URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 12/12/23

www.uodo.gov.pl

SPIS TREŚCI

WPROWADZENIE

Jan Nowak, Prezes Urzędu Ochrony Danych Osobowych S. 2

Jakub Groszkowski, Zastępca Prezesa Urzędu Ochrony Danych Osobowych S. 3

1. ROZMOWA Z EKSPERTEM

Adam Sanocki, Dyrektor Departamentu Komunikacji Społecznej, Rzecznik Prasowy UODO S. 4

2. WYBRANE DECYZJE UODO

Adnotacja o stanie zdrowia na skierowaniu stanowi naruszenie przepisów o ochronie danych osobowych S. 8

3. UODO SYGNALIZUJE

1,5 proc. dla OPP S. 10

4. NARUSZENIA I KONTROLE

Przewodnik Agencji Praw Podstawowych po prawach osób w systemie Euroda S. 11

5. NOWE TECHNOLOGIE

VR - jak bezpiecznie korzystać z wirtualnej rzeczywistości? S. 13

6. SPRAWY MIĘDZYNARODOWE

TSUE potwierdza, że VIN pojazdu może być daną osobową S. 15

Projekt aktu w sprawie sztucznej inteligencji - Opinia EIOD S. 16

Francuski organ nadzorczy nałożył karę na GROUPE CANAL+ S. 17

TSUE: Administrator musi bezpłatnie przekazać pacjentowi pierwszą kopię jego danych S. 18

7. WSPÓŁPRACA Z UODO

Ochrona danych osobowych – wyzwania 2024 S. 19

Praktyczne aspekty monitorowania kodeksu postępowania dla sektora ochrony zdrowia przez akredytowany podmiot monitorujący S. 22

Szanowni Państwo!

Święta Bożego Narodzenia to moment, w którym na chwilę zwalniamy – spędzając go z bliskimi, obdarowując się czasem, uwagą i prezentami. To sposobność do rodzinnych i osobistych przemyśleń. Dla mnie tegoroczne Święta będą wyjątkowe, bo zbiegają się one z pożegnaniem z Urzędem Ochrony Danych Osobowych, miejscem mi wyjątkowo bliskim, w którym spędziłem kilkanaście lat i zawsze będę o nim myślał z sentymentem. To okazja, by podziękować wszystkim pracownikom za ich pracowitość, kompetencje i zaangażowanie w pomoc obywatelom w sprawach dotyczących ochrony danych osobowych. Urząd działa skutecznie i jest blisko obywateli, właśnie dzięki inicjatywom i aktywnej postawie swoich pracowników – doskonałych ekspertów, zasilających kadry UODO. Wielu z nich pracuje tu od początku powstania biura Generalnego Inspektora Ochrony Danych Osobowych – ich dwudziestokilkuletni staż pracy i kwalifikacje przekładają się na efektywne funkcjonowanie Urzędu. Czego chciałbym życzyć Urzędowi Ochrony Danych Osobowych i mojemu następcy z okazji nadchodzących Świąt i nowej kadencji? W pierwszej kolejności na pewno wzmocnienia finansowego, dodatkowych środków w budżecie, by odciążyć pracowników i zatrudnić więcej osób, co usprawniłoby jego pracę na rzecz społeczeństwa. W ciągu 12 miesięcy do Urzędu samych skarg i naruszeń wpływa ok 20 tys., a przecież Urząd zajmuje się także innymi sprawami. Życzę także powstania skutecznych regulacji nadążającymi za innowacjami, które stawiają na pierwszym miejscu dobro i prawa człowieka, tworzenia kodeksów dobrych praktyk, wytycznych, cennych z punktu widzenia danych osobowych, które powinny powstawać zarówno na poziomie europejskim, jak i krajowym. Życzę Urzędowi także owocnej współpracy z innymi organami oraz by wykładnia prawa – orzecznictwo i decyzje organów nadzorczych – pozwalały obecnie obowiązujące przepisy interpretować w taki sposób, żeby odpowiadały potrzebom rynku i respektowały prawa obywateli. W tym miejscu chciałbym również pogratulować nie tylko Urzędowi, ale i obywatelom, że są coraz bardziej świadomi swoich praw, więc ich oczekiwania wobec UODO narastają – i powiem przewrotnie – bardzo mnie to cieszy. Świadczy to również o naszym sukcesie edukacyjnym. Wydawane przez nas komunikaty, Biuletyn UODO, działania m.in. w szkołach, takie jak ogólnopolski program „Twoje dane – Twoja sprawa", uświadamiający młodzież, stworzenie Instytutu Prawa Ochrony Danych Osobowych wywierają wpływ na świadomość społeczeństwa. Oczywiście pozostawia to też ślad w narastającej liczbie składanych skarg i naruszeń, ale chcemy przecież żyć w społeczeństwie świadomym swoich praw. Jako Prezes tego Urzędu, zawsze stałem po stronie człowieka i jego prawa do ochrony danych osobowych i prywatności. Bardzo dziękuję wszystkim, którzy razem ze mną budowali to miejsce w trosce o dane obywateli i życzę nowemu Prezesowi wdrożenia skutecznych środków, by mógł zmierzyć się z nadchodzącymi wyzwaniami jakie czekają UODO.

Jan Nowak

Prezes Urzędu Ochrony Danych Osobowych

Szanowni Państwo!

Zanim zaczną się Święta Bożego Narodzenia i choć na moment w każdym domu zatrzyma się czas, Urząd Ochrony Danych Osobowych, jak co roku, pracuje bez wytchnienia do ostatniej chwili. Jak Państwo wiecie, przedświąteczny okres obfitował w liczne wydarzenia z zakresu ochrony danych osobowych. Takie incydenty jak podsłuchy sieci jednej z aptek czy wyciek danych z firmy ALAB wymagały szybkiej reakcji Urzędu. Między innymi dlatego podjęliśmy decyzje, by połączyć siły z innymi instytucjami i wzajemnie wesprzeć się w realizacji ustawowych zadań. Efektem współpracy Urzędu z innymi organami były podpisane przez nas porozumienia z Głównym Inspektorem Farmaceutycznym i Naczelną Izbą Pielęgniarek i Położnych. Jesteśmy świadomi, że wzmożone wysiłki obu stron przełożą się na opracowanie w przyszłości rekomendacji, które pozwolą ograniczyć ryzyka związane z poważnymi naruszeniami ochrony danych, jak i niwelować ich skutki. Porozumienia są też doskonałym ogniwem, łączącym organy we wspólnych aktywnościach, umożliwiających wymianę wiedzy, informacji i doświadczeń, służących do wypracowania w przyszłości spójnych i przemyślanych przepisów z zakresu ochrony danych osobowych. Z radością informuję Państwa, że Prezes Urzędu Ochrony Danych Osobowych zatwierdził Dodatkowe wymogi akredytacji podmiotów certyfikujących. W oparciu o ten dokument będzie dokonywana akredytacja podmiotów certyfikujących, których zadaniem jest weryfikacja zgodności operacji przetwarzania danych osobowych prowadzonych przez administratorów i podmioty przetwarzające. Certyfikacja ma na celu zwiększenie przejrzystości i poprawę przestrzegania norm ochrony danych osobowych z uwzględnieniem specyfiki branży. Kolejnym wydarzeniem, o którym nie sposób nie wspomnieć jest zatwierdzenie przez Prezesa Urzędu Ochrony Danych Osobowych „Kodeksu postępowania dla sektora ochrony zdrowia" przygotowanego przez Polską Federację Szpitali. Nie bez powodu jesteśmy z niego bardzo dumni – podpisany dokument to pierwszy w Europie kodeks obejmujący podmioty publiczne i prywatne z sektora medycznego. Kodeks stanowi ważny krok w zapewnieniu cyberbezpieczeństwa oraz ochrony danych osobowych dla sektora zdrowia. Chciałbym zatrzymać się też na moment przy programie „Twoje dane – Twoja sprawa". To już XIV edycja przedsięwzięcia, którym chętnie się chwalimy z uwagi na jego siłę edukacyjną. Ta inicjatywa poszerza wiedzę na temat danych osobowych nie tylko wśród najmłodszych, ale również uświadamia rady pedagogiczne czy koordynatorów programu, tworzących sieci wsparcia dla dzieci i innych nauczycieli w zakresie ochrony danych osobowych. Wierzymy, że ta międzypokoleniowa sztafeta, jaką budują szkoły, biorące udział w programie, znacząco podnosi poziom znajomości materii danych osobowych. Tegoroczna edycja jest rekordowa pod względem frekwencji, biorą w niej udział aż 303 szkoły i instytucje edukacyjne. Na koniec pozostaje mi podziękować wszystkim zaangażowanym w powyższe działania stronom, przede wszystkim pracownikom Urzędu Ochrony Danych Osobowych, którzy odgrywają kluczową rolę w poszerzaniu wiedzy z zakresu ochrony danych osobowych w Polsce, a Państwu – naszym wiernym czytelnikom, życzę miłej lektury grudniowego biuletynu oraz spokojnych, radosnych Świąt.

Jakub Groszkowski

Zastępca Prezesa Urzędu Ochrony Danych Osobowych

1 ROZMOWA Z EKSPERTEM

KOMUNIKUJEMY SIĘ NA RÓŻNE SPOSOBY

Z Adamem Sanockim, Dyrektorem Departamentu Komunikacji Społecznej oraz Rzecznikiem Prasowym UODO rozmawiał Karol Witowski.

Jaki to był rok dla Departamentu Komunikacji Społecznej?

Bardzo pracowity. Departament Komunikacji Społecznej realizuje szereg działań takich jak: Infolinia UODO, relacje z mediami, w tym odpowiedzi na pytania dziennikarzy, tworzenie informacji prasowych, tekstów problemowych czy poradnikowych. Stale rozwijamy własne kanały komunikacji jak strona internetowa czy Biuletyn UODO. Tworzymy też własne treści wideo, wspieramy komunikacyjnie wszystkie działania edukacyjne, porozumienia i partnerstwa, a także uczestniczymy w organizacji konferencji i innych wydarzeń zarówno w przestrzeni online jak i offline. Zdajemy sobie sprawę, że dzisiejsza komunikacja, aby była skuteczna musi być wielokanałowa, a treści ważne i atrakcyjne stają się potrzebne. W tym roku poza zmianą strony internetowej i rozwojem naszego Biuletynu dużym wyzwaniem była bieżąca obsługa pytań od dziennikarzy, których było nie tylko więcej niż rok wcześniej, ale i często dotyczyły bardzo aktualnych spraw i wymagały szybkiej reakcji oraz sprawnej współpracy z departamentami merytorycznymi. Ponadto jako, że UODO jest bardzo aktywne na polu edukacyjnym, to Departament Komunikacji Społecznej z dużym zaangażowaniem wspierał wydarzenia takie jak webinaria, konferencje, czy szkolenia. Wiele z tych wydarzeń można po ich zakończeniu prześledzić dzięki nagraniom transmisji online, które przygotowywane są do publikacji właśnie w DKS. Co istotne nagrania te spełniają wymogi dostępności cyfrowej, a więc osoby ze specjalnymi potrzebami (np. niesłyszące) są w stanie zapoznać się z wiedzą, którą dzielą się eksperci UODO i zaproszeni goście.

Jaką funkcję pełni infolinia w urzędzie i dla kogo jest przeznaczona?

Infolinia Urzędu to bardzo ważne i intensywnie wykorzystywane narzędzie zarówno na zewnątrz jak i wewnątrz Urzędu. Jest czynna od poniedziałku do piątku w godzinach 10 -14, to znacznie dłużej niż w innych krajach zrzeszonych w ramach EROD. Tworzy ją zespół osób wyspecjalizowanych w ochronie danych osobowych, którzy nieustannie szkolą się zarówno pod kątem merytorycznym, jak i z tzw. miękkich aspektów, tak ważnych w pracy z ludźmi.

1 ROZMOWA Z EKSPERTEM

W tym roku, do końca listopada, pracownicy infolinii odebrali ponad 13 tys. telefonów, co daje średnio ponad 60 rozmów dziennie. To bardzo dużo, zwłaszcza, że duży odsetek rozmów to pomoc w rozwiązywaniu skomplikowanych problemów. O poradę proszą bowiem nie tylko osoby fizyczne, ale i inspektorzy ochrony danych, pracownicy instytucji publicznych czy prawnicy. Infolinia to ważny dla Urzędu kanał komunikacji ze społeczeństwem i rynkiem. Jest swojego rodzaju papierkiem lakmusowym. To właśnie z tego kanału dowiadujemy się często o naruszeniach czy wyciekach danych, także o oczekiwaniach i problemach społeczeństwa. Często zmieniamy np. priorytety działań po telefonach na infolinię. To także nieocenione źródło wiedzy przy doborze wartościowych tematów podczas organizowanych przez nas konferencji czy webinariów.

Biuletyn UODO mocno się zmienił od czasu pierwszych numerów. Czy nadal jest wydawnictwem skierowanym do inspektorów ochrony danych?

Biuletyn UODO prężnie się rozwija, mamy ponad 11500 subskrybentów i liczba ta sukcesywnie rośnie. Przez ostatni rok zyskaliśmy ponad dwa tysiące nowych czytelników zainteresowanych regularnym sięganiem po nasz periodyk. Wydawnictwo powstaje od kwietnia 2019 roku, na początku był to kilkustronicowy Newsletter, teraz jest w zasadzie magazynem – cieszącym się bardzo dużą i wciąż rosnącą popularnością. Przez ten czas mocno się zmienił, doszły stałe rubryki przyporządkowane poszczególnym Departamentom Urzędu, a także Partnerom i gościom z zewnątrz. Natomiast cel jego powstawania jest niezmienny i pozostaje nim podnoszenie wiedzy IOD, co stanowi jeden z priorytetów Prezesa Urzędu Ochrony Danych Osobowych. Naszym zdaniem rola inspektorów jest kluczowa dla funkcjonowania systemu ochrony danych osobowych. W pierwotnych założeniach był to newsletter wyłącznie dla IOD-ów, ale obecnie wydawnictwo dociera do znacznie szerszej grupy osób zainteresowanej tematyką ochrony danych osobowych. Często tematy poruszane na łamach naszego wydawnictwa są początkiem ważnej dyskusji. Na przykład po opublikowanym w tegorocznym, listopadowym numerze artykule o nagrywaniu rozmów z interesantami przez urzędy, pojawiła się w przestrzeni publicznej poważna dyskusja na ten temat. W tej kwestii Biuletyn był cytowany w mediach kilkadziesiąt razy, w tym przez popularne ogólnopolskie tytuły. To duży sukces dla tak specjalistycznego periodyku. Podkreślę też ekskluzywny charakter materiałów jakie publikujemy w Biuletynie. Nie pojawiają się tu przedruki tekstów umieszczanych na stronie internetowej UODO. Biuletyn i strona się uzupełniają, nie kanibalizują. Bardzo cenimy też współpracę z Partnerami z zewnątrz, którzy za naszym pośrednictwem mogą przedstawić także swoje działania czy specjalistyczną wiedzę z zakresu ochrony danych osobowych. Brand journalism to już zakorzeniony trend w komunikacji, cieszę się że w tym aspekcie z Biuletynem UODO osiągnęliśmy spory sukces.

UODO publikuje także raporty z badań rynku. Czego one dotyczą?

Do tej pory zrealizowaliśmy trzy edycje badań we współpracy z Krajowym Rejestrem Długów

i serwisem ChronPESEL.pl pt. „Wiedza na temat bezpieczeństwa ochrony danych osobowych w Polsce". To bardzo dobra współpraca, której efektem są nie tylko ciekawe raporty i webinaria, ale przede wszystkim wiedza od naszej jakże ważnej grupy docelowej jaką są osoby fizyczne. Ta wiedza wspiera nas w realizacji misji Urzędu jaką jest edukacja.
W przyszłym roku także wspólnie z naszymi Partnerami, czyli Krajowym Rejestrem Długów i serwisem ChronPESEL.pl będziemy dodatkowo realizować badanie na temat ochrony danych osobowych w małych i średnich przedsiębiorstwach. To pierwsze tego typu opracowanie dotyczące tego jakże istotnego sektora, będącego nie tylko kluczową gałęzią gospodarki, ale i zatrudniająca mnóstwo osób w naszym kraju.

Jak wygląda zainteresowanie mediów tematyką ochrony danych osobowych? Czy trudno jest się przebić do mediów z tematami, którymi zajmuje się UODO?
Generalnie tematyka ochrony danych osobowych jako niezwykle interdyscyplinarna dziedzina jest potencjalnie interesująca dla każdego, jednak to zainteresowanie przybiera nieco inne oblicze w przypadku różnych mediów. Mamy świadomość, że inaczej musimy komunikować się z różnymi grupami docelowymi. Media opiniotwórcze interesują się głównie głośnymi naruszeniami, wyciekami danych, decyzjami karowymi czy też współpracą UODO z innymi organami. Są też media specjalizujące się w tej tematyce i tam znacznie szerzej omawiamy materię. Przedstawiciele tych mediów są znacznie bardziej zainteresowani aspektami prawnymi i „smaczkami" związanymi z orzecznictwem. Muszę pochwalić dziennikarzy, jest wśród nich grupa specjalizująca się w tematyce ochrony danych. To ludzie mający bardzo dużą wiedzę, zadający ciekawe pytania i przede wszystkim rozumiejący ten trudny obszar. Fakt rosnącej w społeczeństwie świadomości tematów związanych z ochroną danych osobowych jest w dużym stopniu zasługą właśnie świadomych dziennikarzy, którzy skutecznie przekazują wiedzę swoim odbiorcom. Warto nadmienić, że od początku roku do końca listopada otrzymaliśmy prawie 400 pytań z mediów. Na wszystkie staramy się odpowiadać tak szybko jak to możliwe, robimy też wszystko, aby odpowiedzi były precyzyjne i kompletne. Media to ważny kanał komunikacji ze społeczeństwem.

W tym roku powstał Instytut Prawa Ochrony Danych Osobowych? Czym on jest i jakie cele będzie realizował?
IPODO to pierwszy w Polsce instytut zajmujący się zagadnieniami ochrony danych osobowych, który powstał pod patronatem i we współpracy z Urzędem Ochrony Danych Osobowych. Jego celem jest przede wszystkim zwiększenie świadomości społeczeństwa na temat prawa ochrony danych oraz propagowanie najlepszych praktyk i rozwiązań w zakresie przetwarzania i ochrony danych. Będą one realizowane poprzez badania, publikacje raportów, edukację, szeroko rozumiane doradztwo oraz współpracę z innymi instytucjami naukowymi w procesach tworzenia regulacji prawnych w dziedzinie ochrony danych. Instytut tworzy zespół ekspertów, praktyków oraz naukowców mających duży

wpływ na powstanie i kształtowanie się systemu ochrony danych w Polsce. Poza własnymi działaniami IPODO wspiera też inne instytucje i organizacje zajmujące się ochroną prywatności. Brakowało ośrodka naukowego, który jest dedykowany tematyce ochrony danych w takim szerokim aspekcie i będącym w tak ścisłej współpracy z regulatorem.

Minął rok od powstania nowej strony internetowej Urzędu. Jak minął jej proces adaptacji?
Poprzednia strona funkcjonowania wiele lat, jednak odświeżenia wymagała zarówno jej szata graficzna, jak i projekt funkcjonalny. Wiele materiałów należało zaktualizować. Dokonaliśmy przeglądu treści również pod kątem retencji danych osobowych w nich zawartych, co także wpłynęło na decyzję o zmianach i ograniczeniu dotychczasowych zasobów. Ponadto strona UODO jest jednocześnie Biuletynem Informacji Publicznej Urzędu, co ma wpływ na poblokowane tam treści. Dlatego od 1 stycznia br. funkcjonuje nowa strona internetowa Urzędu Ochrony Danych Osobowych, która jest oparta na innej formule. Przede wszystkim widzimy na niej jasny podział na sekcje dedykowane naszym grupom docelowym, jak: obywatele, administratorzy czy IOD. Jest też sekcja „załatw sprawę", która grupuje w jednym miejscu najważniejsze formularze. Obecnie więcej materiałów o charakterze problemowym czy poradnikowym jest publikowanych w wydawanym Biuletynie UODO i gorąco zachęcamy do jego subskrypcji, szczególnie tych którzy chcą być na bieżąco z problematyką ochrony danych osobowych.
Strona UODO jest też jednym z kilku kanałów informowania o działalności Urzędu i z wymienionych wcześniej względów nie może być na niej „wszystkiego". Powinna być czytelna i aktualna i ten cel udało nam się osiągnąć. Dodatkowym szczegółowym uzupełnieniem komunikacji UODO z obywatelami jest wspominany Biuletyn czy infolinia, gdzie zarówno osoby fizyczne, jak i inspektorzy ochrony danych mogą uzyskać informacje na nurtujące ich szczegółowe pytania.

UODO współpracuje intensywnie z EROD. Jaki udział w tej współpracy ma Departament Komunikacji Społecznej?
Jesteśmy częścią sieci Communication Network, skupiającej rzeczników prasowych organów nadzorczych zrzeszonych w ramach EROD. Prowadzimy w związku z tym prace wspólnie z innymi zespołami lokalnymi. Nasz departament uczestniczy też w spotkaniach roboczych, gdzie szczegółowo omawiane są działania komunikacyjne europejskich organów. Taka współpraca jest szczególnie istotna, w sprawach transgranicznych, ale także inspiruje do aktywności, które realizowane są w różnych krajach lub wspólnie.

ADNOTACJA O STANIE ZDROWIA NA SKIEROWANIU STANOWI NARUSZENIE PRZEPISÓW O OCHRONIE DANYCH OSOBOWYCH

Zakres danych, który należy wskazać w treści skierowania nie obejmuje informacji o stanie zdrowia, a dane dotyczące rodzaju badań profilaktycznych są nadmiarowe dla pracodawcy, do przetwarzania których nie jest uprawniony. Tak stwierdził organ nadzorczy po rozpatrzeniu skargi, jaka do niego wpłynęła, uznając, że działanie spółki polegające na umieszczeniu kwestionowanych przez skarżącą adnotacji na drukach skierowań stanowiło naruszenie przepisów RODO.

Do Urzędu Ochrony Danych Osobowych wpłynęła skarga związana z wątpliwościami co do zakresu danych umieszczonych na skierowaniu, na kontrolne badania lekarskie, wystawionym przez pracodawcę. Skarżąca znajdowała się przez okres ponad 30 dni na zwolnieniu lekarskim. Zgodnie z obowiązującymi przepisami prawa, w przypadku niezdolności do pracy spowodowanej chorobą, trwającą dłużej niż 30 dni, pracownik podlega kontrolnym badaniom lekarskim w celu ustalenia zdolności do wykonywania pracy na dotychczasowym stanowisku (art. 229 § 2 kodeksu pracy). Na wystawionym dla skarżącej skierowaniu zamieszczono adnotację, w której jako przyczynę jej niezdolności do pracy podano zły stan psychiczny i wskazano, że zwolnienie lekarskie zostało wystawione przez lekarza psychiatrę. W adnotacji zawarto również prośbę o skierowanie badanej na konsultację psychologiczną lub psychiatryczną. Skarżąca zażądała usunięcia wskazanych danych oraz wniosła skargę do organu nadzorczego.

Pracodawca, spółka z sektora medycznego, tłumaczyła, że skarżąca z własnej inicjatywy informowała go z jakiego rodzaju leczenia specjalistycznego korzysta, a zamieszczenie tego rodzaju adnotacji było uzasadnione rodzajem zadań i zakresem odpowiedzialności związanych z zajmowanym przez nią stanowiskiem. Spółka wskazała również, że w jej organizacji czynności formalno-prawne są wykonywane za pośrednictwem Działu Kadr, Płac i Szkoleń. Skierowanie na badania kontrolne zostało wystawione przez spółkę i przekazane skarżącej przez kierownika ww. działu.

Zakres danych zamieszczonych na skierowaniu jest ściśle określony

Przechodząc do analizy prawnej badanej sprawy organ nadzorczy przypomniał, że przetwarzanie danych osobowych powinno spełniać pewne ściśle określone warunki, wymienione w art. 6 ust. 1, a w przypadku danych szczególnej kategorii, w tym danych dotyczących zdrowia, wskazane w art. 9 ust. 2 RODO. Prezes UODO wyjaśnił następnie, że kwestia pracowniczych badań profilaktycznych unormowana została m.in. w przepisach ustawy z dnia 26 czerwca 1974 r. Kodeks pracy oraz w rozporządzeniu Ministra Zdrowia i Opieki Społecznej z dnia 30 maja 1996 r.

w sprawie przeprowadzania badań lekarskich pracowników, zakresu profilaktycznej opieki zdrowotnej nad pracownikami oraz orzeczeń lekarskich wydawanych do celów przewidzianych w Kodeksie pracy. Rozporządzenie Ministra Zdrowia i Opieki Społecznej zawiera dokładne określenie zakresu danych, jakie powinny zostać zamieszczone w skierowaniu. W załączniku do rozporządzenia zamieszczono również wzór skierowania na badania profilaktyczne.

Pracodawca nie jest uprawniony do podawania danych o stanie zdrowia

Organ nadzorczy uznał, że zakres danych, który należy wskazać w treści skierowania nie obejmuje informacji o stanie zdrowia (w tym o stanie zdrowia psychicznego), a dane dotyczące rodzaju badań profilaktycznych są nadmiarowe dla pracodawcy, do przetwarzania których nie jest uprawniony. Przepisy nie umożliwiają bowiem pracodawcy weryfikacji rodzaju przeprowadzanych badań czy ich wyników i zezwalają tylko na wydanie pracodawcy zaświadczenia o braku przeciwwskazań lub też o przeciwwskazaniach zdrowotnych danego pracownika do pracy na określonym stanowisku.
Tym samym organ nadzorczy uznał, że działanie spółki polegające na umieszczeniu kwestionowanych przez skarżącą adnotacji na drukach skierowań nie znajdowało uzasadnienia w przepisach RODO i stanowiło naruszenie art. 9 ust.2 RODO w zw. z art. 5 ust.1 lit. a RODO.

Nieupoważniony nie powinien upoważniać

Wątpliwości Prezesa UODO wzbudziła również kwestia przetwarzania danych osobowych skarżącej przez kierownika Działu Kadr i Płac na podstawie udzielonego przez pracodawcę upoważnienia. Zgodnie z art. 29 RODO każda osoba działająca z upoważnienia administratora i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenie administratora, a z udzielonego upoważnienia powinien wprost wynikać zakres przetwarzanych danych osobowych oraz cel ich przetwarzania. Zdaniem organu nadzorczego upoważnienie udzielone kierownikowi nie spełniało tych warunków i tym samym, zostało udzielone z naruszeniem art. 29 RODO. Organ zauważył jednocześnie, że administrator, który udzielił powyższego upoważnienia, sam nie był upoważniony do ich przetwarzania.
Organ nadzorczy, w wydanej decyzji administracyjnej, uznał, iż spółka naruszyła przepisy o ochronie danych osobowych poprzez przetwarzanie danych osobowych bez podstawy prawnej oraz poprzez ich udostępnienie osobie nieuprawnionej. Korzystając z uprawnień naprawczych, jakie zapewnia art. 58 ust. 2 RODO, Prezes UODO nakazał usunięcie danych osobowych skarżącej, utrwalonych na drukach skierowań na kontrolne badania lekarskie. Udzielił też administratorowi upomnienia za naruszenie art. 9 ust. 1 polegające na przetwarzaniu danych osobowych skarżącej dotyczących zdrowia bez podstawy prawnej, w tym ich udostępnienie na rzecz osoby nieuprawnionej.

1,5 PROC. DLA OPP

Przed nami okres rozliczeniowy podatku dochodowego za rok 2023. Wielu podatników przekaże kwotę 1,5 proc. należnego podatku na organizację pożytku publicznego (OPP).
Przy tej okazji Prezes UODO przypomina, że jeżeli podatnik w rozliczeniu rocznym wyraził zgodę na przekazanie jego danych organizacji, to może ona je przetwarzać np. po to, by podziękować darczyńcy w imieniu obdarowanego.

Przy wypełnianiu formularza, podatnik może wyrazić zgodę na przekazanie organizacji pożytku publicznego swojego imienia, nazwiska, adresu oraz informacji o darowanej kwocie. Podatnik może także zgodzić się na przekazanie takich danych kontaktowych jak numer telefonu czy adres e-mail.
Dane osobowe darczyńców 1,5 proc. podatku przekazywane są organizacji pożytku publicznego przez naczelników urzędów skarbowych. Uprawnia ich do tego art. 45c ust. 5 ustawy z 26 lipca 1991 r. o podatku dochodowym od osób fizycznych oraz art. 21b ustawy z dnia 20 listopada 1998 roku o zryczałtowanym podatku dochodowym od niektórych przychodów osiąganych przez osoby fizyczne (ustawa o ryczałcie).
Należy podkreślić, że OPP może przetwarzać dane darczyńcy np. po to, aby mu podziękować. Podstawą do podjęcia takiego działania jest art. 6 ust. 1 lit. f RODO, czyli prawnie uzasadniony interes administratora. Zatem organizacja pożytku publicznego staje się administratorem danych, a tym samym decyduje o celach przetwarzania danych.
Na OPP jako na administratorze ciążą liczne obowiązki wynikające z przepisów ogólnego rozporządzenia o ochronie danych osobowych (RODO). Podstawowym jest obowiązek informacyjny, który oznacza, że OPP przy pierwszym możliwym kontakcie powinna poinformować darczyńcę o przysługujących mu prawach.
W tym miejscu warto także zaakcentować, że dane podatnika mogą być jedynie przetwarzane przez wskazaną w zeznaniu podatkowym organizację. Informacja ta ma szczególne znaczenie w przypadku, gdy środki z 1,5 proc.% podatku trafiają na konto konkretnych osób, podopiecznych fundacji czy stowarzyszeń. Prezes UODO informuje, że organizacja pożytku publicznego nie ma jednak żadnych podstaw prawnych do udostępnienia danych darczyńców osobom obdarowanym, chyba że pozyskana byłaby na ten cel uprzednia zgoda.
Na podstawie materiału źródłowego: **https://archiwum.uodo.gov.pl/pl/138/1387**

PRZEWODNIK AGENCJI PRAW PODSTAWOWYCH PO PRAWACH OSÓB W SYSTEMIE EURODAC

Agencja Praw Podstawowych opublikowała dokument, w którym omawia środki, jakimi mogą posłużyć się Państwa Członkowskie, by wyegzekwować obowiązek dostarczenia odcisków palców przez osoby ubiegające się o azyl i migrantów o nieuregulowanym statusie w systemie Eurodac.

15 czerwca 1990 r. w Dublinie Państwa Członkowskie zawarły Konwencję wyznaczającą państwo odpowiedzialne za rozpatrywanie wniosków o azyl złożonych w jednym z Państw Członkowskich Wspólnot Europejskich*, zwaną „Konwencją Dublińską". W celu jej skutecznego stosowania w 2000 r. ustanowiono system Eurodac do porównywania odcisków palców.

Eurodac to system do porównywania danych daktyloskopijnych, który pozwala na dokładne ustalenie tożsamości osób za pomocą sprawdzenia ich odcisków palców. Podstawą prawną dla funkcjonowania Eurodac stanowi Rozporządzenie (UE) nr 603/2013**. Skrót „Eurodac" pochodzi od nazwy systemu European Asylum Dactyloscopy, który gromadzi, przetwarza i porównuje odciski palców osób wnioskujących o udzielenie azylu oraz migrantów zatrzymanych na zewnętrznej granicy UE. Pomaga wskazać państwo członkowskie UE właściwe do weryfikacji prawa do azylu. W przyszłości, poza odciskami palców, będzie on gromadził również takie dane jak m.in: imię i nazwisko oraz wizerunek osób ubiegających się o azyl i migrantów o nieuregulowanym statusie.

Wszystkie Państwa Członkowskie mają możliwość sprawdzenia, czy cudzoziemiec przebywający nielegalnie na jego terytorium wystąpił o azyl w innym państwie członkowskim UE.

W celu zapewnienia skoordynowanego nadzoru nad systemem Eurodac krajowe organy nadzorcze, w tym UODO oraz Europejski Inspektor Ochrony Danych, działając w granicach swych kompetencji, aktywnie współpracują oraz spotykają się przynajmniej dwa razy w roku w ramach Grupy ds. Koordynacji Nadzoru nad Systemem Eurodac.

W wyniku prac tej Grupy, we współpracy z Agencją Praw Podstawowych Unii Europejskiej (FRA), został przygotowany Poradnik dotyczący Prawa do informacji w systemie Eurodac. Przewodnik przypomina, że osoby wnioskujące o udzielenie azylu oraz migranci zatrzymani na granicy zewnętrznej mają obowiązek złożyć odciski palców. Osoby, od których pobiera się odciski palców mają prawo do informacji, kto i dlaczego będzie przetwarzał ich dane oraz jakie to będą dane i jak długo będą przechowywane. Powinny ponadto wiedzieć, w jaki sposób mogą uzyskać dostęp do swoich danych, skorygować je lub usunąć w przypadku pomyłki oraz z kim powinni kontaktować się w tym celu.

4 NARUSZENIA I KOTROLE

Prawo UE wymaga podawania następujących informacji:

- **pobranie odcisków palców jest obowiązkowe** dla każdej osoby wnioskującej o azyl i każdego migranta powyżej 14 roku życia; odciski palców zapisywane są w unijnej bazie danych Eurodac;
- **przechowywane dane**: Dziesięć cyfrowych odcisków palców, informacje na temat płci, państwa pobierającego odciski, miejsca i daty wniosku o udzielenie azylu (w stosownych przypadkach); żadne inne dane osobowe nie są przechowywane; w przypadku gdy dodatkowe dane są gromadzone przez organy do celów krajowych, np. imię, nazwisko, wiek, migranci powinni być poinformowani o znaczeniu podania prawidłowych danych;
- **okres przechowywania danych:** odciski palców przechowywane są przez 10 lat w przypadku osoby ubiegającej się o azyl lub przez 18 miesięcy w przypadku nielegalnego imigranta; po tym czasie system Eurodac automatycznie usuwa dane;
- **dostęp innych organów:** Policja oraz Europol mogą uzyskać dostęp do danych pod ściśle określonymi warunkami; dostęp ten służy zapobieganiu, wykrywaniu i zwalczaniu przestępstw o charakterze terrorystycznym oraz innych poważnych przestępstw; państwo pochodzenia nie ma dostępu do tych danych;
- **prawa osób, których dane dotyczą:** osoba, której dane dotyczą ma prawo dostępu do swoich danych oraz prawo do żądania poprawienia nieprawidłowych danych lub usunięcia danych przetwarzanych niezgodnie z prawem, a także prawo do otrzymywania informacji o procedurach korzystania z tych praw, w tym do danych kontaktowych do administratora danych oraz krajowych organów nadzorczych.

Niepełnosprawność a odmowa pobrania odcisków palców

Osoby wnioskujące o udzielenie azylu oraz migranci z niepełnosprawnością fizyczną mogą nie być w stanie poddać się pobraniu odcisków palców. Inni mogą zaś odmówić pobrania odcisków. W przypadku niezgodności z wymogiem pobrania odcisków powtórzenie informacji oraz skuteczne udzielenie porady może ograniczyć ryzyko konieczności zastosowania środków przymusu.

W tym temacie dostępna jest publikacja Agencji Praw Podstawowych UE:
Wpływ obowiązku podania odcisków palców do system Eurodac na prawa podstawowe.

* **Konwencja** wyznaczająca państwo odpowiedzialne za rozpatrywanie wniosków o azyl złożonych w jednym z Państw Członkowskich Wspólnot Europejskich, sporządzona w Dublinie dnia 15 czerwca 1990, Dz.U. C 254 z 19.8.1997, str. 1—12

** **Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013** z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (przekształcenie); Dz.U. L 180 z 29.6.2013, str. 1—30

VR – JAK BEZPIECZNIE KORZYSTAĆ Z WIRTUALNEJ RZECZYWISTOŚCI?

W ostatnim numerze Biuletynu UODO omówiliśmy kwestię rozszerzonej rzeczywistości, która łączy elementy rzeczywistego świata z dodatkowymi cyfrowymi informacjami czy obiektami, natomiast teraz skupimy się na technologii, która przenosi naszą percepcję do cyfrowego środowiska, tworząc wrażenie bycia w zupełnie innym miejscu. Mowa o wirtualnej rzeczywistości (VR). Niestety, jak większość innowacyjnych technologii, również i VR stawia wyzwania związane z ochroną danych osobowych i prywatnością.

Na przestrzeni ostatnich lat wirtualna rzeczywistość stała się jednym z najbardziej dynamicznie rozwijających się obszarów w dziedzinie technologii, zdobywając popularność w różnych obszarach, wnosząc innowacyjne podejście do nauki, biznesu, zdrowia czy rozrywki.

Co to jest wirtualna rzeczywistość (VR)?

Wirtualna rzeczywistość to zaawansowana technologia, która używa sprzętu, takiego jak gogle VR, aby zanurzyć użytkownika w trójwymiarowym, wirtualnym środowisku. Dzięki sensorom, kamerom i specjalnym kontrolerom, uczestnik może interaktywnie eksplorować cyfrowy świat. Głównym celem jest dostarczenie wrażeń, które są jak najbardziej zbliżone do tych z rzeczywistego świata. Dzięki niej możemy przenieść się w miejsca, do których normalnie nie mielibyśmy dostępu, doświadczyć ekscytujących przygód oraz w pełni oddać się rozrywce.

Aby korzystać z technologii wirtualnej rzeczywistości (VR), potrzebujesz kilku elementów:

1. **Gogle VR.**
Są to urządzenia noszone na głowie, które zapewniają pełną immersję w wirtualnym świecie.
2. Sprzęt komputerowy.
W przypadku bardziej zaawansowanych gogli VR niezbędny jest kompatybilny z nimi sprzęt, taki jak komputer o odpowiednich parametrach, który gwarantuje płynność działania aplikacji VR.
3. Kontrolery ruchu.
Wiele doświadczeń VR wymaga interakcji poprzez ruchy rąk, co osiąga się za pomocą kontrolerów ruchu trzymanych w dłoniach.

Należy podkreślić, że w przypadku korzystania np. z funkcji śledzenia twarzy (mimiki i geometrii), śledzenia ruchów gałki ocznej czy rozpoznawania gestów, mogą być zbierane dane biometryczne, które stanowią szczególną kategorię danych osobowych i zaliczane są do tzw. danych osobowych wrażliwych.

5 NOWE TECHNOLOGIE

Zgodnie z art. 4 pkt 14 RODO „dane biometryczne" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

Biorąc pod uwagę zagrożenia związane z ich przetwarzaniem, cel i zakres ich przetwarzania, a także zakwalifikowanie ich w art. 9 ust. 1 RODO do szczególnych kategorii danych osobowych, każdy przypadek przetwarzania danych biometrycznych należy traktować indywidualnie i zgodnie z art. 35 RODO poprzedzić odpowiednią oceną skutków dla ochrony danych. Istotne jest także wzięcie pod uwagę podstawowych zasad ochrony danych osobowych: niezbędności, celowości i proporcjonalności, o których mowa w art. 5 RODO. Ponadto już na etapie projektowania procesu przetwarzania tych danych należy wdrożyć odpowiednie środki techniczne i organizacyjne zaprojektowane w celu skutecznej ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą. Stosowanie zasady privacy by design powinno uwzględniać takie elementy, jak: koszt wdrażania, charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych.

Jak zatem bezpiecznie korzystać z urządzeń VR?

1. Wybierz urządzenie VR renomowanych firm, które stosują środki bezpieczeństwa i cieszą się dobrą opinią wśród klientów.
2. Zapoznaj się z regulaminem i polityką prywatności urządzenia oraz aplikacji. Udzielaj dostępu tylko do danych, które są niezbędne do korzystania z aplikacji.
3. Upewnij się, że masz pełną świadomość, na co wyraziłeś zgodę oraz do czego zostaną wykorzystane twoje dane.
4. Nie zwlekaj z aktualizacją oprogramowania – takie update'y często wprowadzają poprawki bezpieczeństwa, które pomogą zabezpieczyć twoje dane.
5. Zawsze używaj silnego i unikalnego hasła zabezpieczającego twoje urządzenie VR.
6. Na bieżąco pogłębiaj swoją wiedzę nt. urządzeń VR i potencjalnych zagrożeń z nimi związanych.
7. Jeśli podejrzewasz naruszenie bezpieczeństwa swoich danych osobowych, natychmiast zgłoś ten incydent do odpowiednich organów.

Podsumowując, wirtualna rzeczywistość to ekscytujące pole eksploracji, ale jednocześnie wymaga świadomego podejścia do ochrony danych osobowych. Respektowanie zasad RODO i stosowanie się do zaleceń dotyczących bezpieczeństwa pozwoli nam cieszyć się fascynującym światem VR bez obaw o naszą prywatność.

TSUE POTWIERDZA, ŻE VIN POJAZDU MOŻE BYĆ DANĄ OSOBOWĄ

Trybunał Sprawiedliwości Unii Europejskiej wydał orzeczenie w sprawie C-319/22 Gesamtverband Autoteile-Handel. Rzuciło ono światło na status numerów identyfikacyjnych pojazdów jako danych osobowych w rozumieniu RODO.

Wyrok zapadł 9 listopada 2023 r. w warunkach sprawy, która dotyczyła wynikającego z prawa UE obowiązku producentów samochodów do dostarczania niezależnym podmiotom, takim jak warsztaty i dystrybutorzy części, niezbędnych informacji dotyczących naprawy i konserwacji pojazdów silnikowych. Niemieckie stowarzyszenie zawodowe handlu hurtowego częściami pojazdów (Gesamtverband Autoteile-Handel) zakwestionowało adekwatność danych dostarczonych przez Scania, producenta pojazdów ciężarowych, co doprowadziło do skierowania sprawy przez sąd krajowy do TSUE. Jedną z kwestii podniesionych w sporze było to, czy numer identyfikacyjny pojazdu stanowi dane osobowe, które producenci muszą ujawniać. Trybunał potwierdził, że zgodnie z prawem UE producenci są zobowiązani do udostępniania wszystkich danych dotyczących napraw i konserwacji. Informacje te powinny być dostępne elektronicznie, umożliwiając bezpośrednią ekstrakcję i przechowywanie danych. Trybunał potwierdził, że numer identyfikacyjny pojazdu stanowi dane osobowe, gdy jest powiązany z konkretną osobą. Jest on zawarty w dowodzie rejestracyjnym pojazdu, wraz z nazwiskiem i adresem właściciela. Numer identyfikacyjny pojazdu jest daną osobową w rozumieniu RODO, jeśli ktoś może go użyć do zidentyfikowania właściciela pojazdu lub osoby posiadającej tytuł prawny do tego pojazdu. Jeśli numer identyfikacyjny pojazdu zostanie uznany za daną osobową, musi być przetwarzany zgodnie z wymogami RODO.

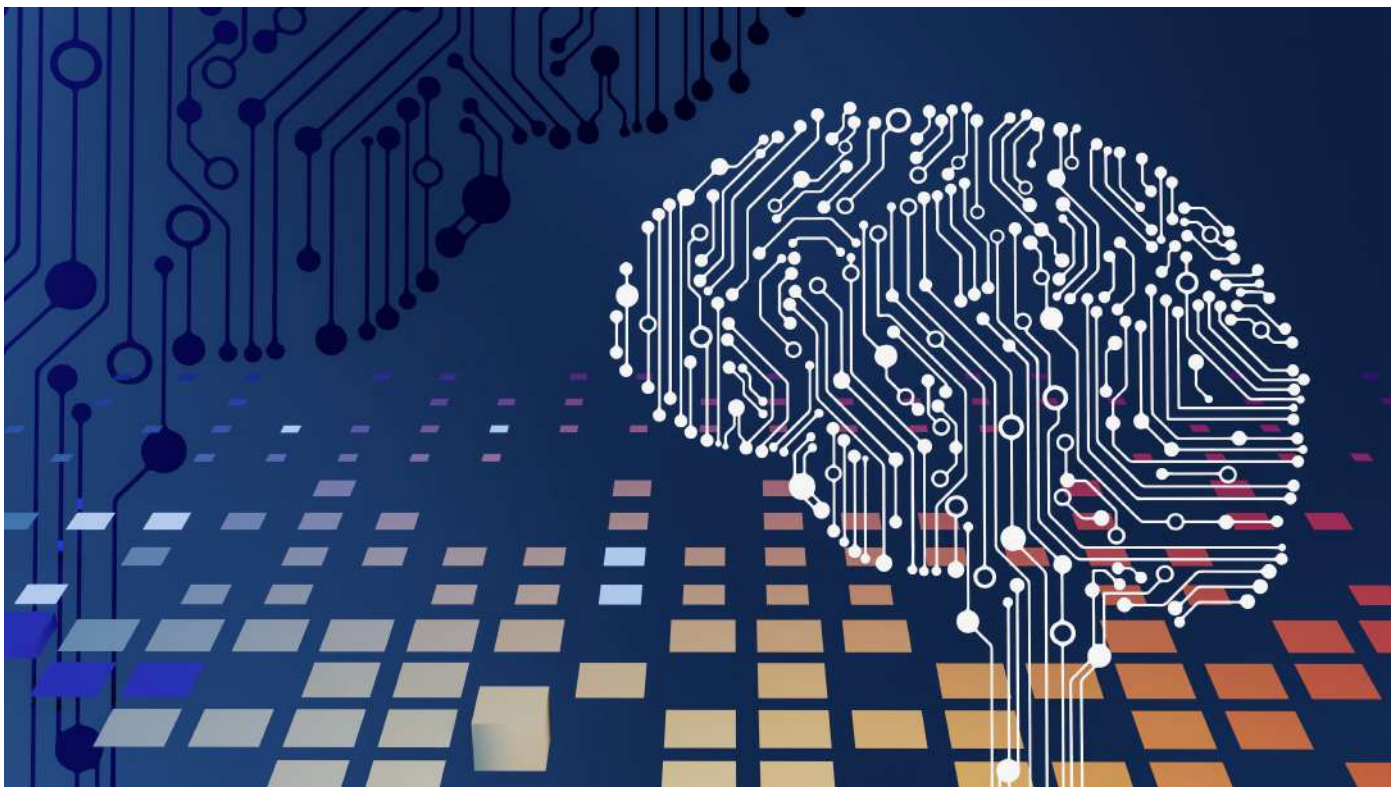
Źródło: Wyrok Trybunału

PROJEKT AKTU W SPRAWIE SZTUCZNEJ INTELIGENCJI OPINIA EIOD

23 października 2023 r. Europejski Inspektor Ochrony Danych opublikował Opinię 44/2023 odnoszącą się do projektu aktu w sprawie sztucznej inteligencji w świetle zmian legislacyjnych, w której podsumował i rozszerzył swoje stanowisko dotyczące procedowanego wniosku legislacyjnego.

W dokumencie EIOD m.in. podkreślił znaczenie wspólnej opinii EROD (Europejskiej Rady Ochrony Danych) i EIOD co do projektu aktu w sprawie sztucznej inteligencji, w szczególności w odniesieniu do wskazanych w niej „czerwonych linii" dotyczących systemów sztucznej inteligencji, które mają być zakazane z powodu ich niedopuszczalnego ryzyka oraz systemów sztucznej inteligencji wysokiego ryzyka. Podkreślił również potrzebę zapewnienia, by istniejące systemy sztucznej inteligencji, w tym elementy wielkoskalowych systemów informatycznych UE, były zgodne z aktem w sprawie sztucznej inteligencji od dnia jego wejścia w życie.

Źródło: Opinia Europejskiego Inspektora Ochrony Danych



FRANCUSKI ORGAN NADZORCZY NAŁOŻYŁ KARĘ NA GROUPE CANAL+

12 października 2023 r. francuski organ nadzorczy Commission nationale de l'informatique et des libertés (CNIL) nałożył administracyjną karę pieniężną w wysokości 600 tys. euro na spółkę GROUPE CANAL+, wydawcę oraz nadawcę kanałów telewizyjnych oraz dystrybutora pakietów płatnej telewizji.

Powodem nałożenia kary były liczne skargi osób fizycznych na uniemożliwienie realizacji praw, jakie im przysługują na podstawie przepisów o ochronie danych osobowych. Wysokość kary została ustalona w świetle zidentyfikowanych naruszeń oraz po uwzględnieniu współpracy administratora z organem. CNIL stwierdził m.in. niedopełnienie obowiązku uzyskania zgody osób fizycznych na otrzymywanie informacji handlowych drogą elektroniczną, niedopełnienie obowiązku informacyjnego wobec tych osób oraz nieprzestrzeganie obowiązku poszanowania prawa dostępu do danych (brak odpowiedzi na wniosek o dostęp).

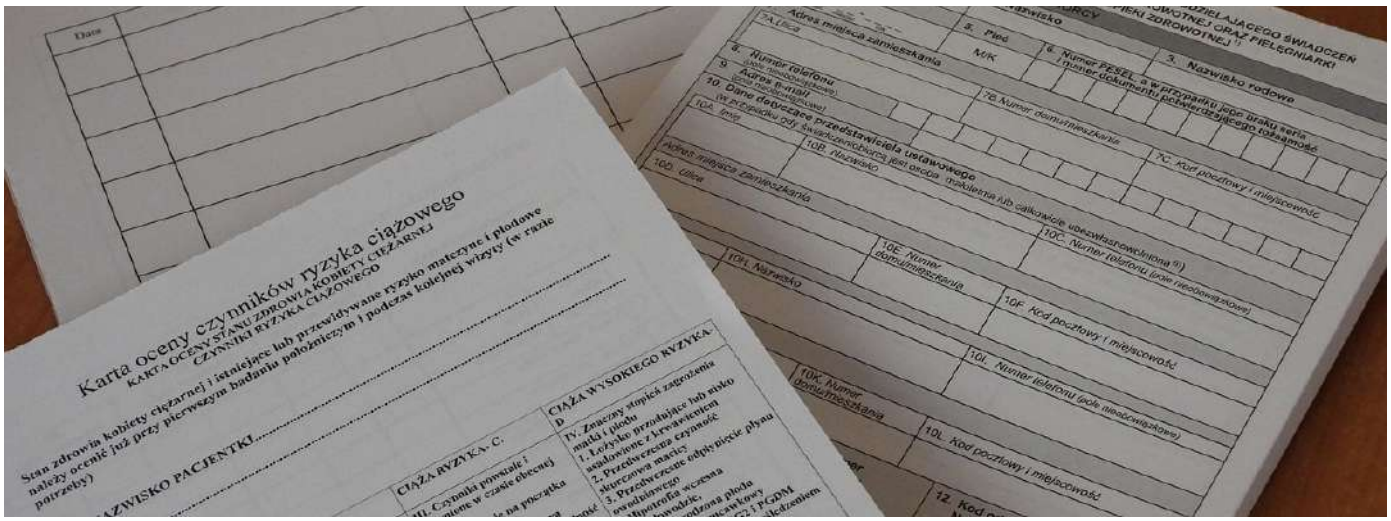
Źródło: komunikat organu nadzorczego

TSUE: ADMINISTRATOR MUSI BEZPŁATNIE PRZEKAZAĆ PACJENTOWI PIERWSZĄ KOPIĘ JEGO DANYCH

26 października 2023 r. zapadł wyrok Trybunału Sprawiedliwości Unii Europejskiej w sprawie C 307/22 FT vs DW. Orzeczenie ma znaczenie dla wykładni przepisów z zakresu ochrony danych osobowych, w szczególności prawa dostępu do danych.

Wyrok zapadł na kanwie sprawy niemieckiego pacjenta, który wystąpił o wydanie kopii dokumentacji medycznej od lekarza dentysty w celu pociągnięcia go do odpowiedzialności za błędy w leczeniu. Opierając się na krajowych przepisach dentysta zażądał, by pacjent pokrył koszty związane z dostarczeniem kopii dokumentacji medycznej. Sąd krajowy zwrócił się do TSUE z szeregiem pytań prejudycjalnych. W swoim wyroku Trybunał przypomniał, że RODO gwarantuje pacjentowi prawo do uzyskania pierwszej kopii jego dokumentacji medycznej bez ponoszenia, co do zasady, kosztów. Administrator danych może pobrać opłatę tylko wtedy, gdy pacjent uzyskał już nieodpłatnie pierwszą kopię swoich danych i ponownie zwraca się o kopię tych samych danych. Dentystę, który był stroną sporu, należy uznać za administratora danych osobowych swojego pacjenta. W związku z tym, w ocenie Trybunału, jest on zobowiązany do bezpłatnego przekazania pacjentowi pierwszej kopii jego danych. Pacjent zaś nie jest zobowiązany do podania uzasadnienia swojego żądania. TSUE uznał, że nawet w celu ochrony interesów ekonomicznych osób świadczących usługi medyczne, przepisy krajowe nie mogą zmuszać pacjenta do ponoszenia kosztów uzyskania pierwszej kopii jego dokumentacji medycznej. Ponadto pacjent ma prawo do otrzymania pełnej kopii dokumentów zawartych w jego dokumentacji medycznej, jeżeli jest to niezbędne do prawidłowego i kompletnego odczytu zawartych w nich danych osobowych.

Źródło: Wyrok Trybunału



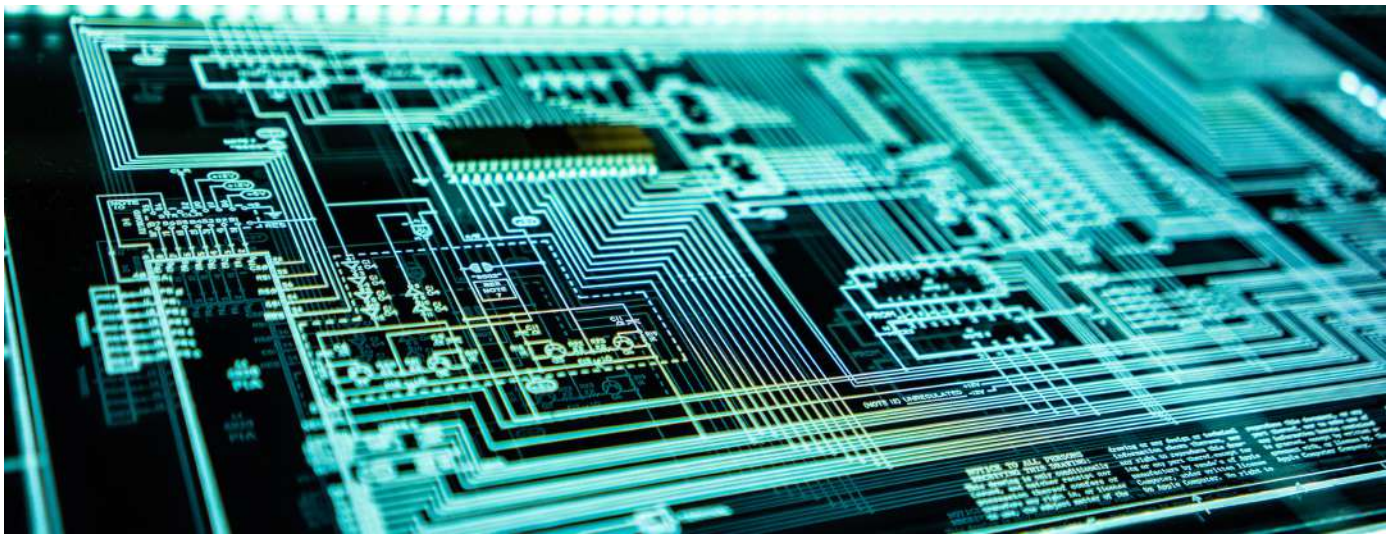
OCHRONA DANYCH OSOBOWYCH – WYZWANIA 2024

Maciej Gawronski, GP Partners, Członek Rady Naukowej Instytutu Prawa Ochrony Danych Osobowych, laureat nagrody im. Michała Serzyckiego w 2021 r

Liczba istotnych wyzwań dla obszaru ochrony danych osobowych stale rośnie. Rok 2024 zapewne upłynie dalej pod znakiem sztucznej inteligencji, tym bardziej że przyjęcie Rozporządzenia UE o Sztucznej Inteligencji jest o krok. Na początku grudnia 2023 Rada i Parlament porozumiały się co do Rozporządzenia AI **www.consilium.europa.eu/en/press/press-releases/2023/12/09/artificial-intelligence-act-council-and-parliament-strike-a-deal-on-the-first-worldwide-rules-for-ai/**, co oznacza, że prawdopodobnie w 2024 r. dostaniemy gotowe Rozporządzenie. W USA 30 października ukazało się Rozporządzenie Wykonawcze Prezydenta Bidena o Sztucznej Inteligencji **www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/**. Dokument kładzie duży nacisk na możliwość i ryzyko podwójnego zastosowania SI (czyli wykorzystania także do zastosowań militarnych), a także na konieczność testowania SI oraz na rolę standardów wypracowywanych przez amerykański National Institute of Standards and Technology. Komputeryzacja, wszechobecność smartfonów, a co za tym idzie wieczne bycie online, technologia bezprzewodowa, a do tego sztuczna inteligencja i wkrótce także komputery kwantowe oraz skanowanie myśli (tak, czytanie myśli nawet za pośrednictwem interfejsów bezinwazyjnych staje się powoli faktem). To wszystko nie pozostawia praktycznie miejsca na prywatność. Globalne technologiczne korporacje podglądają nas cały czas. Dlatego regulacja prywatności i przetwarzania danych osobowych staje się coraz bardziej istotna. Można powiedzieć, że obecnie kontrola nad prywatnością jest w prywatnych rękach wielkich korporacji. Z usług tych korporacji i wyspecjalizowanych firm korzystają służby i organy różnych państw (tu niesławny program Pegasus). Co ciekawe, Unia jedną ręką broni danych osobowych, a drugą chce zaglądać do naszych wiadomości w komunikatorach internetowych, pod pretekstem ochrony dzieci przed pedofilami (równocześnie w zachodnim świecie obserwujemy działania w kierunku normalizacji pedofilii i ingerencji w seksualność dzieci). Wśród tych futurystycznych wyzwań, które dzieją się dziś, jest też zwykły człowiek i nękające go przyziemne problemy, takie jak telefoniczny i internetowy spam,

wścibscy sąsiedzi z telefonami, kamerami i dyktafonami, wieczny problem z zapewnieniem sobie cyberbezpieczeństwa. Wreszcie, jeżeli ten człowiek jest też polskim mikro, małym lub nawet średnim przedsiębiorcą, to samo RODO jest dla niego wyzwaniem.

Dlatego jako wyzwania na rok 2024 w dziedzinie ochrony danych osobowych widzę: aktywność regulacyjną względem komercyjnej sztucznej inteligencji i przygotowywanie się do rozpoczęcia stosowania Rozporządzenia o Sztucznej Inteligencji, walkę z telefonicznymi botami i innym spamem, kontrolę nad tzw. BIG Tech, edukację sędziów na temat wagi i szczegółów ochrony danych osobowych, promocję standaryzacji ochrony danych i zasad cyberbezpieczeństwa, edukację sektora prywatnego, ale przede wszystkim organów władzy, w tym sądów. Liczylibyśmy na większą wrażliwość sędziów na zagadnienia ochrony danych i tu zawsze deklaruję gotowość osobistego wsparcia każdej dyskusji, jak i szkolenia czy innej formy edukacji sędziów na temat wagi i szczegółów zasad ochrony danych osobowych.



Widać, że to są kierunki, którymi Urząd już się aktywnie zajmuje. Kolejne branżowe kodeksy postępowania są zatwierdzane pod kuratelą Krzysztofa Króla, Naczelnika Wydziału kodeksów i certyfikacji UODO. Toczy się sprawa skargi na Open AI w związku z działaniem ChatGPT **www.uodo.gov.pl/pl/138/2823**, którą sam miałem okazję rozpocząć reprezentując skarżącego dra Łukasza Olejnika. Działalność edukacyjna jest coraz bardziej aktywna a Urząd zajmuje mocne stanowisko w dyskusji publicznej głosami swoich przedstawicieli, takich jak Prezes Jan Nowak, Wiceprezes Jakub Groszkowski i Dyrektor Monika Krasińska. Wyzwania stojące przed samym Urzędem doskonale podsumował zresztą Wiceprezes Jakub Groszkowski w dokumencie opublikowanym przez Fundację Panoptykon w związku z debatą kandydatów na stanowisko Prezesa Urzędu Ochrony Danych Osobowy **www.panoptykon.org/kandydaci-na-prezesa-uodo-prezentuja-swoja-wizje-urzedu**

7 WSPÓŁPRACA

Niezmiennie wyzwaniem pozostaje styk przepisów o ochronie danych osobowych z innymi regulacjami w określonych sektorach gospodarki. Doskonałym przykładem jest tutaj sektor finansowy i realizacja obowiązków wynikających z ustawy AML czy regulacji płatniczych. Przepisy nakładają na administratorów z sektora finansowego obowiązek gromadzenia i przetwarzania w określony sposób szerokiego zakresu danych osobowych dotyczących klientów i osób z nimi powiązanych. Pogodzenie tych regulacji z RODO nie jest łatwym zadaniem. W nadchodzącym czasie sektor czekają kolejne zmiany (chociażby nowy pakiet AML, PSD 3 i PSR) i europejskie organy ochrony danych już zwracają uwagę na wyzwania z tym związane. Warto odnotować również rosnące, regulacyjne wymagania w obszarze cyberbezpieczeństwa. Za nieco ponad rok wejdą w życie detaliczne wymagania tzw. Rozporządzenia DORA, jak się wydaje przyszłego standardu „odpowiednich środków technicznych i organizacyjnych", zapewniającego stopień bezpieczeństwa odpowiadający ryzyku przetwarzania danych (art. 32 ust. 1 RODO) dla sektora finansowego.
W „kolejce" transformacyjnych zagadnień społecznych stoją europejska tożsamość cyfrowa i cyfrowa waluta banków centralnych – tak radośnie promowane przez europejskich technokratów, którym wtórują chińscy dygnitarze, baronowie sektora finansowego i menedżerowie globalnych firm technologicznych i farmaceutycznych, ale które mogą stać się narzędziami technologicznego totalitaryzmu. Tych, którzy nie wierzą w to, że dystopijne idee skoringu społecznego nie pojawią się w świecie zachodnim zachęcam do zapoznania się z pomysłami na śledzenie indywidualnego śladu węglowego lub po prostu sprawdzenie swojej oceny w popularnej globalnej platformie transportu osobowego - w zakładce konto (ja mam ocenę 4,79, cokolwiek to znaczy). Jak widać, wyzwań w obszarze ochrony danych nie brakuje. Do niedawna było ich mnóstwo, jednak rozwój technologii dogonił już fantastykę naukową na tyle, że wczorajsze wyzwania chowają się przed dzisiejszymi.

PRAKTYCZNE ASPEKTY MONITOROWANIA KODEKSU POSTĘPOWANIA DLA SEKTORA OCHRONY ZDROWIA PRZEZ AKREDYTOWANY PODMIOT MONITORUJĄCY

Piotr Burzyk

Starszy Menedżer w Zespole Cyberbezpieczeństwa w KPMG w Polsce

Do kogo skierowany jest Kodeks i w jaki sposób można przystąpić do jego stosowania?

Kodeks skierowany jest do podmiotów wykonujących działalność leczniczą (PWDL), zarówno publicznych, jak i prywatnych. Do stosowania Kodeksu mogą również przystępować podmioty, które na zlecenie PWDL przetwarzają dane osobowe pozyskane przez PWDL w celu prowadzenia działalności leczniczej. Przystąpienie do stosowania Kodeksu jest dobrowolne, a jego zdecydowaną zaletą jest otwartość na nowych członków, gdyż nie jest ono uwarunkowane uczestnictwem w żadnej z organizacji branżowych. Kandydat zainteresowany stosowaniem Kodeksu, może zapoznać się z jego pełną treścią na stronie internetowej Urzędu Ochrony Danych Osobowych. Wniosek o uzyskanie statusu podmiotu przestrzegającego postanowień Kodeksu wraz z kwestionariuszem stanowią załączniki do tego dokumentu.

Jaką funkcję będzie pełnił akredytowany podmiot monitorujący?

KPMG Advisory sp. z o.o. sp. k. uzyskało akredytację Prezesa Urzędu Ochrony Danych Osobowych, co potwierdza zapewnianie przez tę spółkę wysokich standardów niezależności oraz odpowiedni poziom wiedzy fachowej z zakresu objętego przedmiotem Kodeksu. Zadaniem podmiotu monitorującego będzie prowadzenie obsługi wniosków oraz oceny kandydatów, którzy złożą wniosek o przyjęcie w poczet członków. Na tym jednak nasza rola się nie kończy, gdyż naszymi dalszymi zadaniami będzie między innymi monitorowanie przestrzegania przepisów Kodeksu czy też rozpatrywanie wniosków i skarg na naruszenie Kodeksu przez jego członków, a w konsekwencji nawet podejmowanie działań, takich jak zawieszanie czy wykluczanie podmiotów spośród stosujących Kodeks. Podmiot monitorujący jest w założeniu pierwszym punktem kontaktu w zakresie stosowania Kodeksu, a jego działania podlegają obowiązkowi sprawozdawczemu wobec organu nadzorczego.

7 WSPÓŁPRACA

Jak wygląda proces audytu wstępnego oraz monitorowania przestrzegania przepisów Kodeksu?

Po złożeniu kompletnego wniosku dokonywany jest wybór metody przeprowadzenia audytu wstępnego, która może przyjąć formę wywiadu telefonicznego (telekonferencji), albo wizyty na miejscu. Bez względu na wynik, po przeprowadzeniu czynności audytowych przygotowany zostanie raport. W przypadku stwierdzenia braków lub niezgodności, kandydatowi przedstawiane będą zalecenia, po których zrealizowaniu przeprowadzony zostanie ponowny audyt wstępny. Pozytywny wynik skutkować będzie wydaniem zaświadczenia o uzyskaniu statusu Członka Kodeksu.

Schemat obsługi wniosku

Sposób monitorowania przestrzegania Kodeksu jest różny dla podmiotów prywatnych oraz publicznych. W pierwszym przypadku monitorowaniem zajmować będzie się KPMG. W odniesieniu do pomiotów publicznych, funkcję taką będą pełniły jednostki audytujące w ramach kontroli zarządczej lub jednostki nadzoru podmiotu tworzącego lub organu rejestrowego. Z uwagi na szczególne uwarunkowania prawne, które znalazły odzwierciedlenie również w samym Kodeksie, nie jest możliwe sprawowanie tej funkcji przez zewnętrzny podmiot monitorujący.

7 WSPÓŁPRACA

Schemat audytów monitoringowych oraz doraźnych

Jakie są różnice dotyczące przystępowania i stosowania Kodeksu pomiędzy organami i podmiotami publicznymi a innymi podmiotami?

Chociaż do stosowania Kodeksu mogą przystępować zarówno podmioty niepubliczne, jak i publiczne, to możemy wyodrębnić pomiędzy nimi trzy podstawowe różnice.

Zakres	Organy i podmioty publiczne	Inne podmioty
Składanie wniosku	Złożenie Wniosku (Załącznik nr 8) wraz z Kwestionariuszem (Załącznik nr 10)	Złożenie Wniosku (Załącznik nr 9) wraz z Kwestionariuszem (Załącznik nr 10)
Dołączenie pozytywnej opinii IOD lub inny podmiot dysponujący odpowiednim poziomem wiedzy	Obowiązkowe (jeśli został powołany)	Fakultatywne
Podmiot monitorujący	Monitorowanie jest prowadzone przez Jednostkę audytującą w ramach mechanizmów monitorowania i oceny kontroli zarządczej – w szczególności poprzez audyt wewnętrzny albo w ramach nadzoru sprawowanego przez podmiot tworzący lub organ rejestrowy	Monitorowanie jest prowadzone przez akredytowany podmiot monitorujący - KPMG Advisory sp. z o.o. sp. k.

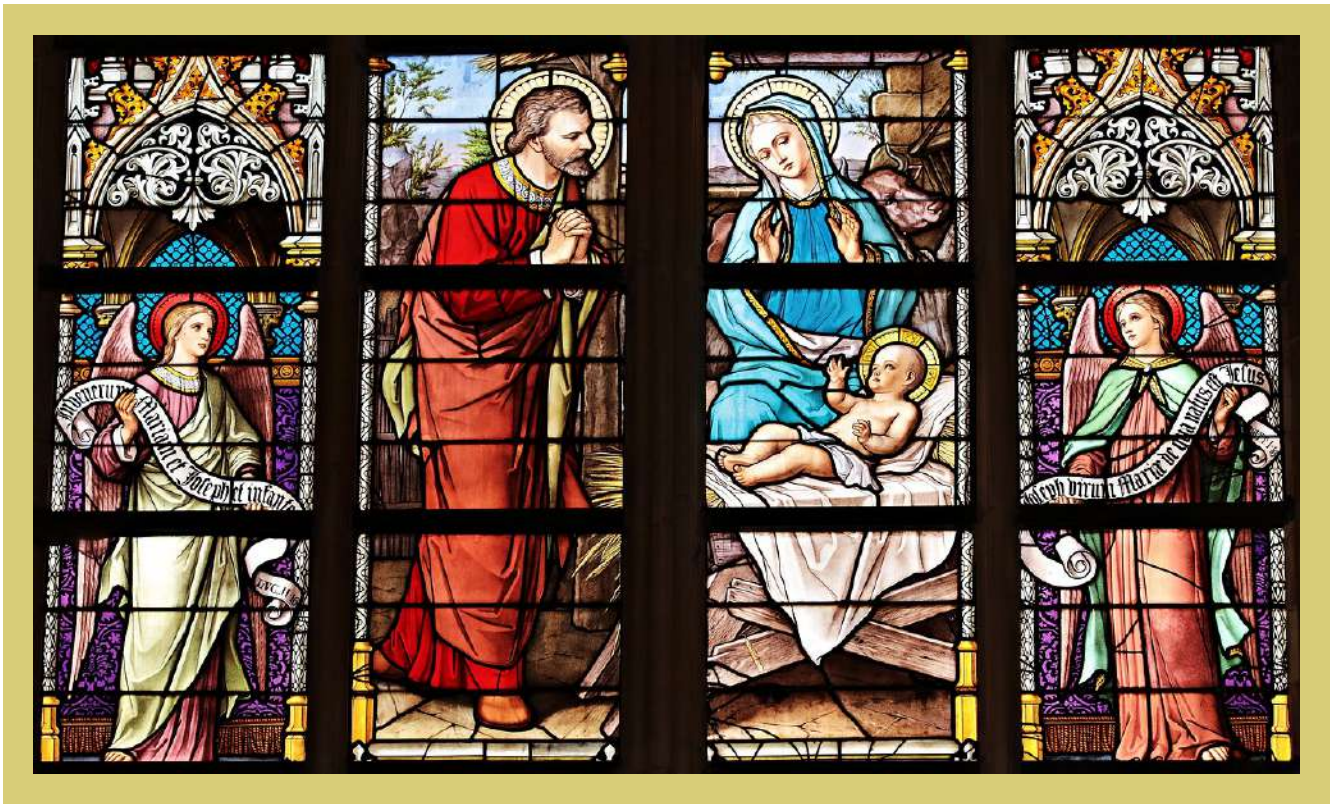
7 WSPÓŁPRACA

W jaki sposób można uzyskać dodatkowe informacje i złożyć wniosek?

Wniosek wraz z niezbędnymi dokumentami, których wzory stanowią załączniki do Kodeksu, można złożyć pisemnie lub drogą elektroniczną. Wszelkie informacje w tym zakresie znajdują się na stronie internetowej podmiotu monitorującego, a osoby zainteresowane mogą skontaktować się w tej sprawie poprzez dedykowany adres e-mail oraz infolinię.

Punkt kontaktowy Podmiotu Monitorującego
adres e-mail: kodeksRODO_PWDL@kpmg.pl
numer infolinii: +48 600960201

Z okazji świąt Bożego Narodzenia życzymy Państwu niezapomnianych i cudownych chwil oraz nowych, wspaniałych możliwości w 2024 roku.
Aby nadchodzący rok upływał Państwu w harmonii i zadumie, by nigdy nie zabrakło ciepła drugiej osoby, a każdy dzień był pełen niezapomnianych chwil.



URZĄD OCHRONY DANYCH OSOBOWYCH

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl