URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 09/09/25

www.uodo.gov.pl

SPIS TREŚCI

WPROWADZENIE

Mirosław Wróblewski, Prezes Urzędu Ochrony Danych Osobowych S. 3

Karol Witowski, Rzecznik Prasowy UODO S. 6

1. ROZMOWA Z EKSPERTEM

Każda podróż zaczyna się od ochrony danych osobowych S. 8
- Joanna Bochniarz, prezeska Fundacji Polskich Portów Lotniczych

2. PRAWO I NOWE TECHNOLOGIE

Gmina nie może przyznać policji stałego dostępu do swojego monitoringu S. 12

4. NARUSZENIA I KONTROLE

Kara po kontroli w Polskim Radiu Szczecin S. 18

5. SPRAWY MIĘDZYNARODOWE

- Ukierunkowane zmiany w RODO: EROD i EIOD z zadowoleniem przyjmują uproszczenie obowiązków dot. prowadzenia rejestrów i proszą o dalsze wyjaśnienia S. 20
- Oświadczenie helsińskie ws. większej przejrzystości, wsparcia i zaangażowania S. 22
- Irlandzka Komisja Ochrony Danych ogłasza zakończenie dochodzenia ws. wykorzystania technologii dopasowywania twarzy w związku z Kartą Usług Publicznych przez Departament Ochrony Społecznej S. 24
- Kara administracyjna dla Rzecznika ds. Równości za zbieranie danych osobowych za pomocą formularza internetowego S. 27
- Pliki cookies umieszczane bez zgody: SHEIN ukarany karą administracyjną w wysokości 150 mln euro przez CNIL S. 28
- Polska aktywnie uczestniczy w debacie o przyszłości prywatności – relacja z 47. Global Privacy Assembly w Seulu S. 30

6. SPRAWY MIĘDZYNARODOWE/ SCHENGEN

- UE-USA: wzmocnione partnerstwo na rzecz bezpieczeństwa granic S. 33
- Eurodac – wyzwania dla ochrony danych S. 35

6. EDUKACJA

Prezes UODO zaprasza na wydarzenia edukacyjne, zaplanowane na ostatni kwartał 2025 r. S. 37

Szanowni Państwo,

1 września rozpoczął się nowy rok szkolny, a wraz z nim kolejny etap kontaktu naszych dzieci z cywilizacją cyfrową. Czy jesteśmy gotowi, aby wspierać je w poznawaniu tego świata?

Zwróciłem na to uwagę w liście do społeczności szkolnej – rodziców, uczniów i nauczycieli. Nowy, dobrowolny przedmiot edukacja zdrowotna oraz obowiązkowa edukacja obywatelska obejmują w podstawach programowych także zagadnienia związane z ochroną danych osobowych, prywatnością i świadomym korzystaniem z nowych technologii – dotyczą one m.in. ryzyka uzależnień cyfrowych czy wyzwań związanych ze sztuczną inteligencją i wirtualną rzeczywistością.

Chcemy wspierać tę edukację. Dlatego we wrześniu uruchomiliśmy w Urzędzie Ochrony Danych Osobowych kolejną edycję programu dla szkół „Twoje dane – Twoja sprawa". Nabór trwa do 31 października. Zapraszamy!

Ochrona praw i bezpieczeństwa dzieci w świecie cyfrowym wymaga wielu działań:

Dlatego o sytuacji dzieci i młodzieży w kontekście cyberataków, odporności placówek oświatowych i organizacji społecznych na te zjawiska, ochrony danych osobowych, a także skali i rodzajów zagrożeń cyfrowych oraz związanych z nimi wyzwań organizacyjnych i legislacyjnych mówiłem 25 września przed sejmową Komisją ds. Dzieci i Młodzieży.

Zjawisko sharentingu, czyli publikowania w mediach społecznościowych zdjęć dzieci bez ograniczeń dostępu przez rodziców lub opiekunów prawnych, przybiera niestety coraz szersze kręgi. Takie działania mogą stać się źródłem materiałów do deepfake'ów, fotomontaży czy narazić dziecko na przemoc rówieśniczą. Wizerunek swoich dzieci upublicznia w sieci aż 40% rodziców. W tym zakresie staramy się prowadzić szerokie działania edukacyjne, także we współpracy z organami państwa i ekspertami. W pewnych jednak przypadkach – gdy promowanie sharentingu przybiera formy zinstytucjonalizowane – edukacja nie wystarcza. Dlatego poprosiłem Ministrę Rodziny, Pracy i Polityki Społecznej o interwencję w sprawie fundacji „Dzieci są z nami", która promuje takie niepokojące praktyki. Ministra Rodziny sprawuje bowiem nadzór nad fundacją.

Przy okazji chciałbym podkreślić, że Urząd Ochrony Danych Osobowych został doceniony na arenie międzynarodowej, otrzymując wyróżnienie w prestiżowym konkursie Global Privacy and Data Protection Awards 2025. Nagroda w kategorii Education and Awareness została przyznana za projekt „Wizerunek dziecka w internecie. Publikować czy nie?", zrealizowany wspólnie z Fundacją Orange. Wszystkim, którzy przyczynili się do tego sukcesu, serdecznie dziękuję.

W ostatnim czasie poprosiłem Ministra Cyfryzacji, wicepremiera Krzysztofa Gawkowskiego, o rozważenie wprowadzenia krajowych przepisów odnoszących się bezpośrednio do rozpowszechniania szkodliwych treści w postaci deepfake'ów i scamu, które zapewnią ofiarom możliwość szybkiej i skutecznej ochrony swoich praw. Ta potrzeba staje się coraz wyraźniejsza.

Podjąłem także współpracę z Irlandzką Komisją Ochrony Danych (Data Protection Commission) oraz jedną z największych platform mediów społecznościowych w celu opracowania rozwiązań zwalczających zjawisko celeb bait – oszustwa internetowego polegającego na wykorzystywaniu wizerunku znanych osób do wyłudzania danych osobowych, pieniędzy lub innych korzyści. Cieszę się, że podjęte przeze mnie działania w ubiegłym roku w sprawach indywidualnych przekuwają się we współpracy z partnerami instytucjonalnymi w poprawę systemową ochrony praw osób fizycznych.

Potrzeba doprecyzowania i dostosowania przepisów

We wrześniu zwróciłem ponownie uwagę Poczcie Polskiej na konieczność wzmocnienia zabezpieczeń przesyłek. Nadal zbyt często dochodzi do zaginięć paczek, wydania ich osobom nieuprawnionym lub doręczania uszkodzonych przesyłek. W ostatnim czasie takie problemy zasygnalizowały mi np. bezpośrednio sądy.

Przedstawiłem również opinię dotyczącą tzw. deregulacji, w tym konkretnym przypadku propozycji rezygnacji z pisemnej formy upoważnień do przetwarzania danych osobowych wydawanych przez administratorów danych. Zaznaczyłem, że RODO nie wymaga sformalizowanej pisemnej formy takich upoważnień, a problemem są nadmiarowe wymagania krajowe. Zmiany mogą być wprowadzane, ale pod warunkiem przeprowadzenia testu prywatności, w tym oceny skutków dla ochrony danych.

W korespondencji z Ministrem Zdrowia wskazałem z kolei na konieczność zmiany modelu dostępu do danych osobowych osób objętych obowiązkiem wpisu do Rejestru Podmiotów Wykonujących Działalność Leczniczą. Zwróciłem uwagę, że w pełni publiczny dostęp do adresów domowych lekarzy może prowadzić do poważnych zagrożeń. Niedawne akty agresji wobec pracowników medycznych pokazują, że należą oni do grupy szczególnie narażonej na ryzyka. Stąd moje wystąpienie do Ministra Zdrowia o podjęcie działań w tym zakresie.

Zmiany wymagają również przepisy dotyczące dokumentacji medycznej wykorzystywanej do badań naukowych. Z postulatem ich nowelizacji zwróciłem się do Ministra Zdrowia oraz Ministra Nauki i Szkolnictwa Wyższego.

Nowe regulacje unijne

We wrześniu weszło w życie ważne rozporządzenie, które wpłynie na życie nas wszystkich – Akt w sprawie danych, czyli unijne rozporządzenie w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania. Od 12 września stosuje się ono bezpośrednio we wszystkich państwach członkowskich UE.

Jest to kolejne, po Akcie w sprawie zarządzania danymi, unijne rozporządzenie realizujące Europejską strategię w zakresie danych, które nie wyłącza ani nie zastępuje RODO, lecz reguluje sprawiedliwy dostęp do danych i ich wykorzystywanie.

Decyzje PUODO i wyroki sądów

Chciałbym zwrócić Państwa uwagę na wyrok WSA w Warszawie, który oddalił skargę Toyota Bank Polska SA na decyzję Prezesa UODO o nałożeniu kary. Sąd zgodził się z oceną, że bank naruszył RODO, profilując dane klientów w celu określenia ich zdolności kredytowej, nie ujawniając tego w rejestrze czynności przetwarzania danych. Ponadto Inspektor Ochrony Danych w tym banku nie podlegał bezpośrednio najwyższemu kierownictwu.

Podobnej kwestii dotyczyła sprawa spółki medycznej, w której funkcję IOD pełnił prezes. Jest to rozwiązanie sprzeczne z RODO, ponieważ nie gwarantuje niezależnego i obiektywnego wykonywania obowiązków związanych z ochroną danych.

Kolejny istotny wyrok, tym razem NSA, dotyczył sędziego, który zgubił trzy pendrive'y z dokumentacją zawierającą dane osobowe. Naruszenie wynikało z braku odpowiednich zabezpieczeń i za to Prezes UODO nałożył karę. WSA ją uchylił, uznając, że naruszenie nie było poważne i wystarczyłoby upomnienie. NSA podtrzymał jednak merytoryczne stanowisko Prezesa UODO.

Informacja dla obywateli

Od kilku miesięcy publikujemy na naszej stronie odpowiedzi na najczęściej zadawane pytania, z jakimi obywatele zwracają się do naszej infolinii. We wrześniu – co nie dziwi – wiele pytań dotyczyło danych osobowych w szkołach, w tym zasad działania monitoringu, ale pojawiały się też inne zagadnienia.

Infolinia UODO czynna jest w dni robocze w godzinach 10:00–14:00 pod numerem telefonu 606 950 000. Zapraszamy do kontaktu.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W najnowszym wydaniu naszego biuletynu znajdziecie wywiad z prezeską Fundacji Polskich Portów Lotniczych Joanną Bochniarz. Głównym tematem rozmowy jest bezpieczeństwo danych w podróży i podnoszenie standardów bezpieczeństwa w lotnictwie. To nad wyraz kluczowe zagadnienie, gdy tylko weźmiemy pod uwagę fakty, które przybliża nam Joanna Bochniarz: w zeszłym roku warszawskie lotnisko Chopina odprawiło ponad 21 mln podróżnych, a w bieżącym roku będzie ich nawet 24 mln. W naszej rozmowie poruszamy też temat wykorzystywania sztucznej inteligencji podczas przetwarzania danych osobowych w portach lotniczych.

W tym wydaniu powracamy do problemów związanych z monitoringiem wizyjnym. Prezes UODO udzielił wyjaśnień jednej z gmin, która z komendą policji zamierzała zawrzeć porozumienie przewidujące przyznanie policji dostępu w czasie rzeczywistym do monitoringu miejskiego prowadzonego przez straż gminną. Jak się okazuje, jednostki samorządu terytorialnego nie mają podstaw prawnych do takiego działania.

Przywołujemy też sprawę kary nałożonej przez Prezesa Urzędu na Polskie Radio – Regionalną Rozgłośnię w Szczecinie „PR Szczecin” SA w likwidacji. Została ona nałożona z powodu braku odpowiedniego poziomu bezpieczeństwa danych, które powinno być oparte na analizie ryzyka wiążącego się z ich przetwarzaniem, oraz za niedostateczną kontrolę skuteczności zabezpieczeń. Jak pamiętamy, kontrowersja dotyczy materiału dziennikarskiego z 2022 r., w którym przedstawiono sprawę pedofila w taki sposób, że łatwo można było ustalić personalia niepełnoletniej ofiary. Skończyło się to jej samobójstwem.

W tym numerze biuletynu, jak zazwyczaj, znajdziecie także zestawienie najważniejszych wydarzeń wokół ochrony danych osobowych w Europie i procesu legislacyjnego w tej sprawie. Podkreślamy zatem m.in., że Europejska Rada Ochrony Danych oraz Europejski Inspektor Ochrony Danych z zadowoleniem przyjmują uproszczenie obowiązków dot. prowadzenia rejestrów. W tej perspektywie niezwykle ważne jest też spotkanie wysokiego szczebla w Helsinkach, w trakcie którego EROD przyjęła przełomowe oświadczenie w kwestii zwiększenia przejrzystości, wsparcia i zaangażowania. Dokument ten przedstawia nowe inicjatywy mające na celu ułatwienie zgodności z RODO, szczególnie dla mikro-, małych i średnich organizacji.

Prezentujemy również podsumowanie 47. Global Privacy Assembly (GPA), które 15–19 września odbyło się w Seulu. To międzynarodowe forum poświęcone ochronie danych i prywatności. Tegoroczne wydarzenie zgromadziło ponad 140 organów nadzorczych z całego świata, a jego głównym tematem była sztuczna inteligencja w codziennym życiu. Na GPA Polskę reprezentowali prezes UODO Mirosław Wróblewski oraz dyrektorka Departamentu Współpracy Międzynarodowej Maria Owczarek.

Jeśli chodzi o kwestie międzynarodowe, staramy się także wyjaśnić, czym jest Eurodac – unijny system informacyjny do porównywania odcisków palców, oraz przybliżamy zalecenie wydane w lipcu przez Komisję Europejską, skupiające się na decyzji Rady UE upoważniającej do rozpoczęcia negocjacji ws. umowy ramowej między Unią a Stanami Zjednoczonymi o wymianie informacji na potrzeby kontroli bezpieczeństwa w czasie procedur granicznych.

Na zakończenie tego wydania informujemy o działaniach edukacyjnych UODO, które zostały zaplanowane na ostatni kwartał tego roku. Już teraz zapraszamy wszystkich na konferencje, seminaria i wykłady, tym bardziej że będzie można w nich uczestniczyć także w formule on-line.

Karol Witowski
Dyrektor Departamentu Komunikacji Społecznej
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

KAŻDA PODRÓŻ ZACZYNA SIĘ OD OCHRONY DANYCH OSOBOWYCH

O bezpieczeństwie danych w podróży – z prezeską Fundacji Polskich Portów Lotniczych Joanną Bochniarz rozmawia Karol Witowski, rzecznik prasowy UODO.

Nasze instytucje zorganizowały wspólnie Galę Finałową Konkursów Prezesa UODO, stanowiącą uroczyste podsumowanie XV edycji ogólnopolskiego programu edukacyjnego dla szkół podstawowych i ponadpodstawowych „Twoje dane – Twoja sprawa". Gala była również symbolicznym rozpoczęciem współpracy między UODO a Fundacją PPL, zgodnie z podpisanym 23 maja 2025 r. porozumieniem. Razem z Fundacją Polskich Portów Lotniczych, która działa na rzecz podnoszenia standardów bezpieczeństwa w lotnictwie oraz edukowania pasażerów w zakresie bezpiecznego podróżowania, czekają nas wspólne przedsięwzięcia: konkursy, webinaria, szkolenia…

Z reguły podróże chcemy spędzić bez zbędnych zmartwień. Tymczasem jest to świetny czas dla oszustów, którzy chcą wykorzystać nasz brak czujności. Jakie wymieniłaby Pani najważniejsze zasady bezpieczeństwa danych podczas lotów samolotem?

W podróży, zwłaszcza zagranicznej, powinniśmy dbać o bezpieczeństwo naszych dokumentów. Warto zrobić kilka kserokopii dowodu osobistego lub paszportu. Możemy wtedy naszą kopię na przykład okazać w hotelu, bez konieczności dawania obsłudze fizycznego dokumentu. Ksero dokumentu będzie również przydatne w sytuacji, gdy utracimy nasz dokument.

Zalecam zabierać z sobą komplet dokumentów – nawet w przypadku podróży w ramach Unii Europejskiej, gdzie wystarcza tylko dowód osobisty. Jeden z dokumentów zamykamy bezpiecznie w hotelowym sejfie, z drugim możemy się przemieszczać. Jeśli zgubilibyśmy jeden z dokumentów – zawsze mamy awaryjny drugi.

1 ROZMOWA Z EKSPERTEM

Warto też przed podróżą zarejestrować się w rządowym programie „Odyseusz”, gdzie podajemy dane dotyczące naszej podróży. Po przyjeździe do kraju docelowego otrzymamy SMS od operatora z numerem telefonu do ambasady. Warto zachować ten SMS.

Pod kątem cyberbezpieczeństwa warto przypomnieć, że skanowanie nieznanych QR kodów czy łączenie się z ogólnodostępnymi sieciami Wi-Fi może być ryzykowne.

Przyjrzyjmy się statystykom. Ilu pasażerów obsługują rocznie Polskie Porty Lotnicze?

W zeszłym roku tylko Lotnisko Chopina odprawiło ponad 21 mln podróżnych. W bieżącym roku spodziewamy się nawet 24 mln. W sezonie letnim przez stołeczny port przewija się około 80 tys. Pasażerów na dobę. Jeśli dodamy do tego około 10 tys. pracowników, to śmiało możemy powiedzieć, że jest to średniej wielkości miasteczko.

Jak wiele osób co roku gubi dokumenty, telefony i inne przedmioty, po których łatwo jest je zidentyfikować?

Tak, jak wspomniałam – lotnisko to małe miasto. Zguby mniejsze lub większe zdarzają się codziennie. Mówimy tu o przedmiotach takich jak biżuteria (nawet obrączki ślubne), komputery, telefony, tablety, dokumenty. Większość z tych przedmiotów trafia do lotniskowego biura rzeczy znalezionych. Rzeczy pozostawione w samolotach przekazywane są do biur agentów obsługi naziemnej danych linii lotniczych. W skali światowej, mówi się o 2 milionach zagubionych dokumentów rocznie.

Ciekawi mnie też, jak wygląda procedura zwrotu tych przedmiotów, szczególnie po przeczytaniu historii ze strony pewnego serwisu internetowego poświęconego technologii. „Podczas przelotu z Pekinu do Shenzhen jeden z serbskich studentów zaproszonych przez Huawei zgubił swój paszport. Zguba została zgłoszona na lotnisku w Shenzhen, które poinformowało obsługę lotniska w stolicy Chin. Już kilka godzin później paszport odnalazł się w hali odlotów lotniska w Pekinie i jeszcze tego samego dnia został wysłany kurierem do Shenzhen”. Jak w takiej sytuacji zachowałyby się PPL, przestrzegając zasad ochrony danych osobowych?

W przypadku zwykłych przedmiotów i elektroniki – wystarczy podać cechy charakterystyczne zguby. W przypadku bardziej zaawansowanej elektroniki, takiej jak komputery czy telefony – należy podać hasło czy kod odblokowania.

Jeśli chodzi o dokumenty – z racji, że Lotnisko Chopina jest portem międzynarodowym – trafiają one do Straży Granicznej. Pasażer, który utraci dokumenty, musi się zgłosić do funkcjonariuszy, aby móc je odzyskać.

1 ROZMOWA Z EKSPERTEM

PPL przetwarza zarówno dane API – dane pasażerów (advance passenger information), jak i PNR – dane dotyczące przelotu pasażera (passenger name record). Jedne i drugie podlegają regulacjom ochrony danych na całym świecie. Jak często macie kontakt z władzami granicznymi i organami ścigania w identyfikacji danych osób?

Na bieżąco! Na Lotnisku Chopina funkcjonuje zarówno oddział Straży Granicznej, jak i komisariat policji lotniskowej. Jesteśmy bramą na świat i jako taki punkt musimy wspólnie ze służbami państwowymi zapewniać bezpieczeństwo – również poprzez poprawną identyfikację podróżnych.

Na pewno trudnym dla PPL czasem z punktu widzenia ochrony danych osobowych był okres pandemii COVID-19. Rządy wymagały wtedy zbierania informacji o stanie zdrowia, wynikach testów i statusie szczepień pasażerów przed ich przybyciem. Czy były to istotne utrudnienia na linii operatorzy lotów – PPL – pasażerowie?

Pandemia koronawirusa była wyjątkowym wydarzeniem w życiu lotniska. Wprowadzane były bezprecedensowe rozwiązania, trzeba było działać w jednej wielkiej niewiadomej, rozwiązania były wypracowywane na bieżąco. Jeśli chodzi o kwestie związane z wywiadem medycznym, to początkowo były one zbierane przez nasz zespół Ratownictwa Medycznego. Później testy prowadziły wyspecjalizowane firmy, a dane były wprowadzane do systemu rządowego.

W trakcie pandemii wprowadzono również karty lokalizacyjne – były to dokumenty, w których zbierano dane kontaktowe pasażerów. Specjalnie na tę okazję stworzyliśmy specjalne urny, aby pasażerowie mogli tam wrzucać karty lokalizacyjne. Do pojemników były specjalne klucze, które były w posiadaniu naszych medyków. Było to autorskie rozwiązanie PPL – wpadliśmy na ten pomysł naprędce, jednocześnie było ono bardzo proste i zapewniało ochronę danych pasażerów.

Jak PPL w swojej działalności korzysta ze sztucznej inteligencji, w aspekcie przetwarzania danych osobowych i cyberbezpieczeństwa?

Sztuczna inteligencja bardzo szybko się rozwija, ale w dalszym ciągu jest to jeszcze technologia niedoskonała. Korzystamy ze sztucznej inteligencji, ale nie do przetwarzania danych osobowych, czy cyberbezpieczeństwa – raczej do wsparcia naszych systemów koordynacyjnych i zarządzania potokami pasażerskimi.

1 ROZMOWA Z EKSPERTEM

Czy przetwarzanie danych przez PPL może kolidować z przepisami o ochronie danych?

Prosta odpowiedź – nie. Wszystko, co PPL robi, robi w granicach i w ramach obowiązującego prawa..

Na terenie lotnisk oraz w przyległych budynkach PPL działa zintegrowany system monitoringu wizyjnego. Dużo słyszymy o sprzęcie chińskich firm, który czuwa nad bezpieczeństwem lotnisk, stacji kolejowych, a nawet budynków rządowych na całym świecie. Ich obecność wzbudza obawy o potencjalne szpiegostwo. Jak działa system monitoringu w PPL?

Lotnisko jest ważnym elementem infrastruktury państwa. Mamy świadomość, jaka ciąży na nas odpowiedzialność i robimy wszystko, aby zapewnić jak najwyższy poziom bezpieczeństwa.

I właśnie z tego powodu nie mogę przekazać więcej informacji na ten temat.

Nadchodzą zmiany: Rada Ministrów ma dostosować przepisy dotyczące bezpieczeństwa lotów do standardów unijnych. Dane osób podróżujących między państwami członkowskimi będą mogły być przetwarzane tylko w przypadku wystąpienia zagrożenia terrorystycznego i mają być przechowywane przez trzy lata. To dobry pomysł na poprawę bezpieczeństwa lotów?

W życiu zawsze należy znaleźć złoty środek. Należy wypracować rozwiązania, które zapewnią odpowiedni poziom bezpieczeństwa, a z drugiej strony właściwy poziom wolności i ochrony danych jednostki.

Jeśli uda nam się to osiągnąć, śmiało możemy uznać, że odnieśliśmy sukces.

Dziękuję za rozmowę

GMINA NIE MOŻE PRZYZNAĆ POLICJI STAŁEGO DOSTĘPU DO SWOJEGO MONITORINGU

Jednostki samorządu terytorialnego nie mają podstaw prawnych, by umożliwić policji dostęp do monitoringu miejskiego w drodze teletransmisji, czyli stałego podglądu w czasie rzeczywistym, z możliwością zapisywania i gromadzenia nagrań.

.

Takich wyjaśnień Prezes UODO udzielił jednej z gmin, która z komendą policji zamierzała zawrzeć porozumienie przewidujące przyznanie policji dostępu w czasie rzeczywistym do monitoringu miejskiego prowadzonego przez straż gminną. Policja miała też uzyskać możliwość utrwalania obrazu. Jednocześnie na mocy porozumienia miała się stać odrębnym administratorem. Jako cel takiej współpracy wskazano umożliwienie policji skutecznej realizacji jej zadań.

W piśmie do gminy organ nadzorczy zaznaczył, że w analizie niniejszej sprawy pod uwagę należy brać dwie kluczowe kwestie, jakimi są:

- cel prowadzenia określonych działań i
- podstawa prawna przetwarzania danych osobowych.

Czy monitoring w czasie rzeczywistym to przetwarzanie danych osobowych?

Wyjaśnił, że zgodnie z art. 4 ust. 2 RODO przetwarzaniem jest operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Zatem monitoring wizyjny w czasie rzeczywistym stanowi przetwarzanie danych osobowych.

2 PRAWO I NOWE TECHNOLOGIE

Czy gmina może udostępnić dane z monitoringu?

Udostępnienie danych z monitoringu odrębnemu podmiotowi (zwłaszcza gdy odbywa się w formie stałej teletransmisji) stanowi odrębną operację przetwarzania danych osobowych.

Każda operacja przetwarzania danych osobowych tzw. zwykłych – dla jej legalności – wymaga, aby zaistniała jedna z przesłanek określonych w art. 6 ust. 1 RODO. Te wymienione w lit. a, b i d powołanego przepisu nie mają w tym przypadku zastosowania. Natomiast wyłączenie zawarte w ostatnim zdaniu art. 6 ust.1 RODO przesądza, że lit. f) nie może mieć zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań (zob. również motywy 45 i 47 RODO).

Zatem w przypadku miejskiego monitoringu stosowanego przez organ publiczny, jakim jest jednostka samorządu terytorialnego (w tym przypadku gmina), udostępnienie mogłoby opierać się zasadniczo jedynie na przesłankach określonych w art. 6 ust. 1 lit. c) oraz lit. e) RODO. Przepisy te stanowią, że przetwarzanie danych osobowych jest dopuszczalne jedynie wówczas, gdy jest niezbędne dla wypełnienia obowiązku prawnego ciążącego na administratorze albo gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Co istotne, art. 6 ust. 3 RODO stanowi, że podstawa przetwarzania, które odbywa się na mocy przesłanek wskazanych w art. 6 ust. 1 lit. c) lub e), musi być określona **w przepisach prawa unijnego lub krajowego.**

Powyższe oznacza, że **gmina może udostępnić dane z monitoringu jedynie wówczas, gdy** taką sytuację przewiduje **(zezwala na to) przepis prawa o randze ustawowej**.

Tymczasem **brak jest jakiejkolwiek normy prawnej, która przewidywałaby możliwość stałego udostępniania przez jednostki samorządu terytorialnego lub straż gminną monitoringu miejskiego organom ścigania**.

Prowadzenie monitoringu przez gminę, straż gminną i policję – różne cele i uprawnienia

Na podstawie art. 20 ust. 1–1d ustawy z 6 kwietnia 1990 o Policji, policja jest uprawniona do przetwarzania informacji i danych osobowych **w zakresie niezbędnym** do realizacji swoich zadań, w tym pozyskiwania ich ze zbiorów prowadzonych przez organy władzy publicznej. Organy te z kolei zobowiązane są do nieodpłatnego udostępniania informacji i danych osobowych.

Udostępnianie tych danych co do zasady powinno mieć charakter jednostkowy i wnioskowy, co oznacza, że policja, chcąc pozyskać określone informacje, powinna zwrócić się do organu z formalnym wnioskiem, w którym określony jest zakres żądanych materiałów, **w granicach niezbędnych dla prowadzonej sprawy**, przy jednoczesnym wskazaniu podstawy prawnej pozyskania danych oraz przynajmniej ogólnym określeniu charakteru prowadzonego postępowania.

Artykuł 20 ust. 1e ustawy o Policji określa wyjątek od tej reguły, dopuszczając sytuację, w której dane zgromadzone w zbiorach danych prowadzonych przez organy władzy publicznej mogą być udostępniane policji w drodze teletransmisji (stałego dostępu), ale tylko w przypadku wyrażenia przez ten organ zgody i gdy spełnione zostały łącznie wszystkie określone w powołanym przepisie warunki. Przed wyrażeniem zgody na udzielenie dostępu do zbioru w trybie teletransmisji wykazane musi zostać, że jednostka organizacyjna policji:

1) posiada urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał;
2) posiada zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania;
3) udostępnianie danych w tej formie jest uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności.

Podkreślić należy, że przepis ten odnosi się jedynie do udzielania stałego dostępu do „zbiorów danych" i jedynie w celu pobierania z nich poszczególnych informacji, niezbędnych dla realizacji zadań ustawowych. **Przepis ten nie formułuje zatem zasady prowadzenia przez organy ścigania stałego, systematycznego nadzoru – w ramach współprowadzenia monitoringu miejskiego (gminnego)** – nad procesami zachodzącymi w przestrzeni publicznej i przetwarzania wszelkich danych osobowych, także osób, co do których nie istnieją żadne przesłanki wszczęcia wobec nich określonych postępowań.

Z kolei dla gminy ustawową podstawą do przetwarzania danych z gminnego monitoringu wizyjnego są art. 9a oraz art. 50 ust. 2 ustawy z 8 marca 1990 r. o samorządzie gminnym. Stanowią one, że gmina może stosować monitoring miejsc publicznych w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, a także ochrony mienia komunalnego.

Cele i zakres przetwarzania zostały jasno i konkretnie określone w ustawie i nie mogą być rozszerzane. Jak stanowi jej art. 9a ust. 3, **„nagrania obrazu zawierające dane osobowe przetwarza się wyłącznie do celów, dla których zostały zebrane”**.

Zauważyć w związku z tym należy, że w przypadku udostępnienia materiałów z monitoringu wizyjnego istotne jest wskazanie trybu udostępnienia danych, a jeśli odbywałoby się to w trybie teletransmisji na rzecz policji, to muszą być spełnione warunki wynikające z ww. przepisów prawa. Pamiętać bowiem należy, że w tym przypadku dane z monitoringu byłyby wykorzystywane do celów odmiennych od tych, które wyznacza art. 9a ust. 1 ustawy o samorządzie gminnym.

Jednocześnie podkreślić należy, że stosowanie trybu bezwnioskowego obarczone jest szeregiem ryzyk. Do pozyskiwania danych w trybie bezwnioskowym przez organy władzy publicznej krytycznie odniósł się również Naczelny Sąd Administracyjny w wyroku z 3 grudnia 2021 r. (sygn. akt III OSK 590/21) dotyczącym pozyskiwania danych z rejestru PESEL przez komorników sądowych.

Jednocześnie zauważyć należy, że zgodnie z art. 15 ust. 1 pkt 5a i 5b ustawy o Policji **funkcjonariusze policji mogą dokonywać rejestrowania obrazu zdarzeń w miejscach publicznych wyłącznie w określonych przypadkach**, a więc gdy na podstawie ustawy podejmowane są czynności operacyjno-rozpoznawcze, administracyjno-porządkowe lub kontrterrorystyczne. Możliwość stosowania monitoringu nie dotyczy zatem wszystkich zadań policji określonych w ustawie i **brak jest podstawy prawnej do stosowania przez policję monitoringu stałego o charakterze i zakresie analogicznym do monitoringu gminnego**. Odmienne są bowiem cele takiego monitoringu.

Analogiczne uwagi odnoszą się do sytuacji, gdy monitorowania przestrzeni publicznej dokonuje straż gminna na podstawie art. 11 ust. 2 ustawy z 29 sierpnia 1997 r. o strażach gminnych. Powyższy przepis stanowi, że straży przysługuje prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, ale **jedynie gdy czynności te są niezbędne do wykonywania zadań wyszczególnionych w ustawie**. Zatem zadania, cele, ale i dopuszczalny zakres przetwarzania również w przypadku stosowania monitoringu na podstawie ustawy o strażach gminnych będzie znacząco odmienny od norm wynikających z ustawy o Policji.

Podstawy do przekazywania nagrań monitoringu w trybie stałej transmisji obrazu w czasie rzeczywistym nie może stanowić także art. 9 ust. 5 pkt 6 ustawy o strażach gminnych, określający, że współpraca policji i straży polega m.in. na „wymianie informacji w zakresie obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych”. Przepis ten należy interpretować w sposób ścisły, a więc jako dopuszczający wymianę informacji o stosowanych środkach monitoringu.

Nie może on jednak stanowić podstawy do wymiany treści nagrań, zwłaszcza gdy taka wymiana miałaby przyjmować formę stałego dostępu w czasie rzeczywistym. Tym bardziej że ustawa o Policji nie określa podstaw prawnych dla prowadzenia tego rodzaju monitoringu przez policję, sposobów, w jaki miałby on funkcjonować, czy trybu postępowania z pozyskiwanymi informacjami.

Tryb wnioskowy

Wyraźnie podkreślić należy, że wszystkie powyższe rozważania dotyczą sytuacji, w której udostępnienie nagrań z monitoringu miałoby odbywać się w drodze teletransmisji, a więc stałego podglądu w czasie rzeczywistym, z możliwością zapisywania i gromadzenia nagrań.

Ustawodawca dopuszcza sytuacje, gdy incydentalne przekazywanie organom ścigania fragmentów nagrań z monitoringu jest dopuszczalne, a wręcz stanowi prawny obowiązek administratora.

Szczególne tryby udostępniania danych osobowych organom ścigania zostały ustawowo określone.

Jako przykład można wskazać art. 217 § 1 Kodeksu postępowania karnego, który zobowiązuje do wydania materiałów z monitoringu (nośników) w przypadku, gdy stanowią one dowód w prowadzonym postępowaniu przygotowawczym.

Należy zauważyć, że w takich przypadkach dozwolone jest przekazywanie jedynie fragmentów nagrań z monitoringu, w zakresie niezbędnym dla celów dowodowych prowadzonego postępowania. Takie materiały są przekazywane w trybie wnioskowym, a więc na formalne żądanie organu (np. w formie postanowienia prokuratora), które określa zakres, w jakim materiały mają zostać udostępnione. Zakres ten powinien być ograniczony tylko do materiałów niezbędnych dla merytorycznego rozstrzygnięcia w prowadzonym postępowaniu.

Stanowisko RPO

Rozpatrując powyższe zagadnienie, warto zwrócić uwagę także na stanowisko Rzecznika Praw Obywatelskich wyrażone w związku z wnioskiem o zapewnienie organom ścigania stałego dostępu do monitoringu zainstalowanego w pojazdach komunikacji publicznej. Wskazuje ono na liczne zagrożenia dla chronionych konstytucyjnie praw i wolności obywateli. W znacznej mierze zachowuje ono aktualność również w odniesieniu do niniejszej sprawy.

Określenie statusu administratora

W analizowanym przypadku nie można pominąć jeszcze jednego aspektu – przyznania policji, na podstawie porozumienia z gminą, statusu odrębnego administratora przetwarzającego dane w sposób niezależny.

Podkreślić należy, że zarówno rola administratora, jak i cele oraz zakres przetwarzania nie mogą wynikać z niedookreślonych porozumień, nieposiadających waloru powszechnie obowiązującego prawa. Muszą być określone w przepisach rangi ustawy.

Wynika to nie tylko z przepisów RODO, ale również wprost z norm konstytucyjnych: zasady legalizmu (art. 7), zasady autonomii informacyjnej jednostki (art. 51 ust. 1 i 2), klauzul limitacyjnych dla ograniczenia praw konstytucyjnych, w tym prawa do prywatności (art. 31 ust. 3 i art. 47), jak również z Karty Praw Podstawowych (art. 8 ust. 1 i 2).

DPNT.023.655.2025 + DPNT.023.645.2025

Treść decyzji Prezesa UODO oraz inne orzeczenia można znaleźć na stronie
https://orzeczenia.uodo.gov.pl/

KARA PO KONTROLI W POLSKIM RADIU SZCZECIN

Prezes Urzędu Ochrony Danych Osobowych nałożył na Polskie Radio – Regionalną Rozgłośnię w Szczecinie „PR Szczecin” SA w likwidacji – administracyjną karę ponad 56 tys. zł (decyzja o sygn. DKN.5112.10.2024).

Kara została nałożona za brak odpowiedniego poziomu bezpieczeństwa danych, które powinno być oparte na analizie ryzyka wiążącego się z ich przetwarzaniem, oraz za niedostateczną kontrolę skuteczności zabezpieczeń. Stosowane środki techniczne i organizacyjne były niewystarczające, a ich skuteczność nie była oceniana. Nakazano również dostosowanie operacji przetwarzania do przepisów RODO w terminie 60 dni od dnia doręczenia decyzji administracyjnej.

Chodzi o materiał dziennikarski z 2022 r., w którym przedstawiono sprawę pedofila w taki sposób, że łatwo można było ustalić personalia niepełnoletniej ofiary. Skończyło się to jej samobójstwem.

Była to pierwsza kontrola w środkach masowego przekazu, do których, z uwagi na wyłączenie ustawowe, szereg przepisów RODO nie ma zastosowania. Wyłączenie to dotyczy głównie przepisów regulujących zarówno zasady i podstawy prawne przetwarzania danych osobowych, jak i obowiązki informacyjne wobec osób, których dane są przetwarzane. Nie obejmuje ono natomiast obowiązków administratora nałożonych m.in. art. 24, 29, 32 i 35 RODO, dotyczących wdrożenia polityk i procedur oraz środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzanych danych osobowych odpowiednie do ryzyka wiążącego się z ich przetwarzaniem.

Ustawodawca wprowadzając do działalności dziennikarskiej odstępstwa od stosowania wymogów RODO, nie bez powodu pozostawił obowiązek wdrożenia środków mających zapewnić stopień bezpieczeństwa przetwarzanych danych odpowiedni do ryzyka naruszenia praw lub wolności osób fizycznych.

Zapewnienie zgodnego z prawem i bezpiecznego przetwarzania danych osobowych bohaterów materiałów medialnych jest warunkiem koniecznym do zachowania właściwej równowagi pomiędzy prawem jednostki do ochrony danych osobowych a wolnością wypowiedzi i prawem do informacji. Wymóg zachowania równowagi między ochroną danych osobowych a wolnością wypowiedzi spoczywa na każdym podmiocie medialnym.

4 NARUSZENIA I KONTROLE

W wyniku przeprowadzonych czynności kontrolnych stwierdzono, że Radio Szczecin dopuściło się naruszenia przepisów RODO polegających na:

1) nieprzeprowadzeniu analizy ryzyka dla operacji przetwarzania danych osobowych w związku z prowadzeniem działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych;

2) niestosowaniu się do postanowień „Polityki bezpieczeństwa danych osobowych w Polskim Radiu Szczecin SA" oraz „Instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych w Polskim Radiu Szczecin SA";

3) niewdrożeniu środków bezpieczeństwa danych gwarantujących zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania z uwagi na:

   a) brak jasnych i przejrzystych zasad postępowania z materiałami prasowymi zawierającymi dane osobowe, regulujących obowiązek weryfikacji tych materiałów przed ich publikacją pod kątem zawartych w nich danych osobowych identyfikujących osoby fizyczne, których opublikowanie może naruszać przepisy prawa lub prawa i wolności osób fizycznych;

   b) brak szyfrowania nośników zawierających dane osobowe używanych poza obszarem przetwarzania;

4) niewdrożeniu odpowiednich środków technicznych i organizacyjnych w celu zapewnienia regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo danych osobowych.

Treść decyzji Prezesa UODO oraz inne orzeczenia można znaleźć na stronie
https://orzeczenia.uodo.gov.pl/

UKIERUNKOWANE ZMIANY W RODO: EROD I EIOD Z ZADOWOLENIEM PRZYJMUJĄ UPROSZCZENIE OBOWIĄZKÓW DOT. PROWADZENIA REJESTRÓW I PROSZĄ O DALSZE WYJAŚNIENIA

Propozycja, będąca częścią czwartego pakietu uproszczeń Omnibus, ma na celu uproszczenie przepisów UE i zmniejszenie obciążeń administracyjnych. Rozszerza ona niektóre środki łagodzące dostępne dla małych i średnich przedsiębiorstw (MŚP) na małe przedsiębiorstwa o średniej kapitalizacji (SMC) i zawiera dodatkowe działania upraszczające.

Zmiany w art. 30 ust. 5 RODO

Propozycja zakłada modyfikację art. 30 ust. 5 RODO, wprowadzając odstępstwo od obowiązku prowadzenia rejestru czynności przetwarzania danych. Obecnie odstępstwo to dotyczy tylko przedsiębiorstw i organizacji zatrudniających mniej niż 250 pracowników, z pewnymi wyjątkami. Zgodnie z nową propozycją odstępstwo miałoby dotyczyć podmiotów zatrudniających mniej niż 750 osób, chyba że przetwarzanie danych może prowadzić do wysokiego ryzyka dla praw i wolności osób fizycznych, zgodnie z art. 35 RODO.

Nowe definicje i rozszerzenie zakresu

Propozycja wprowadza definicje MŚP i SMC w art. 4 RODO oraz rozszerza zakres art. 40 ust. 1 i art. 42 ust. 1 RODO na SMC, odnosząc się do kodeksów postępowania i mechanizmów certyfikacji. Narzędzia te mają pomóc przedsiębiorstwom w wykazaniu zgodności z RODO, uwzględniając specyficzne potrzeby MŚP.

Komentarze przedstawicieli instytucji

Wojciech Wiewiórowski, Europejski Inspektor Ochrony Danych, powiedział: „Popieramy ogólny cel propozycji, jakim jest zmniejszenie obciążeń administracyjnych dla MŚP i SMC, pod warunkiem że nie obniży to poziomu ochrony podstawowych praw jednostki, w szczególności prawa do prywatności i ochrony danych osobowych.

5 SPRAWY MIĘDZYNARODOWE

Z zadowoleniem przyjmujemy fakt, że proponowane zmiany są ukierunkowane, ograniczone i nie naruszają podstawowych zasad oraz innych obowiązków wynikających z RODO".

Anu Talus, Przewodnicząca Europejskiej Rady Ochrony Danych, stwierdziła: „EDPB popiera ogólny cel propozycji, jakim jest zmniejszenie obciążeń administracyjnych dla MŚP i SMC oraz zapewnienie, że w praktyce będą one mogły korzystać z odstępstwa od obowiązku prowadzenia rejestrów czynności przetwarzania. Obecne odstępstwo nie zawsze spełniało swoje zadanie. Jednocześnie rejestr czynności przetwarzania jest użytecznym narzędziem wspierającym zgodność z innymi obowiązkami, takimi jak przejrzystość czy realizacja praw osób, których dane dotyczą. Uproszczenie zapewni większą elastyczność MŚP i SMC w wyborze najbardziej odpowiednich metod zgodności".

Potrzeba dalszych wyjaśnień

W odniesieniu do organizacji objętych odstępstwem EDPB i EDPS oczekują dalszych wyjaśnień, dlaczego nowy próg zatrudnienia poniżej 750 osób jest bardziej odpowiedni w kontekście RODO niż pierwotnie rozważany próg 500 pracowników. Ponadto nowe odstępstwo w art. 30 ust. 5 odnosi się do „przedsiębiorstw zatrudniających mniej niż 750 pracowników", nie uwzględniając nowo wprowadzonych definicji MŚP i SMC, które obejmują również kryteria finansowe. Aby zapewnić, że odstępstwo będzie korzystne dla MŚP i SMC, wspólna opinia EROD i EIOD zaleca odniesienie się do tych definicji.

Wyłączenie organów publicznych

EROD i EIOD apelują również do współprawodawców o doprecyzowanie w propozycji, że termin „organizacja", objęty zakresem proponowanego odstępstwa w art. 30 ust. 5 RODO, nie obejmuje organów i instytucji publicznych.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

Targeted modifications of the GDPR: EDPB & EDPS welcome simplification of record keeping obligations and request further clarifications | European Data Protection Board

OŚWIADCZENIE HELSIŃSKIE WS. WIĘKSZEJ PRZEJRZYSTOŚCI, WSPARCIA I ZAANGAŻOWANIA

Podejście oparte na prawach podstawowych do innowacji i konkurencyjności

Podczas spotkania wysokiego szczebla w Helsinkach 1–2 lipca 2025 r. Europejska Rada Ochrony Danych przyjęła przełomowe Oświadczenie dotyczące zwiększenia przejrzystości, wsparcia i zaangażowania.

Oświadczenie przedstawia nowe inicjatywy mające na celu ułatwienie zgodności z RODO, szczególnie dla mikro-, małych i średnich organizacji, wzmocnienie spójności oraz zwiększenie współpracy między organami regulacyjnymi.

Przewodnicząca EROD, Anu Talus, powiedziała: „Celem EROD jest zapewnienie, że zgodność z RODO będzie łatwiejsza do osiągnięcia. Umieszczając prawa podstawowe w centrum transformacji cyfrowej, organizacje mogą zagwarantować, że postęp technologiczny idzie w parze z poszanowaniem europejskich wartości, co w efekcie buduje silniejszą i bardziej odporną gospodarkę cyfrową”.

Dialog i konsultacje publiczne

EROD zamierza zacieśnić dialog z interesariuszami, prowadząc proaktywne i wczesne działania mające na celu identyfikację obszarów wymagających dodatkowego wsparcia i wyjaśnień. Interesariusze będą mieli możliwość zgłaszania niejasności i przekazywania opinii. EDPB będzie publicznie raportować główne wyniki konsultacji społecznych.

Nowe zasoby praktyczne

EROD uruchomi serię bezpośrednich i praktycznych narzędzi upraszczających stosowanie RODO.

Anu Talus dodała: „EROD zobowiązuje się do wspierania organizacji w osiąganiu zgodności z RODO w sposób łatwiejszy i bardziej efektywny. Dzięki terminowym i zwięzłym wytycznym oraz gotowym do użycia narzędziom, takim jak wspólny szablon zgłoszenia naruszenia danych, listy kontrolne, instrukcje i odpowiedzi na najczęściej zadawane pytania, będziemy nadal czynić zgodność z RODO osiągalną i dostępną dla wszystkich”.

5 SPRAWY MIĘDZYNARODOWE

Spójność i współpraca między organami

Wśród uzgodnionych działań mających na celu zapewnienie spójnej interpretacji i egzekwowania RODO w całej Europie członkowie EROD będą nieustannie dążyć do ujednolicenia krajowych i europejskich wytycznych. Opracują również wspólne praktyki, metody, narzędzia oraz wytyczne dotyczące przeglądu działań, aby zapewnić ich skuteczność w praktyce. EROD będzie publikować stanowiska organów ochrony danych w sprawach priorytetowych, aby pomóc organizacjom zrozumieć i spełniać oczekiwania regulacyjne.

Współpraca międzysektorowa

EROD dostrzega rosnącą złożoność cyfrowego krajobrazu regulacyjnego i ponownie zobowiązuje się do wspierania strukturalnej współpracy z organami regulacyjnymi spoza obszaru ochrony danych, aby stawić czoła wyzwaniom prawnym i praktycznym w sprawach międzysektorowych.

Źródło:

Komunikat Europejskiej Rady Ochrony Danych

The Helsinki Statement on enhanced clarity, support and engagement | European Data Protection Board

IRLANDZKA KOMISJA OCHRONY DANYCH OGŁASZA ZAKOŃCZENIE DOCHODZENIA WS. WYKORZYSTANIA TECHNOLOGII DOPASOWYWANIA TWARZY W ZWIĄZKU Z KARTĄ USŁUG PUBLICZNYCH PRZEZ DEPARTAMENT OCHRONY SPOŁECZNEJ

Irlandzka Komisja Ochrony Danych (DPC) ogłosiła swoją ostateczną decyzję po zakończeniu dochodzenia dotyczącego Departamentu Ochrony Społecznej (DSP). Dochodzenie, rozpoczęte w lipcu 2021 r., dotyczyło przetwarzania przez DSP biometrycznych szablonów twarzy oraz wykorzystania powiązanych technologii dopasowywania twarzy w ramach procesu rejestracji do Karty Usług Publicznych, znanego jako „rejestracja SAFE 2".

Tło sprawy

Dochodzenie to było kontynuacją wcześniejszego postępowania prowadzonego przez DPC w sprawie niektórych aspektów przetwarzania danych osobowych przez DSP w związku z wydawaniem Kart Usług Publicznych, które zakończyło się w 2019 r. DSP początkowo złożył apelację od decyzji DPC do Sądu Okręgowego, jednak została ona ostatecznie wycofana, a wspólne porozumienie między DPC a DSP oraz końcowy raport z tamtego dochodzenia zostały opublikowane w grudniu 2021 r.

W raporcie tym wskazano, że przetwarzanie danych osobowych, w tym danych biometrycznych, przez DSP w ramach rejestracji SAFE 2 miało zostać rozpatrzone osobno przez DPC. Dzisiejsza decyzja jest wynikiem tego odrębnego dochodzenia.

Uzasadnienie dochodzenia

Rejestracja SAFE 2 jest obowiązkowa dla każdej osoby ubiegającej się o Kartę Usług Publicznych. Osoby, które nie poddadzą się temu procesowi, nie mają dostępu do usług DSP, w tym świadczeń socjalnych. Wdrożenie SAFE 2 doprowadziło do masowego gromadzenia, przechowywania i przetwarzania danych osobowych o wysokim stopniu wrażliwości, w tym danych biometrycznych w postaci szablonów twarzy.

5 SPRAWY MIĘDZYNARODOWE

Zgodnie z RODO dane biometryczne są kategorią szczególną, wymagającą wyższych standardów ochrony. W 2021 r. DSP posiadał biometryczne szablony twarzy dotyczące 70 proc. populacji kraju.

Technologia dopasowywania twarzy wykorzystywana przez DSP wiąże się z tworzeniem danych biometrycznych dotyczących znacznej części społeczeństwa. Skala i inwazyjność tego przetwarzania wymagają precyzyjnego uzasadnienia prawnego. Zgodnie z orzecznictwem europejskim konieczne jest, aby przepisy były precyzyjne i przewidywalne, tak żeby chronić przed arbitralną ingerencją w prawa jednostki.

W związku z powyższym rejestracja SAFE 2 musi się opierać na jasnych i precyzyjnych podstawach prawnych, które określają konkretne zasady i zabezpieczenia dotyczące charakteru oraz sposobu przetwarzania danych biometrycznych niezależnie od celów polityki publicznej i korzyści, jakie ma przynieść.

Zakres dochodzenia

Dochodzenie obejmowało analizę następujących kwestii:

- Czy DSP posiadał podstawę prawną do zbierania danych biometrycznych w celu dopasowywania twarzy w ramach rejestracji SAFE 2;
- Czy DSP posiadał podstawę prawną do przechowywania danych biometrycznych zebranych w ramach rejestracji SAFE 2;
- Czy DSP spełnił obowiązki informacyjne wobec osób poddających się rejestracji SAFE 2;
- Czy DSP przeprowadził odpowiednią ocenę skutków dla ochrony danych (DPIA) w ramach rejestracji SAFE 2.

Ustalenia

Decyzja DPC, wydana przez komisarza Dale'a Sunderlanda i przekazana DSP w tym tygodniu, stwierdza, że DSP:

- Naruszył art. 5 ust. 1 lit. a, art. 6 ust. 1 oraz art. 9 ust. 1 RODO, nie wskazując ważnej podstawy prawnej dla zbierania danych biometrycznych w ramach rejestracji SAFE 2;
- W związku z powyższym naruszył art. 5 ust. 1 lit. e RODO, przechowując dane biometryczne zebrane w ramach rejestracji SAFE 2;

- Naruszył art. 13 ust. 1 lit. c oraz art. 13 ust. 2 lit. a RODO, nie zapewniając wystarczająco przejrzystych informacji dla osób rejestrujących się w SAFE 2;
- Naruszył art. 35 ust. 7 lit. b i c RODO, nie uwzględniając określonych informacji w ocenie skutków dla ochrony danych dotyczącej rejestracji SAFE 2.

Środki naprawcze

W związku z powyższymi naruszeniami DPC udzielił DSP upomnienia, nałożył administracyjne kary finansowe w łącznej wysokości 550 tys. euro oraz wydał nakaz zaprzestania przetwarzania danych biometrycznych w ramach rejestracji SAFE 2 w ciągu dziewięciu miesięcy od daty decyzji, jeśli DSP nie wskaże ważnej podstawy prawnej.

Komentarz zastępcy komisarza Grahama Doyle'a:

„Warto podkreślić, że żadne z ustaleń dotyczących naruszeń ani zastosowane środki naprawcze nie odnoszą się do samego wdrożenia rejestracji SAFE 2 jako zasady. DPC nie stwierdziła żadnych uchybień w zakresie technicznych i organizacyjnych środków bezpieczeństwa zastosowanych przez DSP w związku z rejestracją SAFE 2 w ramach tego dochodzenia.

Celem dochodzenia było ustalenie, czy obecne ramy legislacyjne dla rejestracji SAFE 2 są zgodne z przepisami o ochronie danych oraz czy DSP prowadzi rejestrację SAFE 2 w sposób zgodny z RODO. Ogłoszone ustalenia wskazują na szereg niedociągnięć w tym zakresie".

Źródło:

Komunikat Irlandzkiego Organu Ochrony Danych

DPC announces conclusion of investigation into use of facial matching technology in connection with the Public Services Card by the Department of Social Protection | 12/06/2025 | Data Protection Commission

KARA ADMINISTRACYJNA DLA RZECZNIKA DS. RÓWNOŚCI ZA ZBIERANIE DANYCH OSOBOWYCH ZA POMOCĄ FORMULARZA INTERNETOWEGO

Szwedzki Urząd Ochrony Prywatności (IMY) przeprowadził kontrolę incydentu związanego z danymi osobowymi w Biurze Rzecznika ds. Równości. IMY stwierdził, że Biuro nie zastosowało wystarczająco skutecznych środków bezpieczeństwa, i nałożył karę administracyjną w wysokości 100 tys. koron szwedzkich.

Powodem kontroli było naruszenie ochrony danych osobowych, które Biuro zgłosiło do IMY jesienią 2021 r. Incydent dotyczył formularza internetowego służącego do zbierania zgłoszeń i skarg dotyczących dyskryminacji. W trakcie kontroli ujawniono, że wdrożono środek bezpieczeństwa mający na celu ochronę danych osobowych zbieranych za pomocą formularza, tak aby nie były one uwzględniane w analizach użytkowania strony internetowej.

Jednakże środek ten nie zadziałał zgodnie z założeniami, co doprowadziło do przypadkowego ujawnienia części danych, potencjalnie wrażliwych danych osobowych, podmiotowi przetwarzającemu dane, zatrudnionemu przez Biuro do przeprowadzenia analiz. Szacuje się, że incydent dotyczył ok. 500 zgłoszeń i skarg.

Gdy tylko dowiedziano się o incydencie, formularz internetowy został zamknięty.

„Incydent trwał rok i pokazuje, jak ważne jest ciągłe i systematyczne podejście do kwestii bezpieczeństwa, aby móc wcześniej wykrywać niewystarczające środki ochrony” – powiedział Petter Flink, specjalista ds. IT i bezpieczeństwa informacji w IMY.

Źródło:

Komunikat Szwedzkiego Organu Ochrony Danych
Administrative fine against the Equality Ombudsman when personal data was collection via a web form | IMY

PLIKI COOKIES UMIESZCZANE BEZ ZGODY: SHEIN UKARANY KARĄ ADMINISTRACYJNĄ W WYSOKOŚCI 150 MLN EURO PRZEZ CNIL

1 września 2025 r. francuski organ ochrony danych osobowych CNIL nałożył karę administracyjną w wysokości 150 mln euro na INFINITE STYLES SERVICES CO. LIMITED, irlandzką spółkę zależną grupy SHEIN, za naruszenie przepisów dotyczących plików cookies umieszczanych na urządzeniach użytkowników odwiedzających stronę „shein.com".

Informacje ogólne

Grupa SHEIN sprzedaje odzież, obuwie i akcesoria za pośrednictwem strony internetowej „shein.com", którą na terenie Europy zarządza INFINITE STYLES SERVICES CO. LIMITED z siedzibą w Irlandii.

W sierpniu 2023 r. CNIL przeprowadził kontrolę strony „shein.com". Na podstawie ustaleń organ CNIL odpowiedzialny za nakładanie sankcji uznał, że INFINITE STYLES SERVICES CO. LIMITED naruszyła obowiązki wynikające z przepisów dotyczących plików cookies (art. 82 francuskiej ustawy o ochronie danych osobowych) i nałożyła na firmę karę administracyjną w wysokości 150 mln euro.

Wysokość kary uwzględniała fakt, że firma nie spełniła kilku obowiązków: umieszczała pliki cookies bez zgody użytkowników, nie respektowała ich wyborów ani nie informowała ich w sposób właściwy. Organ przypomniał, że od 2020 r. wielokrotnie karał organizacje za podobne naruszenia i publikował swoje decyzje. Uwzględniono również ogromną skalę przetwarzania danych, strona „shein.com" odwiedzana jest miesięcznie przez średnio 12 mln mieszkańców Francji.

Naruszenia objęte sankcją

Organ ukarał firmę za kilka praktyk sprzecznych z francuską ustawą o ochronie danych osobowych (art. 82):

- **Brak uzyskania zgody użytkowników przed umieszczeniem plików cookies**: CNIL stwierdził, że kilka plików cookies, szczególnie o charakterze reklamowym, było umieszczanych na urządzeniach użytkowników już w momencie wejścia na stronę, zanim zdążyli oni wyrazić zgodę poprzez baner informacyjny.

- **Dwa niekompletne banery informacyjne**: na stronie „shein.com” wyświetlane były dwa interfejsy do zarządzania plikami cookies, ale oba były niepełne. Pierwszy baner zawierał trzy przyciski: „Ustawienia cookies”, „Odrzuć wszystkie” i „Akceptuj”, ale nie zawierał informacji o reklamowym celu plików cookies. Drugi wyskakujący baner zawierał jedynie przycisk akceptacji, również bez informacji o celu.
- **Niewystarczające informacje drugiego poziomu**: po kliknięciu przycisku „Ustawienia cookies” nie udostępniano informacji o tożsamości podmiotów trzecich, które mogłyby umieszczać pliki cookies.
- **Nieskuteczne mechanizmy odmowy i wycofania zgody**: po kliknięciu „Odrzuć wszystkie” lub wycofaniu zgody na zapis plików cookies nowe pliki nadal były umieszczane, a już istniejące nadal odczytywane.

W toku postępowania organ zauważył, że firma wprowadziła zmiany na stronie internetowej, dlatego nie było konieczności wydania nakazu dostosowania.

Źródło:

Komunikat Francuskiego Organu Ochrony Danych
Cookies placed without consent: SHEIN fined 150 million euros by the CNIL | CNIL

POLSKA AKTYWNIE UCZESTNICZY W DEBACIE O PRZYSZŁOŚCI PRYWATNOŚCI – RELACJA Z 47. GLOBAL PRIVACY ASSEMBLY W SEULU

W dniach 15–19 września 2025 r. w Seulu odbyła się 47. edycja Global Privacy Assembly (GPA) – międzynarodowego forum poświęconego ochronie danych osobowych i prywatności. Tegoroczne wydarzenie, zorganizowane przez koreański organ PIPC, zgromadziło ponad 140 organów nadzorczych z całego świata, a jego głównym tematem była sztuczna inteligencja w codziennym życiu, jej wpływ na prywatność, społeczeństwo i gospodarkę.

Polskę reprezentowali prezes UODO Mirosław Wróblewski oraz Dyrektorka Departamentu Współpracy Międzynarodowej Maria Owczarek. Udział delegacji UODO był nie tylko okazją do wymiany doświadczeń, lecz także do aktywnego współtworzenia globalnych standardów ochrony danych.

Sztuczna inteligencja a prywatność – wspólne zobowiązanie organów nadzorczych

Jednym z kluczowych punktów programu GPA 2025 była ceremonia podpisania „Wspólnego oświadczenia w sprawie budowania wiarygodnych ram zarządzania danymi w celu wspierania rozwoju innowacyjnej i chroniącej prywatność sztucznej inteligencji". Dokument ten, zainicjowany przez CNIL i DPC, został podpisany przez kolejne organy nadzorcze, tym Polskę, jako wyraz wspólnego zaangażowania w tworzenie bezpiecznych i transparentnych rozwiązań AI.

Oświadczenie zakłada m.in.:

- wypracowanie jasnych standardów dla rozwoju AI z poszanowaniem prywatności,
- wymianę informacji i dobrych praktyk między regulatorami,
- monitorowanie wpływu AI na społeczeństwo i gospodarkę,
- przeciwdziałanie zagrożeniom takim jak dyskryminacja, stronniczość czy dezinformacja.

5 SPRAWY MIĘDZYNARODOWE

Prezes UODO podkreślił, że „prawo najczęściej zostaje w tyle za rozwojem technologii, jednak naszym zadaniem jest robienie wszystkiego, żeby tę lukę możliwie zmniejszyć, by skutecznie chronić prawa podstawowe, umożliwiając jednocześnie tworzenie innowacji potrzebnych ludzkości”.

Edukacja jako filar ochrony danych – międzynarodowe uznanie dla polskiej inicjatywy

Podczas GPA 2025 ogłoszono również laureatów konkursu Global Privacy and Data Protection Awards. UODO otrzymał wyróżnienie w kategorii „Education and Awareness” za projekt „Wizerunek dziecka w internecie. Publikować czy nie?”, zrealizowany wspólnie z Fundacją Orange. Publikacja ta, skierowana do rodziców, nauczycieli i instytucji pracujących z dziećmi, zwraca uwagę na ryzyka związane z udostępnianiem wizerunku najmłodszych w sieci i promuje odpowiedzialne podejście do prywatności dzieci.

Wyróżnienie to potwierdza, że działania edukacyjne UODO mają znaczenie nie tylko lokalne, lecz także globalne, wpisując się w szerszy nurt refleksji nad prawami dzieci w cyfrowym świecie.

Merytoryczne debaty i wspólne kierunki działań

Program konferencji obejmował szereg paneli eksperckich, sesji plenarnych i warsztatów, w których poruszano m.in.:

- wyzwania związane z reklamą ukierunkowaną i profilowaniem użytkowników,
- rozwój technologii PETs (Privacy-Enhancing Technologies),
- ochronę prywatności młodzieży w środowisku cyfrowym,
- transgraniczne transfery danych i interoperacyjność regulacji.

Wspólnym mianownikiem wszystkich dyskusji była potrzeba budowania zaufania społecznego do technologii oraz rola organów nadzorczych jako strażników praw podstawowych w erze cyfrowej.

Udział UODO w GPA 2025 oraz podpisanie międzynarodowego oświadczenia pokazują, że Polska nie tylko śledzi światowe trendy, ale także aktywnie uczestniczy w ich kształtowaniu. Dzięki takim inicjatywom jak projekt edukacyjny o wizerunku dziecka czy zaangażowanie w rozwój etycznej AI UODO wnosi istotny wkład w debatę o przyszłości prywatności.

5 SPRAWY MIĘDZYNARODOWE

UE-USA: WZMOCNIONE PARTNERSTWO NA RZECZ BEZPIECZEŃSTWA GRANIC

23 lipca 2025 r. Komisja Europejska wydała zalecenie dotyczące decyzji Rady upoważniającej do rozpoczęcia negocjacji w sprawie umowy ramowej między Unią Europejską a Stanami Zjednoczonymi w zakresie wymiany informacji na potrzeby kontroli bezpieczeństwa i weryfikacji tożsamości w odniesieniu do procedur granicznych i wniosków wizowych.

Założeniem zalecenia jest dostarczenie wytycznych negocjacyjnych Komisji Europejskiej w celu wynegocjowania umowy ramowej, która określi strukturę prawną i warunki wymiany informacji między właściwymi organami państw członkowskich UE i USA. Na tej podstawie państwa członkowskie będą mogły zawierać dwustronne umowy o wymianie danych z ich krajowych systemów informacyjnych.

Zalecenie jest powiązane z wymogiem dotyczącym uczestnictwa w amerykańskim programie bezwizowym, który umożliwia obywatelom krajów uczestniczących podróżowanie do USA bez wiz przez maksymalnie 90 dni w celach turystycznych lub biznesowych. Nowy wymóg wiąże się z zawarciem „wzmocnionego partnerstwa na rzecz bezpieczeństwa granic" (EBSP) z Departamentem Bezpieczeństwa Wewnętrznego USA. Zawarcie EBSP jest warunkiem przyjęcia i dalszego uczestnictwa w amerykańskim programie bezwizowym i dotyczy państw członkowskich korzystających ze statusu bezwizowego lub zamierzających przystąpić do programu.

Proponowana umowa ramowa różni się od istniejących umów UE z państwami trzecimi, takich jak umowy dotyczące danych pasażerów (PNR), które ograniczają wymianę danych do organów ścigania i wymiaru sprawiedliwości w sprawach karnych. W przeciwieństwie do nich planowana umowa ramowa zakładałaby udostępnianie na dużą skalę danych osobowych, w tym danych biometrycznych, do celów kontroli granicznej i imigracyjnej przez państwo trzecie, co stanowiłoby istotny precedens.

Zalecenie wskazuje, że cele przekazywania i przetwarzania danych obejmują:

1. Kontrolę i weryfikację tożsamości podróżnych w celu ustalenia, czy ich wjazd lub pobyt stanowi zagrożenie dla bezpieczeństwa publicznego lub porządku publicznego.
2. Wsparcie właściwych organów w zapobieganiu przestępstwom i przestępstwom terrorystycznym, ich wykrywaniu, prowadzeniu dochodzeń i ściganiu sprawców.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Departament Bezpieczeństwa Wewnętrznego USA w 2024 r. opublikował dokument „Aktualizacja oceny wpływu na prywatność – Program DHS dotyczący międzynarodowej wymiany informacji", w którym wskazuje cele dwustronnej wymiany danych biometrycznych w ramach EBSP, obejmujące m.in.: bezpieczeństwo granic, podejmowanie decyzji imigracyjnych, działania organów ścigania, zwalczanie przestępczości międzynarodowej, wykrywanie terroryzmu oraz zapobieganie przestępstwom zagrażającym bezpieczeństwu USA.

Przekazywanie danych osobowych w tym celu, choć może znacząco ingerować w prawa podstawowe osób, może być właściwie uzasadnione powagą interesu publicznego, w tym ochroną życia i bezpieczeństwa, i wchodzi w zakres planowanej umowy ramowej oraz przewidzianych w niej zabezpieczeń.

Znaczenie takich środków podkreśla również kontekst polityki migracyjnej UE – niedawno przyjęty pakiet przepisów regulujących migrację oraz nowe wielkoskalowe systemy informatyczne UE, takie jak ETIAS i EES, pokazują strategiczną rolę zarządzania granicami i migracją dla Unii.

W związku z opracowaniem projektu mandatu negocjacyjnego Europejski Inspektor Ochrony Danych wydał opinię – do zapoznania się z nią UODO serdecznie zachęca. Polski organ nadzorczy w pełni popiera stanowisko EIOD i podkreśla potrzebę ścisłego przestrzegania zasady konieczności i proporcjonalności przetwarzania danych, wąskiego i wyczerpującego określenia zakresu osobowego oraz kategorii danych, wyłączenia dostępu do wielkoskalowych systemów informatycznych UE oraz zapewnienia skutecznych mechanizmów nadzoru i egzekwowalnych praw osób, których dane dotyczą.

EURODAC – WYZWANIA DLA OCHRONY DANYCH

Eurodac to unijny system informacyjny służący do porównywania odcisków palców osób ubiegających się o ochronę międzynarodową. Jego funkcjonowanie ma kluczowe znaczenie dla stosowania tzw. rozporządzenia dublińskiego, które określa państwo członkowskie odpowiedzialne za rozpatrzenie wniosku o ochronę międzynarodową.

System działa od 2003 r., a obecnie korzystają z niego wszystkie państwa członkowskie UE oraz Islandia, Liechtenstein, Norwegia i Szwajcaria. Zarządzanie operacyjne sprawuje agencja eu-LISA, natomiast nadzór nad przestrzeganiem zasad ochrony danych odbywa się dwutorowo – na szczeblu krajowym przez krajowe organy ochrony danych, a na szczeblu centralnym przez Europejskiego Inspektora Ochrony Danych (EIOD). Współpraca między tymi organami jest koordynowana w ramach Grupy ds. Koordynacji Nadzoru Eurodac (SCG Eurodac).

Ewolucja regulacji prawnych

Pierwsze przepisy dotyczące Eurodac przyjęto w 2000 r. Od tego czasu system był kilkukrotnie reformowany. Najnowsze rozporządzenie (UE) 2024/1358 zostało przyjęte przez Parlament Europejski i Radę w maju 2024 r. i zacznie obowiązywać od 12 czerwca 2026 r. (z pewnymi wyjątkami).

Nowe regulacje przewidują m.in.:

- obniżenie wieku pobierania odcisków palców do 6 lat,
- gromadzenie wizerunków twarzy,
- rejestrowanie decyzji o wydaleniu, relokacji czy powrocie,
- możliwość oznaczania osób potencjalnie stwarzających zagrożenie dla bezpieczeństwa,
- dodatkowe dane statystyczne dotyczące osób sprowadzonych na ląd w wyniku operacji poszukiwawczo-ratowniczych.

Zmiany te budzą szczególne wyzwania w zakresie poszanowania praw podstawowych, zwłaszcza ochrony danych osób małoletnich i osób znajdujących się w sytuacjach wrażliwych.

5 SPRAWY MIĘDZYNARODOWE/ SCHENGEN

Koordynowany nadzór nad Eurodac

SCG Eurodac, złożona z przedstawicieli krajowych organów ochrony danych i EIOD, spotyka się regularnie, aby omawiać bieżące wyzwania. Podczas ostatnich posiedzeń dyskutowano m.in. o:

- konieczności wprowadzenia wspólnego wzoru raportowania wyników krajowych kontroli,
- zasadach dostępu organów ścigania do danych Eurodac,
- problemie fałszywych trafień w systemie,
- wpływie projektowanych zmian legislacyjnych na praktykę nadzoru.

W tym okresie przyjęto również program prac obejmujący monitorowanie procesu legislacyjnego, analizę praktyk stosowania dostępu przez organy ścigania oraz wymianę doświadczeń między organami nadzorczymi.

Wyzwania na przyszłość

Od 2026 r. nowy system Eurodac będzie stanowił jedno z głównych narzędzi unijnej polityki migracyjnej i azylowej. Równocześnie zwiększony zakres danych, w tym biometrycznych, będzie wymagać szczególnie wnikliwego nadzoru ze strony organów ochrony danych. Kluczowe będzie zapewnienie równowagi między skutecznością działań państw w obszarze migracji a poszanowaniem praw podstawowych, w szczególności prawa do prywatności i ochrony danych osobowych.

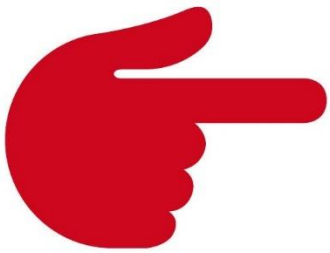
Prezes UODO zaprasza na wydarzenia edukacyjne, zaplanowane na ostatni kwartał 2025 r. Wszystkie będzie można obejrzeć on-line. Będą dotyczyć szerokiego spektrum tematów, tak aby każdy znalazł coś ciekawego dla siebie. Serdecznie zapraszamy.

- **Seminarium „Rewolucja technologiczna w relacji z klientami. Jak budować rozwiązania technologiczne zgodne z zasadami ochrony danych osobowych"**

Termin: **2 października** 2025 r., godz. 10:00–14:30

Miejsce: **Uniwersytet Rzeszowski**, budynek A1 przy al. Rejtana 16C, Aula im. Stanisława Zająca

Organizatorzy: Urząd Ochrony Danych Osobowych oraz Zakład Ubezpieczeń Społecznych
Formuła: hybrydowa



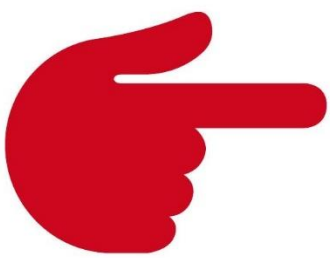
W programie przewidziano trzy panele dyskusyjne z udziałem m.in. przedstawicieli kluczowych departamentów ZUS, UODO oraz Społecznego Zespołu Ekspertów przy Prezesie UODO, specjalistów z zakresu cyberbezpieczeństwa i sztucznej inteligencji, prawników i menedżerów.
Seminarium będzie poświęcone współczesnym wyzwaniom w relacjach z klientami, będzie łączyło tematykę personalizacji i ochrony prywatności.

- **Konferencja „Bezpieczne dane dzieci i młodzieży oraz nowe kierunki rozwoju w obszarze kultury fizycznej. Jak sprostać współczesnym wyzwaniom?"**

Termin: **10 października** 2025 r., godz. 9:00–17:00

Miejsce: **Akademia Kultury Fizycznej** im. Bronisława Czecha w Krakowie, al. Jana Pawła II 78

Organizatorzy: Urząd Ochrony Danych Osobowych, Krakowski Szkolny Ośrodek Sportowy, AKF im. Bronisława Czecha, Urząd Miasta Kraków
Formuła: hybrydowa



Konferencja szkoleniowo-metodyczna będzie skierowana do przedstawicieli jednostek realizujących działalność sportową na terenie Gminy Miejskiej Kraków, a także do nauczycieli wychowania fizycznego oraz instruktorów zajęć sportowych z dziećmi i młodzieżą.
Konferencja będzie się składać z sesji tematycznych, podczas których zostanie zaprezentowana aktywność KSOS w obszarze działalności dydaktycznej i sportowo-rekreacyjnej oraz podsumowanie dotychczasowych osiągnięć Ośrodka; przedstawione również zostaną wyzwania stojące przed działaczami i organizatorami imprez sportowych w zakresie ochrony prywatności i danych osobowych młodych sportowców.

• Konferencja „Prywatność i sztuczna inteligencja w edukacji”

Termin: **22–23 października 2025 r.**, godz. 10:00–15:00

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

Organizatorzy: Urząd Ochrony Danych Osobowych
Formuła: hybrydowa

Konferencja zainauguruje XVI edycję ogólnopolskiego programu edukacyjnego Prezesa UODO „Twoje dane – Twoja sprawa”, adresowanego do szkół podstawowych i ponadpodstawowych. Program ten jest jednym z kluczowych działań edukacyjnych Urzędu i wspiera placówki oświatowe w kształtowaniu świadomego i odpowiedzialnego podejścia uczniów do ochrony danych osobowych oraz prywatności w środowisku cyfrowym. Tematyka tegorocznego spotkania koncentruje się na wyzwaniach wynikających z dynamicznego rozwoju sztucznej inteligencji oraz na jej wpływie na procesy edukacyjne – ze szczególnym uwzględnieniem kwestii ochrony danych osobowych dzieci.

• Konferencja „Komentarz do Rozporządzenia ws. Europejskiego Zarządzania Danymi”

Termin: **24 października** 2025 r.

Miejsce: **on-line**

Organizatorzy: Urząd Ochrony Danych Osobowych, Społeczny Zespół Ekspertów przy Prezesie UODO
Formuła: on-line

Akt w sprawie zarządzania danymi (Data Governance Act – DGA) to przełomowa regulacja, która stanowi podstawę strategii Unii Europejskiej dotyczącej tworzenia jednolitego rynku danych. Jej celem jest zwiększenie dostępności danych, jak również ułatwienie ich ponownego wykorzystywania przy jednoczesnym zapewnieniu wysokiego poziomu zaufania i ochrony danych osobowych oraz tajemnic handlowych. W trakcie konferencji będzie można wysłuchać komentarzy ekspertów z zakresu prawa ochrony danych, nowych technologii i prawa europejskiego do przepisów DGA w kontekście ułatwienia ich bezpośredniego stosowania w polskim porządku prawnym.

URZĄD OCHRONY DANYCH OSOBOWYCH

- **Seminarium „Postępowania cywilne w zakresie ochrony danych osobowych. Sądy powszechne i Prezes UODO jako gwaranci spójności stosowania RODO”**

Termin: **6 listopada** 2025 r., godz. 10:00–15:00

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

Organizatorzy: Urząd Ochrony Danych Osobowych, Stowarzyszenie Sędziów Polskich „Iustitia” oraz Naczelna Rada Adwokacka
Formuła: hybrydowa

Seminarium będzie poświęcone kluczowym zagadnieniom dotyczącym praw osób, których dane dotyczą w postępowaniach cywilnych – od prawa do odszkodowania i odpowiedzialności wynikających z art. 82 RODO po współpracę Prezesa UODO z sądami w tym obszarze. Wydarzenie ukaże również działania pełnomocników w tym zakresie, będące wsparciem dla skutecznej ochrony praw jednostek, a także budowania zaufania obywateli do systemu ochrony danych osobowych.

- **Konferencja „Dane osobowe na antenie – standardy i granice ochrony prywatności w mediach”**

Termin: **19 listopada** 2025 r., godz. 10:00–14:30

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

Organizatorzy: Urząd Ochrony Danych Osobowych oraz Społeczny Zespół Ekspertów przy Prezesie UODO
Formuła: hybrydowa

W programie zostały przewidziane trzy panele dyskusyjne z udziałem ekspertów prawa prasowego, przedstawicieli mediów, praktyków ochrony danych oraz reprezentantów instytucji nadzorczych; poruszone zostaną kwestie dotyczące misji mediów w kontekście prawa do prywatności, granic ujawniania tożsamości w materiałach prasowych czy sposobów ochrony danych osobowych przez media.
Celem konferencji jest stworzenie przestrzeni do dialogu i wypracowania wspólnych standardów działania, które będą zgodne nie tylko z obowiązującym prawem, ale przede wszystkim będą służyć etycznemu i odpowiedzialnemu dziennikarstwu. Chcemy podkreślić, że mimo iż przepisy ogólnego rozporządzenia o ochronie danych (RODO) przewidują wyjątki dla działalności dziennikarskiej, nie zwalnia to przedstawicieli mediów z obowiązku stosowania odpowiednich środków ochrony danych – zarówno na gruncie prawa prasowego, jak i ogólnych przepisów o ochronie danych osobowych, co pozwoli chronić dane wrażliwe, zapobiegać nadużyciom oraz budować zaufanie odbiorców.

URZĄD OCHRONY DANYCH OSOBOWYCH

- **Konferencja „Biometria pod nadzorem: prawo, etyka i technologia w ochronie danych osobowych" (tytuł niepotwierdzony)**

Termin: **26 listopada** 2025 r., godz. 10:00–16:00

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

Organizatorzy: Urząd Ochrony Danych Osobowych, Fundacja AIoneHealth
Formuła: hybrydowa

Oblicza biometrii, jej dotychczasowe osiągnięcia i perspektywy rozwoju, a także prawne aspekty jej wykorzystania – to główne tematy tego wydarzenia. Eksperci przedstawią uczestnikom możliwości i korzyści, jakie niesie z sobą wdrożenie oraz stosowanie technologii biometrycznych, oraz przykłady wdrożeń rozwiązań biometrycznych. Skuteczne zarządzanie danymi biometrycznymi wymaga bowiem równowagi między innowacjami a ochroną prywatności, co oznacza ich ochronę przed nieautoryzowanym dostępem i konieczność określenia wyraźnego celu.

- **Konferencja „Nowe wyzwania prawne: regulacje, zadania regulatorów i ochrona danych w 2025 roku"**

Termin: **27 listopada** 2027 r., godz. 10:00–14:30

Miejsce: **Centrala ZUS** przy ul. Szamockiej 3/5, Warszawa

Organizatorzy: Urząd Ochrony Danych Osobowych oraz Zakład Ubezpieczeń Społecznych
Formuła: hybrydowa

Konferencja obejmie tematykę nowych regulacji prawnych, które zaczęły obowiązywać w 2025 r., ze szczególnym uwzględnieniem roli instytucji, które uczestniczą w ich wdrażaniu. Paneliści zabiorą głos ws. odpowiedzialności regulatorów w zakresie nadzoru nad rynkiem danych i zapewnienia przez nich bezpieczeństwa prawnego. Istotnym zagadnieniem będzie ochrona danych osobowych i nowe wyzwania, jakie niesie z sobą dalsza cyfryzacja.

URZĄD OCHRONY DANYCH OSOBOWYCH

- **Konferencja „Nowe zadania UODO” (tytuł niepotwierdzony)**

Termin: **1 grudnia** 2025 r., godz. 10:00–14:00

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

Organizatorzy: Urząd Ochrony Danych Osobowych
Formuła: hybrydowa

Konferencja ta zawiera się w cyklu wydarzeń poświęconych nowym zadaniom Prezesa Urzędu Ochrony Danych Osobowych w zakresie zarządzania danymi. Projekt ustawy o zarządzaniu danymi, która ma na celu wdrożenie unijnego Aktu w sprawie zarządzania danymi (DGA), przyznaje Prezesowi UODO nowe zadania i kompetencje związane m.in. z nadzorem nad instytucjami pośredniczącymi w udostępnianiu danych. Tej tematyce będzie poświęcona konferencja.

- **Konferencja „Rola Konwencji ramowej Rady Europy o sztucznej inteligencji w ochronie prywatności i danych osobowych – wyzwania prawne, etyczne i społeczne w erze sztucznej inteligencji” (konferencja prowadzona po angielsku, tłumaczenie na polski tylko dla uczestników stacjonarnych)**

Termin: **10 grudnia** 2025 r., godz. 10:00–14:00

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

Organizatorzy: Prezes Urzędu Ochrony Danych Osobowych, Społeczny Zespół Ekspertów przy Prezesie UODO, Komitet Rady Europy ds. Sztucznej Inteligencji (CAI), Komitet Konwencji 108 (T-PD) oraz Europejska Komisja na rzecz Efektywności Wymiaru Sprawiedliwości (CEPEJ)
Formuła: hybrydowa

W trakcie konferencji planowane są wystąpienia przedstawicieli Rady Europy oraz polskich i zagranicznych ekspertów w dziedzinie ochrony danych osobowych i sztucznej inteligencji. Wezmą oni udział w trzech panelach dyskusyjnych, dotyczących głównych aspektów ochrony danych w świetle Konwencji Rady Europy o sztucznej inteligencji, praktycznych aspektów wdrażania i oceny ryzyka związanego z przetwarzaniem danych przez sztuczną inteligencję oraz wpływu sztucznej inteligencji na wymiar sprawiedliwości i prawa obywateli.

Przypominamy, że UODO na stałe zmienił swoją siedzibę

Dlatego od lipca 2025 r. prosimy kierować korespondencję na nowy adres: **Urząd Ochrony Danych Osobowych, ul. Moniuszki 1A, 00-014 Warszawa**. Pod nim znajdują się biura Urzędu oraz punkt kancelaryjny.

W wypadku kierowania korespondencji na stary adres Urzędu (ul. Stawki 2, 00-193 Warszawa) będzie ona do końca 2025 roku przekierowywana na nowy adres.

Zmiana siedziby nie wiąże się z obowiązkiem zamieszczenia nowego adresu Urzędu w klauzulach informacyjnych administratorów ochrony danych.

Jednak administratorzy, którzy w swoich klauzulach informacyjnych zamieścili poprzedni adres UODO muszą usunąć informacje adresowe UODO albo zaktualizować je.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl