URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 12_01/12_01/24_25

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo,

nowy 2025 rok, drugi rok mojej kadencji, zaczęliśmy w Urzędzie Ochrony Danych Osobowych już zreorganizowani. Nowa struktura ma nam pomóc lepiej i sprawniej wykonywać naszą pracę i rozwiązywać problemy dotyczące danych osobowych i stosowania przepisów dotyczących danych. Większy nacisk postawiliśmy na komunikację i działalność edukacyjną – chodzi nam bowiem o to, by edukacja i prewencja w zakresie ochrony danych była równie ważną aktywnością UODO jak egzekwowanie przepisów.

Koniec stycznia zastał więc nas w drodze – w Brukseli podczas Konferencji Ochrony Danych Osobowych zorganizowanej przez Europejskiego Inspektora Ochrony Danych prof. Wojciecha Wiewiórowskiego, a także obchodów Dniach Ochrony Danych w polskim przedstawicielstwie – I. połowa 2025 r. to wszak prezydencja Polski w Unii Europejskiej. Kolejny przystanek w RODO-drodze to Pomorze, gdzie spotykaliśmy się z ekspertami, inspektorami ochrony danych, samorządowcami i obywatelami w ramach akcji „UODO rusza w kraj". O znaczeniu danych osobowych mieliśmy też szansę opowiedzieć w ramach obchodów Dnia Ochrony Danych Osobowych podczas konferencji o analizie ryzyka zorganizowanej przez UODO we współpracy z Uniwersytetem Warszawskim. Z kolei 24 stycznia członkini Społecznego Zespołu Ekspertów przy Prezesie UODO Mariola Więckowska wygłosiła niezwykle interesujący wykład pt. „Proces monitorowania postępu technologicznego jako element rozliczalności stosowania zasady ochrony danych w fazie projektowania oraz domyślnej ochrony danych".

W styczniu przedstawiłem prawodawcy uwagi do zmian prawa w kilku istotnych kwestiach, m.in.:

- do projektu ustawy o bonie senioralnym
- do projektu ustawy o zmianie ustawy o odpadach
- do projektu ustawy o systemach sztucznej inteligencji

Uwagi te są dowodem na to, jak rośnie znaczenie danych osobowych – stają się one częścią już praktycznie każdego rozwiązania dotyczącego polityk publicznych. Stale więc przypominam, że wprowadzając do prawa przepisy dotyczące danych osobowych należy przeprowadzać analizę skutków dla ochrony danych. To powinien być obowiązkowy element ocen skutków regulacji, przygotowywanych na początku pracy nad każdym nowym rozwiązaniem prawnym.

Chciałbym też zwrócić Państwa uwagę na istotne wyroki sądów:

• NSA potwierdził - bank nie może przetwarzać danych na zapas

• NSA przesądził, że numer księgi wieczystej to dana osobowa

• Wyrok TSUE dotyczący przetwarzania danych w komunikacji elektronicznej pokazał, że zakres zbierania i przetrzymywania danych telekomunikacyjnych, na które pozwala polskie prawo, budzi coraz większe wątpliwości.

• Przeanalizowaliśmy też wyrok TSUE w sprawie o sygn. C- 590/22: naszym zdaniem może mieć znaczenie dla stosowania przepisów w postępowaniach sądowych o zasądzenie odszkodowania z tytułu naruszenia ochrony danych osobowych.

Warto też zwrócić uwagę na to, że 16 stycznia 2025 roku Europejska Rada Ochrony Danych (EROD) przyjęła wytyczne dotyczące pseudonimizacji, a także oświadczenie dotyczące wzajemnych zależności pomiędzy prawem konkurencji a ochroną danych.

Chciałbym też wspomnieć o podpisaniu przez Prezesa UODO porozumień z Polskim Towarzystwem Legislacji oraz z Rządowym Centrum Legislacji. Celem współpracy naszych instytucji jest wzmocnienie znaczenia ochrony danych osobowych w procesie legislacyjnym.

W styczniu Prezes UODO ogłosił plan kontroli sektorowych na rok 2025. Obejmuje on:

• organy, które przetwarzają dane osobowe w Wielkoskalowych Systemach Unii Europejskiej.

• podmioty, które przetwarzają dane o stanie zdrowia – sposób zapewnienia bezpieczeństwa danych osobowych.

• podmioty, które przetwarzają dane dzieci – przetwarzanie wizerunku dzieci, gdy wymagana jest zgoda wyrażona przez rodziców lub opiekunów prawnych.

• administratorów danych – realizacja obowiązku wynikającego z art. 33 ust. 5 RODO, polegającego na dokumentowaniu wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutków oraz podjętych działań zaradczych.

W styczniu Prezes UODO był zmuszony nałożyć karę na Toyota Bank. Powody były dwa. Podmiot pominął profilowanie w rejestrze czynności przetwarzania danych oraz przy ocenie skutków dla ochrony danych. Poza tym Toyota Bank jako administrator danych doprowadził do sytuacji, że inspektor danych osobowych nie był w pełni niezależny w swojej pracy.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Tradycyjnie początek roku zbiega się z Europejskim Dniem Ochrony Danych Osobowych, przypadającym na 28 stycznia. To wyjątkowo intensywny w Urzędzie czas podsumowań, a jednocześnie wyznaczania kolejnych zadań. To również moment wzmożonej aktywności przedstawicieli UODO w mediach, termin licznych spotkań, konferencji i webinariów, których celem jest oczywiście upowszechnianie w społeczeństwie wiedzy o tym jak ważne są dane osobowe i o tym jak należy je chronić.

W tym numerze zdecydowaliśmy się zastąpić tradycyjny wywiad z ekspertem zestawem krótkich pytań i odpowiedzi kilku reprezentantów UODO. Pozwalają one przyjrzeć się jak poszczególne osoby oceniają ostatni rok – niektóre refleksje oczywiście się ze sobą pokrywają, inne unaoczniają jak z różnymi wyzwaniami mierzą się poszczególne departamenty.

W tym numerze m.in. rozstrzygamy wątpliwości obywatela, co do dopuszczalności przetwarzania jego danych osobowych przez organ administracji publicznej. Zdaniem UODO udzielenie przez osobę prywatną informacji istotnych dla prowadzonego postępowania administracyjnego może być wystarczającym uzasadnieniem dla podania jej danych osobowych w treści wydanego w sprawie postanowienia.

Kodeks postępowania mógłby ułatwić jednostkom samorządu terytorialnego właściwe wdrożenie zasad ochrony danych osobowych. Obecnie miewają one z tym problemy m.in. ze względu na nieprecyzyjne przepisy prawa czy różny poziom świadomości w zakresie realizacji obowiązków w związku z przetwarzaniem danych osobowych. Dlatego UODO zachęca przedstawicieli samorządu do podjęcia wysiłku w tym zakresie i deklaruje eksperckie wsparcie.

WSA w Warszawie podtrzymał decyzję PUODO, oddalając skargę C. Sp. z o.o. Na spółkę poskarżył się były pracownik: zarzucił jej, że przetwarza jego dane w zakresie adresu e-mail zawierającego pierwszą literę imienia oraz nazwisko, bez podstawy prawnej. Okazało się, że spółka korzystała z tego adresu do kontaktów z potencjalnymi klientami i nie chciała go kasować.

Jak dokumentować naruszenia ochrony danych osobowych? W podwójnym wydaniu „Biuletynu UODO" przedstawiamy rolę rejestru naruszeń ochrony danych osobowych oraz wskazówki dotyczące jego prowadzenia.

Przybliżamy również przewidywania na podstawie wniosków z najnowszego raportu TechSonar 2025. To inicjatywa Europejskiego Inspektora Ochrony Danych (EIOD), która identyfikuje najważniejsze trendy technologiczne w kontekście ochrony danych osobowych. Raport ma na celu przewidywanie kierunków rozwoju technologii i ich wpływu na prywatność, umożliwiając podejmowanie działań prewencyjnych, zanim ryzyka związane z nowymi technologiami staną się realnym zagrożeniem.

UODO dołącza do gratulacji dla hiszpańskiego organu ochrony danych (AEPD). Stworzony przez niego system weryfikacji wieku w celu ochrony dzieci i młodzieży w internecie został wyróżniony dwiema z pięciu nagród przyznanych podczas 46. Global Privacy Assembly, które zrzesza organy ochrony danych i prywatności na całym świecie. Hiszpański regulator może się również pochwalić zatwierdzeniem „Kodeksu postępowania w zakresie rozstrzygania sporów dotyczących ochrony danych w sektorze łączności elektronicznej", opracowanego przez operatorów telefonicznych należących do grup Orange, Telefónica, Vodafone i MásMóvil.

Zatwierdzony został też trzeci kodeks europejski, w tym drugi zatwierdzony przez francuski organ ochrony danych, po przyjętym w 2021 roku kodeksie CISPE (w zakresie przetwarzania w chmurze). Nowy kodeks uzyskał poparcie Federacji EUCROF, która podjęła inicjatywę jego opracowania w odpowiedzi na kwestie ochrony danych zidentyfikowane przez sektor. Kodeks ten skierowany jest do dostawców usług badań klinicznych, którzy działają jako podwykonawcy w imieniu sponsorów.

Piszemy o licznych karach norweskiego organu ochrony danych: na Uniwersytet w Agder, na gminę Eidskog, a także Urząd Pracy i Opieki Społecznej.

Z kolei irlandzki organ ochrony danych (DPC) ogłosił ostateczną decyzję po zakończeniu postępowania wyjaśniającego wobec LinkedIn Ireland Unlimited Company. Komisja wszczęła formalne postępowanie w celu oceny, czy Temu mogło naruszyć Akt o usługach cyfrowych (DSA) w obszarach związanych ze sprzedażą nielegalnych produktów, potencjalnie uzależniającą konstrukcją usługi, systemami wykorzystywanymi do rekomendowania zakupów użytkownikom, a także dostępem do danych dla badaczy.

2025 rok zaczął się równie intensywnie co poprzedni. Pewien pogląd na to, daje podwójne wydanie „Biuletynu UODO", które stanowi zapowiedź tego, co czeka nas w nadchodzących miesiącach.

Karol Witowski
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

PODSUMOWANIE 2024 ROKU W UODO. WKRACZAMY W KOLEJNY ROK WYZWAŃ

Do serii krótkich pytań i odpowiedzi podsumowujących 2024 rok zaprosiliśmy wybranych przedstawicieli UODO: Mirosława Wróblewskiego, prezesa UODO, Agnieszkę Grzelak, zastępczynię prezesa UODO, Annę Dudkowską, dyrektor Departamentu Inicjatyw Edukacyjnych, Monikę Krasińską, dyrektor Departamentu Prawa i Nowych Technologii, Paulinę Dawidczyk, dyrektor Departamentu Skarg oraz Piotra Drobka, radcę w UODO.

Najważniejsze wydarzenia, które określają rok 2024

Agnieszka Grzelak, zastępczyni prezesa UODO:

1 sierpnia 2024 r. wszedł w życie AI Act – rozporządzenie mające na celu zapewnienie bezpieczeństwa, przejrzystości i zgodności z wartościami europejskimi w rozwoju i stosowaniu AI. Uważam to za istotny symbol – element w drodze do rozważnej regulacji nowych technologii i wyzwań, jakie się z tym się wiążą. Przed nami wszystkimi (UODO, innymi organami administracji publicznej, obywatelami) droga do oswojenia się z wszechobecnością sztucznej inteligencji i konieczność przedefiniowania niektórych problemów.

Anna Dudkowska, dyrektor Departamentu Inicjatyw Edukacyjnych:

Rok 2024 to rok, w którym bardzo intensywnie kontynuowaliśmy działania edukacyjne na rzecz szerokiego grona odbiorców. Otwartość na dialog z różnymi grupami społecznymi, zaowocowała szeregiem działań, w których podkreślaliśmy ogromną potrzebę ochrony wizerunku i prywatności dzieci oraz młodzieży w erze cyfrowej. Jednym z ważniejszych wydarzeń ostatniego roku było zawarcie porozumienia Prezesa UODO i Rzeczniczki Praw Dziecka w zakresie inicjatyw edukacyjnych dotyczących danych osobowych dzieci i młodzieży, które ugruntowało obrane kierunki działań. Współpraca obu instytucji na rzecz ochrony danych osobowych najmłodszych przerodziła się w szereg inicjatyw skierowanych do nich oraz do instytucji sprawujących nad dziećmi opiekę. Inicjatywy te będą kontynuowane również w roku 2025.

1 ROZMOWA Z EKSPERTEM

Nie zabrakło działań edukacyjnych skierowanych do seniorów. Uwieńczeniem ich było podpisanie porozumienia Prezesa UODO i Prezeski Ogólnopolskiej Federacji Stowarzyszeń Uniwersytetów Trzeciego Wieku Pani Wiesławy Borczyk, na rzecz promowania zasad ochrony danych osobowych i udziału we wspólnych projektach i inicjatywach edukacyjno-informacyjnych, mających na celu pogłębienie świadomości słuchaczy uniwersytetów trzeciego wieku o przysługujących im prawach i środkach ochrony danych osobowych.

Monika Krasińska, dyrektor Departamentu Prawa i Nowych Technologii:

Za nami rok wytężonej pracy. Rok wielu spotkań z różnorodnymi środowiskami, by wymienić tylko te z organizacjami reprezentującymi inspektorów ochrony danych, wspierające ich i propagujące prawidłowe wzorce pełnienia tej funkcji, jakże ważnej dla ochrony naszych praw, czy spotkania informacyjno-uzgodnieniowe z podmiotami pracującymi nad kodeksami postępowania, organizacjami pozarządowymi, a także zrzeszającymi przedstawicieli biznesu. Za nami wiele konferencji uzgodnieniowych i setki opinii legislacyjnych tworzonych w trosce o prawo zgodne z RODO i w jak największym stopniu chroniące nasze dane osobowe.

Istotne było również przyjęcie AI Act. W związku z „modą" na rozwiązania oparte na „sztucznej inteligencji" bardzo ważne jest nałożenie ograniczeń prawnych na dostawców i użytkowników rozwiązań informatycznych, które mogą bardzo głęboko ingerować w prywatność każdego z nas.

Najtrudniejsza decyzja 2024 roku

Agnieszka Grzelak:

Wybór najtrudniejszej decyzji Prezesa UODO w 2024 r. zależy od kryteriów oceny, jakie przyjmiemy. Decyzja dotycząca spółki American Heart of Poland wyróżnia się zarówno wysoką karą finansową, jak i poważnymi konsekwencjami dla ochrony danych osobowych pacjentów i pracowników, co może przemawiać za uznaniem jej za jedną z bardziej skomplikowanych i znaczących. Tym bardziej, że w 2025 r. zamierzamy przyjrzeć się dokładniej problemowi ochrony danych osobowych w placówkach medycznych.

1 ROZMOWA Z EKSPERTEM

Najlepsza współpraca tego roku

Agnieszka Grzelak:

Prezes UODO podejmował szereg działań zmierzających do wzmocnienia lub odnowienia współpracy z różnymi organami, wskazując na konieczność efektywnej współpracy i ustanowienia kanałów komunikacji. Najlepszym pomysłem jednak, który zaowocował już wieloma konkretnymi efektami, było powołanie i współpraca ze Społecznym Zespołem Ekspertów, pod przewodnictwem dr Gumularza. Zorganizowanych zostało wiele konferencji, dyskusji merytorycznych, na ukończeniu są poradniki – to konkretne owoce, a jeszcze dalej idące są plany na kolejny rok.

Anna Dudkowska:

W 2024 roku UODO intensywnie współpracował z Rzeczniczką Praw Dziecka, realizując liczne inicjatywy edukacyjne związane z ochroną danych dzieci i młodzieży. Kluczowym wydarzeniem była konferencja „Wyzwania dla ochrony danych osobowych dzieci", podczas której poruszono kwestie publikacji zdjęć dzieci w mediach społecznościowych, wyrażania zgód na przetwarzanie danych oraz wykorzystania wizerunku przez sztuczną inteligencję. Stworzono także specjalne materiały edukacyjne we współpracy z Fundacją Orange, które trafiły do organizacji odpowiedzialnych za bezpieczeństwo dzieci.

Ponadto 4 czerwca 2024 r. w Warszawie Prezes UODO powołał Społeczny Zespół Ekspertów, który pełni funkcję opiniodawczo-doradczą, wspierając Prezesa Urzędu w realizacji jego ustawowych zadań. W ramach tej współpracy zrealizowano szereg inicjatyw edukacyjnych, takich jak konferencje i seminaria dotyczące praktycznych problemów w stosowaniu przepisów ustawy o ochronie sygnalistów z perspektywy RODO, ochrony danych osobowych przez związki zawodowe czy jako element odporności społeczeństwa i państwa. Rozmawiano również o ochronie danych w robotyce medycznej w dobie AI ACT i EHDS i ochronie zdrowia w zatrudnieniu w kontekście przepisów ogólnego rozporządzenia o ochronie danych. Dodatkowo w ramach współpracy z SZE rozpoczęto prace nad aktualizacją dwóch kluczowych poradników: dotyczącego zatrudnienia oraz zgłaszania naruszeń ochrony danych osobowych.

Rok 2024 r. to również czas kontynuacji współpracy UODO ze szkołami na rzecz ochrony danych osobowych dzieci w szkołach, realizowanej w ramach ogólnopolskiego programu UODO „Twoje dane – Twoja sprawa".

1 ROZMOWA Z EKSPERTEM

Najważniejsza rozmowa roku 2024

Paulina Dawidczyk, dyrektor Departamentu Skarg:

W minionym roku takich ważnych rozmów było bardzo wiele. Departament Skarg czynnie uczestniczył m.in. w licznych spotkaniach zastępcy prezesa Urzędu Ochrony Danych Osobowych Konrada Komornickiego z przedstawicielami samorządów. Podczas tych spotkań prowadzono rozmowy na temat możliwych obszarów współpracy samorządów z UODO, w związku z rosnącymi wyzwaniami i zagrożeniami dla samorządów w zakresie ochrony danych osobowych.

Agnieszka Grzelak:

Najważniejsza rozmowa roku 2024 to ta w styczniu 2024 r., kiedy to Prezes UODO zaproponował mi funkcję jego zastępczyni. Ponieważ uznałam, że wybór Mirosława Wróblewskiego na Prezesa UODO był bardzo trafną decyzją, to i ja nie wahałam się długo.

Anna Dudkowska:

W roku 2024 odbyliśmy wiele ciekawych spotkań. Ważne były wszystkie rozmowy, ale szczególną uwagę zwracam na rozmowy z przedstawicielami różnych środowisk w ramach inicjatywy „UODO Rusza w Kraj".

W 2024 r. były to spotkania w Małopolsce i na Śląsku. Takie działania pokazały, że Urząd jest dostępny dla obywateli i gotowy na rozmowy o realnych wyzwaniach w ochronie danych osobowych.

Warto podkreślić, że UODO nie posiada jednostek terenowych, dlatego takie przedsięwzięcia są kluczowe, aby lepiej zrozumieć realne problemy związane z ochroną danych osobowych, które mogą występować wszędzie tam, gdzie są ludzie. Spotkania te są też wyrazem otwartości na współpracę i chęci budowania systemowych rozwiązań dostosowanych do lokalnych potrzeb.

Największe zaskoczenie roku 2024

Anna Dudkowska:

Ogromnym sukcesem i zaskoczeniem okazała się obecność UODO na Pol'and'Rock Festiwal. Festiwal, który zwykle kojarzy się z muzyką i zabawą, stał się przestrzenią do poważnych rozmów o danych osobowych i nowych technologiach.

Wydarzenie zgromadziło dziesiątki tysięcy uczestników w różnym wieku, którzy obok muzyki szukali także możliwości zdobycia wiedzy i wzięcia udziału w inspirujących dyskusjach. UODO, w odpowiedzi na ten trend, aktywnie włączył się w edukacyjną część festiwalu, organizując warsztaty na temat sztucznej inteligencji oraz prowadząc punkt porad, gdzie uczestnicy mogli uzyskać praktyczne wskazówki

na temat ochrony swojej prywatności i świadomego korzystania z nowych technologii. Obecność UODO była możliwa dzięki wsparciu Okręgowej Izby Radców Prawnych z Poznania, która udostępniła przestrzeń, w której eksperci mogli prowadzić konsultacje i dzielić się wiedzą z uczestnikami festiwalu. To wyjątkowe połączenie edukacji i zabawy pokazało, że tak ważne tematy jak ochrona danych osobowych mogą być poruszane w sposób przystępny, angażujący i skuteczny, nawet w miejscach o nieformalnym charakterze. Sukces tej inicjatywy dowodzi, że wychodzenie do społeczeństwa i podejmowanie dialogu w niestandardowych miejscach jest nie tylko potrzebne, ale i niezwykle efektywne.

Największy sukces UODO w 2024 roku

Mirosław Wróblewski, prezes UODO:

Pierwsza kwestia to skuteczne egzekwowanie przepisów o ochronie danych osobowych, co znajduje wyraz w nakładanych karach administracyjnych – w 2024 r. wyniosły one łącznie 13,3 mln zł, co stanowi ok. 44 proc. wszystkich kar wydanych od początku stosowania RODO w Polsce, czyli od 2018 r., ale także we wszystkich innych działaniach podejmowanych przez Urząd. To działalność w obszarach, które do tej pory nie były objęte nadzorem, takie jak fałszywe reklamy, czyli dwóch wydanych postanowień zabezpieczających w stosunku do Mety, podtrzymanych następnie przez Wojewódzki Sąd Administracyjny.

Drugą kwestią jest edukacja i budowanie świadomości na temat ochrony danych osobowych. Poprawiła się komunikacja Urzędu – zarówno z administratorami danych, jak i z obywatelami. Wraz ze współpracownikami odbyłem wiele spotkań z organizacjami branżowymi, biznesowymi, czyli zrzeszającymi administratorów z różnych dziedzin i obszarów gospodarki, ale też z organami państwa, szeroko pojętą administracją publiczną oraz organizacjami inspektorów ochrony danych.

Urząd Ochrony Danych Osobowych jest dzięki temu postrzegany jako aktywny regulator, który zna potrzeby rynku oraz obywateli. Jest dla nich dostępny i godny zaufania. W 2024 roku zorganizowaliśmy wiele seminariów i konferencji. Zainteresowanie wydarzeniami dotyczącymi ustawy o sygnalistach, przekroczyło nawet nasze możliwości techniczne. W tych działaniach ważną rolę odegrał Społeczny Zespół Ekspertów przy prezesie UODO.

Podejmowaliśmy też działania edukacyjne dotyczące praw dzieci i młodzieży, np. na temat wykorzystywania wizerunku osób niepełnoletnich. Edukowaliśmy również

seniorów. Do osiągnięć zaliczyłbym także realizację działań regionalnych w ramach programu „UODO rusza w kraj".

Agnieszka Grzelak:

To jeszcze nie sukces, ale uważam, że dwa postanowienia zabezpieczające w sprawie Mety, podtrzymane przez WSA, są początkiem drogi zmierzającej docelowo do uporządkowania kwestii scamu. Chcemy ukrócić działania oszustów, wykorzystujących czyjeś dane osobowe, w tym wizerunek, najczęściej po to, by zachęcić do wpłacania pieniędzy.

Współpraca z prezesem Naczelnej Rady Lekarskiej również uwidoczniła problem wykorzystywania wizerunku znanych lekarzy, autorytetów w branży, do reklamowania nieprawdziwych leków. Niestety, niektórzy pacjenci padają ofiarami fałszywych reklam i rezygnują z naukowo udowodnionych metod leczenia i lekarstw.

Paulina Dawidczyk:

Jeśli chodzi o sukcesy dotyczące postępowań skargowych, niewątpliwie cieszą te związane z orzecznictwem sądów administracyjnych w sprawach skargowych. W minionym roku w zdecydowanej większości spraw zawisłych przed ww. sądami w wyniku skarg złożonych na decyzje i postanowienia wydane przez Prezesa Urzędu Ochrony Danych Osobowych w postępowaniach skargowych, sądy zgadzały się ze stanowiskiem organu nadzorczego.

Anna Dudkowska:

W 2024 roku Urząd z powodzeniem zorganizował szereg inicjatyw edukacyjnych oraz konsultacyjnych, które cieszyły się dużym zainteresowaniem. Dzięki swoim działaniom UODO nie tylko odpowiedział na bieżące wyzwania, lecz także wyznaczył kierunki działania na kolejne lata, wzmacniając swoje miejsce jako kluczowy podmiot wspierający ochronę danych i prawo do prywatności w Polsce.

Ważnym krokiem Prezesa było powołanie Społecznego Zespołu Ekspertów (SZE), którego celem jest nie tylko wspieranie bieżących działań urzędu, lecz także zapewnienie eksperckiego doradztwa oraz podejścia opartego na nowoczesnych metodach zarządzania i analizy danych.

Nowy prezes UODO aktywnie angażował się w spotkania z przedstawicielami różnych sektorów, organizacji pozarządowych oraz instytucji międzynarodowych. Działania te miały na celu wzmocnienie dialogu społecznego i wypracowanie wspólnych rozwiązań dla najważniejszych problemów.

1 ROZMOWA Z EKSPERTEM

Najlepsze wspomnienie z 2024 roku

Monika Krasińska:

Udział w Przystanku Konstytucja i UODO rusza w kraj (Katowice). Wobec braku oddziałów regionalnych ważne jest, by przedstawiciele UODO reprezentowali Urząd na różnego rodzaju wyjazdach „w teren”. Wspomnienie to na długo pozostanie w mojej pamięci, z uwagi na dużą otwartość organizatorów, IOD i osób, których dane są przetwarzane, którzy dzielili się z nami swoimi doświadczeniami i troskami.

Anna Dudkowska:

Rok 2024 obfitował w wyjątkowe wydarzenia edukacyjne skierowane do dzieci i młodzieży, w których UODO miał przyjemność uczestniczyć. Każde z tych spotkań było okazją do dzielenia się wiedzą o ochronie danych osobowych oraz do poznania spojrzenia najmłodszych – wymagających, ale niezwykle otwartych i kreatywnych odbiorców.

UODO włączyło się m.in. w szerzenie wiedzy o prawach i wolnościach konstytucyjnych w ramach ogólnopolskiej akcji edukacyjnej Tour de Konstytucja. W trakcie spotkań organizowano warsztaty dla dzieci i młodzieży, które przybliżały im znaczenie ochrony danych osobowych jako elementu praw człowieka. Były to wartościowe momenty, które podkreślały rolę edukacji na wczesnym etapie życia.

Z kolei podczas programu „Lekcje o finansach” UODO przeprowadziło warsztaty, w których poprzez zabawę uczono dzieci zasad ochrony danych w kontekście finansowym. Spotkania te zwracały uwagę na praktyczne aspekty, takie jak korzystanie z aplikacji czy dokonywanie płatności, budując świadomość ochrony danych w codziennych sytuacjach.

Na Olimpiadzie dla Przedszkolaków UODO miało okazję dotrzeć do około 300 dzieci z 10 przedszkoli. Podczas wydarzenia przygotowano interaktywne zajęcia oraz stanowisko informacyjne, które w przystępny sposób uczyły najmłodszych o prywatności i ochronie danych. Była to niezwykle inspirująca inicjatywa, pokazująca, że nawet przedszkolaki potrafią być zaangażowane i ciekawe tego ważnego tematu.

Szczególnym doświadczeniem były warsztaty dla dzieci poszkodowanych w powodzi, zorganizowane na zaproszenie Fundacji „Odzyskaj siebie” oraz Centrum Reset. UODO, oprócz nauki zasad ochrony danych, wskazało, jak ważna jest edukacja dostosowana do potrzeb i sytuacji życiowych dzieci.

1 ROZMOWA Z EKSPERTEM

Postanowienia na kolejny rok

Mirosław Wróblewski:

Liczę, że 2025 rok będzie równie owocny co poprzedni. Zaczęliśmy go od przebudowy struktury Urzędu Ochrony Danych Osobowych, aby nasza praca była jeszcze bardziej efektywna.

Będziemy wprowadzać kolejne zmiany związane z wdrożeniem unijnego Aktu o zarządzaniu danymi – nadchodzi przyjęcie polskiej ustawy o zarządzaniu danymi. Jej przyjęcie oznaczać będzie nowe zadania dla UODO, przede wszystkim dotyczące usług pośrednictwa danych oraz rejestracji instytucji altruizmu danych. Priorytetami będzie skuteczne egzekwowanie przepisów o ochronie danych i dalsze działania edukacyjne oraz wzmacniające świadomość praw podmiotów danych, zwłaszcza w kontekście nowych technologii.

Paulina Dawidczyk:

Kluczowym i najważniejszym postanowieniem dotyczącym procedowania spraw skargowych jest utrzymanie wysokiej aktywności organu nadzorczego w zakresie wydawanych decyzji. Zadanie to jest bardzo ważne, dlatego w Departamencie Skarg przykładamy do niego ogromną wagę. Jednak jego skuteczna realizacja wiąże się z wieloma wyzwaniami związanymi chociażby z ograniczonym budżetem, warunkującym liczbę pracowników zaangażowanych w prowadzenie postępowań skargowych, utrzymującym się wysokim wpływem skarg do urzędu (ok 7-8 tys. skarg rocznie) oraz zwiększającym się stopniem skomplikowania spraw skargowych, którymi zajmuje się Urząd i których skuteczne rozpatrywanie wymaga stałej aktualizacji wiedzy z różnych dziedzin.

Anna Dudkowska:

W 2025 roku Urząd Ochrony Danych Osobowych zamierza znacząco rozszerzyć swoje działania edukacyjne, ze szczególnym uwzględnieniem ochrony danych osobowych dzieci oraz osób starszych. Celem jest dotarcie do jeszcze większej liczby odbiorców poprzez intensyfikację organizacji warsztatów i szkoleń, które będą dostosowane do potrzeb różnych grup wiekowych i społecznych.

Istotnym priorytetem na nadchodzący rok będzie także promocja programu „Twoje Dane – Twoja Sprawa”, który odgrywa kluczową rolę w kształtowaniu świadomości w zakresie ochrony danych w polskich szkołach i instytucjach edukacyjnych. UODO będzie dążył do zwiększenia liczby placówek zaangażowanych w program oraz do rozwijania jego treści, tak aby lepiej odpowiadały na aktualne wyzwania związane z rozwojem nowych technologii.

Jednym z kluczowych obszarów działań będzie również ochrona wizerunku małoletnich. W związku z coraz częstszym umieszczaniem zdjęć dzieci w przestrzeni publicznej, zarówno przez rodziców, jak i instytucje, UODO dostrzega pilną potrzebę zwiększenia świadomości na temat zagrożeń z tym

związanych. Chodzi tu nie tylko o ryzyko niewłaściwego wykorzystania wizerunku, ale także o długofalowe konsekwencje, jakie mogą wynikać z nieprzemyślanego udostępniania zdjęć dzieci w internecie. Planowane działania będą obejmowały zarówno kampanie informacyjne, jak i współpracę z instytucjami edukacyjnymi.

Piotr Drobek, radca w UODO:

Jednym z celów UODO na 2025 r. jest dobre przygotowanie się do wykonywania nowych zadań, które Prezes UODO będzie wykonywał na podstawie planowanych przepisów wdrażających w polskim systemie prawnym Akt w sprawie zarządzania danymi.

Chcemy się również podjąć regularnej organizacji otwartych wykładów eksperckich w ramach cyklu „Ochrona danych i technologia".

Największe wyzwanie w 2025 roku

Mirosław Wróblewski:

Wyzwaniem pozostaje dalsze skuteczne wdrażanie przepisów o ochronie danych osobowych, ale także budowanie świadomości i edukacja w zakresie ochrony danych. Chcę dotrzeć do osób najmłodszych i najstarszych, które są szczególnie zagrożone w świecie cyfrowym.

Kolejne zadanie to sprostanie kwestiom związanym z przetwarzaniem danych osobowych w kontekście nowych technologii, przede wszystkim sztucznej inteligencji i zagrożeń związanych z cyberprzestępczością. Zamierzam powołać nową grupę roboczą w tym zakresie.

Inny obszar pełen wyzwań to ochrona danych medycznych, co pokazały zarówno decyzje, które podjąłem w zeszłym roku, jak i skargi na administratorów w związku z naruszaniem przepisów o ochronie danych osobowych, które trafiają do Urzędu. Z tego powodu jednostki prowadzące działalność leczniczą stały się przedmiotem priorytetowych kontroli Prezesa UODO w tym roku.

Duże znaczenie ma intensyfikacja skuteczności działań w sprawach transgranicznych. Tymi zadaniami zajmie się świeżo wyodrębniony przeze mnie Departament Współpracy Międzynarodowej. Chodzi tu np. o kwestię chińskich platform sprzedażowych czy transferu danych poza Unię Europejską – to na pewno będzie jednym z ważnych punktów działalności UODO. To sprawy wielowątkowe, w których współpracujemy z innymi organami państwa, na przykład z Ministerstwem Technologii i Rozwoju, z partnerami społecznymi, czyli z Polską Izbą Gospodarki Elektronicznej, a także z organami nadzorczymi z innych państw unijnych i z Europejską Radą Ochrony Danych Osobowych.

Dochodzą też nowe zadania urzędu. Lista nowych kompetencji zajmuje ponad 20 stron.

1 ROZMOWA Z EKSPERTEM

Agnieszka Grzelak:
W 2025 r. chcielibyśmy rozpocząć szerszą rozmowę o koniecznych zmianach legislacyjnych, które powinny zostać przyjęte w celu usprawnienia postępowań i zmniejszenia niektórych barier administracyjnych. Jeszcze większym wyzwaniem będzie jednak przekonanie do konieczności przeprowadzenia zmian w ustawie wdrażającej tzw. dyrektywę policyjną, która obecnie nie funkcjonuje prawidłowo i nie gwarantuje właściwego postrzegania praw obywatelskich przez organy policyjne.

Monika Krasińska:
Przed nami rok wyzwań, które określiłabym trzema słowami - spójność, multidyscyplinarność i współpraca. To słowa kluczowe, a zarazem warunki niezbędne do zapewnienia skutecznej ochrony naszej prywatności.

Nieprzypadkowo używam słowa „prywatność", bo dziś w dobie cyfrowej rewolucji, to chyba w tym kontekście powinniśmy patrzeć na ochronę informacji nas dotyczących.

Rozwój technologiczny powoduje bowiem m.in. to, że informacje, które dziś postrzegamy jako neutralne, wkrótce mogą stać się danymi osobowymi.

Nietrudno wyobrazić sobie, że w wyniku połączenia przez sztuczną inteligencję różnych anonimowych – wydawałoby się – informacji może dojść do wygenerowania danych osobowych.

Czy jednak dostrzegając dobrodziejstwa, jakie wiążą się z rozwojem AI, myślimy o towarzyszących temu ryzykach? Planujemy, jak zapewnić poszanowanie praw osób, choćby takich, jak prawo do sprostowania danych czy prawo do ich usunięcia? Dyskutujemy, jak „uczyć" sztuczną inteligencję, ale czy zastanawiamy się, jak ją „oduczać", gdy wyciągnie niewłaściwe wnioski?

To tylko jeden z przykładowych problemów, z jakimi przyjdzie nam się zmierzyć.

Jednocześnie w czasach, gdy różne podmioty zbierają o nas tak wiele informacji, gdy nas profilują i z jednej strony bombardują przekazami dopasowanymi do naszych zainteresowań i poglądów, a z drugiej materiałami mającymi je zmieniać, nie możemy reagować na wiele zjawisk po fakcie. Musimy działać proaktywnie i w miarę możliwości uprzedzać trendy technologiczne, które często są trudne do przewidzenia. Musimy na nowo znaleźć równowagę między innowacjami a prawami człowieka.

Pierwszy krok na tej drodze został już zrobiony. W Unii Europejskiej powstał bowiem pakiet przepisów regulujących funkcjonowanie gospodarki cyfrowej. Teraz kluczowe będzie właściwe ich implementowanie do porządku krajowego i konsekwentne oraz spójne stosowanie.

Nie da się tego zrobić bez zapewnienia – zarówno w wymiarze europejskim, jak i krajowym – spójności przepisów, porozumienia różnych regulatorów (zwłaszcza tych działających w obszarze regulacji

cyfrowych czy ochrony praw konsumenta) oraz multidyscyplinarnego spojrzenia na poszczególne przypadki, w których dochodzi do przetwarzania informacji na nasz temat. Dla właściwej ich oceny potrzebna jest bowiem wiedza z zakresu prawa, technologii, a niekiedy nawet etyki, a słuchanie, ciągłe uczenie się i wymiana doświadczeń będą miały znaczenie kluczowe.

Paulina Dawidczyk:

Do najważniejszych wyzwań z jakimi zmierzy się UODO należeć będzie kontynuowanie wdrażania usprawnień w procesie rozpatrywania spraw skargowych. Skokowy wzrost liczby wniesionych skarg zaobserwowaliśmy w 2018 r., a w kolejnych latach liczba wnoszonych skarg jeszcze wzrosła. Porównując dane dotyczące liczby skarg wpływających do Urzędu w ostatnich latach, prognozować należy, że także w bieżącym roku oraz w kolejnych latach liczba wpływających skarg utrzyma się na podobnym, bardzo wysokim poziomie. Dlatego bardzo ważne jest stałe monitorowanie procesu rozpatrywania skarg i wdrażanie usprawnień w tym zakresie, tak, aby zapewnić odpowiednią ochronę osobom, których dane dotyczą. Bardzo ważnym krokiem w tym kierunku było wprowadzenie na początku roku 2025 przez Prezesa Urzędu Ochrony Danych Osobowych zmian organizacyjnych, m.in. poprzez utworzenie Departamentu Wstępnej Kontroli Skarg i Naruszeń, do którego w pierwszej kolejności wpływają skargi, w celu usprawnienia ich weryfikacji pod kątem formalnym.

Piotr Drobek:

Jednym z wyzwań będzie zapewnienie właściwej roli polskiego organu ochrony danych w przyszłych ramach instytucjonalnych wprowadzanych w związku z toczącymi się i planowanymi pracami nad wdrożeniem kolejnych unijnych regulacji, w szczególności Aktu w sprawie sztucznej inteligencji.

Wyzwaniem mogą się również okazać możliwe działania nowej administracji amerykańskiej, które mogą negatywnie wpłynąć na funkcjonowanie Ram prawnych ochrony danych UE-USA, powodując obniżenie zapewnianego przez nie poziomu ochrony danych, a tym samym utrudnić przekazywanie danych do USA.

Anna Dudkowska:

Największym wyzwaniem będzie sprostanie wymaganiom nowych zadań wynikających z wdrożenia do polskiego porządku prawnego unijnego Aktu o zarządzaniu danymi. Wzmacnianie Urzędu i jego zasobów jest więc zadaniem ciągłym. UODO będzie musiał jednocześnie zwiększać świadomość społeczeństwa w zakresie ochrony danych i dostosowywać swoje działania do zmieniających się regulacji.

Ważnym wyzwaniem Urzędu jest także mówienie o ochronie danych osobowych w sposób precyzyjny, ale też zrozumiały dla obywateli niebędących ekspertami w tej dziedzinie. Oznacza to konieczność budowania efektywnej komunikacji, która nie tylko informuje, ale również edukuje w przystępny

sposób o nowych obowiązkach, prawach i zagrożeniach związanych z przetwarzaniem danych. Kluczowe będzie tworzenie treści, które będą uwzględniały potrzeby różnych grup społecznych, które często potrzebują wsparcia w dostosowywaniu się do nowych regulacji.

Jednocześnie UODO musi kłaść większy nacisk na promowanie odpowiedzialności za dane wśród obywateli, pokazując, że ochrona danych osobowych to nie tylko obowiązek wynikający z przepisów prawa, ale również kluczowy element budowania zaufania w relacjach społecznych i zawodowych. Szczególną rolę odegra tutaj współpraca z sektorem edukacyjnym, organizacjami pozarządowymi oraz przedsiębiorstwami technologicznymi, które mogą przyczynić się do upowszechniania dobrych praktyk i zwiększania świadomości w tej dziedzinie. Dostosowanie działań Urzędu do zmieniających się potrzeb społeczeństwa, rozwijających się technologii oraz nowych regulacji unijnych będzie wymagało elastyczności, innowacyjności i skutecznego zarządzania zasobami.

DANE OSOBOWE W POSTANOWIENIU WYDANYM PRZEZ ORGAN ADMINISTRACJI PUBLICZNEJ

Udzielenie przez osobę prywatną informacji istotnych dla prowadzonego postępowania administracyjnego może być wystarczającym uzasadnieniem dla podania jej danych osobowych w treści wydanego w sprawie postanowienia.

Pewien obywatel zwrócił się niedawno do UODO z prośbą o rozstrzygnięcie wątpliwości co do dopuszczalności przetwarzania jego danych osobowych przez organ administracji publicznej. W tym celu przesłał swoją korespondencję z wydziałem architektury jednego z urzędów miejskich.

Wydział ów pisemnie zawiadomił go o wszczęciu postępowania dotyczącego wskazanej inwestycji budowlanej. Mężczyzna odpowiedział na nie e-mailem, informując, że inwestycja, której dotyczy pismo, została ukończona już wiele tygodni temu. W związku z tym wydział architektury wydał postanowienie, w którym – cytując fragment otrzymanego e-maila – zamieścił dane osobowe jego nadawcy oraz jego córki, której był on pełnomocnikiem. Postanowienie to zostało przekazane do kilkunastu innych adresatów – zdaniem zwracającego się do UODO obywatela – nieuprawnionych do ich pozyskania. Nabrał więc wątpliwości, czy nie doszło w ten sposób do naruszenia RODO.

W odpowiedzi UODO wskazał, że jedną z podstaw legalizujących przetwarzanie danych osobowych jest art. 6 ust. 1 lit. c) RODO. Stanowi on, że jest ono zgodne z prawem, gdy jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze.

Z treści przedstawionych dokumentów wynika, iż dane osobowe pytającego i jego córki przetwarzane są w treści postanowienia wydanego w postępowaniu administracyjnym. Z uzasadnienia orzeczenia wynika, iż był on ustanowionym w sprawie pełnomocnikiem córki, która z kolei była stroną postępowania administracyjnego. Ponadto z treści uzasadnienia postanowienia można wywnioskować, iż podana przez obywatela informacja stała się bezpośrednią przyczyną wydania przez organ administracyjny postanowienia o zawieszeniu postępowania z urzędu na podstawie art. 97 § 1 pkt 4 Kodeksu postępowania administracyjnego.

Z kolei art. 125 § 3 Kodeksu postępowania administracyjnego stanowi, że postanowienie, które może być zaskarżone do sądu administracyjnego, doręcza się stronie wraz z pouczeniem o dopuszczalności wniesienia skargi oraz **uzasadnieniem faktycznym i prawnym**. Z brzmienia tego przepisu wynika więc, iż postanowienie wydane w toku postępowania administracyjnego powinno zawierać m.in.. okoliczności faktyczne stanowiące podstawę jego wydania.

2 UODO SYGNALIZUJE

W niniejszej sprawie okolicznością wydania przez organ administracji postanowienia o zawieszeniu z urzędu postępowania w sprawie było przekazanie przez pytającego informacji o zakończeniu inwestycji budowlanej, względem której niezakończone zostało postępowanie w sprawie wydania pozwolenia na budowę. W tym kontekście wskazanie w uzasadnieniu danych osoby, która udzieliła istotnych dla postępowania informacji, może być uznane za istotny element uzasadnienia faktycznego wydanego postanowienia (art. 125 § 3 kpa), co uzasadniać może przetwarzanie tych danych w treści uzasadnienia.

Postanowienie zostało doręczone osobom, które były stronami postępowania administracyjnego. Z art. 101 § 1 Kodeksu postępowania administracyjnego wynika bowiem, iż o postanowieniu w sprawie zawieszenia albo podjęcia postępowania organ administracji publicznej **zawiadamia strony**. Uznać więc należy, iż obowiązek doręczenia orzeczenia do określonych podmiotów wynika z przepisów dotyczących procedury administracyjnej i krąg odbiorców takiego orzeczenia jest ograniczony, tj. może je otrzymać jedynie podmiot posiadający status strony postępowania (względnie pełnomocnik takiej strony).

Fot. pexels

UODO ZACHĘCA JEDNOSTKI SAMORZĄDU TERYTORIALNEGO DO OPRACOWANIA KODEKSU POSTĘPOWANIA

Kodeks postępowania mógłby ułatwić jednostkom samorządu terytorialnego właściwe wdrożenie zasad ochrony danych osobowych. Obecnie miewają one z tym problemy m.in. ze względu na nieprecyzyjne przepisy prawa czy różny poziom świadomości w zakresie realizacji obowiązków w związku z przetwarzaniem danych osobowych. UODO zachęca przedstawicieli samorządu do podjęcia wysiłku w tym zakresie i deklaruje eksperckie wsparcie.

W 2024 roku z inicjatywy Prezesa Urzędu Ochrony Danych Osobowych odbył się cykl spotkań z przedstawicielami najważniejszych organizacji zrzeszających jednostki samorządu terytorialnego (JST) wszystkich szczebli:

- Unią Metropolii Polskich,
- Związkiem Miast Polskich,
- Związkiem Gmin Wiejskich,
- Związkiem Województw Rzeczypospolitej Polskiej,
- Związkiem Powiatów Polskich.

Były one okazją do omówienia problemów związanych ze stosowaniem przepisów dotyczących ochrony danych osobowych przez administratorów i podmioty przetwarzające z sektora samorządu terytorialnego oraz do wymiany poglądów i doświadczeń.

Przeprowadzone rozmowy potwierdzają, że główną przyczyną rozbieżności i wątpliwości w stosowaniu zasad ochrony danych osobowych są przede wszystkim nieprecyzyjne przepisy prawa, na podstawie których zobowiązane są działać jednostki samorządu terytorialnego. Problemem jest także różny poziom świadomości i wiedzy administratorów oraz podmiotów przetwarzających z tego sektora co do obowiązków, jakie ciążą na nich w związku z przetwarzaniem danych osobowych. To z kolei powoduje m.in. niewłaściwe usytuowanie w strukturze organizacyjnej urzędu inspektora ochrony danych, a także błędne określenie jego zadań.

Na kłopoty – kodeks postępowania

Ogólne rozporządzenie o ochronie danych (RODO) umożliwia administratorom oraz podmiotom przetwarzającym z danego sektora (branży) zbudowanie wspólnej bazy dobrych praktyk w zakresie ochrony danych osobowych w postaci kodeksu postępowania. Zasady jego tworzenia i procedurę zatwierdzenia przed Prezesem UODO regulują:

- **art. 40 RODO,**
- **art. 27 ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz**
- **wydane przez Europejską Radę Ochrony Danych (EROD) Wytyczne 1/2019 dotyczące kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679.**

Taki dokument może być bardzo pomocny w codziennej pracy, gdyż wskazuje, jak zastosować RODO i przepisy branżowe w konkretnych sytuacjach. Jednocześnie pozwala wyeliminować ryzyko niewłaściwej interpretacji przepisów prawa, a także ryzyko nieadekwatnego przetwarzania danych czy wprowadzania zbędnych procesów przetwarzania danych.

Oprócz standaryzacji w zakresie realizacji obowiązków wynikających z RODO kodeksy postępowania mają także stanowić narzędzie rozliczalności (por. art. 5 ust. 2, art. 24 ust. 3, art. 28 ust. 5, art. 32 ust. 3, art. 46 ust. 2 lit. e RODO). Ponadto ich stosowanie jest brane pod uwagę przez Prezesa UODO przy podejmowaniu decyzji o ewentualnym nałożeniu administracyjnej kary pieniężnej i jej wysokości (art. 83 ust. 2 lit. j RODO).

Z kolei dla osób, których dane przetwarzają podmioty, które przystąpiły do kodeksu, to gwarancja odpowiedzialnego i zgodnego z prawem podchodzenia do ochrony tych danych.

Zatem korzyści ze stosowania kodeksu postępowania są bezdyskusyjne.

Warto zatem, by **jednostki samorządu terytorialnego rozważyły zasadność opracowania takiego dokumentu wspólnie lub oddzielnie dla poszczególnych jego szczebli.**

Nie ma zamkniętego katalogu zagadnień, które kodeks postępowania musi regulować. Może więc powstać kodeks obejmujący niewielki wycinek spraw, za to charakterystycznych i ważnych dla danego sektora.

Pierwsze kroki na tej drodze zostały już zresztą zrobione. Prace nad kodeksem postępowania z danymi osobowymi w jednostkach samorządu terytorialnego zostały bowiem zainicjowane przez Instytut Szkoleniowo – Doradczy z Łodzi oraz Związek Województw RP. W lipcu 2024 r. z przedstawicielami tej inicjatywy spotkali się pracownicy Wydziału Kodeksów i Certyfikacji w Departamencie Orzecznictwa i Legislacji UODO, a w październiku również Zastępca Prezesa UODO – Konrad Komornicki.

Główne wyzwania

Mając jednak na uwadze:

• wymogi, jakie musi spełniać kodeks, aby został zatwierdzony przez Prezesa UODO (por. p. 19 - 41 Wytycznych EROD 1/2019 oraz przepisy Kodeksu postępowania administracyjnego w zw. z art. 7 ustawy z 10 maja 2018 r. o ochronie danych osobowych)

• oraz dużą liczbę jednostek samorządu terytorialnego różnego szczebla (gminy, powiaty, województwa) i szeroki zakres realizowanych przez nie zadań

wydaje się, że największymi wyzwaniami dla twórców kodeksów dla tego sektora będzie ustalenie przez nich następujących kwestii:

1) zakresu podmiotowego kodeksu, czyli wskazanie, którzy administratorzy/ podmioty przetwarzające będą mogli przystąpić do kodeksu, np. czy tylko z gmin, powiatów, województw, czy jednostki organizacyjne tych samorządów, a może kodeks będzie dedykowany wszystkim;

2) kto będzie twórcą kodeksu, czyli podmiotem reprezentującym określone kategorie administratorów lub podmioty przetwarzające, którzy będą mogli zostać członkami kodeksu (por. pkt. 21 i 22 Wytycznych EROD 1/2019). W postępowaniu przed Prezesem UODO ws. zatwierdzenia kodeksu jego twórca musi wykazać, że jest faktycznym organem przedstawicielskim i że rozumie potrzeby swoich członków. Wpływ na określenie twórcy kodeksu dla JST będzie miał zakres podmiotowy stosowania kodeksu, o którym mowa powyżej;

3) zakresu przedmiotowego kodeksu, czyli operacji przetwarzania danych osobowych, do których kodeks będzie miał zastosowanie, a także kategorii administratorów/podmiotów przetwarzających, którzy w nich uczestniczą. To twórca kodeksu, znając specyfikę problemów ze stosowaniem zasad ochrony danych osobowych pojawiających się w reprezentowanym przez niego sektorze, podejmuje decyzję, co powinno zostać uregulowane w kodeksie. Kodeks ma standaryzować i rozwiązywać problemy związane z przetwarzaniem danych osobowych – ma przedstawiać praktyczne rozwiązania. Twórcy kodeksu powinni mieć zatem na uwadze art. 40 ust. 2 RODO, z zastrzeżeniem, że nie jest to katalog zamknięty i obowiązkowy do uwzględnienia w pracach nad kodeksem. Identyfikując zagadnienia do uregulowania, twórcy kodeksów muszą uwzględnić cele, jakie ma spełniać ten kodeks (por. pkt 20 Wytycznych EROD 1/2019) oraz przyjąć rozwiązania zgodne z tzw. kryteriami zatwierdzenia kodeksu (por. pkt. 32-41 Wytycznych EROD 1/2019);

4) mechanizmu monitorowania, czyli ustanowienie struktur i procedur, które umożliwią przede wszystkim:

• weryfikowanie, czy administratorzy/podmioty przetwarzające, którzy chcą przystąpić do kodeksu

postępowania, spełniają warunki wynikające z tego kodeksu,

• bieżący nadzór nad przestrzeganiem postanowień kodeksu przez jego członków (np. audyty planowe i doraźne),

• rozpatrywanie skarg na członków kodeksu,

• cykliczny przegląd funkcjonowania kodeksu w celu dostosowania jego treści do obowiązujących przepisów prawa czy wprowadzenie zmian wynikających z praktyki stosowania kodeksu itd.,

• przekazywanie Prezesowi UODO sprawozdań dotyczących funkcjonowania kodeksu oraz innych niezbędnych informacji.

Twórcy kodeksu postępowania dla JST muszą sami zaprojektować taki mechanizm, który obejmowałby powyższe czynności, mając jednak na uwadze treść art. 41 ust. 6 RODO, który wyłącza możliwość prowadzenia monitorowania kodeksu skierowanego do sektora publicznego przez podmiot monitorujący. W ocenie EROD sektor publiczny może rozważyć dostosowanie wymogów w zakresie audytu, tak aby obejmowały one również monitorowanie kodeksu (por. pkt 88 Wytycznych EROD 1/2019). Warto przypomnieć, że w grudniu 2023 r. Prezes UODO zatwierdził Kodeks postępowania dla sektora ochrony zdrowia (PFSz), który zawiera m.in. rozwiązania dotyczące mechanizmu monitorowania przestrzegania jego postanowień przez podmioty z sektora publicznego;

5) przeprowadzenie konsultacji treści projektu kodeksu ze wszystkimi zainteresowanymi, czyli przede wszystkim z sektorem, który ma stosować kodeks i z osobami, których będzie dotyczyło opisane w tym kodeksie przetwarzanie danych osobowych. W przypadku kodeksu dla JST zapewne należałoby również nawiązać kontakt z resortami spraw wewnętrznych i administracji oraz cyfryzacji, ale nie tylko – będzie to uzależnione od tego, jakich procesów przetwarzania danych osobowych będzie dotyczył kodeks.

Twórcy kodeksów, które zostały już zatwierdzone przez Prezesa UODO, kontaktowali się także z organizacjami statutowo zajmującymi się ochroną danych osobowych. Dobrym sposobem na przeprowadzenie konsultacji projektu kodeksu jest zamieszczenie jego treści np. na stronie internetowej twórcy kodeksu czy jego przyszłych członków i wyznaczenie terminu, do którego można zgłaszać uwagi co do jego treści. Należy podkreślić, że Prezes UODO nie jest uczestnikiem tych konsultacji, ale może na tym etapie promować i wspierać inicjatywę kodeksową.

Twórca kodeksu w postępowaniu w sprawie zatwierdzenia projektu kodeksu ma obowiązek wykazać przeprowadzenie konsultacji (por. art. 27 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz pkt 28 Wytycznych EROD 1/2019). Projekt kodeksu musi zawierać informację dotyczącą zakresu przeprowadzonych konsultacji, a do wniosku o zatwierdzenie projektu kodeksu

należy dołączyć raport z tych konsultacji, z którego będzie wynikało m.in., czy zgłoszone uwagi zostały uwzględnione.

Wsparcie UODO

Informacje na temat opracowania kodeksu postępowania, wymogów formalnych, które musi spełniać wniosek o zatwierdzenie takiego kodeksu i przebiegu takiego postępowania są dostępne **na stronie internetowej UODO w zakładce: DLA ADMINISTRATORA/Kodeksy i certyfikacja. Ponadto Prezes UODO zaprasza wszystkie inicjatywy planujące rozpoczęcie prac nad kodeksem do kierowania** pytań na adres e-mail Departamentu Prawa i Nowych Technologii dpnt@uodo.gov.pl.

Jednym ze sposobów zachęcania różnych środowisk do sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu RODO – co należy do zadań organu nadzorczego – są też spotkania przedstawicieli UODO z inicjatywami, które rozważają opracowanie lub już pracują nad tymi dokumentami.

Doskonałą okazją do omawiania zasad i procedur związanych z tworzeniem kodeksów postępowania oraz do wymiany doświadczeń w zakresie stosowania zasad ochrony danych osobowych przez jednostki samorządu terytorialnego są wydarzenia organizowane przez Prezesa Urzędu Ochrony Danych Osobowych w ramach akcji „UODO rusza w kraj". Pierwsze spotkania odbyły się już w województwie małopolskim i śląskim (komunikat po tym wydarzeniu). Kolejne odbędą się w 2025 r., a szczegółowe informacje na ich temat będą sukcesywnie zamieszczane na stronie internetowej UODO.

Fot. pixabay

WSA W WARSZAWIE PODTRZYMAŁ DECYZJĘ PUODO, ODDALAJĄC SKARGĘ C. SP. Z O.O.

Na spółkę poskarżył się były pracownik: zarzucił jej, że przetwarza jego dane w zakresie adresu e-mail zawierającego pierwszą literę imienia oraz nazwisko, bez podstawy prawnej. Nie pracuje bowiem w tej firmie od pięciu miesięcy.

Okazało się jednak, że spółka korzystała z tego adresu do kontaktów z potencjalnymi klientami i nie chciała ryzykować skasowania go. Twierdziła, że usunięcie tego konta spowodowałoby negatywne konsekwencje w postaci utraty intratnych relacji handlowych z kontrahentami oraz klientami.

PUODO podkreślił, że rozumie problem spółki, ale przetwarzanie służbowego adresu mailowego byłego pracownika powinno zostać ograniczone do automatycznej wiadomości wysłanej do nadawców (że ten adres nie jest już aktualny, ze wskazaniem, jaki mail służy teraz do kontaktu z przedstawicielami spółki). PUODO nakazał spółce usunięcie adresu. Ta zaś zaskarżyła tę decyzję do WSA.

Sąd skargę odrzucił. Stwierdził m.in.: „imienne oznaczenie elektronicznej skrzynki pocztowej przypisanej do uczestnika postępowania (pierwszą literą jego imienia i nazwiskiem), stanowiące dane osobowe podlegające przepisom RODO, implikuje – w sytuacji zakończenia stosunku pracy uczestnika postępowania – konieczność usunięcia takiego adresu skrzynki, np. poprzez zastąpienie go innym oznaczeniem. Zachowanie ww. adresu e-mail (nawet zdezaktywowanego) nie jest niezbędne do kontynuacji prowadzonych uprzednio przez uczestnika postępowania działań na rzecz podtrzymania więzi handlowych lub pozyskania nowych kontrahentów/klientów spółki. Co więcej, może ono wprowadzać w błąd, że uczestnik postępowania nadal jest zatrudniony w spółce. Zatem sama dezaktywacja spornego adresu nie jest wystarczająca”.

Z treścią decyzji PUODO można zapoznać się na stronie UODO.

Sygnatura akt: II SA/Wa 1007/23

Sygnatura sprawy: DS.523.2244.2022

JAK DOKUMENTOWAĆ NARUSZENIA OCHRONY DANYCH OSOBOWYCH?

Administratorzy mają obowiązek gromadzić informacje o wszystkich naruszeniach ochrony danych osobowych – także tych, których nie trzeba zgłaszać Prezesowi UODO. Przedstawiamy rolę rejestru naruszeń ochrony danych osobowych oraz wskazówki dotyczące jego prowadzenia.

Dlaczego dokumentowanie naruszeń ochrony danych osobowych jest ważne?

Prowadzenie takiej dokumentacji jest nie tylko obowiązkiem prawnym. **To narzędzie, które pomaga organizacjom lepiej zarządzać naruszeniami ochrony danych osobowych.** Gromadzenie informacji na ten temat umożliwia pogłębioną analizę zagrożeń i ułatwia dobieranie skutecznych zabezpieczeń.

Obowiązek prawny dokumentowania naruszeń ochrony danych osobowych wynika z **art. 33 ust. 5 RODO:**

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu [na] weryfikowanie przestrzegania niniejszego artykułu.

Dokumentacja zawierająca informacje o wykrytych naruszeniach ochrony danych osobowych jest **podstawą do wykazania, że administrator działa zgodnie z przepisami**. Ma to związek z **zasadą rozliczalności** (art. 5 ust. 2 RODO).

Kogo dotyczy obowiązek dokumentowania?

Dokumentowanie naruszeń ochrony danych osobowych jest **wyłącznym obowiązkiem administratorów.** Podmioty przetwarzające powinny jednak **pomagać** w jego realizacji, np. poprzez przekazywanie administratorom wszelkich niezbędnych informacji o naruszeniach ochrony danych osobowych (art. 28 ust. 3 lit. f RODO).

Organizacje powinny też korzystać ze wsparcia inspektorów ochrony danych, polegającego na formułowaniu **wskazówek i opinii** dotyczących projektowania dokumentacji i zarządzania nią. Inspektorzy powinni także kontrolować, czy rejestry prowadzone są w sposób prawidłowy. Należy przy tym pamiętać, aby nie nakładać na inspektora zadań w zakresie obsługi naruszeń ochrony danych osobowych, które zagrażałyby jego **niezależności**, w szczególności **powodowały konflikt interesów** (art. 38 ust. 6 RODO)[1].

4 NARUSZENIA I KONTROLE

Jak prawidłowo dokumentować naruszenia ochrony danych osobowych?

Administratorzy powinni **na bieżąco** aktualizować katalog wykrytych naruszeń ochrony danych osobowych, utrwalając informacje w odpowiednich rejestrach. Choć odrębna ewidencja nie jest formalnie wymagana, musi być **wyraźnie oznaczona i dostępna do wglądu** na żądanie Prezesa UODO.

Obowiązek obejmuje **wszystkie naruszenia ochrony danych osobowych**, bez względu na to, czy wymagają one zgłoszenia organowi nadzorczemu. Rejestr naruszeń ochrony danych osobowych jest miejscem, w którym administrator powinien zamieścić m.in. **uzasadnienie decyzji o niezgłaszaniu naruszenia ochrony danych osobowych**, w przypadku zaistnienia ku temu stosownej przesłanki (art. 33 ust. 1 RODO). Ma to szczególne znaczenie, gdy z czasem ocena incydentu ulegnie zmianie i jego notyfikacja stanie się konieczna.

W RODO nie wskazano okresów przechowywania informacji o naruszeniach ochrony danych osobowych. Administratorzy powinni więc dysponować pełną dokumentacją tak długo i w takim zakresie, w jakim związani są zasadą rozliczalności. Innymi słowy, **jak najdłużej**. Z tego powodu umieszczanie w takim rejestrze jakichkolwiek danych osobowych **nie jest zalecane**. Jeżeli jednak tam się znajdą, należy pamiętać o ich prawidłowej ochronie, w tym o zasadzie ograniczenia przechowywania (art. 5 ust. 1 lit. e RODO).

Jakie informacje powinny znaleźć się w dokumentacji?

Rejestr naruszeń ochrony danych osobowych powinien uwzględniać m.in.:

• **okoliczności** naruszenia ochrony danych osobowych (takie jak data i czas wystąpienia, „stwierdzenia" i zakończenia naruszenia, sposób wykrycia naruszenia, przyczyny naruszenia, rodzaj naruszenia, przebieg naruszenia, rodzaj i zakres danych objętych naruszeniem, liczba i kategorie osób, których dane dotyczą);

• **skutki** (jeżeli wystąpiły) i/lub **możliwe skutki** naruszenia ochrony danych osobowych dla osób, których dane dotyczą;

• uzasadnienie oceny ryzyka;

• **podjęte działania zaradcze** (w celu powstrzymania i ograniczenia naruszenia ochrony danych osobowych oraz zminimalizowania jego skutków) i **zapobiegawcze** (w celu zminimalizowania wystąpienia podobnych naruszeń ochrony danych osobowych w przyszłości);

• **szczegóły dotyczące zgłoszenia naruszenia ochrony danych osobowych Prezesowi UODO** (takie jak data zgłoszenia, ewentualne przyczyny opóźnienia w zgłoszeniu, inne istotne informacje zawarte w zgłoszeniu; jeżeli administrator je zgłosił) lub **uzasadnienie decyzji o niezgłoszeniu naruszenia**

ochrony danych osobowych Prezesowi UODO (art. 33 ust. 1 RODO);

• **szczegóły dotyczące zawiadomienia osób, których dane dotyczą, o naruszeniu ochrony danych osobowych** (takie jak data zawiadomienia, treść zawiadomienia, metoda zawiadomienia, liczba zawiadomionych osób; jeżeli administrator je zawiadomił) lub – w stosownym przypadku – **uzasadnienie decyzji o niezawiadomieniu osób, których dane dotyczą, o naruszeniu ochrony danych osobowych** (art. 34 ust. 3 RODO).

Podsumowanie

Staranne dokumentowanie naruszeń ochrony danych osobowych to ważny element realizacji zasady rozliczalności i zapewnienia bezpieczeństwa przetwarzania. Dlatego też warto pamiętać o kilku dobrych praktykach:

1. Dokumentuj wszystkie naruszenia ochrony danych osobowych – Każdy przypadek naruszenia ochrony danych osobowych, niezależnie od tego, czy wymaga zgłoszenia Prezesowi UODO, musi zostać zarejestrowany.

2. Szczegółowo opisuj okoliczności zdarzenia – Uwzględnij takie informacje jak data i czas wystąpienia oraz wykrycia naruszenia ochrony danych osobowych, jego przyczyny, przebieg, liczba objętych nim osób oraz rodzaj i zakres naruszonych danych.

3. Rejestruj skutki – Wskaż faktyczne oraz potencjalne konsekwencje naruszenia ochrony danych osobowych dla osób, których dane dotyczą.

4. Dokumentuj działania zaradcze i zapobiegawcze – Opisz środki podjęte w celu ograniczenia skutków naruszenia ochrony danych osobowych oraz kroki mające zapobiec podobnym incydentom w przyszłości.

5. Aktualizuj rejestr na bieżąco – Utrwalaj informacje o naruszeniach ochrony danych osobowych niezwłocznie po ich wykryciu oraz uzupełniaj dane w miarę ich pozyskiwania.

6. Monitoruj proces dokumentowania – Regularnie weryfikuj prawidłowość i kompletność rejestru oraz procedur związanych z dokumentowaniem naruszeń ochrony danych osobowych, aby uniknąć ewentualnych braków.

7. Dbaj o przejrzystość i dostępność dokumentacji – Rejestr naruszeń ochrony danych osobowych powinien być kompletny, czytelny oraz dostępny dla organu nadzorczego na jego żądanie.

[1] Więcej na ten temat w artykule „Rola IOD przy naruszeniach ochrony danych osobowych” opublikowanym w „Biuletynie UODO” nr 10/10/24.

2025: ROK REWOLUCJI TECHNOLOGICZNEJ W OCHRONIE DANYCH – PRZEWIDYWANIA NA PODSTAWIE WNIOSKÓW Z NAJNOWSZEGO RAPORTU TECHSONAR 2025

Technologia rozwija się w niesamowitym tempie, a rok 2024 był tego najlepszym dowodem. Świat doświadczył przełomów takich jak zastosowanie generatywnej sztucznej inteligencji w medycynie, dynamiczny rozwój kwantowej kryptografii oraz praktyczne wdrożenia cyfrowych bliźniaków w zarządzaniu miastami. Każda z tych innowacji wyznaczała nowe standardy, ale też prowokowała pytania o ich wpływ na prywatność i ochronę danych.

Czy tempo tych zmian utrzyma się, a nawet przyspieszy? Warto przyjrzeć się prognozom zawartym w raporcie TechSonar 2025, który stanowi przewodnik po nadchodzących trendach i ich możliwym wpływie na ochronę danych.

Czym jest TechSonar?

TechSonar to inicjatywa Europejskiego Inspektora Ochrony Danych (EIOD), która identyfikuje najważniejsze trendy technologiczne w kontekście ochrony danych osobowych. Raport ten ma na celu przewidywanie kierunków rozwoju technologii i ich wpływu na prywatność, umożliwiając podejmowanie działań prewencyjnych, zanim ryzyka związane z nowymi technologiami staną się realnym zagrożeniem.

TechSonar 2025 wskazuje sześć kluczowych trendów technologicznych, które mogą zmienić sposób, w jaki chronimy dane osobowe. Niektóre technologie opisane w najnowszym raporcie TechSonar mogą pomóc w ograniczaniu ryzyka związanego z podstawowymi prawami jednostek. Z kolei inne, choć obiecują znaczące korzyści ekonomiczne, mogą stanowić poważne zagrożenie dla osób, jeśli nie będą właściwie zarządzane. Dlatego kluczowe stają się analizy ryzyka i wdrażanie solidnych środków ochronnych.

W kontekście sztucznej inteligencji, dostawcy i użytkownicy systemów AI muszą dokładnie oceniać ich wpływ, identyfikować potencjalne zagrożenia i podejmować działania zapobiegawcze, tym bardziej, że dynamiczny rozwój tej dziedziny, w połączeniu z możliwością wysokich zysków, napędza wyścig

w obszarze sztucznej inteligencji, co sprawia, że systemy AI stają się coraz bardziej obecne w naszym codziennym życiu.

Ponadto w raporcie przedstawiono scenariusze dotyczące każdego z sześciu trendów związanych ze sztuczną inteligencją. Opisujemy je poniżej. Warto podkreślić, że EIOD nie aprobuje tych przypadków użycia – ich jedynym celem jest zobrazowanie potencjalnych sytuacji, które mogą wynikać z zastosowania tych technologii. Scenariusze te mogą poruszać istotne kwestie związane z prawem do prywatności, ochroną danych osobowych, a także z szerszym wpływem na społeczeństwo.

Najważniejsze trendy technologiczne na 2025 rok

1. Retrieval-Augmented Generation (RAG)

Modele generatywne takie jak ChatGPT, są wzbogacane o dostęp do zewnętrznych baz wiedzy. Dzięki temu mogą dostarczać bardziej precyzyjne i aktualne odpowiedzi, jednocześnie zmniejszając ryzyko generowania nieprawdziwych informacji.

Należy jednak podkreślić, że systemy RAG wykorzystują dane zewnętrzne i zasoby informacji, które mogą zawierać dane osobowe. Jeśli zapytanie użytkownika jest bardzo szczegółowe, system RAG może przypadkowo pobrać i ujawnić takie dane, zwłaszcza jeśli znajdują się one w materiałach źródłowych lub w danych szkoleniowych. Takie ujawnienie stanowiłoby naruszenie ochrony danych osobowych, co jest szczególnie problematyczne w kontekście zgodności z przepisami RODO.

2. AI działające na urządzeniach (On-Device AI)

Dzięki edge computing możliwe jest lokalne przetwarzanie danych na urządzeniach użytkownika. To nie tylko przyspiesza działanie systemów, ale także minimalizuje konieczność przesyłania wrażliwych informacji do chmury, co zwiększa bezpieczeństwo. Chociaż przetwarzanie danych lokalnie może poprawić prywatność, jeśli urządzenie nie jest odpowiednio zabezpieczone (np. brak szyfrowania lub słabe hasła), to dane mogą być łatwiejszym celem dla atakujących.

3. AI multimodalna (Multimodal AI)

Nowe modele AI łączą dane różnych typów, takich jak tekst, obraz czy dźwięk, umożliwiając bardziej kompleksowe analizy i zastosowania. Tego rodzaju integracja może jednak wymagać zaawansowanych mechanizmów ochrony danych, aby zapobiec nadużyciom. Systemy te mają tendencję do zbierania danych z wielu źródeł jednocześnie, co może prowadzić do nadmiernego gromadzenia informacji, nie zawsze niezbędnych do celów przetwarzania. W efekcie firmy mogą posiadać ogromne ilości danych osobowych, których zbieranie i przetwarzanie może być niezgodne z zasadami minimalizacji danych zgodnie z RODO.

4. Skalowalny nadzór (Scalable Oversight)

Złożoność nowoczesnych systemów AI wymaga bardziej efektywnych metod monitorowania ich działania. Skalowalny nadzór pozwala na bieżące śledzenie zgodności z przepisami i zasadami etycznymi, co ma kluczowe znaczenie w kontekście dynamicznie rozwijających się technologii.

5. Neuro-symboliczna sztuczna inteligencja (Neuro-Symbolic AI)

Połączenie sieci neuronowych z tradycyjną logiką symboliczną pozwala AI lepiej rozwiązywać złożone problemy. Może to zwiększyć efektywność systemów AI, ale jednocześnie stawia wyzwania związane z odpowiedzialnością za podejmowane decyzje.

6. Oduczanie się maszyn (Machine Unlearning)

Jednym z najbardziej przełomowych osiągnięć przedstawionych w TechSonar 2025 jest bez wątpienia technologia „oduczania się maszyn". Odgrywa kluczową rolę w kontekście wymagań stawianych przez RODO, w szczególności w zakresie prawa do bycia zapomnianym (art. 17 RODO). Zgodnie z tym przepisem, osoby fizyczne mają prawo żądać usunięcia swoich danych osobowych, jeśli dalsze ich przetwarzanie nie jest uzasadnione prawnie lub narusza ich prywatność. W przypadku sztucznej inteligencji, która opiera swoje działanie na dużych zbiorach danych, realizacja tego prawa może być wyzwaniem. Technologia „oduczania się maszyn" może okazać się rozwiązaniem tego problemu, umożliwiając efektywne zarządzanie danymi w zgodzie z regulacjami prawnymi.

W kontekście RODO technologia ta pozwoli na:

• realizację prawa do bycia zapomnianym. Modele AI mogą usuwać wpływ konkretnych danych treningowych, co zapewni, że dane osoby, która żąda ich usunięcia, nie są już wykorzystywane w procesach decyzyjnych.

• zgodność z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO) poprzez redukcję zbiorów danych do tych, które są niezbędne, oraz eliminację danych, które nie powinny być już przetwarzane.

• zapobieganie naruszeniom bezpieczeństwa danych (art. 32 RODO), ponieważ usuwanie nieaktualnych lub nieautoryzowanych danych minimalizuje ryzyko błędnych lub niepożądanych decyzji modeli AI, które mogłyby prowadzić do naruszenia praw osób fizycznych.

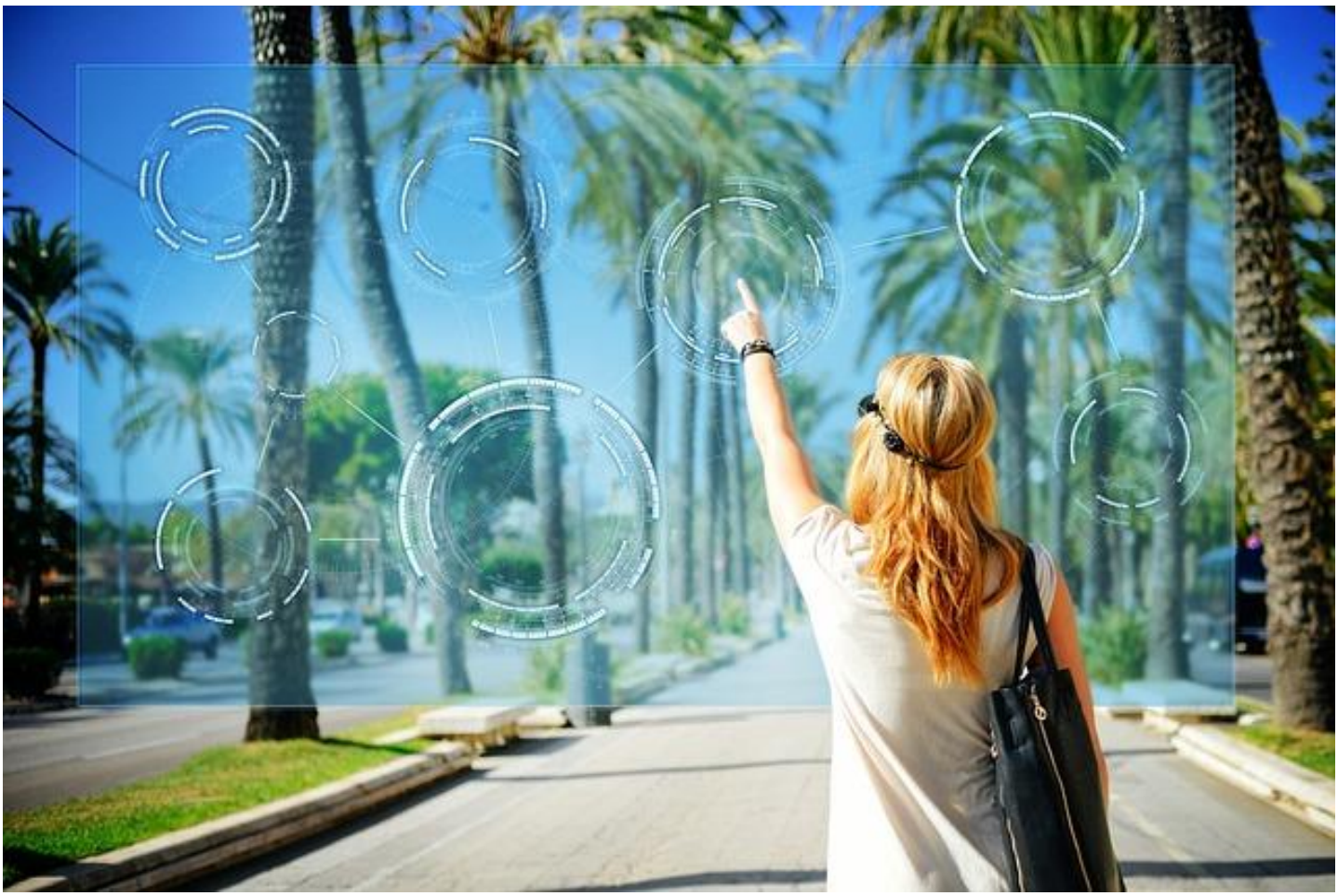
Ponadto technologia „oduczania się maszyn" może wesprzeć przejrzystość działań przetwarzania danych (art. 12 RODO), umożliwiając użytkownikom lepsze zrozumienie, jak ich dane są przetwarzane i w jaki sposób mogą być usunięte z modeli AI. Dla administratorów danych staje się to cennym narzędziem, pozwalającym skuteczniej odpowiadać na żądania podmiotów danych oraz spełniać obowiązki wynikające z zasad ochrony prywatności w fazie projektowania (privacy by design) i domyślnej ochrony danych (privacy by default) zgodnie z art. 25 RODO.

5 NOWE TECHNOLOGIE

Podsumowując: nie wiemy, jakie nowe technologie przyniosą kolejne lata, ale jedno jest pewne: nadążanie za tymi zmianami i zapewnianie zgodności z przepisami to klucz do budowania zaufania w cyfrowym świecie.

TechSonar 2025 pokazuje, że odpowiedzialne podejście do innowacji może być fundamentem zrównoważonej przyszłości, w której technologia służy człowiekowi, a nie na odwrót.

Niezwykle istotne jest nadążanie za zmianami poprzez edukację i budowanie świadomości zarówno wśród użytkowników, jak i w organizacjach. Kampanie społeczne, szkolenia i inwestowanie w kompetencje cyfrowe przyczyniają się do lepszego zrozumienia zagrożeń, ale także zwiększenia świadomości na temat ochrony danych. Rok 2025 może stać się rokiem, w którym odpowiedzialność za ochronę danych będzie naturalnym elementem korzystania z nowych technologii, a społeczeństwo zyska większą kontrolę nad swoją prywatnością w cyfrowym świecie.



Fot. pixabay

EROD SPOTYKA SIĘ Z KRAJAMI ZAPEWNIAJĄCYMI ODPOWIEDNI STOPIEŃ OCHRONY

8 października 2024 r. Europejska Rada Ochrony Danych spotkała się z rzecznikami i przedstawicielami organów ochrony danych z 15 państw, wobec których UE wydała decyzję stwierdzającą odpowiedni stopień ochrony. Spotkanie odbyło się przy okazji październikowego posiedzenia plenarnego EROD i odzwierciedla zobowiązanie EROD do zaangażowania na arenie międzynarodowej.

Do tej pory Komisja Europejska uznała następujące kraje za zapewniające odpowiedni stopień ochrony: **Andorę, Argentynę, Kanadę, Wyspy Owcze, Guernsey, Izrael, Wyspę Man, Japonię, Jersey, Nową Zelandię, Republikę Korei, Szwajcarię, Zjednoczone Królestwo, Urugwaj i Stany Zjednoczone.**

Decyzje stwierdzające odpowiedni stopień ochrony są wynikiem wysokiego stopnia konwergencji przepisów o ochronie danych i umożliwiają bezpieczniejszy przepływ danych.

Decyzje stwierdzające odpowiedni stopień ochrony są wynikiem kluczowego mechanizmu w ramach UE w zakresie ochrony danych. Umożliwia on swobodny przepływ danych osobowych z UE do krajów zapewniających odpowiedni stopień ochrony, pod warunkiem, że Komisja Europejska zdecydowała, że kraje te zapewniają odpowiedni stopień ochrony danych. W takim przypadku przekazanie danych nie wymaga żadnego szczególnego zezwolenia. Decyzje stwierdzające odpowiedni stopień ochrony promują międzynarodowe przekazywanie danych, nie wymagając od przedsiębiorstw w tych krajach posiadania standardowych klauzul umownych ani wiążących reguł korporacyjnych.

Źródło: komunikat Europejskiej Rady Ochrony Danych

NORWESKI ORGAN OCHRONY DANYCH NAŁOŻYŁ KARĘ ADMINISTRACYJNĄ NA UNIWERSYTET W AGDER

Na mocy decyzji z dnia 4 września 2024 r. norweski organ ochrony danych nałożył administracyjną karę pieniężną w wysokości około 12 700 euro na Uniwersytet w Agder za naruszenie przepisów RODO.

Powodem było niezapewnienie odpowiednich środków ochrony danych osobowych przy użyciu Microsoft Teams. Naruszenie zostało wykryte w lutym 2024 roku, gdy pracownik odkrył, że dokumenty zawierające dane osobowe były dostępne w otwartych folderach. Umożliwiało to dostęp do nich osobom nieupoważnionym. Dane dostępne były od sierpnia 2018 roku, czyli odkąd Uniwersytet rozpoczął korzystanie z platformy Teams.

W wyniku tego naruszenia dane osobowe około 16 tys. osób, w tym pracowników, studentów oraz osób zewnętrznych, były dostępne dla innych pracowników Uniwersytetu. Dokumenty zawierały informacje takie jak imiona i nazwiska, numery identyfikacyjne, informacje o egzaminach specjalnych, liczba podejść do egzaminów oraz dodatkowe ustalenia. Naruszenie objęło również dane uchodźców z Ukrainy związanych z Uniwersytetem, w tym ich dane kontaktowe, status osiedlenia oraz informacje o edukacji.

Norweski organ ochrony danych stwierdził, że Uniwersytet w Agder nie zastosował odpowiednich środków bezpieczeństwa, które byłyby zgodne z wymogami RODO, szczególnie w zakresie art. 32 (bezpieczeństwo przetwarzania) i art. 24 (obowiązki administratora). Organ norweski nakazał Uniwersytetowi wdrożenie skuteczniejszych zabezpieczeń, aby uniknąć podobnych naruszeń w przyszłości i lepiej chronić dane osobowe przechowywane i udostępniane w Microsoft Teams.

Źródło: komunikat Europejskiej Rady Ochrony Danych
Dalsze informacje: komunikat norweskiego organu ochrony danych

NORWESKI ORGAN OCHRONY DANYCH NAŁOŻYŁ KARĘ ADMINISTRACYJNĄ NA GMINĘ EIDSKOG

Norweski organ ochrony danych nałożył karę administracyjną na gminę Eidskog w wysokości około 21 tysięcy euro (250 tysięcy NOK) za naruszenie wymogów RODO dotyczących podstaw prawnych przetwarzania danych.

Decyzja, podjęta 28 czerwca 2024 roku, wynika z przypadków niezgodnego z przepisami udostępniania poufnych informacji. Przez kilka lat gmina Eidskog publikowała w rejestrach publicznych szczegóły na temat osoby zgłaszającej nieprawidłowości, nie zachowując wymaganego poziomu poufności.

Norweski organ ochrony danych uznał, że gmina złamała przepisy, ujawniając dane bez odpowiedniej podstawy prawnej i nie dokonała właściwego zanonimizowania informacji, co doprowadziło do ujawnienia wrażliwych danych o stanie zdrowia fizycznego i psychicznego oraz sytuacji finansowej osoby zgłaszającej.

Norweski organ ochrony danych wskazał, że gmina naruszyła przepisy RODO (artykuł 6 – zgodność przetwarzania z prawem, artykuł 9 – przetwarzanie szczególnych kategorii danych osobowych) oraz złamała obowiązek zachowania poufności wynikający z ustawy o dostępie do informacji publicznej. Nieprawidłowości te wykazały, że gmina Eidskog nie stosuje zasad ochrony danych wymaganych przez prawo.

W związku z powyższymi naruszeniami norweski organ ochrony danych zdecydował o nałożeniu administracyjnej kary pieniężnej na gminę Eidskog. Władze wezwały też do wdrożenia lepszych procedur ochrony danych osobowych, szczególnie dotyczących przetwarzania informacji wrażliwych, aby zapobiec podobnym naruszeniom w przyszłości.

Źródło: komunikat Europejskiej Rady Ochrony Danych

Dalsze informacje: komunikat norweskiego organu nadzorczego

NORWESKI ORGAN OCHRONY DANYCH NAŁOŻYŁ KARĘ ORAZ WYDAŁ ZALECENIA NORWESKIEMU URZĘDOWI PRACY I OPIEKI SPOŁECZNEJ

18 marca 2024 roku norweski organ ochrony danych ogłosił swoją finalną decyzję w sprawie norweskiego Urzędu Pracy i Opieki Społecznej (NAV) po kontroli przeprowadzonej we wrześniu 2023 roku.

Sprawa dotyczyła naruszeń przepisów dotyczących ochrony danych osobowych przez NAV, w tym niewystarczającego systemu zarządzania danymi i braku odpowiednich zabezpieczeń poufności danych.

Norweski organ ochrony danych stwierdził, że system zarządzania NAV nie zapewnia odpowiedniej zgodności z regulacjami dotyczącymi ochrony danych. Co więcej, praktyki związane z zarządzaniem dostępem do danych oraz kontrolą logów były niewystarczające, co mogło skutkować naruszeniem poufności danych osobowych, w tym danych wrażliwych.

W związku z tym organ podjął decyzję o nałożeniu na NAV administracyjnej kary pieniężnej w wysokości około 1,7 miliona euro. Dodatkowo wydano szereg nakazów, których celem jest zapewnienie pełnej zgodności działań NAV z wymogami RODO oraz poprawa bezpieczeństwa przetwarzania danych osobowych.

Źródło: komunikat Europejskiej Rady Ochrony Danych

Dalsze informacje: komunikat norweskiego organu nadzorczego

MONITOROWANIE PRACOWNIKÓW I TRANSMITOWANIE NAGRAŃ Z KAMER MONITORINGU WIZYJNEGO: SŁOWEŃSKI ORGAN OCHRONY DANYCH NAŁOŻYŁ KARĘ NA DODO PIZZA

Słoweński organ ochrony danych przeprowadził w 2023 roku postępowanie przeciwko spółce FOVELLA, która jest właścicielem franczyzy DODO PIZZA w Słowenii.

Postępowanie wykazało niezgodne z prawem monitorowanie pracowników w kuchni restauracji za pomocą kamer monitoringu wizyjnego oraz nielegalne transmitowanie tych nagrań na żywo na stronie internetowej przedsiębiorstwa.

Słoweński organ ochrony danych stwierdził dwa naruszenia w toku postępowania kontrolnego. Po pierwsze, nielegalną instalację kamer monitoringu wizyjnego w miejscu pracy – w kuchni restauracji, ponieważ monitoring pracowników może być przeprowadzany jedynie w wyjątkowych przypadkach i gdy jest to absolutnie konieczne dla bezpieczeństwa ludzi lub mienia (naruszenie artykułu 78 krajowej ustawy o ochronie danych osobowych). Po drugie, nagrania z tych kamer były transmitowane na żywo na stronie internetowej przedsiębiorstwa.

Administrator nie wykazał zgodności z art. 6 RODO zgodnie z zasadą rozliczalności. Słoweński organ nadzorczy zdecydował, że nie ma podstawy prawnej na mocy art. 6 RODO do transmisji na żywo na stronie internetowej firmy nagrań z kamer monitoringu pracowników pracujących w kuchni, ani nawet uzasadnionego interesu administratora, ponieważ już monitoring wewnątrz pomieszczeń roboczych został uznany za niezgodny z prawem na mocy przepisów krajowych.

Słoweński organ ochrony danych nałożył na spółkę FOVELLA administracyjną karę pieniężną w wysokości 25 tysięcy euro za nielegalny monitoring CCTV w kuchni restauracji oraz transmisję tych nagrań na stronie internetowej firmy. Decyzja została również zgłoszona innym organom ochrony danych, ponieważ DODO PIZZA prowadzi franczyzy w innych krajach UE.

Z tytułu naruszenia artykułów 76, ust. 3 i 4 krajowej ustawy o ochronie danych osobowych oraz artykułu 13 RODO, wydano upomnienie, gdyż przedsiębiorstwo nie poinformowało podmiotów danych o ich przetwarzaniu.

Źródło: komunikat Europejskiej Rady Ochrony Danych

SYSTEM WERYFIKACJI WIEKU ZAPROPONOWANY PRZEZ HISZPAŃSKI ORGAN OCHRONY DANYCH OTRZYMAŁ DWIE NAGRODY GLOBAL PRIVACY ASSEMBLY

System weryfikacji wieku zaproponowany przez hiszpański organ ochrony danych w celu ochrony dzieci i młodzieży w internecie został wyróżniony dwiema z pięciu nagród przyznanych podczas 46. Global Privacy Assembly, które zrzesza organy ochrony danych i prywatności na całym świecie.

Global Privacy Assembly to globalne forum, na którym niezależne organy nadzorcze ds. prywatności, ochrony danych i wolności informacji co roku przyjmują uchwały wysokiego szczebla i zalecenia dla rządów i organizacji międzynarodowych.

Podobnie jej wizją jest utrzymanie środowiska, w którym organy ochrony prywatności i danych na całym świecie mogą skutecznie działać, aby wypełniać swoje zadania, zarówno indywidualnie, jak i wspólnie, poprzez rozpowszechnianie wiedzy.

W grudniu 2023 r. hiszpański organ ochrony danych przedstawił propozycję systemu weryfikacji wieku i ochrony małoletnich w internecie przed dostępem do treści dla dorosłych, wykazując, że technicznie możliwa jest ochrona małoletnich przed dostępem do nieodpowiednich treści, przy jednoczesnym zagwarantowaniu anonimowości dorosłych podczas przeglądania internetu. System składa się z Dekalogu określającego zasady, których powinien przestrzegać system weryfikacji wieku, noty technicznej zawierającej szczegóły projektu oraz trzech dowodów koncepcji działających na Androidzie, iPhonie i Windowsie.

Całość uzupełnia wykres przedstawiający zagrożenia związane z obecnie używanymi systemami weryfikacji wieku.

Global Privacy Assembly doceniło nowatorski charakter tej propozycji, która wywarła znaczący wpływ na arenie międzynarodowej, przyznając jej, oprócz nagrody za innowacyjność, Nagrodę Publiczności. Celem tego rozwoju jest wykazanie, że można zbudować system gwarancji, który jedynie potwierdzi atrybut pełnoletności, pokazując, że nie jest konieczne ustanawianie równoległych usług tożsamości cyfrowej specjalnie w celu uzyskania dostępu do treści dla dorosłych, a tym samym oddzielenie tożsamości ludzi od weryfikacji wieku.

Źródło: strona internetowa hiszpańskiego organu nadzorczego

BADANIA KLINICZNE: FRANCUSKI ORGAN OCHRONY DANYCH ZATWIERDZA EUROPEJSKI KODEKS POSTĘPOWANIA FEDERACJI EUCROF

Kodeks ten skierowany jest do dostawców usług badań klinicznych, którzy działają jako podwykonawcy w imieniu sponsorów. Nadaje on wymiar operacyjny wymogom RODO.

To trzeci kodeks europejski, a drugi zatwierdzony przez francuski organ ochrony danych, po przyjętym w 2021 roku kodeksie CISPE (w zakresie przetwarzania w chmurze). Nowy kodeks uzyskał poparcie Federacji EUCROF, która podjęła inicjatywę jego opracowania w odpowiedzi na kwestie ochrony danych zidentyfikowane przez sektor.

Jego celem jest zapewnienie operacyjnego opisu zobowiązań podjętych przez prywatne firmy, które świadczą usługi w dziedzinie badań zdrowotnych na podstawie umowy, w szczególności dla przemysłu farmaceutycznego, jako podmiotu przetwarzającego (w rozumieniu art. 28 RODO) w wykonaniu umowy wiążącej je ze sponsorem (osobą fizyczną lub prawną, która jest odpowiedzialna za badania kliniczne, zapewnia zarządzanie nimi, weryfikuje, czy ich finansowanie jest zapewnione oraz określa cele i środki przetwarzania wymagane dla nich). W ofercie dostawców usług w zakresie badań klinicznych, które mogą być objęte kodeksem, znajduje się opracowanie protokołu lub broszury obserwacyjnej, wybór umowy z ośrodkami badawczymi, gromadzenie i hosting danych, ich analiza i tworzenie raportów, a także usługi archiwizacji i wsparcia technicznego.

Kodeks postępowania zapewnia pewność prawną i pomaga stworzyć klimat zaufania.

„To dostępne, ogólnoeuropejskie narzędzie, skierowane do dostawców usług w zakresie badań klinicznych, umożliwi zharmonizowane rozpowszechnianie dobrych praktyk wśród szerokiego grona podmiotów. Prace przeprowadzone przez grupę roboczą pozwoliły na skonsolidowanie pragmatycznych i konkretnych odpowiedzi w tym kodeksie, dostosowanych do wyzwań stojących przed profesjonalistami w tym sektorze.

Dlatego też, zdając sobie sprawę z zaangażowania wymaganego do pomyślnego zakończenia takiego projektu, chciałbym wyrazić uznanie dla wkładu EUCROF w tę inicjatywę, który świadczy o zaangażowaniu EUCROF i jej członków w zapewnienie większego bezpieczeństwa prawnego ich działań związanych z danymi osobowymi” – powiedziała Marie Laure Denis, przewodnicząca francuskiego organu nadzorczego CNIL.

Co zawiera ten kodeks postępowania?

Kodeks ten jest podzielony na dwie części. W pierwszej z nich szczegółowo opisano szeroki zakres środków prawnych, organizacyjnych i technicznych mających na celu zapewnienie zgodności z RODO przetwarzania danych realizowanego przez dostawców usług badań klinicznych:

• zakres zastosowania;

• przypomnienie głównych zasad w zakresie ochrony danych obowiązujących przyszłych członków;

• konkretne środki, które mają zostać wdrożone przez dostawców usług badań klinicznych (jak również procedury przeglądu i aktualizacji tych obowiązków);

• mechanizmy zarządzania wprowadzone w celu zapewnienia skuteczności kodeksu, w szczególności opis sposobów przestrzegania kodeksu lub procedur rozpatrywania skarg.

Druga część przedstawia tabelę identyfikującą obowiązki mające zastosowanie do dostawców usług badań klinicznych w oparciu o różne rodzaje usług, jakie świadczy.

Celem tego kodeksu postępowania nie jest regulowanie przekazywania danych poza Unię Europejską.

W jaki sposób monitorowane jest prawidłowe stosowanie niniejszego kodeksu postępowania?

Skuteczność kodeksu postępowania opracowanego zgodnie z założeniami RODO jest zapewniona poprzez interwencję organu odpowiedzialnego za weryfikację prawidłowego stosowania kodeksu przez członków. Kodeks postępowania opracowany przez federację EUCROF przewiduje utworzenie wewnętrznego komitetu nadzorczego. Kodeks zacznie obowiązywać, w momencie gdy tylko komitet ten zostanie akredytowany przez francuski organ nadzorczy.

Źródło: strona internetowa francuskiego organu nadzorczego

IRLANDZKI ORGAN OCHRONY DANYCH NAKŁADA NA LINKEDIN IRELAND KARĘ W WYSOKOŚCI 310 MILIONÓW EURO

Irlandzki organ ochrony danych (DPC) ogłosił ostateczną decyzję po zakończeniu postępowania wyjaśniającego wobec LinkedIn Ireland Unlimited Company (LinkedIn). Postępowanie to zostało wszczęte przez DPC, w charakterze wiodącego organu nadzorczego dla siedziby LinkedIn, na podstawie skargi złożonej pierwotnie do francuskiego organu ochrony danych.

Przedmiotem postępowania było przetwarzanie danych osobowych przez LinkedIn w celach analizy behawioralnej oraz reklamy ukierunkowanej wobec użytkowników, którzy utworzyli profile na platformie LinkedIn. Decyzja podjęta przez Komisarzy ds. Ochrony Danych, dr. Desa Hogana oraz Dale'a Sunderlanda, została przekazana platformie LinkedIn 22 października 2024 r. Dotyczyła zgodności z prawem, rzetelności oraz przejrzystości przetwarzania danych. Decyzja obejmuje upomnienie, nakaz dostosowania operacji przetwarzania do przepisów RODO oraz nałożenie administracyjnej kary pieniężnej w łącznej wysokości 310 milionów euro.

Źródło: strona internetowa irlandzkiego organu nadzorczego

Fot. pexels

KOMISJA WSZCZYNA FORMALNE POSTĘPOWANIE PRZECIWKO TEMU NA MOCY AKTU O USŁUGACH CYFROWYCH

Komisja wszczęła formalne postępowanie w celu oceny, czy Temu mogło naruszyć Akt o usługach cyfrowych (DSA) w obszarach związanych ze sprzedażą nielegalnych produktów, potencjalnie uzależniającą konstrukcją usługi, systemami wykorzystywanymi do rekomendowania zakupów użytkownikom, a także dostępem do danych dla badaczy.

Decyzja jest wynikiem wstępnych analiz sprawozdania z oceny ryzyka dostarczonego przez Temu pod koniec września 2024 r., odpowiedzi na formalne wnioski Komisji o udzielenie informacji z 28 czerwca 2024 r. i 11 października 2024 r., a także informacji udostępnionych przez strony trzecie. Komisja oparła się również na informacjach udostępnionych za pośrednictwem mechanizmu współpracy z organami krajowymi w ramach Europejskiej Rady Koordynatorów Usług Cyfrowych, w szczególności z irlandzkim koordynatorem ds. usług cyfrowych.

W szczególności dochodzenie skupi się na następujących obszarach:

• Systemy stosowane przez Temu w celu **ograniczenia sprzedaży niezgodnych produktów w Unii Europejskiej**. Dotyczy to między innymi systemów zaprojektowanych do tego, by ograniczyć ponowne pojawienie się wcześniej zawieszonych nieuczciwych sprzedawców, o których wiadomo, że w przeszłości sprzedawali produkty niezgodne z przepisami, a także systemów ograniczających ponowne pojawienie się towarów niezgodnych z przepisami.

• Ryzyko związane z **uzależniającą konstrukcją usługi**, w tym z programami nagród przypominającymi gry, oraz systemami stosowanymi przez Temu w celu ograniczenia ryzyka wynikającego z takiej uzależniającej konstrukcji, która może mieć negatywne konsekwencje dla fizycznego i psychicznego samopoczucia danej osoby.

• Zgodność ze zobowiązaniami DSA związanymi ze **sposobem, w jaki Temu rekomenduje treści i produkty użytkownikom**. Obejmuje to wymóg ujawnienia głównych parametrów wykorzystywanych w systemach rekomendacji Temu oraz zapewnienia użytkownikom co najmniej jednej łatwo dostępnej opcji, która nie jest oparta na profilowaniu.

• Zgodność z obowiązkiem DSA w zakresie zapewnienia badaczom dostępu do publicznie dostępnych danych Temu.

Gdyby podejrzenia Komisji okazały się słuszne, Temu groziłaby odpowiedzialność na mocy DSA, ponieważ niedociągnięcia te stanowiłyby naruszenie art. 27, 34, 35, 38 i 40 DSA. Komisja przeprowadzi teraz szczegółowe dochodzenie w trybie priorytetowym. Wszczęcie formalnego postępowania nie przesądza o jego wyniku.

Kolejne kroki

Po formalnym wszczęciu postępowania Komisja będzie nadal gromadzić dowody, na przykład wysyłając dodatkowe wnioski o udzielenie informacji do Temu lub stron trzecich lub prowadząc działania monitorujące lub wywiady.

Wszczęcie formalnego postępowania upoważnia Komisję do podjęcia dalszych kroków w zakresie egzekwowania prawa, w tym do przyjęcia decyzji o braku zgodności. Komisja jest również uprawniona do przyjęcia zobowiązań podjętych przez Temu w celu naprawienia kwestii będących przedmiotem postępowania.

DSA nie określa żadnego prawnego terminu zakończenia formalnego postępowania. Czas trwania szczegółowego postępowania zależy od kilku czynników, w tym od złożoności sprawy, zakresu współpracy danego przedsiębiorstwa z Komisją i korzystania z prawa do obrony.

Ponadto wszczęcie formalnego postępowania nie przesądza o jego wyniku ani o innych postępowaniach, które Komisja może zdecydować się wszcząć na podstawie innych artykułów DSA.

Podobnie nie wyklucza to żadnych przyszłych działań w zakresie egzekwowania prawa, które mogą zostać podjęte przez krajowe organy ochrony konsumentów należące do sieci współpracy w zakresie ochrony konsumentów (CPC) w odniesieniu do przestrzegania przez Temu zobowiązań wynikających z unijnego prawa konsumenckiego. Komisja będzie kontynuować wysiłki na rzecz współpracy z organami krajowymi przy egzekwowaniu DSA, w tym za pośrednictwem specjalnej grupy roboczej ds. konsumentów i rynków internetowych Europejskiej Rady Koordynatorów Usług Cyfrowych.

Podobnie, wszczęcie formalnego postępowania nie wyklucza również działań i decyzji, które mogą zostać podjęte przez organy nadzoru rynku na podstawie dyrektywy w sprawie ogólnego bezpieczeństwa produktów (rozporządzenie w sprawie ogólnego bezpieczeństwa produktów z 13.12.2024 r.).

Kontekst

Temu zostało wyznaczone jako bardzo duża platforma internetowa (VLOP) w dniu 31 maja 2024 r. na mocy unijnego aktu prawnego o usługach cyfrowych, po zadeklarowaniu posiadania ponad 45 milionów aktywnych użytkowników miesięcznie w UE. Cztery miesiące po wyznaczeniu Temu

musiało spełnić najbardziej rygorystyczne obowiązki mające zastosowanie do VLOP, określone w DSA. Obejmują one obowiązek należytej oceny i ograniczenia wszelkich ryzyk systemowych wynikających z jego usługi. Temu po raz ostatni zadeklarował 92 miliony użytkowników miesięcznie we wrześniu 2024 roku.

Więcej informacji

Tekst Dziennika Urzędowego UE dotyczący DSA

Bardzo duże platformy internetowe i wyszukiwarki w świetle DSA

Ramy egzekwowania przepisów na mocy aktu prawnego o usługach cyfrowych

Akt prawny o usługach cyfrowych - pytania i odpowiedzi

Źródło: strona internetowa Komisji Europejskiej

Fot. pixabay

PODSUMOWANIE PROJEKTU ARC II

W dniu 28 września 2024 r. partnerzy projektu ARC II (Kampania na rzecz podnoszenia świadomości małych i średnich przedsiębiorstw) zorganizowali hybrydowe spotkanie podsumowujące we Włoszech. Gospodarzem spotkania był Uniwersytet we Florencji.

Projekt ARC II, współfinansowany w ramach programu Unii Europejskiej „Obywatelstwo, równość, prawa i wartości" (CERV), był wspólnym wysiłkiem trwającym dwa lata. Partnerami projektu są:

1. Chorwacka Agencja Ochrony Danych Osobowych (koordynator projektu).
2. Włoski Urząd Ochrony Danych (Garante per la protezione dei dati personali).
3. Wydział Organizacji i Informatyki, Uniwersytet w Zagrzebiu.
4. Vrije Universiteit Brussel.
5. Uniwersytet we Florencji.

Głównym celem ARC II było wspieranie małych i średnich przedsiębiorstw (MŚP) w ich wysiłkach na rzecz zapewnienia zgodności z ogólnym rozporządzeniem o ochronie danych (RODO) przy jednoczesnym zmniejszeniu ich obciążeń administracyjnych.

W swoim przemówieniu Zdravko Vukić, dyrektor chorwackiego organu ochrony danych, wiceprzewodniczący Europejskiej Rady Ochrony Danych i członek Komitetu Sterującego, podkreślił:

„Dlaczego poświęciliśmy tyle czasu i zasobów MŚP? Najpierw w projekcie ARC I, który realizowaliśmy z irlandzkim organem ochrony danych, a następnie w projekcie ARC II, przez ponad 4 lata inwestowaliśmy wiele wysiłku i czasu, aby pomóc MŚP w zrozumieniu i przestrzeganiu ich obowiązków wynikających z RODO. Nie dzieje się tak bez powodu.

Ponad 99% wszystkich przedsiębiorstw w UE to MŚP. Małe i średnie przedsiębiorstwa odgrywają kluczową rolę w gospodarce europejskiej i oczywiście w gospodarce chorwackiej. Przedsiębiorstwa te są często określane jako kręgosłup gospodarki, ponieważ stanowią większość firm w Europie. Nawet po ponad 6 latach od pełnego wdrożenia RODO, wiele z nich uważa RODO za ogromne obciążenie administracyjne i finansowe.

Dzięki wdrożonym przez nas działaniom małe i średnie przedsiębiorstwa nie tylko uzyskały dostęp do cennych informacji i osiągnęły wyższy poziom zgodności z RODO, ale także były w stanie uzyskać znaczne oszczędności finansowe".

6 SPRAWY MIĘDZYNARODOWE

Celem spotkania podsumowującego było przedstawienie interesariuszom głównych rezultatów projektu ARC II – narzędzia internetowego Olivia, podsumowanie wyników projektu, określenie działań, które należy podjąć w celu pomyślnego zakończenia projektu, a także wymiana doświadczeń i spostrzeżeń dotyczących wdrażania RODO w MŚP z interesariuszami. Wydarzenie zostało podzielone na dwie części: pierwszą w języku angielskim i drugą w języku włoskim, poświęconą prezentacji Olivii włoskim MŚP.

Spotkanie przyciągnęło zróżnicowaną grupę uczestników, w tym przedstawicieli Komisji Europejskiej, Europejskiej Rady Ochrony Danych (EROD), różnych organów ochrony danych, małych i średnich przedsiębiorstw (MŚP) oraz prawników.

Najważniejszym punktem wydarzenia była prezentacja narzędzia internetowego Olivia, opracowanego w ramach projektu ARC II. Olivia będzie stale dostępna, bezpłatnie dla wszystkich zainteresowanych stron.

Ponadto Marianna Colonna z EROD zaprezentowała **praktyczne narzędzie zaprojektowane specjalnie dla MŚP (przewodnik EROD dla MŚP)**. Zasób ten, dostępny w 17 językach, jest dostępny na stronie EROD.

Uczestnicy skorzystali również z prezentacji Pavliny Penevy z Komisji Europejskiej, która szczegółowo przedstawiła możliwości oferowane przez program „Obywatelstwo, równość, prawa i wartości" (CERV).

Zaproszenie do składania wniosków CERV-2021-Data Call koncentrowało się na dwóch głównych priorytetach:

1. Ułatwienie MŚP wdrożenia obowiązków wynikających z ogólnego rozporządzenia o ochronie danych (RODO).

2. Podnoszenie świadomości na temat RODO wśród ogółu społeczeństwa.

Dzięki finansowaniu zapewnionemu w ramach programu CERV organy ochrony danych w całej Unii Europejskiej będą miały możliwość wdrożenia działań skierowanych do MŚP i ogółu społeczeństwa. Inicjatywy te mają na celu zwiększenie świadomości i wiedzy na temat zasad i praktyk ochrony danych.

To wspólne podejście, łączące zasoby instytucji UE, organów krajowych i partnerów akademickich, pokazuje wspólne wysiłki na rzecz wzmocnienia praktyk ochrony danych w całej Europie, w szczególności koncentrując się na potrzebach MŚP i zwiększając zrozumienie przez społeczeństwo praw i obowiązków w zakresie ochrony danych.

Pavlina Peneva podkreśliła również niektóre zalecenia z drugiego raportu na temat RODO:

- Dalsze wspieranie wysiłków przedsiębiorstw w zakresie zgodności, zwłaszcza MŚP,
- Jasne i wykonalne wytyczne od organów ochrony danych,
- Organy ochrony danych powinny aktywnie współpracować z organizacjami, zwłaszcza MŚP,
- Wykorzystanie kodeksów postępowania i certyfikatów RODO.

Zgodnie z podejściem opartym na ryzyku w RODO, MŚP prowadzące działania dotyczące przetwarzania o niskim ryzyku nie ponoszą znacznego obciążenia związanego z przestrzeganiem przepisów. MŚP prowadzące przetwarzanie o niskim ryzyku mogą przestrzegać przepisów poprzez prowadzenie uproszczonej dokumentacji opartej na szablonach dostarczonych przez organy ochrony danych. Ponadto takie rejestry powinny być postrzegane jako przydatne narzędzie dla MŚP do podsumowania ich działań związanych z przetwarzaniem danych.

Olivia to innowacyjna platforma, która została zaprojektowana specjalnie w celu ułatwienia małym i średnim przedsiębiorstwom w Chorwacji i we Włoszech zapewnienia zgodności z RODO. Olivia jest obecnie dostępna w języku chorwackim, włoskim i angielskim, dostosowana do potrzeb chorwackich i włoskich MŚP.

Olivia została opracowana w oparciu o otwarty kod źródłowy i umożliwia wszystkim organom ochrony danych dostosowanie jej do krajowych przepisów i języka. Nowe języki i moduły można łatwo zintegrować, co oznacza, że **Olivia może być przydatna dla MŚP i administratorów danych w całej UE.**

To, co wyróżnia Olivię, to kompleksowe dostosowanie nie tylko do RODO, ale także chorwackich i włoskich ram prawnych ochrony danych, co czyni ją szczególnie cenną dla MŚP w tych krajach.

Olivia to platforma e-learningowa składająca się z 15 modułów edukacyjnych, które dotyczą wszystkich obowiązków związanych z RODO. Każdy moduł zawiera część teoretyczną i praktyczną:

1. Część teoretyczna: MŚP mogą zapoznać się z podstawami RODO, oceną skutków dla ochrony danych, podstawą prawną, zasadami ochrony danych, środkami technicznymi i organizacyjnymi, polityką prywatności i nie tylko. Użytkownicy mogą oglądać webinaria, brać udział w testach, a po uzyskaniu 80% lub wyższego wyniku otrzymują certyfikat pomyślnego ukończenia.

2. Część praktyczna: MŚP mogą tworzyć niezbędne dokumenty w celu wykazania zgodności, w tym polityki prywatności, rejestry czynności przetwarzania, oceny uzasadnionego interesu, oceny wpływu na ochronę danych, zbiory zasad nadzoru wideo, zbiory zasad ochrony danych osobowych i wytyczne dotyczące bezpieczeństwa informacji.

Źródło: https://olivia-gdpr-arc.eu/en/news/show/7

CNIL: REKLAMY UMIESZCZANE MIĘDZY E-MAILAMI: 50 MILIONÓW EURO KARY DLA ORANGE

14 listopada 2024 r. francuski organ nadzorczy (CNIL) nałożył na firmę ORANGE karę 50 mln euro za wyświetlanie reklam między wiadomościami e-mail bez uzyskania uprzednio zgody na to użytkowników poczty elektronicznej.

ORANGE udostępnia swoim klientom usługę poczty elektronicznej „Orange Mail".
Po przeprowadzeniu kilku kontroli CNIL ustalił, że firma wyświetlała reklamy w formie wiadomości e-mail pomiędzy wiadomościami znajdującymi się w skrzynkach odbiorczych użytkowników.

W związku z tym CNIL stwierdził, że takie działanie wymaga uzyskania uprzedniej zgody użytkowników Orange Mail, zgodnie z francuskim Kodeksem Łączności Pocztowej i Elektronicznej.

Dodatkowo kontrole wykazały, że w przypadku użytkowników strony **orange.fr**, którzy wycofali zgodę na umieszczanie i odczytywanie plików cookie na ich urządzeniach, wcześniej zapisane pliki cookie były nadal odczytywane.

W związku z tymi dwoma naruszeniami CNIL podjął następujące decyzje:

• Nałożenie na firmę ORANGE kary grzywny w wysokości **50 mln euro**, z podaniem informacji do wiadomości publicznej.

• Nakaz zaprzestania odczytywania plików cookie po wycofaniu zgody przez użytkownika, z wyznaczonym terminem trzech miesięcy na dostosowanie się do wymogu. W przypadku opóźnienia nałożono karę w wysokości **100 tysięcy euro za każdy dzień zwłoki**.

Wysokość nałożonej kary uwzględnia przede wszystkim ogromną liczbę osób, których dane zostały naruszone – sporne reklamy wyświetlono w skrzynkach odbiorczych ponad 7,8 mln użytkowników. Pod uwagę wzięto również pozycję firmy na rynku, jako wiodącego operatora telekomunikacyjnego we Francji. CNIL częściowo uwzględnił także korzyści finansowe, jakie przedsiębiorstwo osiągnęło w wyniku umieszczania reklam pomiędzy wiadomościami e-mail bez odpowiedniej zgody użytkowników.

CNIL, powołując się na orzeczenie Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z 25 listopada 2021 r., stwierdził, że wiadomości promujące usługi lub towary, które nie są przesyłane przez jednego użytkownika do drugiego, lecz umieszczane w przestrzeni zazwyczaj zarezerwowanej dla

prywatnych wiadomości e-mail i przypominającej wyglądem prawdziwe wiadomości, stanowią formę marketingu bezpośredniego za pośrednictwem poczty elektronicznej. W związku z tym, zgodnie z przepisami, konieczne jest uzyskanie wyraźnej zgody od osób, których to dotyczy.

Źródło: komunikat francuskiego organu nadzorczego

Fot. pixabay

FIŃSKI ORGAN NADZORCZY NAŁOŻYŁ NA SERWIS INTERNETOWY POSTI ADMINISTRACYJNĄ KARĘ PIENIĘŻNĄ W WYSOKOŚCI 2,4 MLN EURO

Fiński organ nadzorczy przeprowadził postępowanie w sprawie przetwarzania danych osobowych Posti w związku z utworzeniem elektronicznej skrzynki pocztowej. Otrzymał skargi dotyczące przekazywania listów do serwisu internetowego Posti bez zgody osób, których dane dotyczą.

Administrator automatycznie utworzył elektroniczną skrzynkę pocztową dla klientów, choć o to nie wystąpili. Elektroniczna skrzynka pocztowa została powiązana z szerszym zestawem usług. Postępowanie wykazało, że klient nie mógł wybrać, czy chce korzystać ze skrzynki pocztowej, czy nie, ponieważ różne usługi były ze sobą powiązane w ramach jednej umowy. Nie można było zrezygnować z elektronicznej skrzynki pocztowej bez rezygnacji z innych usług.

Fiński organ nadzorczy uważa, że usługa, o którą wnioskował klient, mogła zostać zrealizowana bez automatycznego utworzenia elektronicznej skrzynki pocztowej. Administrator nie poinformował również w sposób wyraźny swoich klientów o aktywacji elektronicznej skrzynki pocztowej. W serwisie znajdowały się również ustawienia techniczne, które nie spełniały wymogów ochrony danych. Obejmowały one automatycznie aktywowaną funkcję wyboru i wstępnie zaznaczone pole wyboru.

Fiński organ nadzorczy nałożył na administratora administracyjną karę pieniężną w wysokości 2,4 mln euro za niezgodne z prawem przetwarzanie (art. 5 i 6 ust. 1 RODO). Administrator został upomniany za niedopełnienie obowiązku informacyjnego oraz nakazano mu sprostowanie niezgodnych z prawem praktyk (art. 13 RODO). Ponadto organ nadzorczy polecił administratorowi, aby ten wziął pod uwagę, że usługi elektroniczne muszą być od początku budowane w taki sposób, aby przetwarzane były tylko niezbędne dane osobowe (art. 25 RODO).

Więcej informacji znajduje się na stronie fińskiego organu nadzorczego (angielski, suomi, szwedzki)

Źródło: komunikat EROD

AEPD ZATWIERDZA NOWY SYSTEM MEDIACJI, KTÓRY MA PRZYSPIESZYĆ DOCHODZENIE ROSZCZEŃ Z TYTUŁU OCHRONY DANYCH W KOMUNIKACJI ELEKTRONICZNEJ

20 listopada 2024 r. hiszpański organ nadzorczy (AEPD) zatwierdził „Kodeks postępowania w zakresie rozstrzygania sporów dotyczących ochrony danych w sektorze łączności elektronicznej", opracowany przez operatorów telefonicznych należących do grup Orange, Telefónica, Vodafone i MásMóvil.

Kodeks określa procedurę mediacji, której celem jest osiągnięcie porozumienia między obiema stronami – obywatelami a podmiotami przestrzegającymi kodeksu. Dzięki mediacji użytkownik może rozwiązać swoją skargę bez konieczności wszczynania postępowania administracyjnego lub sądowego, jeśli zdecyduje się na tę ścieżkę.

Kodeksy postępowania, do których przystąpienie jest dobrowolne, lecz wiążące dla podmiotów członkowskich, stanowią formę samoregulacji. W tym przypadku oznacza to wprowadzenie uproszczonej procedury, która umożliwia obywatelom sprawniejsze zgłaszanie i rozwiązywanie skarg wobec podmiotów przestrzegających kodeksu.

Kodeks postępowania wejdzie w życie 17 grudnia. Dzięki zawartej w nim procedurze obywatele zyskają możliwość zgłaszania roszczeń dotyczących m.in. przetwarzania danych bez podstawy prawnej, niewłaściwego realizowania ich praw, błędnego wprowadzania danych do systemów informacji kredytowej czy nieuczciwego zawierania umów.

Organ monitorujący kodeks postępowania zapozna się z otrzymanymi skargami na podmioty stosujące Kodeks, wszczynając postępowanie mediacyjne. Maksymalny czas trwania tej procedury wyniesie 30 dni.

Źródło: komunikat hiszpańskiego organu nadzorczego

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl