydanej na wniosek Komisji*, EROD i EIOD odnoszą się do proponowanej rewizji CSA oraz ukierunkowanych zmian dyrektywy NIS2. W odniesieniu do propozycji CSA2 oba organy popierają ogólne cele, jakimi są: **wzmocnienie roli Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA), ułatwienie stosowania certyfikacji cyberbezpieczeństwa**, a także dalsze przeciwdziałanie różnym (w tym nietechnicznym) zagrożeniom dla łańcuchów dostaw ICT.

–Cyberbezpieczeństwo i ochrona danych są wzajemnie i głęboko powiązane**. Cyberbezpieczeństwo wspiera ochronę danych osobowych poprzez ograniczanie ryzyka niepożądanego dostępu, modyfikacji lub niedostępności danych, jednak kluczowe jest, aby środki bezpieczeństwa były wdrażane w sposób nienaruszający podstawowych praw i wolności jednostek** – powiedziała przewodnicząca EROD, Anu Talus.

Wzmocniona rola i nowy mandat dla ENISA

Propozycja doprecyzowania sposobu, w jaki ENISA udziela wsparcia różnym interesariuszom, została dobrze przyjęta. EROD i EIOD ze szczególnym zadowoleniem przyjmują fakt, że porady ENISA miałyby być wydawane na wcześniejszy wniosek EROD, co zapewni jasną koordynację i wyraźny podział odpowiedzialności. Sugerują także dodanie **EIOD jako podmiotu uprawnionego do występowania o takie porady.**

Obie instytucje przypominają, że jeśli Rada Zarządzająca ENISA zdecyduje o przyjęciu dodatkowych środków niezbędnych do stosowania unijnego rozporządzenia o ochronie danych, decyzje te powinny być **ograniczone do bardzo technicznych (praktycznych) szczegółów dotyczących przetwarzania danych osobowych**. Propozycja powinna również przewidywać **obowiązek wcześniejszych konsultacji z EIOD** przed przyjęciem takich zasad. Wspólna opinia pozytywnie ocenia synergie, które mogą wynikać ze współpracy ENISA z innymi instytucjami i organami UE, a także **zaleca dodanie wyraźnego odniesienia do EIOD jako organu UE, z którym ENISA powinna współpracować**.

—**Maksymalizacja skuteczności środków cyberbezpieczeństwa jest niezwykle ważna, ale musimy zapewnić, że przetwarzanie danych osobowych pozostanie ograniczone do tego, co absolutnie niezbędne. Z zadowoleniem przyjmujemy wzmocnioną rolę ENISA w promowaniu odporności cyfrowej; mamy nadzieję, że nowy mandat wzmocni synergie potrzebne do stworzenia solidnego ekosystemu, w którym bezpieczeństwo i prywatność idą w parze** — podkreślił Europejski Inspektor Ochrony Danych, Wojciech Wiewiórowski.

Zalecenia dotyczące systemu certyfikacji

Choć cel ułatwienia stosowania certyfikacji cyberbezpieczeństwa jest słuszny, zakres Europejskich Ram Certyfikacji Cyberbezpieczeństwa oraz ich relacja do certyfikacji RODO powinny zostać dodatkowo doprecyzowane. Aby zapewnić spójność**, ENISA powinna konsultować się z EROD przed przyjęciem schematu certyfikacji dotyczącego bezpieczeństwa przetwarzania danych osobowych.** Ponadto **schematy certyfikacji produktów, usług i procesów**, które prawdopodobnie będą wykorzystywane w operacjach przetwarzania danych, **powinny** — w miarę możliwości — **uwzględniać środki bezpieczeństwa** pomagające wykazać spełnienie wymogów RODO. Autorzy opinii zalecają, aby Europejskie Ramy Umiejętności w zakresie Cyberbezpieczeństwa **obejmowały nie tylko specjalistów ds. cyberbezpieczeństwa, ale także ogólne profile pracowników.**

Zgodnie z niedawną wspólną opinią EROD–EIOD dotyczącą propozycji rozporządzenia Digital Omnibus obie instytucje **wyrażają poparcie dla ustanowienia pojedynczego punktu zgłaszania naruszeń ochrony danych osobowych**, ponieważ zmniejszyłoby to obciążenia administracyjne dla organizacji zgłaszających, bez wpływu na poziom ochrony osób fizycznych. W odniesieniu do proponowanych zmian dyrektywy NIS2, EROD i EIOD **z zadowoleniem przyjmują uznanie dostawców Europejskich Portfeli Tożsamości Cyfrowej oraz Europejskich Portfeli Biznesowych za „podmioty kluczowe".**

Źródło:

Komunikat Europejskiej Rady Ochrony Danych:

EDPB and EDPS support strengthening EU's cybersecurity and easing compliance while protecting individuals' personal data | European Data Protection Board

UDZIAŁ PREZESA UODO W CAMBRIDGE FORUM ON INTERNATIONAL PRIVACY & DATA LAWS 2026

25–27 marca 2026 r. odbyło się Cambridge Forum on International Privacy & Data Laws, w którym uczestniczył również prezes Urzędu Ochrony Danych Osobowych. Spotkanie zgromadziło przedstawicieli organów nadzorczych, ekspertów i praktyków z wielu regionów świata. Program obejmował sześć sesji tematycznych, z których każda dotyczyła innego obszaru współczesnych wyzwań w ochronie danych.

Już na początku Forum uczestnicy weszli w tematykę związaną z rosnącą złożonością regulacji dotyczących danych osobowych**. Rozmowy skupiały się zarówno wokół działań egzekucyjnych, jak i konsekwencji naruszeń,** które mogą prowadzić do wysokich kar, utraty reputacji oraz spadku zaufania użytkowników. Wskazywano na różnice w podejściu regulatorów z Europy, Ameryki Północnej, Azji i Ameryki Łacińskiej, co wpływa na praktyki organizacji działających globalnie.

1. Dane bez granic – globalne wyzwania regulacyjne

Szczególne miejsce w dyskusji zajęły **transfery danych**, które nadal pozostają obszarem pełnym wyzwań. **Uczestnicy analizowali funkcjonowanie różnych mechanizmów**, takich jak ramy UE–USA, standardowe klauzule umowne czy nowe modele adekwatności regionalnej. Zwracano uwagę na trudności związane z pogodzeniem wymogów wielu jurysdykcji przy jednoczesnym utrzymaniu sprawności operacyjnej.

W dalszej części panelu omówiono **ochronę danych dzieci i małoletnich**, w tym **zmieniające się podejście do zgody** oraz **projektowania usług cyfrowych z myślą o młodszych użytkownikach**. Wskazywano na rosnące znaczenie regulacji dotyczących środowisk edukacyjnych, gier i mediów społecznościowych. Zamykając sesję, uczestnicy przyjrzeli się **ramom regulacyjnym dotyczącym sztucznej inteligencji**, porównując podejścia różnych regionów do zasad odpowiedzialności, przejrzystości i sprawiedliwości algorytmicznej.

2. Akt o danych – impuls do współpracy czy nowe wyzwanie zgodności?

Kolejna część Forum skupiła się na unijnym **Data Act**, który wprowadza nowe zasady dotyczące dostępu do danych generowanych przez urządzenia połączone oraz zmienia sposób formułowania umów dotyczących ich wykorzystania. Uczestnicy zastanawiali się, **jak organizacje mogą dostosować swoje strategie zgodności i które jednostki powinny odpowiadać za wdrażanie nowych obowiązków.** Ważnym elementem rozmów było **nakładanie się Data Act na inne regulacje**, takie jak RODO, AI Act czy przepisy ePrivacy. Wskazywano **na konieczność wypracowania spójnych podejść,** zwłaszcza w organizacjach działających w wielu państwach.

Szczegółowo omówiono także **urządzenia zdrowotne i aplikacje mobilne**, które generują dane o wysokiej wartości i wrażliwości. Dyskusja dotyczyła tego, jak osoby fizyczne mogą korzystać ze swoich praw w sytuacji, gdy dane podlegają jednocześnie kilku reżimom prawnym, a część metadanych może być wykorzystywana przez producentów w sposób nie w pełni przejrzysty.

3. Sztuczna inteligencja w ochronie zdrowia – między innowacją a odpowiedzialnością

W kolejnej sesji uczestnicy przenieśli się do obszaru ochrony zdrowia, gdzie rozwój sztucznej inteligencji stawia przed organizacjami zarówno nowe możliwości, jak i wyzwania. **Omawiano wpływ AI na badania naukowe, przetwarzanie danych medycznych oraz ochronę prywatności pacjentów.** Zwracano uwagę na kwestie związane z zakresem przetwarzania, potencjalnymi naruszeniami praw własności intelektualnej oraz koniecznością uwzględniania aspektów etycznych.

Szczególne zainteresowanie wzbudziła tematyka **agentic AI**, czyli **systemów podejmujących działania w sposób bardziej autonomiczny.** Uczestnicy przedstawiali perspektywy z różnych regionów świata, wskazując na różnice w podejściu do regulacji i nadzoru nad takimi rozwiązaniami. W końcowej części panelu zastanawiano się, które instytucje – w tym firmy farmaceutyczne, uczelnie, administracja publiczna i organizacje międzynarodowe – powinny odgrywać kluczową rolę w dalszym kształtowaniu zasad stosowania AI w sektorze zdrowia.

4. Anonimizacja – wymagania, raktyki i różnice regulacyjne

Następna sesja była poświęcona **anonimizacji danych**, czyli **procesowi, który pozwala wyłączyć dane spod rygorów RODO.** Uczestnicy omawiali warunki, jakie muszą zostać spełnione, aby dane mogły zostać uznane za anonimowe, oraz **przedstawiali techniczne i prawne aspekty minimalizowania ryzyka ponownej identyfikacji**. Ważnym elementem rozmów było porównanie najnowszych wytycznych dotyczących anonimizacji i de-identyfikacji, w szczególności stanowisk kanadyjskiego IPC oraz brytyjskiego ICO. Zestawienie to pokazało, jak **różnice legislacyjne wpływają na praktyczne rekomendacje i podejścia do oceny ryzyka.**

5. Ryzyko i niezgodność – wyważone podejście

W piątej sesji uczestnicy przyglądali się temu, **jak organizacje podejmują decyzje dotyczące akceptowalnego poziomu ryzyka** oraz **kiedy decydują się na działania naprawcze**. Analizowano przykłady sytuacji, w których ryzyko staje się impulsem do zmian, oraz omawiano mechanizmy eskalacji i struktury zarządzania, które pomagają podejmować decyzje w warunkach niepewności. Rozmowy dotyczyły również sposobów komunikacji z regulatorami w przypadkach niejasności interpretacyjnych oraz narzędzi, które pozwalają identyfikować i ograniczać ryzyko, zanim doprowadzi ono do naruszeń lub postępowań egzekucyjnych.

6. Najważniejsze tematy bieżące

Ostatnia sesja miała charakter otwarty i była **poświęcona zagadnieniom, które zyskały szczególne znaczenie w okresie poprzedzającym Forum**. Tematy zostały **wybrane na podstawie ankiety** skierowanej do uczestników i obejmowały aktualne propozycje legislacyjne, nowe obowiązki regulacyjne oraz technologie wpływające na praktyki przetwarzania danych. Sesja umożliwiła wymianę doświadczeń dotyczących najnowszych trendów oraz przypadków, które w ostatnim czasie przyciągały uwagę opinii publicznej.

WŁOSKI ORGAN NADZORCZY NAŁOŻYŁ NA BANK INTESA SANPAOLO KARĘ ADMINISTRACYJNĄ W WYSOKOŚCI 31,8 MLN EURO

Pracownik banku dokonywał wglądu do danych osobowych objętych tajemnicą bankową i przetwarzał je niezgodnie z prawem ponad dwa lata – od 21 lutego 2022 roku do 24 kwietnia 2024 roku. Nie zostało to w tym okresie wychwycone przez administratora w ramach wewnętrznych procedur kontrolnych. Bank będzie musiał za to zapłacić ponad 30 mln euro.

Postępowanie zostało wszczęte **w lipcu 2024 r.** na podstawie zgłoszonego przez administratora naruszenia ochrony danych osobowych. Organ nadzorczy wykazał, że **wewnętrzny system przetwarzania danych umożliwiał pracownikowi dostęp do danych 3 573 klientów.** We wskazanym czasie pracownik ten dokonał wglądu do bazy danych poprzez uzyskanie odpowiedzi na **ponad 6,6 tys. zapytań.** Kontom, które były przedmiotem jego zainteresowania, nadano uprzednio status „wysokiego ryzyka" – obejmowały one dane bankowe osób publicznych. **Odrębny status nie był jednak zabezpieczeniem i nie miał żadnego wpływu na proces udostępniania danych**. System pozwalał użytkownikom na dokonywanie wglądu do wszystkich rejestrów danych osobowych zawartych w bazie.

Wysokie ryzyko dla praw i wolności

Natomiast w 2024 r., po zgłoszeniu przez administratora naruszenia danych osobowych, **organ nadzorczy uznał, że w jego ocenie naruszenie stanowiło wysokie ryzyko dla praw i wolności osób**, których one dotyczyły. Pierwotnie bank twierdził, że naruszenie takiego ryzyka ze sobą nie niosło, więc jako administrator nie poinformował osób o zaistniałym incydencie**. Organ nadzorczy w związku z dokonaną oceną ryzyka nakazał administratorowi podjęcie właściwych działań wskazanych w RODO** oraz przekazanie w terminie 30 dni udokumentowanych wyjaśnień obejmujących podjęte przez bank środki zaradcze.

W decyzji z 26 marca 2026 roku włoski organu nadzorczy uznał, że **administrator nie wdrożył odpowiednich środków technicznych i organizacyjnych**, które uniemożliwiałyby uzyskanie nieuprawnionego dostępu – wglądu w dane osobowe objęte tajemnicą bankową. Na wysokość nałożonej kary miała wpływ liczba osób, których dane objęło naruszenie, oraz fakt, że trwało ono tak długo. Nie bez znaczenia była też nieadekwatna reakcja administratora po stwierdzeniu naruszenia w 2024 r.

UDZIAŁ PRZEDSTAWICIELI UODO W WYDARZENIU EROD DOTYCZĄCYM WYTYCZNYCH W SPRAWIE REKLAMY POLITYCZNEJ

27 marca 2026 r. odbyło się zdalne wydarzenie zorganizowane przez Europejską Radę Ochrony Danych (EROD), poświęcone konsultacjom nad przygotowywanymi wytycznymi dotyczącymi przetwarzania danych osobowych wykorzystywanych do targetowania lub dostarczania reklam politycznych. W spotkaniu uczestniczyli przedstawiciele Departamentu Współpracy Międzynarodowej oraz Departamentu Innowacyjności i Zarządzania Danymi Urzędu Ochrony Danych Osobowych.

Wydarzenie stanowiło **element prac EROD wynikających z programu na lata 2024–2025** oraz realizację zobowiązania do dialogu z interesariuszami, podkreślonego w tzw. deklaracji helsińskiej. Dyskusja była ukierunkowana na zebranie informacji o praktykach rynkowych oraz na identyfikację obszarów wymagających doprecyzowania w przyszłych wytycznych.

1. Zasady targetowania reklam politycznych

Na początku spotkania uczestnicy odnieśli się do zmian, jakie zaszły na rynku od wejścia w życie rozporządzenia 2024/900. **Wymiana doświadczeń dotyczyła sposobów dostosowania procesów przetwarzania danych do wymogów art. 18**, w tym ograniczeń dotyczących wykorzystywania danych szczególnych kategorii. Interesariusze przedstawiali przykłady działań wdrażanych w celu zapewnienia zgodności, a także **wskazywali obszary, w których potrzebne są dodatkowe wyjaśnienia ze strony EROD.**

W dalszej części rozmów analizowano **praktyki rynkowe związane z pozyskiwaniem danych do celów reklamy politycznej**, **mechanizmy uzyskiwania wyraźnej zgody oraz sposoby zapobiegania targetowaniu osób poniżej określonego wieku**. Uczestnicy dzielili się także doświadczeniami dotyczącymi oferowania tzw. równoważnych alternatyw oraz **wdrażania procedur umożliwiających skuteczne wycofanie zgody.**

2. Obowiązki w zakresie przejrzystości i dokumentacji

Kolejny blok tematyczny dotyczył art. 19 rozporządzenia, który **nakłada na podmioty zaangażowane w reklamę polityczną szereg obowiązków informacyjnych i dokumentacyjnych.** Interesariusze wskazywali, które pojęcia i obowiązki wymagają doprecyzowania, zwłaszcza w kontekście różnorodnych modeli współpracy między podmiotami zaangażowanymi w kampanie polityczne. Ważnym elementem dyskusji była **rola systemów sztucznej inteligencji wykorzystywanych do targetowania lub dystrybucji reklam**. Uczestnicy omawiali, jak informować osoby, których dane dotyczą, o stosowaniu takich narzędzi oraz **jakie praktyki mogą wspierać przejrzystość i zrozumiałość komunikatów.**

W ramach rozmów poruszono również kwestie związane z przygotowywaniem corocznych ocen ryzyka, o których mowa w art. 19 ust. 1 lit. d. Interesariusze przedstawiali **przykłady kategorii danych wykorzystywanych w reklamie politycznej** oraz **typowych ryzyk branych pod uwagę** przy opracowywaniu takich analiz.

3. Współpraca i wymiana informacji w łańcuchu dostaw reklamy politycznej

W kolejnej części spotkania skupiono się na praktycznych aspektach współpracy pomiędzy administratorami, wydawcami oraz dostawcami usług reklamowych. Omawiano **standardy i procedury stosowane w celu zapewnienia terminowej i rzetelnej wymiany informacji**, a także sposoby określania ról poszczególnych podmiotów w ramach RODO.

Uczestnicy przedstawiali **rozwiązania organizacyjne ułatwiające przepływ informacji w złożonych strukturach reklamowych**, w tym w sytuacjach, gdy w kampanię zaangażowanych jest wielu wydawców. Rozmowy dotyczyły również **koordynacji obowiązków informacyjnych** oraz sposobów **zapewnienia spójności komunikacji** kierowanej do odbiorców reklam.

4. Podsumowanie i dalsze kroki

Wydarzenie umożliwiło zebranie szerokiego zakresu informacji na temat praktyk rynkowych oraz wyzwań związanych z wdrażaniem rozporządzenia 2024/900. Zebrane opinie posłużą EROD do **opracowania wytycznych, które mają wspierać organy nadzorcze w ocenie zgodności działań podmiotów zaangażowanych w reklamę polityczną**. Udział przedstawicieli UODO w wydarzeniu pozwolił na zapoznanie się z perspektywami różnych interesariuszy oraz na wniesienie polskiego doświadczenia do dyskusji nad kształtem przyszłych wytycznych.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych:

Stakeholder event on political advertising: agenda available now | European Data Protection Board

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

W marcowym numerze Biuletynu UODO przedstawiliśmy systemowe problemy związane z zakresem wyłączeń w wymiarze sprawiedliwości oraz modelem nadzoru nad przetwarzaniem danych osobowych przez sądy i prokuratury w Polsce. Niniejsza część koncentruje się na praktycznym funkcjonowaniu instrumentów przewidzianych w dyrektywie 2016/680, w szczególności na uprawnieniach organów nadzorczych, modelu sankcyjnym oraz realizacji praw osób, których dane dotyczą.

Ewaluacja wdrożenia Dyrektywy 2016/680 w Polsce po raz kolejny wykazała, że mimo formalnej transpozycji przepisów ich skuteczność jest ograniczona przez bariery proceduralne, niejednoznaczny zakres kompetencji oraz niepełne wykorzystanie dostępnych instrumentów.

Uprawnienia Prezesa UODO w zakresie prowadzenia postępowań należy co do zasady ocenić jako **funkcjonalne i wystarczające**. Pracownicy Urzędu, działający z jego upoważnienia, mają **możliwość wglądu do danych oraz dokumentacji związanej z kontrolą**, a także pozyskiwania informacji niezbędnych **do monitorowania i egzekwowania przepisów ustawy wdrażającej dyrektywę 2016/680**, w tym w postępowaniach skargowych.

Uzupełniająco **Prezes UODO może zwrócić się do inspektora ochrony danych o przeprowadzenie sprawdzenia zgodności i przedstawienie sprawozdania z jego wyników**. Nie odnotowano sytuacji, w których brak dostępu do danych uniemożliwiałby prowadzenie postępowania w trybie DODO.

Prawo pośredniego dostępu do danych

W polskim systemie prawnym brakuje mechanizmu pośredniego dostępu do danych, który umożliwiałby osobie, której dane dotyczą, skorzystanie z dodatkowej gwarancji ochronnej w przypadku odmowy udostępnienia informacji, sprostowania lub usunięcia danych przez organy ścigania. **Obywatel nie może zatem zwrócić się do Prezesa UODO o przeprowadzenie niezależnej weryfikacji legalności przetwarzania danych** w tym obszarze. W praktyce oznacza to pozbawienie jednostki możliwości skorzystania z jednego z kluczowych instrumentów ochronnych przewidzianych w dyrektywie 2016/680, a tym samym **osłabienie prawa do skutecznego środka ochrony prawnej.**

Argumentacja polskiego ustawodawcy, zgodnie z którą funkcję tę miałoby realizować prawo do wniesienia skargi, nie jest trafna, zważywszy na komplementarny, a nie zastępczy charakter obu instrumentów. W projekcie ustawy wdrażającej DODO przedłożonym w 2018 r. projektodawca wskazywał, że mechanizm przewidziany w art. 17 dyrektywy 2016/680 ma być realizowany za pośrednictwem skargi do Prezesa UODO, o której mowa w art. 52 tej dyrektywy. Prezes UODO od

początku podnosił jednak, że **są to odrębne instrumenty prawne, realizujące odmienne cele i wymagające odrębnych procedur**. Stanowisko to zostało potwierdzone w orzecznictwie Trybunału Sprawiedliwości UE (wyrok w sprawie C-333/22).

W konsekwencji należy stwierdzić, że w prawie polskim – w odróżnieniu od 23 państw członkowskich UE – art. 17 dyrektywy 2016/680 nie został skutecznie wdrożony. Do analogicznych wniosków doszli również ewaluatorzy przeprowadzający w 2024 r. ocenę stosowania przez Polskę dorobku Schengen. **W wyniku Ewaluacji Schengen Polska została zobowiązana do usunięcia stwierdzonych nieprawidłowości** oraz do zapewnienia, aby osoby, których dane dotyczą, mogły wykonywać swoje prawa dostępu, sprostowania i usunięcia danych osobowych w Systemie Informacyjnym Schengen oraz Wizowym Systemie Informacyjnym za pośrednictwem Prezesa UODO w przypadku odmowy realizacji tych praw przez właściwe organy.

Czego najczęściej dotyczą wnoszone skargi

W obszarze realizacji prawa do wniesienia skargi w obszarze ochrony porządku publicznego obserwuje się w Polsce umiarkowaną, zasadniczo **stabilną liczbę spraw kierowanych do organów nadzorczych w latach 2022–2025**. Na tle państw UE Polska nie należy do jurysdykcji o najwyższej liczbie skarg – rozkład w Unii jest silnie zróżnicowany – jednak **skargi pozostają w Polsce istotnym źródłem sygnałów o nieprawidłowościach** w przetwarzaniu danych w sektorze operacyjnym.

W sprawach pozostających w zakresie właściwości Prezesa UODO **dominowały skargi dotyczące funkcjonowania policyjnych systemów informacyjnych**, w szczególności Krajowego Systemu Informacyjnego Policji, a także – w mniejszym zakresie – Krajowego Centrum Informacji Kryminalnych oraz Centralnej Bazy Osób Pozbawionych Wolności. Wśród najczęściej podnoszonych zarzutów pojawiały się **kwestie udostępniania danych osobom nieuprawnionym, przetwarzania danych po upływie ustawowych okresów** retencji, **braku podstawy prawnej przetwarzania lub udostępniania danych**, **niewykonywania obowiązków informacyjnych wobec osób, których dane dotyczą, a także odmów usunięcia danych w systemach**. Odnotowywano również **skargi związane z udostępnianiem danych przez podmioty penitencjarne** (w tym sytuacje, w których dane miały trafić do innych osadzonych) oraz przypadki dotyczące udostępniania danych w toku czynności policyjnych.

Z perspektywy proceduralnej znaczenie ma także to, że **część skarg nie mogła być merytorycznie rozpoznana z przyczyn formalnych** (np. z uwagi na ich wniesienie po przewidzianym terminie 30 dni od powzięcia wiadomości o tym naruszeniu lub otrzymania informacji od administratora), co w konkretnych sprawach przekłada się na **ograniczenie możliwości uzyskania rozstrzygnięcia co do meritum.**

Odnotowano ponadto **skargi wnoszone przez straże miejskie**, które dotyczyły **odmowy udostępnienia danych przez operatorów telekomunikacyjnych** lub **zakłady ubezpieczeń**, co – w ocenie skarżących – utrudniało ustalenie sprawców wykroczeń. Pokazuje to, że spory na tle DODO mogą dotyczyć **nie tylko nieprawidłowości po stronie organów, ale również praktycznych barier w pozyskiwaniu danych w ramach czynności służbowych**, wymagających każdorazowo oceny podstaw prawnych i zasadności żądania.

6 SPRAWY MIĘDZYNARODOWE - SCHENGEN

W zakresie właściwości organów nadzorczych funkcjonujących w strukturach prokuratur wskazywano **skargi odnoszące się m.in. do ujawniania danych w treści rozstrzygnięć** wydawanych w postępowaniach przygotowawczych, **braku anonimizacji danych** w aktach spraw karnych**, gromadzenia materiałów zawierających dane genetyczne oraz realizacji praw dostępu i usunięcia danych**. Jednocześnie podkreślano, że w odniesieniu do danych przetwarzanych w ramach postępowań karnych wykonywanie praw osób, których dane dotyczą, bywa w praktyce ograniczone do zakresu wynikającego z przepisów szczególnych regulujących przebieg tych postępowań, a nie na podstawie ustawy grudniowej.

Powiadomienia o naruszeniach ochrony danych

Prezes Urzędu Ochrony Danych Osobowych odnotowuje sytuacje, w których administratorzy danych nie przekazują organowi informacji o naruszeniu ochrony danych w terminie 72 godzin od jego stwierdzenia, powołując się na trwające czynności operacyjne lub konieczność zachowania poufności zdarzenia. Choć **obowiązek zgłoszenia powinien być zrealizowany niezwłocznie po ustaniu przeszkód wraz z wyjaśnieniem przyczyn opóźnienia, w praktyce zdarza się, że Urząd otrzymuje te informacje ze znacznym opóźnieniem**. Bywają także przypadki całkowitego odstąpienia od zgłoszenia. Powoduje to istotne ograniczenia w dostępie do danych i informacji wymaganych do prowadzenia postępowań i pełnej oceny skali naruszeń.

Model sankcyjny

Istotnym problemem pozostaje **brak skutecznych sankcji o charakterze odstraszającym**. W obecnym modelu Prezes UODO nie ma możliwości nakładania administracyjnych kar pieniężnych za naruszenia przepisów tej ustawy, a jednocześnie nie dysponuje także „miękkim" instrumentem prewencyjnym w postaci upomnienia (analogicznego do rozwiązania znanego z RODO). Oznacza to, że **postępowania mogą tracić walor oddziaływania prewencyjnego**: nawet jeśli naruszenie zostanie stwierdzone, a następnie usunięte, organ nie ma do dyspozycji środka, który w sposób wyraźny „zamyka" sprawę konsekwencją o charakterze wychowawczym lub odstraszającym.

Jednocześnie należy zauważyć, że **organy nadzorujące ochronę danych osobowych w sądach i prokuraturze posiadają możliwość stosowania upomnienia, podczas gdy Prezes UODO** – jako organ o najszerszej roli systemowej – **takiego narzędzia nie ma**. Z perspektywy spójności i skuteczności systemu nadzoru osłabia to jednolity standard reakcji na naruszenia w obszarze objętym DODO i utrudnia realizację wymogu, aby sankcje były „skuteczne, proporcjonalne i odstraszające".

Wnioski

Praktyka stosowania przepisów wdrażających dyrektywę 2016/680 jednoznacznie wskazuje, że **główne problemy mają charakter systemowy**. Formalna implementacja nie przekłada się w pełni na skuteczną ochronę praw jednostki, w szczególności w warunkach ograniczeń proceduralnych i niepełnego wykorzystania dostępnych instrumentów.

6 SPRAWY MIĘDZYNARODOWE - SCHENGEN

Istotną luką pozostaje **brak mechanizmu pośredniego dostępu**, co oznacza **niepełną implementację dyrektywy i osłabienie prawa do skutecznego środka ochrony prawnej**. Model sankcyjny pozbawiony jest zarówno kar pieniężnych, jak i instrumentów „miękkich", przez co nie zapewnia wystarczającego efektu prewencyjnego.

Całościowo system nadzoru nad przetwarzaniem danych w obszarze egzekwowania prawa wymaga zmian o charakterze systemowym – zarówno na poziomie instrumentów prawnych, jak i ich praktycznego stosowania.

Wnioski te znalazły odzwierciedlenie w **wystąpieniu Prezesa UODO z 16 marca 2026 r., skierowanym do Ministra Spraw Wewnętrznych i Administracji oraz Ministra Sprawiedliwości**, w którym wskazano potrzebę pilnych zmian legislacyjnych zapewniających pełną i skuteczną implementację dyrektywy (UE) 2016/680.

KLUCZEM JEST ZAUFANIE I REALNA KORZYŚĆ PO STRONIE PACJENTA

Pacjenci są gotowi dzielić się swoimi danymi, jeśli widzą sens: lepszą diagnostykę, skuteczniejsze leczenie, szybszy dostęp do innowacji. Raport pokazuje, że tam, gdzie system jest transparentny – jak w krajach skandynawskich – pacjent wie, kto, kiedy i po co korzysta z jego danych. Dane nie należą do pojedynczego zespołu czy projektu – są dobrem wspólnym, które powinno pracować na rzecz pacjentów i systemu – mówi wiceprezes Naukowej Fundacji Polpharmy Krzysztof Kurowski.

Raport „Mapa źródeł danych medycznych", jak sugeruje tytuł, pokazuje, gdzie te dane się znajdują. Ale czy dziś większym wyzwaniem jest ich brak… czy brak odwagi, by je wykorzystać?

Zdecydowanie **brak odwagi – rozumianej jako gotowość systemowa, prawna i organizacyjna** do realnego korzystania z danych. Raport bardzo jasno pokazuje, że w Polsce **nie cierpimy na deficyt danych**, lecz na deficyt wiedzy, gdzie one są, jakiej są jakości i na jakich zasadach mogą być wykorzystane. Mamy miliardy rekordów w systemach centralnych, setki rejestrów klinicznych i ogromne zasoby danych w szpitalach – ale funkcjonują one w silosach. Brakuje jasnych reguł wtórnego wykorzystania danych, odwagi decydentów do ich otwarcia w sposób bezpieczny oraz kultury pracy opartej na danych, a nie wyłącznie na intuicji czy procedurze.

Jaką lukę w polskim systemie ochrony zdrowia ten raport miał przede wszystkim wypełnić?

Najważniejszą luką był **brak mapy wiedzy o zasobach danych medycznych w Polsce**. Do tej pory nikt nie potrafił odpowiedzieć na fundamentalne pytanie: jakie dane mamy, gdzie są, kto nimi zarządza i w jakim celu można je wykorzystać. Raport jest „fotografią rzeczywistości" – pierwszym tak kompleksowym uporządkowaniem źródeł danych, rejestrów, systemów i alternatywnych zasobów, od EDM po dane generowane przez pacjentów czy biobanki. Bez takiej mapy nie da się sensownie projektować reform, wdrażać EHDS ani rozwijać medycyny opartej na danych.

Dlaczego właśnie teraz temat danych medycznych staje się tak istotny?

Bo **zbiegły się trzy procesy**. Po pierwsze – cyfryzacja ochrony zdrowia osiągnęła masę krytyczną: e-recepty, e-skierowania, EDM, IKP. Po drugie – **sztuczna inteligencja** realnie wchodzi do praktyki klinicznej

i bez wysokiej jakości danych nie będzie ani bezpieczna, ani skuteczna. Po trzecie – **Europejska Przestrzeń Danych Zdrowotnych (EHDS)** wymusza uporządkowanie zasad dostępu do danych i ich wtórnego wykorzystania. To moment, w którym brak decyzji oznacza marginalizację Polski w europejskiej nauce i innowacjach.

Jakie są najważniejsze wnioski z raportu – co najbardziej Pana zaskoczyło?

Najbardziej uderzające było to, jak **dużo danych istnieje poza oficjalnymi wykazami** – w lokalnych rejestrach, projektach naukowych, systemach szpitalnych. Zaskakuje też skala nieefektywności: dane są zbierane ogromnym kosztem pracy lekarzy, ale **nie wracają do nich w postaci analiz, benchmarków czy wsparcia decyzyjnego**. Raport pokazuje, że bez informacji zwrotnej dane przestają być narzędziem jakości, a stają się obciążeniem.

Gdyby miał Pan wskazać jedną zmianę, która najbardziej przyspieszyłaby wykorzystanie danych medycznych w Polsce – co by to było?

Jedna kluczowa zmiana to **jasne, centralne ramy prawne dla wtórnego wykorzystania danych medycznych**, oparte na pseudonimizacji, interoperacyjności i odpowiedzialności, a nie na strachu. Inicjatywa Prezesa UODO oraz wdrażanie EHDS idą w dobrym kierunku – teraz potrzebne są konkretne przepisy i instytucjonalne mechanizmy, które umożliwią nauce i systemowi ochrony zdrowia bezpieczne korzystanie z danych w skali populacyjnej.

Co można zrobić, by zachęcić instytucje do wymiany danych i ograniczyć zamknięcie ich w systemie silosowym?

Po pierwsze – **standaryzacja i interoperacyjność**, bo bez wspólnego języka danych współpraca jest niemożliwa. Po drugie – **zmiana bodźców**: instytucje muszą widzieć wartość wymiany danych, np. w postaci lepszego finansowania, benchmarków jakości czy dostępu do analiz. Po trzecie – **kultura współpracy**, a nie „własności" danych. Raport jasno pokazuje, że dane nie należą do pojedynczego zespołu czy projektu – są dobrem wspólnym, które powinno pracować na rzecz pacjentów i systemu.

Jak przekonać ludzi do dobrowolnego dzielenia się danymi o stanie zdrowia w świecie, w którym te dane są coraz bardziej traktowane jak waluta?

Kluczem jest **zaufanie i realna korzyść po stronie pacjenta**. Pacjenci są gotowi dzielić się swoimi danymi, jeśli widzą sens: lepszą diagnostykę, skuteczniejsze leczenie, szybszy dostęp do innowacji. Raport pokazuje, że tam, gdzie system jest transparentny – jak w krajach skandynawskich – pacjent wie, **kto, kiedy i po co korzysta z jego danych**. To właśnie transparentność, możliwość kontroli (np. wgląd w historię dostępu do danych w IKP) oraz jasne komunikowanie celu wykorzystania danych budują społeczną gotowość do ich udostępniania, nawet w epoce „danych jako waluty".

URZĄD OCHRONY DANYCH OSOBOWYCH

Prezes UODO zaprasza na wydarzenia

Pierwsze spotkanie w ramach **Cyklu Otwartych Wykładów Eksperckich**
Tworzenie prawa ekosystemu danych w UE. Uwagi z perspektywy praktycznych doświadczeń i wyzwania na przyszłość

Termin: **15 maja 2026 r.,** godz. **10:00-12:00**

Organizatorzy: **Urzęd Ochrony Danych Osobowych i Krajowa Izba Radców Prawnych**

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

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

Dynamiczny rozwój nowych technologii oraz rosnące znaczenie ochrony danych osobowych i prywatności sprawiają, że potrzebujemy dziś rzetelnej i praktycznej rozmowy o wyzwaniach w tym obszarze. Odpowiedzią na tę potrzebę jest Cykl Otwartych Wykładów Eksperckich, którego celem jest stworzenie przestrzeni do wymiany wiedzy, doświadczeń oraz refleksji nad najważniejszymi problemami i kierunkami zmian. Wydarzenie rozpocznie się wykładem eksperckim pt. „Tworzenie prawa ekosystemu danych w UE. Uwagi z perspektywy praktycznych doświadczeń i wyzwania na przyszłość", który wygłosi dr Karolina Mojzesowicz, Zastępca Szefa Działu Ochrona Danych Osobowych w Dyrekcji Generalnej ds. Sprawiedliwości i Konsumentów w Komisji Europejskiej. Po wykładzie zaplanowano panel dyskusyjny z udziałem przedstawicieli środowiska naukowego i praktyków. Spotkanie zakończy się otwartą rozmową z uczestnikami – będzie to doskonała okazja do wymiany perspektyw oraz wspólnego spojrzenia na aktualne wyzwania w obszarze ochrony danych i prywatności.

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

Drugie spotkanie w ramach **Cyklu Otwartych Wykładów Eksperckich**

Wrażliwe dane osobowe w dobie genomiki

Termin: **11 czerwca 2026 r.**

Organizatorzy: **Urzęd Ochrony Danych Osobowych**

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

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

Dynamiczny rozwój technologii w kontekście danych genetycznych sprawia, że kwestia ochrony danych osobowych szczególnej kategorii nabiera dziś ogromnego znaczenia. Dane genetyczne, ze względu na swój unikalny charakter i potencjał identyfikacyjny, stawiają przed prawem oraz praktyką nowe, złożone wyzwania. Odpowiedzią na te zmiany jest potrzeba pogłębionej, interdyscyplinarnej refleksji nad sposobami ich przetwarzania i ochrony. Wykład ekspercki pt. „Wrażliwe dane osobowe w dobie genomiki", przedstawi prof. dr hab. Michał Witt, Przewodniczący Komitetu Genetyki Człowieka i Patologii Molekularnej Wydziału Medycznego PAN, który wprowadzi uczestników w najważniejsze zagadnienia związane z wykorzystaniem danych genetycznych oraz wynikającymi z tego konsekwencjami prawnymi i etycznymi, szczególną uwagę poświęcając testom genetycznym. Następnie, już tradycyjnie, zgodnie z formułą Cyklu Otwartych Wykładów Eksperckich, odbędzie się panel dyskusyjny z udziałem przedstawicieli środowiska naukowego i praktyków, podczas którego poruszone zostaną aktualne problemy oraz kierunki zmian w tym obszarze. Spotkanie zakończy się również rozmową z uczestnikami, która stanowić będzie przestrzeń do wymiany doświadczeń i perspektyw oraz wspólnego namysłu nad wyzwaniami związanymi z ochroną danych szczególnej kategorii w erze dynamicznego rozwoju genomiki.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl