URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 03/03/24

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo!

Ochrona danych osobowych we współczesnym świecie nie jest możliwa bez wsparcia organizacji i stowarzyszeń. Taka sieć społeczna może z jednej strony zbierać informacje o tym, co dla obywateli i rynku jest ważne. Z drugiej strony – może wesprzeć nas w szerzeniu wiedzy o ochronie danych i prawie do prywatności.

Dlatego staram się konsekwentnie taką sieć budować. W marcu spotkałem się z:

- prezesem Konfederacji Lewiatan Maciejem Wituckim i przedstawicielami firm zrzeszonych w Lewiatanie
- prezesem Zarządu Izby Gospodarki Elektronicznej Patrycją Sass-Staniszewską
- prezesem Związku Firm Ochrony Danych Osobowych Przemysławem Zegarkiem i przedstawicielami Związku
- prezesem Stowarzyszenia Inspektorów Ochrony Danych Osobowych Jarosławem Felińskim i przedstawicielami SIODO
- prezeską Stowarzyszenia Praktyków Ochrony Danych SPOD Magdaleną Sołtysiak i członkami Stowarzyszenia
- prezesem Stowarzyszenia Inspektorów Ochrony Danych SABI Maciejem Byczkowskim i zarządem Stowarzyszenia
- prezesem Krajowej Rady Radców Prawnych Włodzimierzem Chróścikiem

Rozmawiałem też z europejskim inspektorem ochrony danych osobowych Wojciechem Wiewiórowskim, który odwiedził naszą siedzibę. Dobrze rozumiemy, że wyzwania dla danych osobowych pojawiają się nie tylko w Polsce, ale w całej Europie. Należy do nich m.in. rosnąca potrzeba uczulania osób spoza branży na znaczenie ochrony danych osobowych i samego prawa do prywatności.

Prawo to mamy zapisane w naszej Konstytucji, ale rzadko o tym rozmawiamy. Dlatego też postanowiłem włączyć się w akcję edukacyjną Tour de Konstytucja – spotkania organizowane w całym kraju szerzące wiedzę o prawach i wolnościach konstytucyjnych.

Od początku marca informacje i materiały edukacyjne w zakresie ochrony danych osobowych UODO publikuje na platformie LinkedIn oraz Mastodon. Urząd ma też profil na platformie X (dawniej Twitter). Reaktywowany został kanał UODO na YouTube.

Mówienie o ochronie danych osobowych w sposób precyzyjny, ale też zrozumiały dla obywateli nie będących ekspertami w tej dziedzinie, jest ważnym wyzwaniem Urzędu.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

W tym wydaniu Biuletynu chciałbym zwrócić Państwa uwagę na materiał dotyczący wyzwań, jakie dla ochrony danych osobowych tworzą nowe narzędzia edukacyjne. Znaczenie tego zagadnienia będzie niewątpliwie rosło i warto już teraz poświęcać mu uwagę.

Jak widać, problemy związane z ochroną danych osobowych obejmują kolejne dziedziny naszego życia. Dlatego polecam też lekturę informacji o tym, jak o prawa osób młodych zamierza zadbać hiszpański organ ochrony danych.

Zawarte w Biuletynie informacje o rozstrzygnięciach UODO, TSUE i ETPCz, choć z pozoru specjalistyczne, dotykają już praktycznie każdego. Dla rynku reklamowego ciekawa będzie sprawa IAB Europe przed TSUE. Przedstawicieli wymiaru sprawiedliwości zainteresują dwie sprawy z ETPCz: dotycząca przetwarzania danych biometrycznych osób skazanych i publikowania informacji o zakażeniu wirusem HIV. Pouczająca jest historia sporu spółki Tagadamedia z francuskim organem ochrony danych osobowych. Chodziło o to, jak można pozyskiwać dane o potencjalnych klientach, a skończyło się karą w wysokości 75 tys. euro. Dla tych, którzy interesują się problemem migracji, ważne okażą się uwagi Europejskiego Inspektora Danych Osobowych na temat prywatności rozporządzenia w celu zwalczania przemytu migrantów i handlu ludźmi.

Wszystkie te sprawy są oczywiście ciekawe także dla ekspertów z dziedziny ochrony danych osobowych.

Stały wzrost znaczenia ochrony danych osobowych dla naszego Urzędu oznacza skokową zmianę. Musimy z informacjami docierać do coraz szerszej publiczności. I musimy się tego wszyscy uczyć. Z tego punktu widzenia interesująca może się okazać opisana w tym Biuletynie korespondencja UODO z firmą, która postępowała w zgodzie ze swoim regulaminem, ale nie poinformowała klienta o swoim stanowisku w sposób dla niego jasny i zrozumiały.

W rozmowie numeru, Anna Dudkowska, Dyrektor Departamentu Współpracy Międzynarodowej i Edukacji opowiedziała o funkcjonowaniu Departamentu, współpracy UODO z licznymi środowiskami oraz kontaktach z Europejską Radą Ochrony Danych.

W tym wydaniu Biuletynu mamy także specjalną sekcję dla ekspertów, poświęconą certyfikacji i kodeksom postępowania.

Zapraszamy do lektury

Adam Sanocki
Dyrektor Departamentu Komunikacji Społecznej,
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

Z NASZYMI INICJATYWAMI WYCHODZIMY POZA MURY URZĘDU

Z Anną Dudkowską, Dyrektor Departamentu Współpracy Międzynarodowej i Edukacji w UODO rozmawiał Karol Witowski, Zastępca Rzecznika Prasowego UODO.

Departament Współpracy Międzynarodowej i Edukacji, którym Pani kieruje, jest odpowiedzialny za inicjatywy edukacyjne realizowane przez Urząd Ochrony Danych Osobowych. Flagowy program UODO „Twoje dane – Twoja sprawa" jest bardzo popularny pomimo tego, że udział w nim wymaga dużego zaangażowania. Obecnie trwa już jego czternasta edycja. Do kogo jest skierowany Program i jakie korzyści przynosi uczestnikom?

Program jest skierowany do szkół i placówek doskonalenia nauczycieli, a jego celem jest upowszechnienie wiedzy o ochronie danych osobowych wśród uczniów i grona pedagogicznego, aby świadomie korzystali z praw gwarantowanych przez RODO, co jest szczególnie istotne i bywa trudne w dobie dynamicznego rozwoju nowych technologii. Co więcej, działania podejmowane w ramach Programu w postaci realizacji wielu inicjatyw, o których informują nas uczestnicy, angażują całe społeczności szkolne tj. nauczycieli, uczniów i ich rodziców. W ramach Programu UODO zapewnia uczestnikom materiały edukacyjne i specjalistyczne szkolenia oraz wykłady online, podczas których eksperci naszego Urzędu poruszają zagadnienia dotyczące ochrony danych osobowych i prywatności, najbardziej interesujące i potrzebne z punktu widzenia wyzwań, z jakimi mogą się zmagać placówki oświatowe i uczniowie. Realizując tę inicjatywę, niezmiennie od 14 lat, staramy się dotrzeć do kadry nauczycielskiej z wiedzą o bezpiecznym przetwarzaniu danych osobowych, identyfikacji ryzyka i przeciwdziałaniu naruszeniom ochrony danych osobowych. Zależy nam również na tym, aby wyposażyć uczniów w niezbędne umiejętności i wiedzę dotyczącą świadomego i rozważnego dzielenia się swoimi danymi osobowymi podczas aktywności w Internecie czy w życiu codziennym.

Co roku, do Programu przystępuje około 300 szkół, wśród których wiele to kontynuatorzy Programu już od kilku lat. Tegoroczna edycja poświęca szczególną uwagę mediom społecznościowym i koncentruje się na kwestiach związanych z wyzwaniami, jakie dla ochrony danych osobowych może przynieść aktywność młodzieży właśnie w tym obszarze.

1 ROZMOWA Z EKSPERTEM

Program „Twoje dane – Twoja sprawa" jest przeznaczony dla szkół podstawowych oraz ponadpodstawowych. A jak wygląda edukacja skierowana do innych grup? Czy Pani Departament prowadzi także działania w tym kierunku?

Jak najbardziej, szczególnie pamiętamy o seniorach, których należy wyposażać w wiedzę o ochronie danych osobowych w czasach błyskawicznego rozwoju nowych technologii. I tak ostatnio, w styczniu 2024 roku gościliśmy w siedzibie naszego Urzędu grupę seniorów. Podczas takich inicjatyw zwracamy uwagę na wyzwania dla ochrony danych osobowych osób starszych, koncentrujemy się na problemach, które dotyczą właśnie ich. Spotkania te są bardzo wdzięczne, zazwyczaj przychodzą do nas osoby zaangażowane i z dużą uwagą uczestniczą w naszych wydarzeniach. Bardzo chętnie dzielą się też zdobytą wiedzą, stając się niejako ambasadorami ochrony danych osobowych, co bardzo nas cieszy, ponieważ pozwala dotrzeć z przekazem znacznie szerzej.

Pamiętamy również o studentach, których zapraszamy do siedziby naszego Urzędu na warsztaty, podczas których nasi przedstawiciele starają się aktywnie zaangażować uczestników do przemyśleń na temat przetwarzania danych osobowych zgodnie z ogólnym rozporządzeniem o ochronie danych. W ubiegłym roku, właśnie dla studentów, zorganizowaliśmy cykl wykładów w ramach inicjatywy edukacyjnej pn. Letnia Akademia Liderów RODO.

Wychodzimy też poza mury Urzędu i z naszymi wykładami odwiedzamy uczelnie wyższe czy inne instytucje zainteresowane rozważnym i bezpiecznym zarządzaniem danymi osobowymi w kontekście wyzwań technologicznych, jakim przykładowo jest rozwój sztucznej inteligencji.

Jak zmienia się tematyka programów edukacyjnych i szkoleń UODO? Czy rozwój technologii takich jak sztuczna inteligencja wpływa na działania edukacyjne UODO?

Dane w formie cyfrowej zdominowały świat danych osobowych. Rozwój nowych technologii bezpowrotnie zmienił podejście do ochrony danych. Pojawiły się inne, nieznane do tej pory wyzwania dla ochrony danych osobowych, co determinuje nowe sposoby radzenia sobie z nimi. Pokazują to również statystyki naruszeń ochrony danych, skarg czy nakładanych kar, coraz częściej dotyczących niewłaściwego zabezpieczenia danych cyfrowych, utraty nośnika danych, przesłania cyfrowej kopii danych do niewłaściwego adresata czy publikacji danych w mediach społecznościowych. To pokazuje jak silna jest potrzeba edukowania społeczeństwa, które przecież coraz częściej musi funkcjonować w świecie cyfrowym. Uświadamianie obywateli w zakresie niebezpieczeństw jakie się z tym wiążą, jest ważną częścią działalności UODO.

1 ROZMOWA Z EKSPERTEM

Warto podkreślić, że wszystkie inicjatywy edukacyjne UODO realizowane są bezpłatnie.

Zgadza się, nie pobieramy żadnych opłat podczas naszych działań edukacyjnych. Organizujemy je w ramach ważnej misji Urzędu, jaką jest edukacja społeczeństwa, którą nasi pracownicy realizują ze szczególną troską i przyjemnością, uczestnicząc w inicjatywach edukacyjnych na równi z innymi zadaniami wykonywanymi w UODO. Naszym celem jest stałe podnoszenie świadomości społeczeństwa na temat ochrony danych osobowych oraz dostarczanie wiedzy i praktycznych umiejętności, pozwalających zwiększyć ich bezpieczeństwo danych osobowych.

Departament Współpracy Międzynarodowej i Edukacji jest odpowiedzialny za współpracę z Europejską Radą Ochrony Danych (EROD), która jest niezależnym organem Unii Europejskiej. UODO jest członkiem EROD. Jak wygląda ta współpraca?

Przyjęcie ogólnego rozporządzenia o ochronie danych osobowych było punktem zwrotnym w historii europejskiej ochrony danych osobowych. Rozporządzenie przyniosło szereg zmian, przede wszystkim zharmonizowało przepisy o ochronie danych na poziomie unijnym i stworzyło złożone mechanizmy współpracy i spójności, które gwarantują jednolite stosowanie prawa w całej Unii Europejskiej. Tym samym RODO przyniosło wiele zmian na poziomie dotychczasowych doświadczeń Urzędu Ochrony Danych Osobowych w zakresie współpracy międzynarodowej. W ciągu ostatnich 6 lat zacieśniliśmy współpracę między europejskimi organami nadzorczymi, dzięki utworzeniu właśnie na gruncie RODO Europejskiej Rady Ochrony Danych, w pracach której aktywnie biorą udział przedstawiciele Urzędu Ochrony Danych Osobowych. W ramach działań podgrup i grup zadaniowych Europejskiej Rady Ochrony Danych, przedstawiciele polskiego organu nadzorczego, wraz z reprezentantami pozostałych organów, opracowali w ostatnich latach szereg dokumentów, w tym opinie, wytyczne, zalecenia i najlepsze praktyki w celu promowania wspólnego zrozumienia rozporządzenia zarówno przez organy nadzorcze, jak i administratorów i podmioty przetwarzające. W efekcie osoby, których dane dotyczą oraz administratorzy danych i podmioty przetwarzające są bardziej świadomi swoich praw i obowiązków, a organy nadzorcze posiadają instrumenty, które ułatwiają stosowanie i egzekwowanie RODO.

Ponadto, właśnie dzięki współpracy międzynarodowej, polski organ nadzorczy zebrał ogrom doświadczeń związanych z mechanizmem współpracy i mechanizmem spójności w związku z prowadzeniem postępowań transgranicznych.

1 ROZMOWA Z EKSPERTEM

UODO współpracuje z uczelniami wyższymi. Na czym polega taka współpraca?

Tak, to prawda. UODO współpracuje z licznymi uczelniami wyższymi, wspierając je w zakresie działalności edukacyjnej na rzecz ochrony prywatności i danych osobowych. Przedstawiciele Urzędu uczestniczą w wydarzeniach organizowanych przez uczelnie, a wpisujące się w zakres naszej działalności konferencje i inne działania edukacyjne są obejmowane patronatem honorowym UODO.

Czy na liście instytucji, z którymi współpracuje UODO są też organizacje pozarządowe, popularne NGO-sy?

Oczywiście, jeśli tylko są im bliskie zagadnienia ochrony danych osobowych i prywatności.
W ostatnim czasie Prezes Urzędu Ochrony Danych Osobowych spotkał się z organizatorem projektu Tour de Konstytucja, Prezesem Fundacji Aktywna Demokracja, w celu nawiązania współpracy w zakresie promowania wartości ochrony danych osobowych. Urzeczywistnieniem deklaracji współpracy, jaka padła podczas wizyty, jest udział przedstawiciela Urzędu w spotkaniach z młodzieżą w szkołach, organizowanych w ramach projektu Tour de Konstytucja. To doskonały przykład tego, że wsparcie UODO ma rzeczywisty wymiar, wychodzący daleko poza deklarację wsparcia.

W ostatnim czasie Prezes Urzędu Ochrony Danych Osobowych spotyka się z organizacjami zrzeszającymi inspektorów ochrony danych. Departament Współpracy Międzynarodowej i Edukacji również aktywnie uczestniczy w tych rozmowach. W jaki sposób odbywają się takie spotkania? Czy każdy IOD może spotkać się z Prezesem i opowiedzieć o swoich problemach?

W marcu 2024 roku Prezes Urzędu Ochrony Danych Osobowych rozpoczął serię spotkań z organizacjami zrzeszającymi IOD-ów. To bardzo dobry sposób na wysłuchanie tego środowiska, które podczas spotkań może przedstawić wyzwania, z jakimi spotykają się inspektorzy ochrony danych oraz zakomunikować aktualne potrzeby. Głównym celem wizyt jest wypracowanie rozwiązań usprawniających współpracę na rzecz odpowiedniej ochrony danych osobowych.

Do tej pory Prezes UODO spotkał się z przedstawicielami Stowarzyszenia Inspektorów Ochrony Danych (SABI), Stowarzyszenia Praktyków Ochrony Danych (SPOD), Stowarzyszenia Inspektorów Ochrony Danych Osobowych (SIODO) oraz przedstawicielami Związku Firm Ochrony Danych Osobowych (ZFODO). W planach są kolejne spotkania również w szerszym gronie, wszystkich inspektorów ochrony danych zainteresowanych wspólnymi rozmowami. Już na początku kwietnia organizujemy wydarzenie przeznaczone właśnie dla IOD-ów, podczas którego omówione zostaną

wybrane zagadnienia dotyczące niezależności ich pozycji w związku ze sprawozdaniem EROD podsumowującym działania i rekomendacje organów nadzorczych w ramach CEF DPO.

Jakie wydarzenia w UODO w najbliższym czasie organizuje DWME?

W planach mamy kilka wydarzeń. Już w kwietniu odbędzie się konferencja pn. *Wyzwania dla ochrony danych osobowych dzieci*, podczas której eksperci zajmujący się tematyką bezpieczeństwa danych osobowych dzieci, w związku z dynamicznym rozwojem technologii i dostępem do usług społeczeństwa informacyjnego, przedstawią między innymi aktualne wyzwania i ogromne zagrożenia związane z powszechnym udostępnianiem wizerunku dzieci w Internecie czy weryfikacją ich wieku podczas korzystania z treści dostępnych w sieci.

Ponadto, pod koniec maja przygotujemy konferencję z okazji 20-lecia Polski w Unii Europejskiej. Jest to dla Urzędu Ochrony Danych Osobowych szczególna rocznica ze względu na mnogość zadań, jakie realizuje nasza instytucja w zakresie prawodawstwa unijnego.

Wszystkich zainteresowanych serdecznie zapraszamy do uczestnictwa.

CERTYFIKACJA I KODEKSY POSTĘPOWANIA – PODOBIEŃSTWA I RÓŻNICE

Przystąpienie do kodeksu postępowania lub otrzymanie certyfikatu dla konkretnego procesu przetwarzania danych jest dla klientów i partnerów biznesowych sygnałem, że podmiot w sposób odpowiedzialny podchodzi do ochrony danych osobowych i spełnia określone w RODO wymagania.

Zarówno kodeksy postępowania, jak i certyfikacja to przewidziane w RODO narzędzia służące wykazywaniu zgodności z rozporządzeniem. O podobieństwach i różnicach między nimi dyskutowano podczas trzeciego webinarium z serii „Certyfikacja w ochronie danych".

W grudniu 2023 r. Prezes UODO zatwierdził i opublikował na stronie internetowej Urzędu Dodatkowe wymogi akredytacji podmiotów certyfikujących. Obecnie trwa **akcja edukacyjna,** której celem jest zachęcanie rynku do tworzenia mechanizmów certyfikacji w zakresie ochrony danych osobowych zgodnie z art. 42 RODO. **Ma ona formę cyklu webinariów „Certyfikacja w ochronie danych". Dotychczas odbyły się trzy spotkania poświęcone tej tematyce (12.12.2023 r., 30.01.2024 r. oraz 26.02.2024 r.), a nagrania z ich przebiegu udostępnione są na stronie internetowej UODO**.

– Dotychczas w większości państw członkowskich nie zgromadzono szerokich doświadczeń związanych z certyfikacją w dziedzinie ochrony danych osobowych. Dlatego po rozpoczęciu stosowania rozporządzenia ogólnego przed pięcioma laty bardzo ważne było wypracowanie na poziomie europejskim dodatkowych ram prawnych i organizacyjnych. Powinny one – dzięki dopracowaniu i rozwinięciu przede wszystkim art. 42 i 43 RODO umożliwić spójne stosowanie tego instrumentu w całej Unii Europejskiej – **mówił w wystąpieniu otwierającym lutowe webinarium Mirosław Wróblewski, Prezes Urzędu Ochrony Danych Osobowych**. Jak dodał, dzisiaj takie ramy już mamy, a tworzą je m.in. zatwierdzone przez Prezesa UODO Dodatkowe wymogi akredytacji podmiotów certyfikujących.

2 UODO SYGNALIZUJE

W części głównej spotkania specjaliści UODO, wychodząc naprzeciw oczekiwaniom uczestników styczniowego webinarium, omówili najważniejsze cechy kodeksów postępowania i certyfikacji, podkreślając zwłaszcza ich zalety i wskazując różnice. Na potrzeby niniejszej publikacji Wydział Kodeksów i Certyfikacji w Departamencie Orzecznictwa i Legislacji przygotował zestawienie omawianych treści w formie tabeli.

Kodeksy postępowania i certyfikacja – porównanie narzędzi

Kryterium porównawcze	Kodeks postępowania	Certyfikacja
Definicje	**Brak definicji „kodeksu postępowania" w RODO[1], u.o.d.o.[2]** **Kodeks postępowania to zbiór instrukcji dla administratorów danych i podmiotów przetwarzających (p. 7 Wytycznych 1/2019[3])**	**Brak definicji „certyfikacji" w RODO, u.o.d.o.** **Certyfikat, znak jakości lub oznaczenie na podstawie RODO mogą zostać przyznane wyłącznie po przeprowadzeniu przez akredytowany podmiot certyfikujący lub właściwy organ nadzorczy niezależnej oceny dowodów, w której zostanie stwierdzone, że spełniono kryteria certyfikacji (p. 18 Wytycznych 1/2018[4]).**
Funkcja, cel	**Ma pomóc we właściwym stosowaniu RODO. Doprecyzowuje zastosowanie RODO (art. 40 ust. 1 i 2 RODO).** **Stanowi mechanizm umożliwiający wykazywanie zgodności z RODO (art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 46 ust. 2 lit. e RODO).**	**Pozwala osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi (motyw 100 RODO).** **Ma świadczyć o zgodności z RODO operacji przetwarzania prowadzonych przez administratorów i podmioty przetwarzające (art. 42 ust. 1 RODO).** **Stanowi mechanizm umożliwiający wykazywanie zgodności z RODO (art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 46 ust. 2 lit. f RODO).**

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 04.05.2016, str. 1, ze zm.).

[2] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781).

[3] Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679. Wersja 2.0, 4 czerwca 2019 r. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-0_pl

[4] Wytyczne 1/2018 w sprawie certyfikacji i określenia kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia. Wersja 3.0, 4 czerwca 2019 r. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying_pl

Kto może opracować	**Zrzeszenia i inne podmioty reprezentujące określone kategorie administratorów lub podmioty przetwarzające (art. 40 ust. 2 RODO).** **Przykłady ww. podmiotów - p. 21-22 Wytycznych 1/2019.**	**RODO nie przewiduje ograniczeń w tym zakresie.** **Warto zwrócić uwagę na p. 2 procedury zatwierdzania kryteriów certyfikacji przez EROD[5].**
Proces opracowania i zatwierdzania	**Wniosek o zatwierdzenie kodeksu postępowania oraz jego projekt muszą być przygotowane z uwzględnieniem art. 40 RODO, art. 27 u.o.d.o. oraz p. 19 – 59 Wytycznych 1/2019.** **Kodeks krajowy – oznacza kodeks, który obejmuje czynności przetwarzania prowadzone w obrębie jednego państwa członkowskiego.** **Kodeks transgraniczny – oznacza kodeks, który obejmuje czynności przetwarzania prowadzone w więcej niż jednym państwie członkowskim.** **Prezes UODO zatwierdza kodeks postępowania w formie decyzji administracyjnej (art. 40 RODO, art. 27 i art. 7 u.o.d.o. oraz Kpa[6]).**	**Wskazówki dot. opracowywania mechanizmów certyfikacji znajdują się w dokumentach wydanych przez EROD – ich katalog jest dostępny na stronie UODO w zakładce Certyfikacja.** **Kryteria certyfikacji, stanowiące integralną część mechanizmu certyfikacji, są zatwierdzane odpowiednio przez organ nadzorczy (krajowy lub wielonarodowy mechanizm certyfikacji) lub EROD (ogólnoeuropejski mechanizm certyfikacji) (art. 42 ust. 5 RODO).** **Przed zatwierdzeniem kryteriów certyfikacji przez organ nadzorczy wymagana jest opinia EROD (art. 64 ust. 1 lit. c RODO).** **Zatwierdzanie kryteriów certyfikacji przez Prezesa UODO będzie miało formę decyzji administracyjnej (art. 42, art. 58 ust. 3 lit. f i ust. 4 RODO, Kpa)** **Wniosek o zatwierdzenie kryteriów certyfikacji przez EROD składa się do właściwego organu nadzorczego.**
Kto może przystąpić do kodeksu/ uzyskać certyfikat	**Administratorzy/podmioty przetwarzające:** • **podlegający RODO,** • **niepodlegający RODO** **(art. 40 ust. 3 RODO).Okres członkostwa w kodeksie uzależniony jest od woli członka kodeksu i przestrzegania kodeksu.**	**Administratorzy/podmioty przetwarzające:** • **podlegający RODO,** • **niepodlegający RODO.** **(art. 42 ust. 1 i 2 RODO)** **Certyfikat jest przyznawany na okres 3 lat, z możliwością jego przedłużenia lub cofnięcia (art. 42 ust. 7 RODO).**

[5] EDPB Document on the procedure for the adoption of the EDPB opinions regarding national criteria for certification and European Data Protection Seals https://edpb.europa.eu/our-work-tools/our-documents/procedure/edpb-document-procedure-adoption-edpb-opinions-regarding_pl

[6] Ustawa z 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2023 r. poz. 775, ze zm.)

Terytorialny obszar obowiązywania	**Państwo EOG, w którym kodeks został zatwierdzony przez organ nadzorczy, np. w Polsce – kodeks zatwierdzony przez Prezesa UODO.** **Kodeks transgraniczny i kodeks stanowiący odpowiednie zabezpieczenie w rozumieniu art. 46 ust. 2 lit. e RODO może stać się powszechnie obowiązujący w EOG (art. 40 ust. 9 i 10 RODO).**	**Państwo EOG, w którym zostały zatwierdzone kryteria certyfikacji.** **Państwa EOG, w których zostały zatwierdzone kryteria certyfikacji.** **EOG – w przypadku mechanizmu certyfikacji, którego kryteria certyfikacji zostały zatwierdzone przez EROD.**
Akredytacja: podmiotu monitorującego przestrzeganie kodeksu/ podmiotu certyfikującego	**Monitorowanie przestrzegania kodeksu postępowania dla podmiotów prywatnych to obowiązek akredytowanego podmiotu monitorującego.** **Podmiot monitorujący jest akredytowany przez Prezesa UODO do konkretnego kodeksu postępowania – Wymogi akredytacji podmiotów monitorujących kodeksy postępowania.** **Akredytacja jest udzielana na 5 lat, z możliwością jej cofnięcia.** **(art. 41 RODO, art. 29-32 u.o.d.o., Kpa).** **Prezes UODO prowadzi publicznie dostępny wykaz podmiotów akredytowanych (art. 33 u.o.d.o.).**	**Certyfikacja może być udzielana przez organ nadzorczy lub akredytowany podmiot certyfikujący (art. 42 ust. 5 RODO).** **Postępowanie akredytacyjne podmiotu certyfikującego prowadzone będzie w Polsce przez Polskie Centrum Akredytacji (art. 43 ust. 1 lit. b RODO, art. 12 ust. 1 u.o.d.o.).** **Akredytacja będzie dokonywana na podstawie normy EN-ISO/IEC 17065/2012 i Dodatkowych wymogów akredytacji podmiotów certyfikujących.** **Akredytacja jest udzielana na 5 lat, z możliwością jej przedłużenia lub cofnięcia (art. 43 ust. 4 i 7 RODO).**
Czas obowiązywania	**RODO nie określa okresu czasu obowiązywania kodeksu postępowania.** **Wymagane są procedury regularnego przeglądu treści kodeksu (art. 41 ust. 2 lit. b RODO).**	**RODO nie określa okresu czasu ważności mechanizmu certyfikacji.** **Wymagane są procedury regularnego przeglądu treści kryteriów certyfikacji (p. 75 Wytycznych 1/2018; sekcja 9 Dodatek do Wytycznych 1/2018[7]).**

[7] Guidance on certification criteria assessment (Addendum to Guidelines 1/2018 on certification and identifying certification criteria in accordance with Articles 42 and 43 of the Regulation) https://edpb.europa.eu/our-work-tools/documents/public-consultations/2021/guidance-certification-criteria-assessment_pl

Publiczny dostęp do treści: zatwierdzonego kodeksu/zatwierdzonych kryteriów certyfikacji	**Prezes UODO ma obowiązek publikacji zatwierdzonego kodeksu postępowania (art. 40 ust. 6 RODO, art. 53 ust. 1 p. 2 u.o.d.o.).** **Rejestr wszystkich zatwierdzonych kodeksów postępowania jest prowadzony przez EROD (art. 40 ust. 11 RODO).**	**Prezes UODO ma obowiązek udostępnienia zatwierdzonych kryteriów certyfikacji (art. 43 ust. 6 RODO, art. 16 u.o.d.o.).** **EROD gromadzi w rejestrze wszystkie mechanizmy certyfikacji (art. 42 ust. 8 RODO).**
Koszty	**Koszty uzyskania statusu członka kodeksu i dalszego monitorowania przestrzegania kodeksu (tylko dla członków z sektora prywatnego) ustalają akredytowane podmioty monitorujące – dla zobrazowania: cennik RS Jamano sp. z o.o. sp.k. i KPMG Advisory sp. z o.o. sp. k.**	**Koszt certyfikacji, która będzie udzielana przez podmiot certyfikujący, nie jest jeszcze znany.** **W przypadku certyfikacji, która może być udzielana przez Prezesa UODO, jej maksymalny koszt został określony w art. 26 u.o.d.o.**
Potwierdzenie członkostwa w kodeksie / uzyskania certyfikacji	**RODO nie przewiduje żadnego dokumentu, który potwierdzałby członkostwo w kodeksie.** **Z dotychczas zatwierdzonych przez Prezesa UODO kodeksów postępowania wynika, że promowanie członkostwa w kodeksie odbywa się przez podanie do publicznej wiadomości informacji o uzyskaniu statusu podmiotu przestrzegającego kodeks przez twórcę kodeksu, podmiot monitorujący i samego zainteresowanego[8] .**	**Certyfikat (art. 21 u.o.d.o.)** **Wykaz podmiotów, które uzyskały certyfikat lub go im cofnięto prowadzony przez Prezesa UODO (art. 23 u.o.d.o.).**
Zasady monitorowania	**Zarówno kodeks dla podmiotów prywatnych, jak i publicznych musi zawierać mechanizmy monitorowania przestrzegania jego postanowień (p. 88 Wytycznych 1/2019).** **Monitorowanie przestrzegania kodeksu przez podmioty prywatne prowadzi akredytowany podmiot monitorujący, który jest zobowiązany posiadać odpowiednie procedury w tym zakresie, które są przedmiotem postępowania akredytacyjnego (art. 41 ust. 2 lit. b RODO).** **Dla przykładu, mechanizm monitorowania przestrzegania kodeksu przez jego członków z sektora publicznego został opisany w p. 7.3 Kodeksu postępowania dla sektora ochrony zdrowia[9].**	**Z RODO wynika wymóg posiadania przez podmiot certyfikujący procedur okresowego przeglądu i cofania certyfikacji, znaków jakości i oznaczeń w dziedzinie ochrony danych (art. 43 ust. 2 lit. c RODO).**

[8] Np. p. 7.3.11.1 Kodeks postępowania dla sektora ochrony zdrowia (PFSz) https://uodo.gov.pl/pl/426/1110
[9] Kodeks postępowania dla sektora ochrony zdrowia (PFSz) https://uodo.gov.pl/pl/426/1110

Utrata statusu członka kodeksu/certyfikatu	**Akredytowany podmiot monitorujący podejmuje odpowiednie działania w przypadku naruszenia kodeksu przez administratora lub podmiot przetwarzający, w tym zawiesza go lub wyklucza spośród stosujących kodeks. O działaniach tych i powodach ich podjęcia informuje on właściwy organ nadzorczy (art. 41 ust. 4 RODO).**	**Akredytowany podmiot certyfikujący cofa certyfikację w przypadku stwierdzenia, że podmiot, któremu udzielono certyfikacji, nie spełnia lub przestał spełniać kryteria certyfikacji (art. 42 ust. 7 RODO, art. 22 u.o.d.o.).**

Przystąpienie do kodeksu postępowania lub otrzymanie certyfikatu dla konkretnego procesu przetwarzania danych będzie dla klientów i partnerów biznesowych sygnałem, że podmiot mający status członka kodeksu lub dysponujący certyfikatem w sposób odpowiedzialny podchodzi do ochrony danych osobowych i spełnia określone w RODO wymagania. Jednocześnie stosowanie zatwierdzonych kodeksów postępowania lub mechanizmów certyfikacji będzie brane pod uwagę przy podejmowaniu przez Prezesa UODO decyzji o ewentualnym nałożeniu administracyjnej kary pieniężnej i jej wysokości (art. 83 ust. 2 lit. j RODO).

Webinarium było także okazją do przedstawienia kodeksów postępowania zatwierdzonych przez Prezesa UODO oraz omówienia współpracy z inicjatywami pracującymi nad kodeksami. Prowadzący spotkanie zachęcili do zapoznania się z treściami publikowanymi w zakładce Kodeksy postępowania oraz w zakładce Certyfikacja na stronie internetowej UODO. Poinformowali także, gdzie na stronie EROD szukać rejestru zatwierdzonych w EOG kodeksów postępowania oraz rejestru wszystkich zatwierdzonych mechanizmów certyfikacji.

Podczas webinarium wskazano także, że wszystkie podmioty zainteresowane opracowaniem kodeksu postępowania lub mechanizmu certyfikacji, czy uzyskaniem statusu akredytowanego podmiotu monitorującego kodeks lub akredytowanego podmiotu certyfikującego proszone są o kontakt z Wydziałem Kodeksów i Certyfikacji (dol@uodo.gov.pl).

KORESPONDENCJA Z KLIENTEM O ZASADACH USUNIĘCIA JEGO DANYCH OSOBOWYCH MUSI BYĆ DLA NIEGO ZROZUMIAŁA

Prezes UODO udzielił upomnienia firmie prowadzącej serwis do obsługi wpłat gotówki za sposób, w jaki potraktowała klienta, który chciał skasować u niej swoje konto i związane z tym dane.

Klient spółki wniósł o usunięcie konta i związanych z nim danych osobowych. Wniosek przesłał mailem. Spółka odpowiedziała, że do usunięcia konta zgodnie z jej regulaminem potrzebny jest pisemny wniosek przesłany tradycyjną pocztą. Klient zauważył, że RODO tego nie wymaga, jednak, by rozwiązać problem, przesłał wniosek elektroniczny podpisany kwalifikowanym podpisem cyfrowym. Na co spółka powtórzyła, że do usunięcia konta potrzebny jest wniosek na papierze.

Prezes UODO zauważył, że rzeczywiście podpisując ze spółką umowę klient zaakceptował jej regulamin, zatem powinien był się do niego zastosować. Elektroniczne wypowiedzenie umowy było nieskuteczne. Niemniej kiedy klient wyraźnie wyraził swoją wolę, że nie chce, by spółka dalej przetwarzała jego dane, spółka nadal to robiła. Tłumaczyła, że była do tego zobowiązana wciąż obowiązującą umową.

Problem w tym, że w korespondencji z klientem spółka nie pisała wyraźnie, że usunięcie danych osobowych jest dla niej równoznaczne z usunięciem konta. Cała korespondencja dotyczyła usunięcia konta – a nie związanych z nią danych osobowych. Tymczasem klient domagał się nie tylko usunięcia konta, ale i związanych z nim danych osobowych. Miał prawo zakładać, że do samego prowadzenia konta nie są potrzebne wszystkie dane o nim, jakie spółka zebrała.

Problemem był więc brak zwięzłej, przejrzystej i łatwo dostępnej komunikacji. A obowiązek taki ciąży na administratorze danych zgodnie z art. 12 ust. 1 zdanie pierwsze RODO. Stąd upomnienie.

Sygnatura: DS.523.6932.2022

WIELOZNACZNOŚĆ TERMINU „NARUSZENIE” W ŚWIETLE PRZEPISÓW RODO

W pracy inspektorów ochrony danych oraz urzędników organu nadzorczego termin „naruszenie” pojawia się często. Niestety, praktyka pokazuje, że okoliczności jego użycia, a co za tym idzie – kryjące się za nim znaczenia – mogą się od siebie bardzo różnić. Utrudnia to komunikację i prowadzi do kłopotliwej niepewności interpretacyjnej. Jak rozwiązać tę semantyczną łamigłówkę?

Źródłem nieporozumień jest fakt, iż w polskojęzycznej wersji RODO prawodawca niezmiennie posługuje się terminem „naruszenie”, odnosząc się do wielu odmiennych sytuacji prawnych. Możemy zatem odnaleźć w jego treści m.in.

- pojawiające się wielokrotnie „**naruszenie** praw lub wolności osób fizycznych” (np. w art. 24 ust. 1, art. 25 ust. 1 i art. 32 ust. 1 RODO),
- „**naruszenie** kodeksu [postępowania]” (w art. 41 RODO),
- „**naruszenie** warunków certyfikacji” (w art. 43 RODO), „**naruszenie** wiążących reguł korporacyjnych” (w art. 47 RODO),
- „**naruszenie** ochrony danych osobowych” (np. w art. 33 RODO),
- oraz „**naruszenie** niniejszego rozporządzenia” (np. w art. 83 RODO).

Dwa ostatnie przypadki są szczególnie istotne, ponieważ ich zamienne stosowanie jest powszechnym zjawiskiem.

4 NARUSZENIA I KONTROLE

Naruszenie ochrony danych osobowych a naruszenie RODO

„Naruszenie ochrony danych osobowych", którego definicję odnajdziemy w art. 4 pkt 12 RODO, nie powinno być utożsamiane z „naruszeniem niniejszego rozporządzenia".

Innymi słowy, wykrycie w organizacji administratora naruszenia ochrony danych osobowych nie musi oznaczać, że administrator ten złamał jakiekolwiek przepisy RODO.

Zgłoszenie naruszenia ochrony danych osobowych Prezesowi UODO nie powoduje także automatycznego wszczęcia postępowania administracyjnego wobec administratora (w przeciwieństwie do jego niezgłoszenia w określonej przepisami sytuacji *). Zdarza się jednak, że incydent i okoliczności jego wystąpienia mogą stać się impulsem do podjęcia przez organ nadzorczy czynności. Może on wtedy sprawdzać:

- czy przetwarzanie przez administratora danych osobowych w obszarze, którego dotyczyło zdarzenie, było prawidłowe,
- jak administrator realizował spoczywające na nim obowiązki,
- czy mamy do czynienia z przesłanką wskazującą na możliwość wdrożenia przez administratora nieodpowiednich zabezpieczeń.

Dopiero ewentualne uchybienia w tym zakresie mogą przesądzić o zastosowaniu przez Prezesa UODO przysługujących mu uprawnień naprawczych, w tym nałożeniu administracyjnej kary pieniężnej.

Stanowisko NSA i TSUE

Kwestię tę poruszył w 2023 r. NSA, który wyjaśnił, że „(…) *sankcji administracyjnej za naruszenie obowiązków (…) podlega nie ten, kto jako administrator albo podmiot przetwarzający dopuścił do nieuprawnionego przetwarzania danych osobowych, a tylko podmiot, który nie dochował odpowiedniego, w danych okolicznościach, standardu środków bezpieczeństwa. Karze nie podlega jednostka za nielegalne działanie osoby trzeciej (np. hakera), polegające na nieuprawnionym dostępie do danych przezeń przetwarzanych, a za dopuszczenie do tego dostępu w związku z nieodpowiednim poziomem stosowanych zabezpieczeń. O naruszeniu (…) przepisu nie przesądza sama okoliczność nieuprawnionego dostępu do danych, ponieważ taki stan rzeczy jest potencjalnie możliwy do zaistnienia również przy dochowaniu najwyższego poziomu zabezpieczeń*."**

Pogląd ten potwierdził niedawno także TSUE, wskazując, iż administratorzy zobowiązani są do wdrożenia odpowiednich technicznych i organizacyjnych środków celem zapewnienia zgodności przetwarzania z przepisami RODO, w tym właściwego zabezpieczenia danych osobowych, nie zaś

do zapobieżenia wszelkim ewentualnym naruszeniom ich ochrony.***

Terminologia zastosowana w innych wersjach językowych RODO

Zwróćmy uwagę, że w anglojęzycznej wersji RODO posłużono się terminem breach w kontekście „**naruszenia** ochrony danych osobowych" (ang. „personal data **breach**") oraz terminem infringement w kontekście „**naruszenia** niniejszego rozporządzenia" (ang. „**infringement** of this Regulation").

W wersji niemieckojęzycznej również mamy do czynienia z wyodrębnieniem w ramach RODO niezależnych terminów. W przypadku „**naruszenia** ochrony danych osobowych" jest to Verletzung (niem. „**Verletzung** des Schutzes personenbezogener Daten"), natomiast w przypadku „**naruszenia** niniejszego rozporządzenia" – Verstoß (niem. „**Verstoß** gegen diese Verordnung").

Widać zatem wyraźnie, że polskojęzyczna wersja RODO, mimo iż – zgodnie z zasadą wielojęzyczności – równie autentyczna i tak samo wiążąca jak pozostałe wersje językowe aktów prawa unijnego, wyposażyła nas w tym zakresie w nieco uboższą nomenklaturę. Warto mieć to na uwadze w procesie interpretowania i stosowania przepisów o ochronie danych osobowych.

fot. iStock

*** Więcej na ten temat w „Biuletynie UODO" nr 7-8/07-08/23 na str. 16.**

**** Wyrok NSA z 9.02.2023 r., III OSK 3945/21, LEX nr 3508987.**

***** Wyrok TS z 14.12.2023 r., C-340/21, VB PRZECIWKO NATSIONALNA AGENTSIA ZA PRIHODITE, LEX nr 3642726, pkt 34.**

EDUKACJA WSPIERANA TECHNOLOGIĄ: JAK NARZĘDZIA CYFROWE, SZTUCZNA INTELIGENCJA I TECHNOLOGIE IMMERSIVE ZMIENIAJĄ SPOSÓB, W JAKI UCZYMY SIĘ I NAUCZAMY?

W dobie cyfrowej transformacji edukacja przechodzi rewolucję. Narzędzia cyfrowe, sztuczna inteligencja (AI) oraz technologie immersive, takie jak wirtualna (VR) i rozszerzona (AR) rzeczywistość, zyskują na znaczeniu, otwierając nowe horyzonty w nauczaniu i uczeniu się. Jednakże wraz z rosnącym wykorzystaniem tych technologii, pojawiają się również pytania dotyczące ochrony danych i prywatności użytkowników.

Transformacja edukacyjna dzięki technologii

Mamy już wiele narzędzi technologicznych, które wspierają edukację. Są to m.in. platformy e-learningowe, aplikacje edukacyjne i systemy zarządzania nauką (LMS) umożliwiające dostęp do wiedzy bez ograniczeń oraz dopasowanie materiałów dydaktycznych do indywidualnych potrzeb.

Dzięki sztucznej inteligencji możliwe jest stworzenie bardziej interaktywnego i angażującego środowiska edukacyjnego. Największym atutem AI w edukacji jest możliwość personalizacji procesu nauczania. Systemy oparte na sztucznej inteligencji analizują postęp ucznia w czasie rzeczywistym, identyfikując jego mocne, ale i słabe strony. Nauczyciele mogą więc dostosować materiały dydaktyczne i tempo nauki do indywidualnych potrzeb, co zwiększa skuteczność nauczania i motywację do nauki.

Narzędzia do automatycznej oceny prac pisemnych, testów, czy quizów nie tylko oszczędzają czas nauczycieli, ale również zapewniają obiektywną i spójną ocenę aktywności uczniów. Dostarczają też uczniom natychmiastowy feedback, pomagając im zidentyfikować obszary, które wymagają dodatkowej pracy.

Warto również wspomnieć o inteligentnych asystentach i chatbotach, które pomagają w rozwiązywaniu problemów – programy te, dostępne o każdej porze dnia i nocy, są w stanie wyjaśnić trudne koncepcje i poprowadzić przez złożone procesy edukacyjne. Dzięki temu nauka staje się bardziej dostępna i elastyczna.

5 NOWE TECHNOLOGIE

Technologie immersyjne takie jak VR i AR wnoszą nowy wymiar do nauki, umożliwiając uczniom eksplorację wirtualnych środowisk, symulacji historycznych wydarzeń, zanurzenie się w świecie biologii na poziomie komórkowym, czy też realizację eksperymentów naukowych w bezpiecznym środowisku wirtualnym.

Wyzwania ochrony danych

Te narzędzia edukacyjne gromadzą jednak ogromne ilości danych, w tym informacje osobiste, dane o postępach w nauce i zachowaniach użytkowników. Dlatego wraz z postępem technologicznym ochrona danych osobowych uczniów staje się kluczowym wyzwaniem. Instytucje edukacyjne i dostawcy technologii muszą więc przestrzegać kluczowych zasad ochrony danych, w tym zasady minimalizacji danych, przejrzystości, ograniczenia celu, integralności i poufności. Oznacza to, że dane powinny być zbierane tylko w niezbędnym zakresie, użytkownicy powinni być jasno informowani o celu zbierania danych oraz sposobach ich wykorzystania, a dane muszą być chronione przed nieautoryzowanym dostępem lub wyciekiem**.**

Dobre praktyki w ochronie danych

- **Transparentność i zgoda**: Użytkownicy powinni być w pełni informowani o tym, jakie dane są zbierane, w jakim celu i kto ma do nich dostęp. Zgoda na przetwarzanie danych musi być świadoma i dobrowolna.
- **Bezpieczeństwo danych**: Instytucje edukacyjne wdrażają polityki ochrony danych, szkolą personel z zakresu bezpieczeństwa informacji i regularnie audytują używane narzędzia cyfrowe pod kątem zgodności z przepisami o ochronie danych. Ponadto istotne jest budowanie świadomości wśród uczniów i nauczycieli na temat znaczenia ochrony danych i sposobów zabezpieczania prywatności online.
- **Minimalizacja danych**: Zbierane i przechowywane są wyłącznie te dane, które są niezbędne do celów edukacyjnych, co zmniejsza ryzyko naruszenia prywatności.
- **Edukacja użytkowników**: Nauczyciele i uczniowie są edukowani w zakresie bezpiecznego korzystania z technologii cyfrowych oraz ochrony prywatności również w świecie online, z uwzględnieniem zasady poufności dotyczącej przetwarzanych danych.

Bez promowania i wdrażania tych dobrych praktyk i wiedzy o ochronie danych, sektor edukacyjny nie będzie mógł skutecznie wykorzystać potencjału nowych technologii.

RODO A SYSTEMY KODOWANIA DANYCH O ZGODACH UŻYTKOWNIKÓW. TSUE W SPRAWIE SYSTEMU IAB EUROPE

Czy zakodowany zbiór informacji o zgodach użytkowników udostępniany reklamodawcom to dane osobowe w rozumieniu RODO? Czy organizacja, która koduje te dane, jest administratorem danych?

TSUE na pierwsze pytanie odpowiedział twierdząco. Na drugie – że nie do końca.

7 marca 2024 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sporze IAB Europe z belgijskim organem nadzorczym Gegevensbeschermingsautoriteit. Ten stwierdził, że kodowany – dla celów świadczenia reklam – system informacji o zgodach użytkowników na przetwarzanie danych sam w sobie zawiera dane osobowe. Bowiem funkcjonuje on w połączeniu z IP użytkownika i plikami cookie. To w sumie pozwala na identyfikację danej osoby.

IAB Europe odwołała się od tej decyzji, a sąd odwoławczy skierował pytanie prejudycjalne do TSUE.

Na czym polegał problem?

IAB Europe, zrzeszający przedsiębiorstwa z sektora reklamy cyfrowej i marketingu cyfrowego, opracował system pozwalający reklamodawcom na licytowanie w czasie rzeczywistym miejsca reklamowego na stronach i w aplikacjach, które przegląda użytkownik (Real Time Bidding).

System korzysta z danych dotyczących m.in. lokalizacji, wieku, historii wyszukiwania i ostatnich zakupów użytkownika. Przekazywane są one jednak tylko wtedy, gdy użytkownik wyraził na to zgodę. Dane te są kodowane i przechowywane w Transparency and Consent String (TC String) – ciągu składającym się z kombinacji liter i znaków.

Dodatkowo to, co można zrobić z danymi osobowymi, jest szczegółowo określone w obowiązujących uczestników systemu ramach przejrzystości i zgody (Transparency & Consent, TCF). Są w nich wytyczne, instrukcje, specyfikacje techniczne, protokoły i zobowiązania umowne, których stosowanie pozwala na zgodne z prawem przetwarzanie danych osobowych użytkowników.

Zdaniem IAB Europe system jest zgodny z RODO, a samo TC String nie stanowi danych osobowych. Zatem IAB Europe nie jest takich danych administratorem.

6 SPRAWY MIĘDZYNARODOWE

Spór o TC String

W 2019 r. grupa organizacji to rozumowanie podważyła i wskazała, że mamy tu do czynienia z danymi osobowymi, bo TC String w powiązaniu z umieszczanym na urządzeniu użytkownika plikiem cookie i numerem IP pozwala już człowieka zidentyfikować.

Organizacje te wniosły do krajowych organów ochrony danych osobowych skargi na IAB Europe. Była wśród nich polska Fundacja Panoptykon. Wniosła skargę do Prezesa UODO.

Ponieważ IAB Europe ma siedzibę w Belgii, wszystkie skargi były rozpatrywane tam – pod jedną sygnaturą DOS - 2019 - 01377.

Decyzja

Belgijski organ nadzorczy w decyzji z 2 lutego 2022 r. uznał, że kod TC String stanowi dane osobowe w rozumieniu RODO, a IAB jest ich administratorem.

IAB Europe musi więc – zgodnie z tą decyzją – znaleźć ważną podstawę prawną przetwarzania i udostępniania preferencji użytkownika w formie TC String. Nie może po prostu powołać się na uzasadniony interes.

Belgijski organ nakazał też IAB Europe dostosowanie operacji przetwarzania do przepisów RODO poprzez:

- zapewnienie skutecznych środków monitorowania integralności i poufności TC String,
- prowadzenie ścisłego audytu, czy organizacje, które przystąpiły do TCF, spełniają wymogi RODO,
- doprowadzenie do tego, aby niemożliwe było domyślne zaznaczenie zgody oraz autoryzacja w oparciu o uzasadniony interes,
- oraz przyjęcie jednolitego i zgodnego z RODO podejścia do informacji, które są przekazywane użytkownikom.

IAB został również zobowiązany do:

- zaktualizowania rejestrów czynności tak, aby uwzględniały przetwarzanie danych w ramach TCF,
- przeprowadzenia oceny skutków dla ochrony danych w odniesieniu do czynności przetwarzania w ramach TCF oraz ich wpływu na późniejsze przetwarzanie,
- dostosowania oceny skutków dla ochrony danych do przyszłych wersji bądź modyfikacji obecnej wersji TCF,
- wyznaczenia inspektora ochrony danych.

Biorąc pod uwagę skalę stwierdzonych naruszeń, belgijski organ nadzorczy nałożył na IAB Europe administracyjną karę w wysokości 250 000 EUR.

Rola UODO

Prezes UODO współpracował z belgijskim organem nadzorczym oraz pozostałymi organami nadzorczymi przy kolejnych wersjach projektu decyzji. Przesyłał też kierowane do niego stanowiska IAB Europe i IAB Polska. Komentarze i uwagi Prezesa UODO miały przede wszystkim charakter techniczny. Prezes UODO zgodził się z ustaleniami belgijskiego odpowiednika i zastosowanymi środkami zaradczymi.

Pytanie do TSUE

IAB Europe wniosła skargę na decyzję organu belgijskiego do sądu apelacyjnego w Brukseli. Ten zaś zwrócił się z pytaniami prejudycjalnymi do Trybunału Sprawiedliwości. I to właśnie na to pytanie TSUE odpowiedział w wyroku C-604/22.

TSUE potwierdził, że TC String zawiera informacje dotyczące możliwego do zidentyfikowania użytkownika, a zatem stanowi dane osobowe w rozumieniu RODO. Jeżeli bowiem informacje zawarte w TC String powiąże się z identyfikatorem, takim jak adres IP urządzenia użytkownika, mogą one umożliwić stworzenie profilu owego użytkownika i jego identyfikację.

Jednak IAB Europe nie jest administratorem tych danych, ale „współadministratorem” w rozumieniu RODO.

IAB Europe jest administratorem, bo wpływa na operacje przetwarzania danych przy zapisywaniu w TC String informacji o preferencjach w zakresie zgody użytkowników. Ustala też wspólnie ze swoimi członkami zarówno cele tych operacji, jak i sposoby ich dokonywania.

Nie jest jednak administratorem w rozumieniu RODO, bowiem nie ma wpływu na operacje przetwarzania danych, które dzieją się już po zapisaniu w TC String informacji o zakresie zgód użytkowników.

TSUE wskazał, że IAB Europe można by uznać za administratora, gdyby udało się dowieść, że stowarzyszenie wywarło wpływ na ustalenie celów dalszych operacji i sposobów ich dokonywania.

ZNACZENIE PRAWA DO PRYWATNOŚCI I WPŁYW AI – OŚWIADCZENIA Z OKAZJI DNIA OCHRONY DANYCH

„Ogólnoświatowe obchody Dnia Ochrony Danych świadczą o uznaniu faktu, że prawo do prywatności, a w szczególności prawa jednostki w związku z przetwarzaniem jej danych osobowych mają fundamentalne znaczenie w dzisiejszym zdigitalizowanym świecie" – napisała przewodnicząca Komitetu Konwencji 108 Elsa Mein w specjalnym oświadczeniu z okazji 18. Międzynarodowego Dnia Ochrony Danych.

„W roku 2024 stanęliśmy na rozdrożu. Sztuczna inteligencja jest wszechobecna i dotyczy nas wszystkich. Odczuwamy jej skutki, zarówno pozytywne, jak i negatywne. Musimy się więc zaangażować w wyznaczenie jej granic" – napisał w swoim z kolei oświadczeniu komisarz ds. Ochrony Danych Rady Europy Jean-Philippe Walter.

Dzień Ochrony Danych został ustanowiony w rocznicę otwarcia do podpisu Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Konwencja ETS nr 108) z 1981 roku. Konwencja pozostaje jedynym prawnie wiążącym międzynarodowym instrumentem chroniącym dane osobowe i prawo do prywatności, skupiającym 55 państw-stron i około 40 obserwatorów z całego świata.

Wydarzenia i konferencje organizowane z okazji Dnia Ochrony Danych można sprawdzić na liście przygotowanej przez Sekretariat Komitetu Konwencji 108.

BRUKSELA. KONFERENCJA Z UDZIAŁEM EIOD WOJCIECHA WIEWIÓROWSKIEGO I PRZEDSTAWICIELKI UODO

Konferencję poświęconą m.in. globalnemu przepływowi danych, zarządzaniu cyfrowemu, regulacji AI oraz harmonizacji procedur RODO zorganizowali w Brukseli: Rada Europy, Europejski Inspektor Ochrony Danych i organizacja Computers, Privacy & Data Protection (CPDP).

Stałe Przedstawicielstwo Rzeczypospolitej Polskiej przy UE i Ministerstwo Cyfryzacji przygotowały w jej trakcie debatę „Jaka jest przyszłość e-komunikacji? Co osiągnąć, czego unikać?". Wziął w niej udział europejski inspektor ochrony danych Wojciech Wiewiórowski, zastępczyni dyrektora działu odpowiedzialnego za ochronę danych w Komisji Europejskiej (DG Justice and Consumers) Karolina Mojzesowicz, przewodniczący Izby Postępowań Sądowych w belgijskim organie ochrony danych Hielke Hijmans i zastępczyni Dyrektora Departamentu Współpracy Międzynarodowej i Edukacji UODO Maria Owczarek. Panel moderowała Katarzyna Prusak-Górniak, przewodnicząca Działu Spraw Cyfrowych w Stałym Przedstawicielstwie Rzeczypospolitej Polskiej przy UE.

Program konferencji

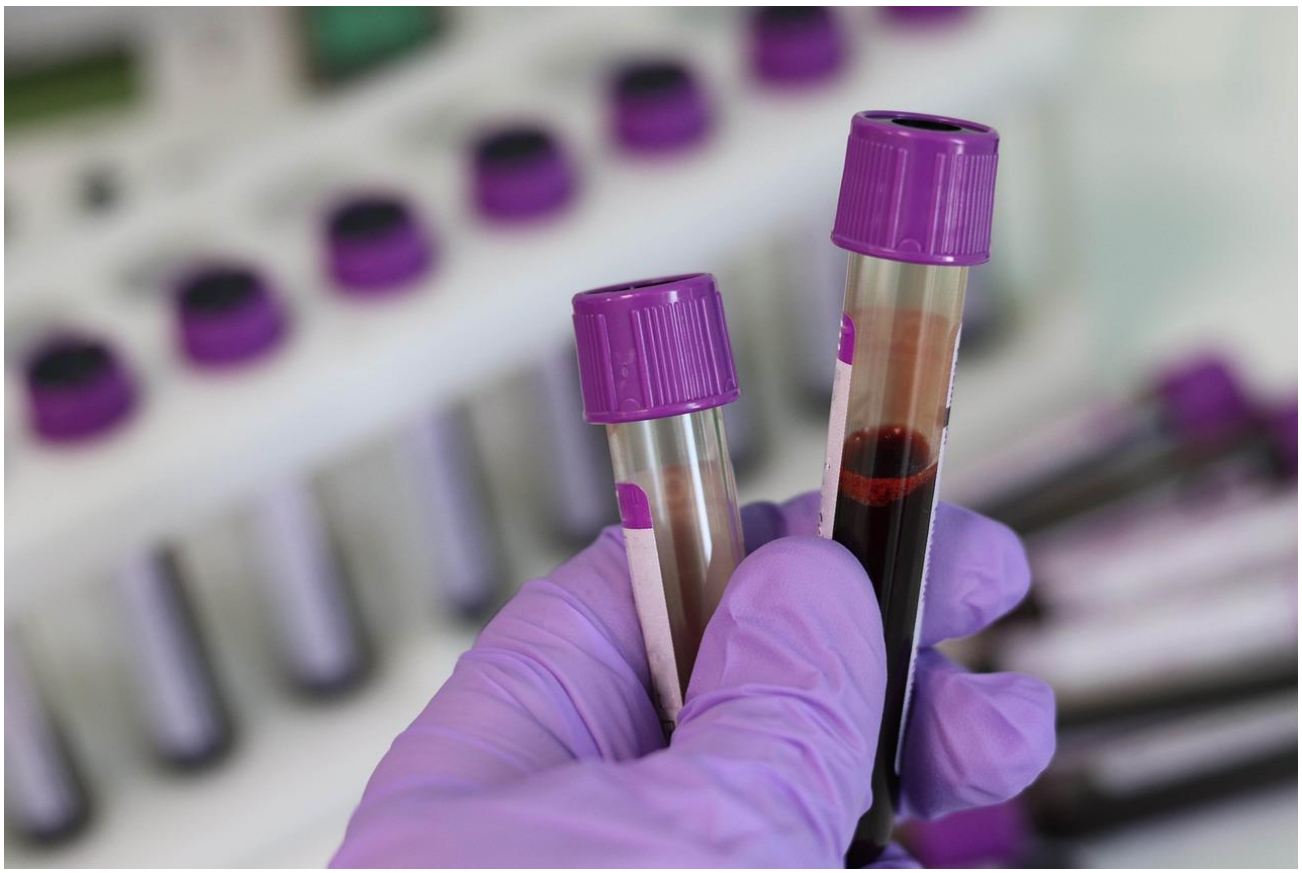
fot. pixabay

ETPCZ: WYROK WS. PUBLIKACJI DANYCH OSOBOWYCH OSÓB ZAKAŻONYCH HIV

Grecja naruszyła prawo do poszanowania życia prywatnego (art. 8 Europejskiej Konwencji Praw Człowieka) ujawniając dane medyczne pracowników seksualnych, u których zdiagnozowano wirus HIV – orzekł Trybunał w Strasburgu (wyrok w sprawie O.G. i inni przeciwko Grecji, skargi nr 71555/12 i 48256/13).

Nazwiska i fotografie skarżących oraz informacja, że są nosicielami wirusa HIV, zostały opublikowane na stronie policji i rozpowszechnione w mediach. Prokurator nie próbował ustalić, czy w ich sprawach można było podjąć inne środki, które zapewniłyby mniejszą ekspozycję medialną skarżących.

Źródło: Europejski Trybunał Praw Człowieka



fot. pixabay

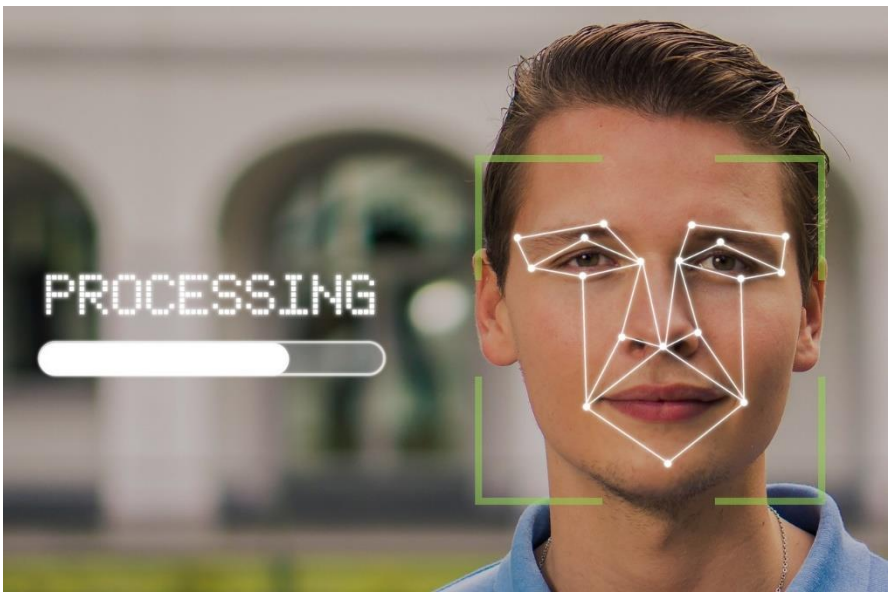
TSUE: WYROK WS. PRZECHOWYWANIA DANYCH BIOMETRYCZNYCH

Ogólne i niezróżnicowane przechowywanie aż do śmierci danych biometrycznych i genetycznych osób skazanych za umyślne przestępstwo jest sprzeczne z prawem Unii – orzekł TSUE (C-118/22 | Direktor na Glavna direktsia „Natsionalna politsia" pri MVR – Sofia).

W Bułgarii pewna osoba trafiła do rejestru policyjnego w czasie dochodzenia w sprawie złożenia fałszywych zeznań. Została za to skazana, karę odbyła i skorzystała z prawa do zatarcia skazania. W rejestrze policyjnym pozostały jednak jej dane: odciski palców, fotografie oraz próbki pobrane w celu ustalenia profilu DNA. Ich usunięcia nie przewiduje bułgarskie prawo – policja używa tych danych do sprawdzania, czy osoba już raz skazana nie popełniła kolejnego przestępstwa. Bułgarski naczelny sąd administracyjny, rozpatrujący skargę kasacyjną, skierował pytania do Trybunału Sprawiedliwości.

Trybunał orzekł, że bułgarskie przepisy wymagają zmiany. Chodzi o to, że nie każdy skazany stwarza takie samo ryzyko popełnienia innych przestępstw. Prawo Unii wymaga, aby uregulowanie krajowe przewidywało obowiązek okresowego przeglądu, czy przechowywanie danych jest nadal niezbędne, i przyznawało zainteresowanej osobie prawo do usunięcia tych danych, w razie gdyby tak już nie było.

Źródło: komunikat TSUE



fot. pixabay

FRANCUSKI ORGAN NADZORCZY UKARAŁ TAGADAMEDIA KARĄ W WYSOKOŚCI 75 000 EURO

Spółka Tagadamedia w swoim serwisie internetowym prowadziła konkursy i testy produktów, zbierając w ten sposób dane osobowe od potencjalnych klientów. Dane te były następnie przesyłane do partnerów spółki. Spółka twierdziła, że zbierała zgody na przetwarzanie danych. Jednak serwis internetowy zbudowany był tak, że sugerował użytkownikom udzielenie zgody. Nie było tu więc mowy o uzyskiwaniu zgody dobrowolnej, świadomej i jednoznacznej – tak jak stanowi RODO.

Francuski organ nadzorczy stwierdził tu dwa naruszenia RODO:

1. niedopełnienie obowiązku posiadania podstawy prawnej przetwarzania danych osobowych (art. 6 RODO);
2. niedopełnienie obowiązku wdrożenia rejestru czynności przetwarzania danych osobowych, (art. 30 RODO).

Dlatego nałożył na firmę Tagadamedia karę w wysokości 75 000 euro.

Źródło: komunikat EROD

fot. pixabay

HISZPAŃSKI ORGAN NADZORCZY PRZEDSTAWIŁ STRATEGIĘ DOTYCZĄCĄ NIELETNICH, ZDROWIA CYFROWEGO I PRYWATNOŚCI

29 stycznia 2024 r. hiszpański organ ochrony danych przedstawił strategię dotycząca osób małoletnich, zdrowia cyfrowego i prywatności.

Obejmuje ona:

- współpracę regulacyjną na rzecz kompleksowej ochrony małoletnich w internecie,
- wzmocnienie gwarancji praw małoletnich na szczeblu krajowym i międzynarodowym poziomie,
- oraz wykonywanie uprawnień w zakresie prowadzenia dochodzeń i karania nielegalnych i szkodliwych praktyk wobec małoletnich.

Organ będzie promować tworzenie aplikacji umożliwiających wdrożenie skutecznych systemów weryfikacji wieku w celu ochrony nieletnich przed dostępem do nieodpowiednich treści. Zamierza promować przyjęcie tych zasad w ramach UE.

Źródło: Komunikat hiszpańskiego organu nadzorczego

fot. pixabay

EUROPEJSKI INSPEKTOR OCHRONY DANYCH (EIOD) OCENIA WPŁYW NA PRYWATNOŚĆ ROZPORZĄDZENIA W CELU ZWALCZANIA PRZEMYTU MIGRANTÓW I HANDLU LUDŹMI

EIOD 23 stycznia 2024 r. opublikował opinię w sprawie rozporządzenia mającego na celu zacieśnienie współpracy policyjnej w związku z zapobieganiem przemytowi migrantów i handlowi ludźmi oraz działań Europolu (Agencji UE ds. Współpracy Organów Ścigania).

W rozporządzeniu istotny wpływ na dane osobowe i prywatność osób fizycznych mają cztery kwestie:

1. wzmożone przetwarzanie danych biometrycznych;
2. rola Europejskiej Agencji Straży Granicznej i Przybrzeżnej (Frontex) we współpracy z Europolem;
3. przekazywanie danych osobowych przez Europol do państw spoza UE/Europejskiego Obszaru Gospodarczego (EOG);
4. oraz wsparcie Europolu dla właściwych organów państw członkowskich UE. W opinii EIOD uwzględniono również ustalenia i bieżące prace w ramach jego działań nadzorczych dotyczących Europolu i Fronteksu.

EIOD postuluje osiągnięcie równowagi między pomocą UE w walce z nielegalną migracją a zapewnieniem bezpieczeństwa osób fizycznych i ich danych osobowych.

Europejski inspektor ochrony danych Wojciech Wiewiórowski komentuje: *„Walka z przemytem migrantów i handlem ludźmi jest ważnym celem leżącym w interesie ogólnym. Podkreślam jednak, że nie ma dowodów, że środki przewidziane w rozporządzeniu są rzeczywiście uzasadnione. Uważam brak oceny skutków dla ochrony danych za niepokojący, biorąc pod uwagę charakter danych osobowych – wrażliwych danych biometrycznych – i to, że dotyczą one osób wymagających szczególnego traktowania – imigrantów. EIOD uważa, że nie powinno to stanowić*

precedensu dla jakichkolwiek przyszłych przepisów mających porównywalny wpływ na podstawowe prawa do prywatności i ochrony danych".

W swoich zaleceniach EIOD zwraca uwagę na zagrożenia związane z przewidywanym wzrostem przetwarzania przez Europol danych biometrycznych, w tym rozpoznawania twarzy. Konieczne jest ustanowienie zabezpieczeń minimalizujących ryzyko nadużyć.

EIOD zauważa też, że rozporządzenie przewiduje ściślejszą współpracę między Europolem a Fronteksem. Dlatego należy doprecyzować rolę ograniczenia i procedury, jakich Frontex ma przestrzegać podczas wykonywania zadań wspierających Europol i Agencję UE ds. Współpracy Wymiarów Sprawiedliwości w Sprawach Karnych (Eurojust), a także organy ścigania państw członkowskich UE. Frontex nie powinien stać się organem ścigania – dodaje EIOD w swoich zaleceniach.

Rozporządzenie przewiduje przekazywanie danych osobowych poza UE/EOG przez Europol, w oparciu o odstępstwa (zwolnienia) od ogólnych zasad przekazywania danych osobowych. EIOD ostrzega, że stosowanie takich zwolnień nie powinno prowadzić do systematycznego, masowego lub strukturalnego przekazywania danych osobowych.

Źródło: Komunikat EIOD

fot. pixabay

EROD PRZEDSTAWI OPINIĘ NA TEMAT MODELU „ZGODA LUB ZAPŁATA”

Model „zgoda lub zapłata” to mechanizm, który polega na żądaniu od użytkowników opłaty w zamian za nieprzetwarzanie ich danych do celów reklamy behawioralnej. Austriacka organizacja noyb (skrót od ang. none of your business), założona przez Maxa Schremsa, jako pierwsza złożyła w tej sprawie skargę przeciwko Meta, która także korzysta z tego modelu.

Noyb zwraca uwagę, że Meta – jak argumentuje organizacja – świadomie obchodzi unijne przepisy.

Ponieważ problem staje się coraz bardziej powszechny organy ochrony danych z Norwegii, Holandii i Niemiec (Hamburg) zwróciły się do Europejskiej Rady Ochrony Danych o wydanie opinii w sprawie modelu „zgoda lub zapłata”, na podstawie art. 64 ust. 2 RODO.

Podczas 90. posiedzenia plenarnego, które odbyło się 13 lutego2024 r., Rada omówiła zakres wytycznych dotyczących modelu „zgoda lub zapłata”. Rada zgodziła się, że oprócz opinii potrzebne będą sukcesywnie opracowywane wytyczne o szerszym zakresie.

Źródło: komunikat norweskiego organu nadzorczego

fot. pixabay

POLSKIE CENTRUM AKREDYTACJI – KRAJOWY SYSTEM AKREDYTACJI

Tadeusz Matras, Kierownik Biura ds. Akredytacji, Polskie Centrum Akredytacji

Polskie Centrum Akredytacji (PCA) jest krajową jednostką akredytującą upoważnioną do akredytacji jednostek oceniających zgodność na podstawie ustawy o systemach oceny zgodności i nadzoru rynku. PCA nadzoruje spełnienie przez te jednostki wymagań i warunków akredytacji. Posiada status państwowej osoby prawnej i jest nadzorowane przez ministra właściwego do spraw gospodarki. Zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (WE) nr 765/2008 z 9 lipca 2008 r., PCA jest jedyną uznaną krajową jednostką akredytującą, która została upoważniona do realizacji działalności akredytacyjnej w kraju i reprezentowania Polski w organizacjach regionalnych i międzynarodowych w tej dziedzinie.

Do najważniejszych zadań PCA należy prowadzenie procesów akredytacji i sprawowanie nadzoru nad jednostkami oceniającymi zgodność, tj.: laboratoriami badawczymi, laboratoriami wzorcującymi, laboratoriami medycznymi, organizatorami badań biegłości, producentami materiałów odniesienia, jednostkami inspekcyjnymi, jednostkami certyfikującymi wyroby, procesy i usługi (w tym działającymi w obszarach, takich jak ochrona danych osobowych), jednostkami certyfikującymi systemy zarządzania, jednostkami certyfikującymi osoby, weryfikatorami EMAS i weryfikatorami rocznych raportów emisji gazów cieplarnianych oraz biobankami.

Akredytacja a ocena zgodności

Akredytacja udzielana przez PCA służy formalnemu wykazaniu kompetencji jednostek oceniających zgodność do wykonywania określonych zadań. Akredytacja stanowi integralną część ogólnoświatowego systemu obejmującego ocenę zgodności i nadzór rynku. PCA, tak jak każda inna jednostka akredytująca, działa w procesie jako strona trzecia. Jest niezależna i bezstronna, a oceny są prowadzone zgodnie z wymaganiami międzynarodowej normy PN-EN ISO/IEC 17011

w odniesieniu do wymagań ustalonych i powszechnie przyjętych międzynarodowych norm akredytacyjnych oraz mających zastosowanie sektorowych wymagań, np. określonych w mających zastosowanie przepisach prawa.

Akredytacje udzielane przez PCA są powszechnie uznawane w Europie i na świecie. Jest to związane z porozumieniami o wzajemnym uznawaniu wyników akredytowanej działalności w ramach: EA (European co-operation for Accreditation) oraz dwóch organizacji o zasięgu światowym: ILAC (International Laboratory Accreditation Cooperation) i IAF (International Accreditation Forum), których PCA jest sygnatariuszem. Dzięki podpisanym porozumieniom certyfikat PCA jest uznawany praktycznie na całym świecie. Wyniki akredytowanej przez PCA działalności (raporty, certyfikaty) są przepustką dla swobodnego przepływu towarów i usług w wymianie i handlu międzynarodowym. System akredytacji wzmacnia zaufanie do kompetencji jednostek oceniających zgodność i – w konsekwencji – do wydawanych przez nie certyfikatów i raportów.

Wiarygodność podstawą akredytacji

Akredytacja i system oceny zgodności różnią się zasadniczo od innych systemów autoryzacji, licencjonowania lub innych form upoważnień.

Istotą akredytacji nie jest weryfikacja spełniania określonych wymagań kompetencyjnych podczas procesu oceny akredytacyjnej.

Podstawą wiarygodności systemu oceny zgodności jest stały nadzór nad akredytowanymi jednostkami oceniającymi zgodność, poprzez coroczne oceny w nadzorze i nadzór doraźny. Takie podejście prowadzi do stałego doskonalenia akredytowanych jednostek oceniających zgodność. Zapewnienia wiarygodność działań technicznych tych jednostek.

Korzyści z akredytacji

Akredytacja buduje publiczne zaufanie do standardów i wymogów jakościowych. Akredytowane usługi oceny zgodności promują wymagania jakościowe (w obszarze regulowanym i dobrowolnym) oraz pozwalają weryfikować ich spełnianie. Szeroki zakres akredytacji udzielanych przez PCA odzwierciedla w szczególności zapotrzebowanie na akredytowane usługi ze strony regulatorów i zainteresowanych stron, praktycznie we wszystkich obszarach administracji rządowej i sektora publicznego. Organy regulacyjne współpracując z PCA zyskują zaufanego i doświadczonego partnera oraz dostęp do uznanej na całym świecie i ugruntowanej usługi akredytacji.

7 WSPÓŁPRACA Z UODO

We wszystkich obszarach sprawowanego systemu akredytacji PCA ma udokumentowane doświadczenie i skuteczne narzędzia, które mogą ułatwić realizację polityki i celów administracji rządowej i wspierać zrównoważony rozwój rynku. Akredytacja wspiera innowacje, pomagając w generowaniu zaufania publicznego do nowych obszarów działalności.
Niezależnie od tego, czy akredytacja jest częścią regulacji prawnych, czy funkcjonuje w ramach systemów dobrowolnych, PCA zapewnia, że odpowiednie normy lub kryteria jakości mogą być zweryfikowane i potwierdzone przez niezależną sieć akredytowanych jednostek oceniających zgodność.

Akredytacja do celów RODO

PCA, w ramach sprawowanego systemu akredytacji udziela akredytacji jednostkom certyfikującym wyroby, procesy i usługi według zasad, i zgodnie z procesami opisanymi w programie akredytacji DACW-01 *Akredytacja jednostek certyfikujących wyroby.*

Akredytacja jednostek certyfikujących w zakresie ochrony danych osobowych (na potrzeby RODO) będzie realizowana przez PCA w ramach ww. programu akredytacji w odniesieniu do wymagań normy akredytacyjnej EN ISO/IEC 17065 *Ocena zgodności – Wymagania dla jednostek certyfikujących wyroby, procesy i usługi.*

W akredytacji do celów RODO, dodatkowo będą stosowane wymagania dla jednostek certyfikujących określone w rozporządzeniu, w tym wymagania określone przez organ nadzorczy. Przedmiotowa akredytacja, tak jak pozostała działalność akredytacyjna PCA, jest realizowana zgodnie z zasadami i warunkami dotyczącymi udzielania i utrzymywania akredytacji określonymi przez PCA zgodnie z wymaganiami normy PN-EN ISO/IEC 17011. Zasady i warunki akredytacji są określone w dokumentach PCA i są dostępne na stronie internetowej www.pca.gov.pl w zakładce Publikacje / PCA. Podstawowe regulacje, mające zastosowanie w odniesieniu do wszystkich jednostek oceniających zgodność (ubiegających się lub posiadających akredytację), są przedstawione w dokumencie DA-01 *Opis systemu akredytacji*. Dokument opisuje zarówno sam proces akredytacji, jak również określa mające zastosowania wymagania akredytacyjne, w powiązaniu z określonymi programami akredytacji.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl