URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
Nr 02/02/24

www.uodo.gov.pl

SPIS TREŚCI

Szanowni Państwo!

26 stycznia br. złożyłem ślubowanie przed Sejmem RP jako Prezes Urzędu Ochrony Danych Osobowych, zobowiązując się dochować wierności postanowieniom Konstytucji RP oraz strzec prawa do ochrony danych osobowych, wypełniając te zadania sumiennie i bezstronnie.

Za mną intensywny czas spotkań z pracowniczkami i pracownikami komórek organizacyjnych Urzędu oraz zapoznawania się z dokumentacją dotyczącą konkretnych spraw i postępowań. Z pomocą kierownictwa UODO podjąłem pierwsze decyzje w ramach realizacji zadań ustawowych oraz priorytetów organu nadzorczego. 2 lutego 2024 r. powołałem na funkcję Zastępczyni Prezesa Urzędu Ochrony Danych Osobowych Agnieszkę Grzelak, która – jestem przekonany – wniesie dużo konstruktywnych zmian w funkcjonowanie Urzędu. To prawniczka, członkini Izby Adwokackiej w Warszawie, specjalizująca się w prawie europejskim, doktor habilitowana nauk prawnych, profesorka Akademii Leona Koźmińskiego w Warszawie, ekspertka, której kompetencje będą pomocne nie tylko w zakresie organizacji systemu ochrony danych osobowych, ale również w zarządzaniu pracą samego Urzędu. Od marca 2024 r. do naszego zespołu dołącza kolejny Zastępca Prezesa UODO – Konrad Komornicki, który od ponad 25 lat zajmuje się obszarem zarządzania bezpieczeństwem informacji. Jako specjalista ochrony danych pomoże z pewnością usprawnić pracę Urzędu i uporządkować sprawy regulacyjne z korzyścią dla procesów ochrony bezpieczeństwa danych osobowych.. Razem z Zastępcami i całym zespołem UODO stawimy czoła nadchodzącym wyzwaniom.

To moje pierwsze spotkanie z Państwem – czytelniczkami i czytelnikami „Biuletynu UODO”. Cieszę się, że Urząd prowadzi kanał komunikacji, którego przekaz dociera do imponującej liczby subskrybentów, a materiały w nim publikowane są szeroko cytowane w mediach, również w najbardziej popularnych ogólnopolskich tytułach. Wydawnictwo to wydaje się nam bardzo potrzebne w prowadzeniu dyskusji w obszarze ochrony danych osobowych.
Co istotne, biuletyn wnosi nowe treści – nie dubluje komunikatów zamieszczanych na stronie, tylko uzupełnia je przede wszystkim o materiały przygotowane przez departamenty.

Jak deklarowałem wielokrotnie, jasna, efektywna komunikacja organu nadzorczego to jeden z celów, jaki chciałbym osiągnąć podczas swojej kadencji. Liczę na Państwa wsparcie w postaci informacji zwrotnej w tym względzie, ponieważ jestem przekonany, że tylko współpracą i otwartością na dialog – z obywatelami, ekspertami ds. ochrony danych, organizacjami pozarządowymi, IOD-ami, administratorami danych, unijnymi oraz krajowymi organami – możemy osiągnąć to założenie. Dlatego w najbliższym czasie będziemy prosić Państwa, np. poprzez badania ankietowe, o wyrażenie opinii dotyczącej komunikowania się UODO, m.in. poprzez „Biuletyn".

Zależy mi na tym, żeby informacje o działalności UODO były łatwo dostępne. Mam na myśli stanowiska Urzędu, ale również opracowania, wytyczne, poradniki. Bardzo ważnym dla mnie aspektem jest upowszechnianie wytycznych EROD oraz czerpanie ze wzorców i dobrych praktyk innych regulatorów, tak by RODO zaczęło być postrzegane jako realne narzędzie skutecznej ochrony danych osobowych, a nie biurokratyczne obciążenie, dlatego na polu komunikacji chciałbym przyjąć stosowanie prostego, zrozumiałego języka w ochronie danych.

Marzy mi się, by działalność organu była przewidywalna dla społeczeństwa – by przyjmowane przez Urząd dokumenty wskazywały kierunki ochrony danych osobowych. Myślę, że życzliwa, czytelna postawa UODO wobec administratorów, zapewnienie im pewności prawnej, wyraziste przedstawianie wykładni przepisów to właściwa droga do sprawnego funkcjonowania Urzędu.

Bardzo liczę na Państwa zaangażowanie oraz chęć do wspólnego wypracowywania rozwiązań służących ochronie naszych danych. Wierzę, że te cykliczne spotkania na stronach wydawnictwa będą kolejną cegiełką, która przyczyni się do lepszej komunikacji w obszarze ochrony danych osobowych.

Mirosław Wróblewski
Prezes UODO

Drodzy Czytelnicy!

Zmiany zazwyczaj związane są z rozwojem, nowym spojrzeniem na sytuację, świeżymi pomysłami i rozwiązaniami. Niewątpliwie jesteśmy w bardzo ciekawym dla Urzędu Ochrony Danych Osobowych miejscu – zyskaliśmy nowego Prezesa – Mirosława Wróblewskiego oraz jego Zastępców – Agnieszkę Grzelak i Konrada Komornickiego. Dokonania naszych czołowych przedstawicieli z pewnością zasługują na uwagę, więc zachęcam Państwa do zapoznania się z ich sylwetkami na stronie Urzędu.

Zatwierdzone przez Prezesa UODO 8 grudnia 2023 r. Dodatkowe wymogi akredytacji podmiotów certyfikujących to ważny krok na drodze do powstania w Polsce rynku certyfikacji w zakresie ochrony danych osobowych. Działania edukacyjne Urzędu w postaci cyklu webinariów, których celem jest promowanie certyfikacji i zachęcanie rynku do tworzenia mechanizmów certyfikacji zgodnie z art. 42 RODO odbywają się raz w miesiącu, a o dokładnych terminach i tematyce tych spotkań będziemy Was informować za pośrednictwem strony internetowej i mediów społecznościowych.

Czy czeka nas kolejny kodeks postępowania? Na to wygląda. W tym numerze piszemy o tym, że Izba Gospodarcza Hotelarstwa Polskiego (IGHP) złożyła do Prezesa UODO wniosek o zatwierdzenie projektu „Kodeksu postępowania i dobrych praktyk w sprawie danych osobowych w branży hotelarskiej". To ważne przedsięwzięcie, które zapewni osobom korzystającym z dostarczanych przez hotele usług, jak najwyższego poziomu ochrony ich danych osobowych, zaś hotelom – jasnych wskazówek, jak przetwarzać dane osobowe.

W opinii UODO na potrzeby potwierdzenia spełnienia kryterium samotnego wychowywania dziecka podczas rekrutacji do szkół i przedszkoli nie powinny być pozyskiwane prawomocne wyroki sądów rodzinnych orzekające rozwód lub separację. Dlatego do Minister Edukacji skierowane zostało wystąpienie dotyczące wprowadzenia stosownych zmian w przepisach ustawy – Prawo oświatowe. Więcej na ten temat w rubryce „UODO sygnalizuje".

Laureat nagrody Prezesa UODO im M. Serzyckiego, entuzjasta prawa nowych technologii, Xawery Konarski, przedstawia najważniejsze zmiany legislacyjne w zakresie cyberbezpieczeństwa, nowych technologii i ochrony danych osobowych w 2024 roku. W tym kontekście warto przeczytać dwa materiały – artykuł odnoszący się do wykorzystania technologii rozpoznawania twarzy w obszarze ścigania przestępstw oraz tekst nt. szczególnie podstępnego ataku cyberprzestępców - juice jackingu. Sprawcy modyfikują publicznie dostępne ładowarki USB co umożliwia im kradzież danych lub zainstalowanie złośliwego oprogramowania na urządzeniu w trakcie gdy jest ono ładowane przy użyciu takiej ładowarki.

UODO niezmiennie podkreśla, że zgodnie z rozporządzeniem o ochronie danych wycofanie zgody musi być równie łatwe, jak jej udzielenie. Jak wskazuje NOYB Meta ignoruje prawo użytkowników do łatwego wycofania zgody. Więcej informacji nt. skargi złożonej przez organizację Maxa Schremsa do austriackiego regulatora uzyskacie z najnowszej publikacji biuletynu. Zostając częściowo w Austrii piszemy też o głośnym wyroku TSUE, stwierdzającym, że parlamentarna komisja śledcza musi co do zasady przestrzegać ogólnego rozporządzenia o ochronie danych. Polecamy przyjrzeć się walce o ochronę danych świadka, którego imię i nazwisko zostały opublikowane po przesłuchaniu przez komisję śledczą na stronie internetowej austriackiego parlamentu.

Jestem świadomy, że zawsze dużym zainteresowaniem cieszą się opisane przez nas decyzje skargowe. W tym wydaniu czeka Was, Drodzy Czytelnicy, podwójna przyjemność – publikujemy wywiad z Pauliną Dawidczyk, Dyrektor Departamentu Skarg oraz decyzję, która stanowi pierwsze orzeczenie Najwyższego Sądu Administracyjnego, potwierdzające stanowisko Urzędu w zaprezentowanej sprawie. Co było jej przedmiotem, dowiecie się z niniejszej lektury, do czego gorąco Was zachęcam.

Adam Sanocki
Dyrektor Departamentu Komunikacji Społecznej,
Rzecznik Prasowy UODO

1 ROZMOWA Z EKSPERTEM

WIEDZĘ POLAKÓW NA TEMAT OCHRONY DANYCH OSOBOWYCH I PRZYSŁUGUJĄCYCH IM PRAW OCENIAM WYSOKO

Z Pauliną Dawidczyk Dyrektor, Departamentu Skarg UODO rozmawiał Karol Witowski, Zastępca Rzecznika Prasowego UODO

Rozpatrywanie skarg to ważny element pracy organu nadzorczego. Kto zajmuje się rozpatrywaniem wniosków skargowych?

Rozpatrywanie skarg jest jednym z podstawowych zadań Prezesa Urzędu Ochrony Danych Osobowych jako organu nadzorczego. Mówi o tym art. 57 ust. 1 lit. f Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

Zgodnie z przepisami, wpłynięcie skargi do organu nadzorczego inicjuje postępowanie administracyjne, zmierzające do rozstrzygnięcia sprawy poprzez wydanie decyzji.

Rozpatrywaniem wszystkich skarg, wpływających do UODO, zajmuje się Departament Skarg (DS). Zadaniem Ds-u jest także procedowanie spraw transgranicznych oraz szereg zadań związanych z prowadzonymi postępowaniami administracyjnymi, takich jak udostępnianie stronom postępowań do wglądu akt, przyjmowanie skarg wnoszonych ustnie czy przygotowywanie pism w toku postępowań przed sądami administracyjnymi. W naszym departamencie powstają też projekty skarg kasacyjnych od wyroków Wojewódzkiego Sądu Administracyjnego w Warszawie, a także odpowiedzi na wezwania sądów i innych organów, związane z prowadzonymi postępowaniami administracyjnymi.

1 ROZMOWA Z EKSPERTEM

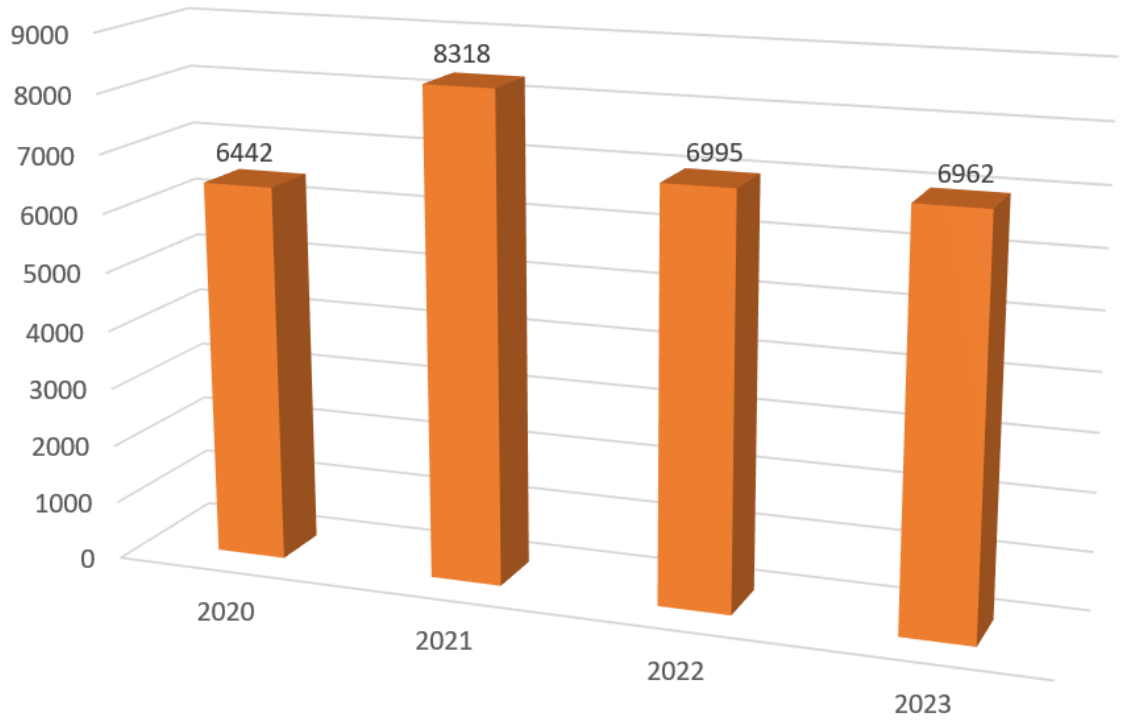
Jak przebiega proces analizy skarg?

Każda ze skarg analizowana jest najpierw pod kątem spełnienia warunków formalnych przewidzianych przepisami Kodeksu postępowania administracyjnego. W przypadku ich nie spełnienia wzywamy wnioskodawcę do uzupełnienia braków formalnych, a jeśli te nie zostaną uzupełnione, skargi pozostawiane są bez rozpoznania. Jeśli warunki formalne zostały spełnione, wzywamy skarżony podmiot o złożenie wyjaśnień oraz przedłożenie dowodów na ich poparcie oraz odniesienie się do zarzutów, podniesionych w skardze. Każdej osobie, która złożyła skargę na naruszenie przepisów RODO w procesie przetwarzania jej danych osobowych przysługuje prawo do informacji o postępach i wynikach rozpatrzenia skargi, dlatego podejmując szereg czynności koniecznych do zebrania materiału dowodowego, niezbędnego do wydania rozstrzygnięcia w każdej sprawie, organ nadzorczy informuje o postępach i wynikach rozpatrzenia skargi.

Ile skarg wpłynęło do UODO w 2023 roku?

W roku 2023 do Departamentu Skarg Urzędu Ochrony Danych Osobowych wpłynęły 6962 skargi krajowe. W porównaniu do roku poprzedniego to o 33 skargi mniej, jednak wysoki wskaźnik skarg w latach poprzednich przełożył się na zwiększoną liczbę spraw prowadzonych w Departamencie Skarg w roku 2023. Chodzi o sprawy, które wpłynęły do naszego departamentu w roku poprzedzającym, ale podjęcie czynności niezbędnych do zebrania materiału dowodowego i wydania decyzji administracyjnej nastąpiło w 2023 roku. Trzeba zaznaczyć, że w minionym roku zakończono 5898 postępowań skargowych, spośród których 1750 spraw zakończyło się wydaniem decyzji administracyjnych.
W decyzjach tych Prezes UODO w 965 przypadkach w oparciu o art. 58 RODO zastosował środki naprawcze, w tym w 630 sprawach udzielił upomnienia za naruszenie przepisów RODO, zaś w 335 przypadkach zastosował środek naprawczy w postaci nakazu.

1 ROZMOWA Z EKSPERTEM



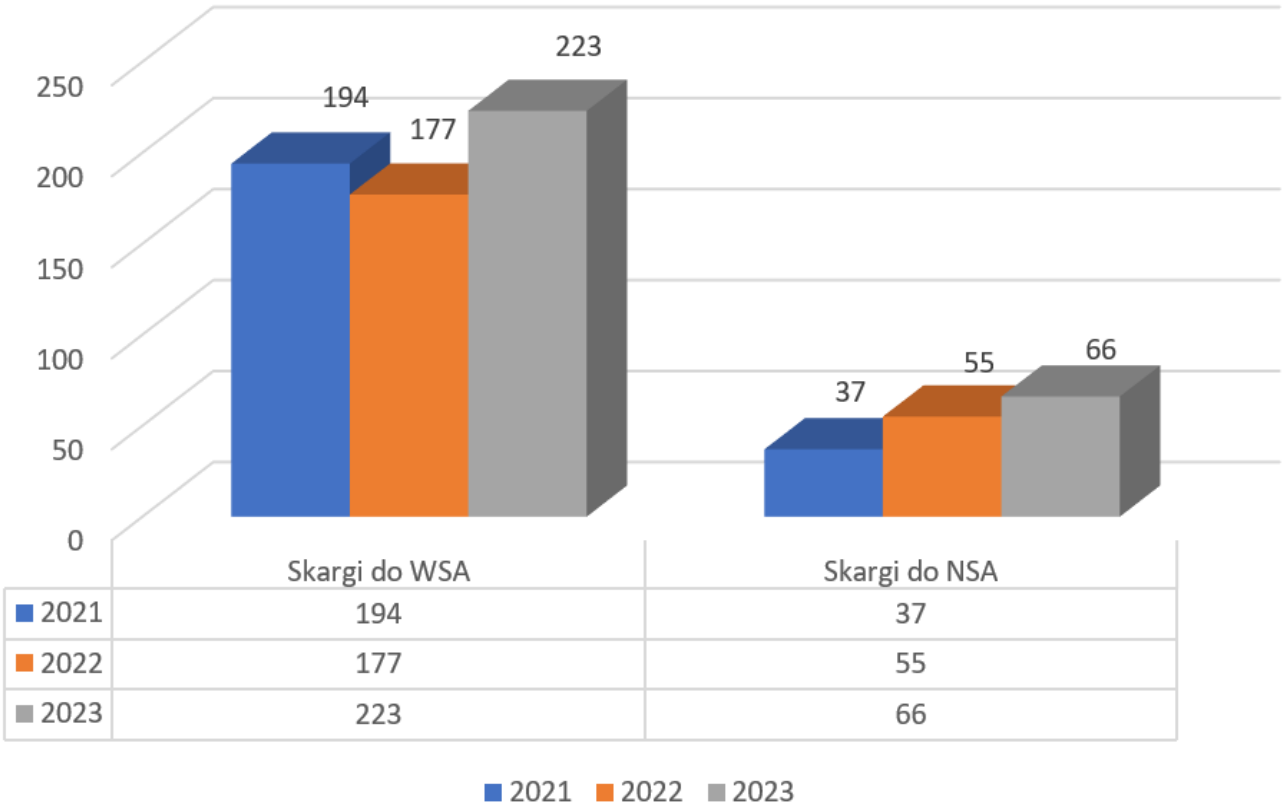
Wykres: Liczba skarg, które wpłynęły do UODO w latach 2020-2023

A co ze skargami na decyzje Prezesa UODO? Liczba skarg rośnie, czy wraz z tym współczynnikiem rośnie liczba wniosków, składanych do sądu, skarżących decyzję PUODO?
W roku 2023 nieznaczenie wzrosła liczba skarg na decyzje Prezesa UODO, składanych do sądów administracyjnych. Do Wojewódzkiego Sądu Administracyjnego w Warszawie w roku 2023 zostały zaskarżone 223 decyzje Prezesa UODO (177 w 2022 r.), zaś do NSA wniesiono 66 skarg kasacyjnych od wyroków w sprawach dotyczących decyzji wydanych przez Prezesa UODO (55 skarg w 2023 r.). Utrzymująca się w ostatnich latach tendencja wzrostowa skarg na decyzje organu nadzorczego w sprawach skargowych wynika nie tylko z utrzymującej się wysokiej liczby wnoszonych skarg osób, których dane dotyczą, na przetwarzanie ich danych, ale przede wszystkim z większej aktywności orzeczniczej organu.

1 ROZMOWA Z EKSPERTEM

Jak ocenia Pani rozbieżności między decyzjami Prezesa a orzeczeniami sądowymi?

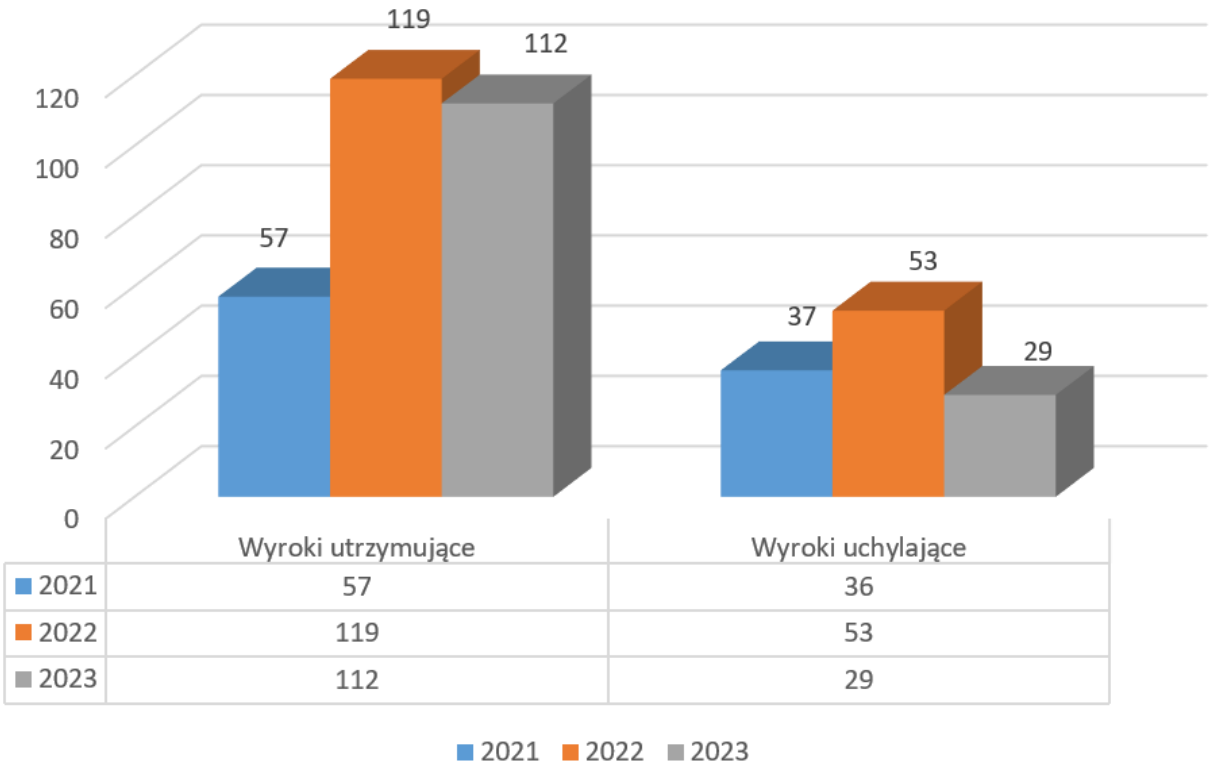
Generalnie zauważyć należy, że sądy administracyjne rzadko uchylają decyzje wydane w sprawach skargowych, co świadczy o dobrym poziomie merytorycznym rozstrzygnięć organu. Z analizy uzasadnień wyroków wpływających do organu wynika ponadto, że częstym powodem uchylenia decyzji nie są kwestie merytoryczne a formalne, przy czym od większości tych rozstrzygnięć organ składa skargi kasacyjne, nie podzielając oceny sądu.



	Skargi do WSA	Skargi do NSA
2021	194	37
2022	177	55
2023	223	66

Skargi wniesione do WSA i NSA w latach 2021-2023 w sprawie decyzji wydanych w Departamencie

1 ROZMOWA Z EKSPERTEM



Wyroki utrzymujące i uchylające decyzję Prezesa UODO w sprawach skargowych w latach 2021-2023

Porównując obydwa ww. wykresy można także zauważyć problem małej aktywności orzeczniczej sądów administracyjnych w sprawach Urzędu Ochrony Danych Osobowych. Liczba wpływających skarg na decyzje jest znacząco wyższa niż liczba wydawanych wyroków w sprawie skarg na decyzje. Obecnie na wyroki w części spraw oczekujemy od 2019 roku. W latach poprzednich zmagaliśmy się także z kwestią wydawanych w WSA w Warszawie licznych sprzecznych ze sobą wyroków w sprawach o niemal takim samym stanie faktycznym i prawnym. Szczególnie widoczne było to w sprawach z sektora finansowego, dotyczących banków. Podkreślić jednak należy że w ostatnim roku widzimy wyraźną korzystną zmianę w tym zakresie.

Czy w ostatnim czasie były jakieś wyroki NSA, potwierdzające stanowisko Urzędu, z których jest Pani szczególnie zadowolona?

Wyroki Sądu Administracyjnego często potwierdzają stanowisko Urzędu. Wszystkie tego typu decyzje cieszą nas, są potwierdzaniem tego, że realizujemy nasze działania skutecznie i podejmujemy słuszne decyzje. To dowód uznania dla wysokiej jakości naszej pracy.

1 ROZMOWA Z EKSPERTEM

Zachęcam do lektury decyzji opisanej w niniejszym wydaniu biuletynu, w której Prezes UODO nakazał zaprzestanie przetwarzania danych osobowych przez bank po stwierdzeniu, że nie spełnił on obowiązku informacyjnego, o którym mowa w art. 105a ust. 3 Prawa bankowego i wskazał, że ciężar udowodnienia spełnienia takiego obowiązku spoczywa na podmiocie udzielającym kredytu. Decyzja Prezesa UODO została zaskarżona do WSA w Warszawie, który uwzględnił zarzuty strony skarżącej i uchylił decyzję organu nadzorczego. W postępowaniu przez NSA, zainicjowanym skargą kasacyjną Prezesa UODO, Sąd II instancji przychylił się jednak do stanowiska organu. Chciałabym nagłośnić tę sprawę, ponieważ temat jest bardzo aktualny – mierzymy się z ogromną liczbą skarg w tym zakresie, różnymi orzeczeniami WSA, a opisywany w biuletynie wyrok NSA to pierwsze orzeczenie, które potwierdza nasze stanowisko.

Czego najczęściej dotyczą skargi? W których sektorach jest najwięcej postępowań?

W roku 2023 najwięcej, 2659 skarg dotyczyło skarg na podmioty sektora prywatnego. Następnie 1519 skarg na podmioty sektora finansowego,1454 skarg na podmioty sektora zdrowia, 1328 skarg na podmioty sektora publicznego, 532 skarg na podmioty sektora transgranicznego.

Liczba skarg wniesionych do UODO w roku 2023 utrzymała się na podobnym poziomie w porównaniu do lat poprzednich. Jednakże wartość ta wciąż pozostaje na bardzo wysokim poziomie. Spadek liczby wnoszonych skarg odnotowano w sektorze prywatnym, w pozostałych sektorach, w tym w sektorze transgranicznym, liczba ta wzrosła.

Czy to oznacza, że zmienia się świadomość społeczeństwa dotycząca praw związanych z ochroną danych osobowych?

Zdecydowanie tak, społeczeństwo jest coraz bardziej świadome przysługujących im praw w zakresie ochrony danych osobowych i prywatności. Wiedzę Polaków na temat ochrony danych osobowych i przysługujących im praw oceniam wysoko. Wskazują na to powody składania skarg. Osoby, których dane dotyczą często skarżyły się na przetwarzanie ich danych osobowych bez podstawy prawnej, w tym na udostępnienie ich danych osobowych podmiotom nieuprawnionym, czy też nieuprawnione działania marketingowe z wykorzystaniem ich danych.

Duża część skarg dotyczyła także niespełnienia obowiązków informacyjnych, wynikających z RODO, w tym nieprzekazania kopii danych, zgodnie z art. 15 ust. 3 RODO. Odnotowano także liczne skargi na nieprawidłowe wykonanie obowiązku sprostowania danych oraz niewłaściwą realizację prawa do usunięcia danych wynikającego z art. 17 RODO i prawa sprzeciwu, o którym mowa w art. 21 RODO.

Jakich naruszeń dotyczą skargi na podmioty z sektora publicznego?
Skargi na podmioty z sektora publicznego, podobnie jak w latach ubiegłych najczęściej dotyczą udostępnienia danych osobowych. Zanotowaliśmy wiele przypadków skarg dotyczących udostępnienia danych osobowych na stronach internetowych Biuletynu Informacji Publicznej. Przypadki te często dotyczyły publikacji na stronach instytucji publicznych dokumentów, które nie zostały prawidłowo zanonimizowane i zawierały dane osobowe. Sprawa może się wydawać trywialna, ale jednak chodzi tu o dane osobowe, które powinny być bezwzględnie chronione i w takich sytuacjach reakcja organu nadzorczego musi być stanowcza.

A jak wygląda sprawa w przypadku sektora finansów, ubezpieczeń czy telekomunikacji, gdzie administratorzy przetwarzają ogromne ilości danych osobowych?
Działalność Prezesa Urzędu Ochrony Danych Osobowych w obszarze sektora finansowego, ubezpieczeń i telekomunikacji od lat skupiała się na rozpatrywaniu skarg osób kwestionujących proces przetwarzania ich danych związanych z zawieraniem różnego rodzaju umów. Są to głównie umowy skutkujące powstaniem zobowiązań finansowych po stronie osób skarżących i najczęściej wiążą się z dochodzeniem roszczeń majątkowych przez firmy windykacyjne, którym wierzyciele zlecali dochodzenie wierzytelności, ale także przez fundusze inwestycyjne, które w drodze cesji wierzytelności nabyły wierzytelności od wierzycieli pierwotnych oraz przez podmioty zarządzające portfelem wierzytelności funduszy inwestycyjnych.
UODO często podkreślał, że rozwiązywanie sporów dotyczących istnienia roszczeń, czy też skuteczności zawierania umów, w tym umów będących źródłem tychże roszczeń, pozostaje poza zakresem kompetencji przysługujących Prezesowi UODO. Organ władny jest wyłącznie do oceny procesu przetwarzania danych związanego z powyższymi zagadnieniami.

1 ROZMOWA Z EKSPERTEM

Znaczna część skarg wpływających do organu nadzorczego dotyczyła działalności podmiotów sektora finansowego, takich jak banki, instytucje pożyczkowe, spółdzielcze kasy oszczędnościowo-kredytowe, instytucje utworzone na podstawie art. 105 ust. 4 Prawa bankowego, związanej z przetwarzaniem danych osobowych w związku z dokonywaniem oceny zdolności kredytowej i analizy ryzyka kredytowego.

Zaskakujące jest jak duży odsetek skarg nie spełnia wymogów formalnych. Może warto jeszcze raz podkreślić, przypomnieć jakie elementy musi zawierać skarga, żeby UODO mógł ją przyjąć do rozpatrzenia.

Z pewnością warto to powtarzać. Każda skarga złożona do Prezesa Urzędu musi zawierać pięć elementów:

1. dane osoby skarżącej: imię, nazwisko, adres zamieszkania;
2. wskazanie podmiotu, na który osoba, której dane dotyczą, składa skargę;
3. dokładny opis naruszenia;
4. żądanie skarżącego – jakich działań oczekuje od Prezesa UODO;
5. własnoręczny podpis bądź, jeśli skarga jest składana drogą elektroniczną, podpis właściwy dla tej formy.

Należy pamiętać, że składając skargi należy dołączyć dowody potwierdzające nieprawidłowe działanie administratora. Warto też pamiętać, że zgłaszając więcej niż jedno żądanie w ramach jednej skargi, należy zwrócić uwagę, by nie były one ze sobą sprzeczne. Szczegóły dotyczące składania skarg znaleźć można na stronie Urzędu.

Urząd cały czas daje możliwość składania wniosków za pośrednictwem tradycyjnej poczty czy nawet osobiście. Jaki procent wniosków jest składany właśnie w taki tradycyjny sposób z pominięciem internetu?

Tradycyjne sposoby składania wniosków, czy też innego kontaktu z Urzędem są dla nas bardzo ważne. Nie chcemy wykluczać nikogo również w sposób cyfrowy. Ten aspekt nie ogranicza się do składania wniosków, pomimo bardzo rozbudowanej i przejrzystej strony internetowej prowadzimy Infolinię UODO, która jest bardzo ważnym kanałem komunikacji Urzędu ze społeczeństwem. Obserwujemy stale rosnący odsetek liczby skarg zgłaszanych drogą elektroniczną.

1 ROZMOWA Z EKSPERTEM

Czy spodziewa się Pani zmian w statystykach składanych wniosków w 2024 roku? Może jest jakiś sektor, który zapowiadał intensyfikację działań w tym aspekcie?

Z tego co obserwujemy, ilość skarg wpływających do organu w ostatnim czasie utrzymuje się na wysokim, ale dość stałym poziomie. Stosunkowo nowym zjawiskiem jest duża liczba skarg osób, których dane zostały naruszone wskutek wycieków u dużych administratorów. Obowiązek notyfikowania tych naruszeń przez administratorów organowi nadzorczego i jednocześnie informowanie osób, których dane naruszono, powoduje, że chcą one dochodzić swoich praw również w indywidualnych postępowaniach prowadzonych przez organ.

Czego życzyłaby Pani sobie i swojemu departamentowi w 2024 roku? Co mogłoby usprawnić działania Departamentu Skarg?

Życzę, nie sobie czy departamentowi, ale przede wszystkim społeczeństwu, jeszcze większej świadomości. Znajomość swoich praw i umiejętność korzystania z nich to bardzo ważne aspekty życia. Jednocześnie chciałabym, żeby większy odsetek wniosków trafiających do nas był pozbawiony błędów formalnych, żeby większa część złożonych wniosków kończyła się decyzją organu. Nieustannie edukujemy w tym zakresie społeczeństwo, ale niestety dostrzegamy sporą niedbałość klientów przy składaniu wniosków – to o tyle przykre, że nie możemy ich wtedy rozpatrzeć. Oczywiście w takich sytuacjach składający dostaje informację zwrotną i zostaje poproszony o uzupełnienie braków czy poprawienie błędów, mamy jednak świadomość, że dużej części nieprawidłowości można by uniknąć.

Dziękuję za rozmowę.

WNIOSEK O ZMIANĘ PRZEPISÓW DOTYCZĄCYCH REKRUTACJI DO SZKÓŁ I PRZEDSZKOLI

W opinii UODO na potrzeby potwierdzenia spełnienia kryterium samotnego wychowywania dziecka podczas rekrutacji do szkół i przedszkoli nie powinny być pozyskiwane prawomocne wyroki sądów rodzinnych orzekające rozwód lub separację. Również okres retencji danych zebranych w toku rekrutacji budzi zastrzeżenia organu nadzorczego. Dlatego do Minister Edukacji skierowane zostało wystąpienie dotyczące wprowadzenia stosownych zmian w przepisach ustawy – Prawo oświatowe.

W wystąpieniu tym Prezes UODO wskazał, że jego wątpliwości budzi brzmienie art. 150 i art. 160 ustawy z dnia 14 grudnia 2016r. – Prawo oświatowe.

Pozyskiwanie wyroków sądów rodzinnych to za dużo

Artykuł 150 ust. 2 pkt 1 lit. c powołanej ustawy przewiduje, że do wniosku rekrutacyjnego do publicznego przedszkola, oddziału przedszkolnego w publicznej szkole podstawowej, publicznej innej formy wychowania przedszkolnego, publicznej szkoły, publicznej placówki, na zajęcia w publicznej placówce oświatowo-wychowawczej, na kształcenie ustawiczne w formach pozaszkolnych lub kwalifikacyjny kurs zawodowy dołącza się prawomocny wyrok sądu rodzinnego orzekający rozwód lub separację lub akt zgonu oraz oświadczenie o samotnym wychowywaniu dziecka oraz niewychowywaniu żadnego dziecka wspólnie z jego rodzicem.

W ocenie UODO, obowiązek załączania do wniosku rekrutacyjnego prawomocnego wyroku sądu rodzinnego orzekającego rozwód lub separację na potwierdzenie spełniania przez kandydata kryterium, jakim jest samotne wychowywanie kandydata w rodzinie, narusza określoną w RODO zasadę minimalizacji danych. Zgodnie z nią przetwarzanie powinno obejmować tylko takie dane, jakie są niezbędne dla realizacji konkretnego i określonego celu przetwarzania.
Tymczasem zakres i kategorie spraw oraz okoliczności oceniane przez sąd w związku z orzekaniem o rozwodzie (całokształt spraw małżeńskich, rodzicielskich i alimentacyjnych, mieszkaniowych czy majątkowych wskazany w przepisach ustawy z dnia 25 lutego 1964 r. - Kodeks rodzinny i opiekuńczy) determinują konieczność głębokiej ingerencji w sprawy rodziny i poszczególnych jej członków. Nierzadko informacje dotyczą także osób trzecich, a zatem dotykają w sposób niezwykle istotny prywatności rodziny, jej poszczególnych członków, ewentualnie innych osób.

W konsekwencji dyrektorzy szkół, do których wpływają wnioski rekrutacyjne zawierające w załączeniu wyroki sądów rodzinnych orzekające rozwód lub separację (zwłaszcza gdyby były przedkładane również z uzasadnieniem), pozyskują wiele różnego rodzaju danych odnoszących się do różnych kategorii osób, które nie są niezbędne do rozpatrzenia i weryfikacji spełnienia kryterium samotnego wychowywania kandydata w rodzinie. W ocenie organu nadzorczego konieczne jest zrezygnowanie z konieczności dołączania do składanego wniosku rekrutacyjnego pełnej treści dokumentów dotyczących sytuacji rodzinnej i przeanalizowanie innych form potwierdzania spełnienia kryterium samotnego wychowywania dziecka w rodzinie.

Możliwe rozwiązanie

Organ nadzorczy w wystąpieniu do Minister Edukacji wskazał, że skoro zgodnie z treścią art. 4 pkt 43 ustawy - Prawo oświatowe pojęcie „samotnego wychowywania dziecka" oznacza wychowywanie dziecka przez pannę, kawalera, wdowę, wdowca, osobę pozostającą w separacji orzeczonej prawomocnym wyrokiem sądu, osobę rozwiedzioną, chyba że osoba taka wychowuje wspólnie co najmniej jedno dziecko z jego rodzicem – wykazanie tej okoliczności mogłoby nastąpić poprzez złożenie zaświadczenia o stanie cywilnym lub odpisu skróconego aktu małżeństwa. Przyjęcie takiego rozwiązania dodatkowo sprzyjałoby ujednoliceniu zakresu danych pozyskiwanych od osób samotnie wychowujących dzieci, niezależnie od ich stanu cywilnego.

Konieczna ocena wpływu przepisów na prywatność

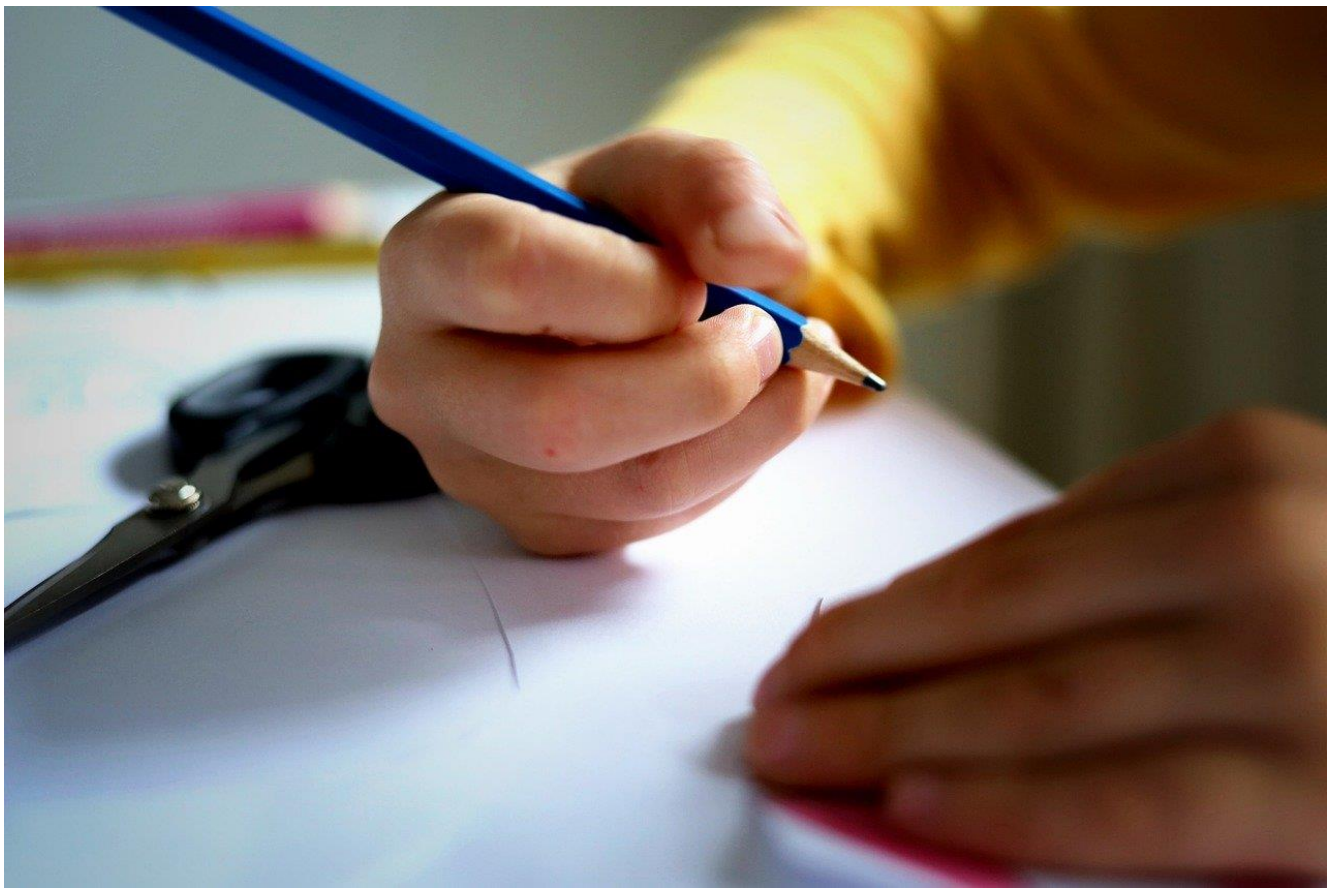
W przypadku podjęcia prac legislacyjnych nad zmianami w postulowanym zakresie niezwykle istotnym aspektem poprzedzającym przyjęcie podstawy prawnej przetwarzania danych będzie przeprowadzenie oceny wpływu projektowanych regulacji na ochronę danych osobowych. Zasadą przyjmowanych rozwiązań powinno być wprowadzenie przez projektodawcę określonych gwarancji dla pozyskiwania i dalszego przetwarzania danych osobowych. Ocena skutków projektowanej regulacji powinna wykazać ryzyka związane z zakresem pozyskiwanych danych i doprowadzić do ograniczenia ich gromadzenia jedynie do minimum niezbędnego dla realizacji zakładanego celu, a w rezultacie wyeliminować nadmiarową ingerencję w prawa i wolności wielu osób.

Potrzebna prawidłowa retencja

Wątpliwości organu nadzorczego wzbudza także okres retencji danych osobowych kandydatów (przyjętych) zgromadzonych w celach postępowania rekrutacyjnego. Zgodnie z art. 160 ust. 1 ustawy - Prawo oświatowe są one przechowywane nie dłużej niż do końca

okresu, w którym uczeń korzysta z wychowania w danej placówce publicznej. Tym samym dane osobowe pozyskane w celu przeprowadzenia postępowania rekrutacyjnego mogą być przetwarzane przez cały okres wychowania w danej placówce. Tymczasem zarówno zakres danych osobowych gromadzonych w procesie rekrutacji (np. zawartych w dokumentach potwierdzających samotne wychowywanie dziecka), jak i cel ich przetwarzania nie wymagają tak długiego okresu przechowywania. Pozyskiwane informacje mają bowiem służyć wyłącznie przeprowadzanej rekrutacji, a nie dokumentowaniu całego procesu kształcenia w danej placówce. Ponadto powinny być przetwarzane z poszanowaniem określonej w RODO zasady ograniczenia przechowywania, a więc przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te zostały zebrane.

Tym samym należy rozważyć weryfikację powołanego wyżej przepisu, którego aktualne brzmienie umożliwia przechowywanie danych przez długi okres, wykraczający poza osiągnięcie celu, jakim jest weryfikacja kryterium rekrutacyjnego. Stąd wniosek organu nadzorczego o przeanalizowanie powołanych wyżej przepisów pod kątem ich spójności z przepisami ogólnego rozporządzenia o ochronie danych.



BRANŻA HOTELARSKA ZŁOŻYŁA WNIOSEK O ZATWIERDZENIE KODEKSU POSTĘPOWANIA

Izba Gospodarcza Hotelarstwa Polskiego (IGHP) złożyła do Prezesa UODO wniosek o zatwierdzenie projektu „Kodeksu postępowania i dobrych praktyk w sprawie danych osobowych w branży hotelarskiej". Jego celem jest zapewnienie gościom hoteli, a także osobom korzystającym z dostarczanych przez nie usług, jak najwyższego poziomu ochrony ich danych osobowych, zaś hotelom – jasnych wskazówek, jak przetwarzać dane osobowe podczas świadczenia usług hotelarskich.

Przygotowanie projektu kodeksu postępowania było możliwe dzięki prężnemu i konsekwentnemu działaniu Izby prowadzonemu na przestrzeni ostatnich lat, mimo przejściowych trudności, w jakich sektor hotelarski znalazł się podczas pandemii COVID-19. W okresach normalizacji sytuacji udało się organizować spotkania mające na celu m.in. omawianie postępów w pracach nad projektem kodeksu oraz kwestii jego konsultacji społecznych, których przeprowadzenie jest elementem niezbędnym w procedurze zatwierdzania kodeksu przez organ nadzorczy.

Zakres stosowania

Zgodnie z założeniami Kodeks ma zapewnić adekwatny poziom ochrony danych osobowych gości hoteli oraz osób korzystających z usług świadczonych przez hotel, a jednocześnie zawierać jasne wytyczne dla hoteli co do przetwarzania danych osobowych w związku ze świadczeniem usług hotelarskich. Jego przepisy nie będą miały natomiast zastosowania do przetwarzania danych osobowych pracowników, współpracowników oraz dostawców towarów i usług dla hoteli.

Zawartość

W projekcie Kodeksu uregulowano przede wszystkim kwestie podstaw prawnych przetwarzania danych osobowych gości hotelowych, a także zakres i cel ich przetwarzania. Projekt wskazuje, jakie konkretnie dane mogą być pozyskiwane w związku ze świadczeniem poszczególnych usług hotelarskich oraz opisuje procesy odbywające się w związku z prowadzeniem działalności przez hotele.

2 UODO SYGNALIZUJE

Osobno opisano kwestie związane z pozyskiwaniem zgody na przetwarzanie danych osobowych (w tym do celów marketingowych), dopełnianiem obowiązku informacyjnego, retencją oraz zabezpieczaniem danych osobowych.

Ocena i informacje

Obecnie projekt kodeksu jest poddawany analizie merytorycznej pod kątem zgodności z przepisami, orzecznictwem i stanowiskami organu nadzorczego.
Podmioty zainteresowane projektem i przystąpieniem do Kodeksu mogą skontaktować się z IGHP pod adresem: ighp@ighp.pl.

Wsparcie od UODO

Hotelarze to kolejny przykład branży zainteresowanej podnoszeniem poziomu ochrony danych osobowych, która konsekwentnie prowadziła prace nad kodeksem, korzystając, kiedy było to potrzebne, z możliwości konsultacji z Urzędem.
Zachęcamy inne inicjatywy do kontaktu z Wydziałem Kodeksów i Certyfikacji DOL, by wspólnie podnosić standard ochrony danych klientów, pracowników i współpracowników oraz czerpać korzyści płynące ze stosowania kodeksów postępowania. Szczegółowe informacje na ten temat są dostępne na stronie internetowej UODO w zakładce Kodeksy postępowania.

SEKTOR OPIEKI ZDROWOTNEJ MA JUŻ DWA KODEKSY POSTĘPOWANIA

W związku z zatwierdzeniem dwóch kodeksów postępowania dla sektora ochrony zdrowia UODO podejmuje działania upowszechniające wiedzę o nich. Wkrótce odbędzie się webinarium dotyczące przystępowania do kodeksu opracowanego przez Polską Federację Szpitali.

Kodeks postępowania dla sektora ochrony zdrowia (przygotowany przez Polską Federacja Szpitali) Prezes UODO zatwierdził 11 grudnia 2023 r. Jednocześnie udzielił akredytacji podmiotowi monitorującemu jego przestrzeganie, tj. KPMG Advisory sp. z o.o. sp. k. w Warszawie, który został wpisany do wykazu podmiotów akredytowanych prowadzonego przez Prezesa Urzędu Ochrony Danych Osobowych. Tego samego dnia odbyło się webinarium nt. kodeksów postępowania i akredytacji podmiotów monitorujących, podczas którego głos zabrali Zastępca Prezesa UODO – Jakub Groszkowski, a także przedstawiciele twórców kodeksu z Polskiej Federacji Szpitali i kancelarii Domański Zakrzewski Palinka sp. k. oraz KPMG.

2 UODO SYGNALIZUJE

Webinarium było okazją do wskazania przyczyn opracowania Kodeksu i zakresu jego stosowania oraz zasad przystępowania do niego przez podmioty zainteresowane podnoszeniem poziomu ochrony danych. Przedstawiono także dwie prezentacje: 1) „RODO w sektorze medycznym" – szczegółowo omawiającą prace nad projektem kodeksu oraz 2) „Kodeks postępowania dla sektora ochrony zdrowia" – poświęconą warunkom ubiegania się o przystąpienie do kodeksu razem z omówieniem zadań dla podmiotu monitorującego, którym jest KPMG.

Z kolei w styczniu 2024 r. w ramach obchodów Dnia Ochrony Danych Osobowych Urząd organizował Cykl debat dotyczących ochrony danych osobowych w sektorze zdrowia w dobie rozwoju nowych technologii, które odbyły się 16 stycznia 2024 r. w Akademii Ekonomiczno – Humanistycznej w Warszawie. Motywem pierwszej z nich były właśnie kodeksy postępowania. Dyskutowano o zaletach zatwierdzonych kodeksów, czy istotnie zwiększają poziom ochrony danych w sektorze oraz o tym, jak przekonywać placówki zdrowotne z całego kraju do przystępowania do nich.

Urząd kontynuuje wspieranie inicjatyw kodeksowych w promowaniu tego narzędzia zapewniania zgodności. 28 lutego o godzinie 11:00 odbył się webinar, organizowany przez firmę KPMG – akredytowany podmiot monitorujący stosowanie Kodeksu postępowania dla sektora ochrony zdrowia. Jego uczestnicy mogli dowiedzieć się więcej o zatwierdzonym niedawno kodeksie. Eksperci z KPMG opowiedzieli bowiem między innymi:

- o najważniejszych zaletach stosowania kodeksu i o tym, co wyróżnia go na tle innych kodeksów zatwierdzonych w Europie,
- o tym, kto może przystąpić do stosowania kodeksu i jak to zrobić,
- w jaki sposób przebiegać będzie audyt wstępny oraz dalsze monitorowanie oraz czym będą różnić się te procesy w podmiotach prywatnych i publicznych,
- z jakimi opłatami wiąże się przystąpienie do kodeksu.

CERTYFIKACJA – INFORMACJA O WEBINARIACH

Zatwierdzone przez Prezesa UODO 8 grudnia 2023 r. Dodatkowe wymogi akredytacji podmiotów certyfikujących to ważny krok na drodze do powstania w Polsce rynku certyfikacji w zakresie ochrony danych osobowych. Obecnie Urząd prowadzi działania edukacyjne, których celem jest promowanie certyfikacji i zachęcanie rynku do tworzenia mechanizmów certyfikacji zgodnie z art. 42 RODO.

Certyfikacja to nowe i niezwykle ważne narzędzie, które może ułatwić administratorom i podmiotom przetwarzającym wykazanie zgodności z ogólnym rozporządzeniem o ochronie danych, a osobom, których dane osobowe będą przetwarzane, szybko ocenić stopień ich ochrony. Zanim jednak administratorzy i podmioty przetwarzające będą mogli uzyskać certyfikaty potwierdzające zgodność ich procesów przetwarzania danych z RODO musi powstać rynek, na którym będzie można się o nie ubiegać. Dlatego Urząd prowadzi cykl webinariów, które mają upowszechniać wiedzę w tym zakresie.

Pierwsze webinarium z serii „Certyfikacja w ochronie danych" odbyło się 12 grudnia 2023 r. Podczas tego spotkania zostały omówione podstawowe zagadnienia: ramy prawne, dokumenty wydane przez EROD, przedmiot certyfikacji, podmioty uprawnione do jej uzyskania. Pracownicy Urzędu odpowiadali też na pytania uczestników tego wydarzenia.
30 stycznia 2024 r. przeprowadzone zostało drugie webinarium z tego cyklu. Jego uczestnicy dowiedzieli się, czym są mechanizmy certyfikacji i jak wygląda procedura zatwierdzenia kryteriów certyfikacji, które stanowią ich integralną część. Również i tym razem pracownicy Urzędu odpowiadali na pytania.
Nagrania z tych wydarzeń są dostępne na stronie internetowej UODO w zakładce: Certyfikacja.
Kolejne webinaria będą odbywały się raz w miesiącu, a o dokładnych terminach i tematyce tych spotkań będziemy informować za pośrednictwem strony internetowej i swoich mediów społecznościowych.

Dziękujemy za wszystkie pytania i uwagi, które były i będą zgłaszane podczas webinariów oraz przesyłane do UODO.

Ich analiza przyczyni się do aktualizowania treści publikowanych w zakładce Certyfikacja, tak aby w jak największym stopniu były one przejrzyste i pomocne dla wszystkich podmiotów zainteresowanych tworzeniem programów certyfikacji oraz uzyskaniem akredytacji do udzielania certyfikacji, a także dla administratorów i podmiotów przetwarzających planujących certyfikować prowadzone przez siebie operacje na danych. Przygotowujemy poszerzenie zakładki Certyfikacja o słowniczek pojęć związanych z certyfikacją w ochronie danych oraz będziemy w niej zamieszczać odpowiedzi na pytania zadawane podczas webinariów i te, które będą przesyłane do UODO.

Zachęcamy do kontaktu z Wydziałem Kodeksów i Certyfikacji (dol@uodo.gov.pl) wszystkie podmioty zainteresowane tworzeniem mechanizmów i kryteriów, czy pełnieniem funkcji podmiotu certyfikującego. Obok kodeksów postępowania certyfikacja jest jednym z narzędzi umożliwiających wykazanie spełniania wysokiego standardu ochrony danych.

SKORZYSTANIE Z UPRAWNIENIA JAKIE PRZEWIDUJE ART. 105A UST. 3 PRAWA BANKOWEGO, WYMAGA SKUTECZNEGO POINFORMOWANIA OSOBY, KTÓREJ DANE DOTYCZĄ

Prezes Urzędu Ochrony Danych Osobowych nakazał zaprzestanie przetwarzania danych osobowych przez bank po stwierdzeniu, że nie spełnił on obowiązku informacyjnego, o którym mowa w art. 105a ust. 3 Prawa bankowego i wskazał, że ciężar udowodnienia spełnienia takiego obowiązku spoczywa na podmiocie udzielającym kredytu. Decyzja Prezesa UODO została zaskarżona do WSA w Warszawie, który uwzględnił zarzuty strony skarżącej i uchylił decyzję organu nadzorczego. W postępowaniu przez NSA, zainicjowanym skargą kasacyjną Prezesa UODO, Sąd II instancji przychylił się jednak do stanowiska organu.

Skarżący zawarł z jednym z popularnych banków umowę kredytową, w ramach której podał takie dane jak: imię, nazwisko, nr PESEL, nr dowodu osobistego, płeć, data urodzenia oraz adres zamieszkania. Dane te, zgodnie z treścią art. 105 ust. 4 oraz art. 105a ust 1 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe, zostały następnie przekazane do Biura Informacji Kredytowej (BIK).

W spłacie zobowiązania skarżący dopuścił się trwającej ponad 60 dni zwłoki, w związku z czym bank wysłał mu listem poleconym pismo „Ostateczne wezwanie do zapłaty", które zawierało informację o zamiarze skorzystania przez bank z prawa do przetwarzania informacji stanowiących tajemnicę bankową przez okres 5 lat po wygaśnięciu zobowiązania, bez zgody osoby, której te informacje dotyczą (art. 105a ust. 3 Prawa bankowego).

W związku z powyższym klient banku, wniósł skargę do Prezesa Urzędu Ochrony Danych Osobowych, żądając aktualizacji swoich danych osobowych w Biurze Informacji Kredytowej. Skarżący nie zakwestionował wprawdzie, że dopuścił się zwłoki w spełnieniu świadczenia, podniósł jednak, że bank nie spełnił obowiązku poinformowania go o zamiarze przetwarzania dotyczących go informacji, co jest jednym z warunków przetwarzania danych, o którym mowa we wskazanym powyżej art. 105a ust. 3 Prawa bankowego.

3 WYBRANE DECYZJE UODO

Odpowiednie przepisy Prawa bankowego

Badając sprawę Prezes UODO wskazał, że aktem prawnym zawierającym szczegółowe regulacje dotyczące procesu przetwarzania danych osobowych klientów banków jest przede wszystkim ustawa Prawo bankowe, a podstawą prawną przetwarzania danych osobowych skarżącego przez bank w BIK jest uprawnienie wynikające z art. 105a ust. 3 Prawa bankowego.

BIK, czyli Biuro Informacji Kredytowej, jest instytucją utworzoną na podstawie art. 105 ust. 4 Prawa bankowego, który stanowi, że banki mogą wspólnie z bankowymi izbami gospodarczymi, utworzyć instytucje upoważnione do gromadzenia, przetwarzania i udostępniania informacji stanowiących tajemnicę bankową określonym podmiotom m.in. bankom, instytucjom kredytowym i pożyczkowym w związku z wykonywanymi przez nie czynnościami. Zgodnie z art. 105a ust. 1 Prawa bankowego, przetwarzanie informacji dotyczących osób fizycznych, stanowiących tajemnicę bankową oraz tajemnicę obejmującą dane zebrane przez pozostałe instytucje kredytowo-pożyczkowe wymienione w tym przepisie, może być wykonywane w celu oceny zdolności kredytowej i analizy ryzyka kredytowego.

Zgodnie z art. 105a ust. 3 Prawa bankowego banki oraz inne instytucje kredytowo-pożyczkowe wymienione w tym przepisie mogą przetwarzać informacje stanowiące tajemnicę bankową i tajemnicę obejmującą dane zebrane przez inne instytucje kredytowo-pożyczkowe dotyczące osób fizycznych, po wygaśnięciu zobowiązania wynikającego z umowy zawartej z bankiem lub pozostałymi wymienionymi instytucjami bez zgody osoby, której informacje dotyczą, gdy osoba ta nie wykonała zobowiązania lub dopuściła się zwłoki powyżej 60 dni w spełnieniu świadczenia wynikającego z umowy zawartej z bankiem lub z innymi wymienionymi instytucjami, a po zaistnieniu tych okoliczności upłynęło, co najmniej 30 dni od poinformowania tej osoby przez bank lub inne wymienione w tym przepisie instytucje.

Trzydziestodniowy termin biegnie od momentu skutecznego poinformowania klienta banku

Odnosząc się do przytoczonych przepisów organ nadzorczy wskazał, że moment od którego należy liczyć sześćdziesięciodniowy termin, w którym klient banku dopuszcza się zwłoki w wykonaniu zobowiązania, to termin wykonania zobowiązania. Dopiero po upływie 60 dni zaczyna biec trzydziestodniowy termin, w którym instytucja oczekuje na wykonanie zobowiązania klienta. Termin trzydziestodniowy nie biegnie jednak ex lege, a dopiero od momentu, w którym zostanie on skutecznie poinformowany przez instytucję o zamiarze przetwarzania jego danych osobowych.

Ostatecznie, to bezskuteczny upływ 30 dni od momentu poinformowania stanowi wypełnienie przesłanek z art. 105a ust. 3 Prawa bankowego.
Z powyższych rozważań wynika zatem, iż przepis art. 105a ust. 3 ustawy Prawo bankowe wyraźnie stawia wymóg „poinformowania" osoby, której informacje dotyczą, o zamiarze przetwarzania dotyczących jej informacji stanowiących tajemnicę bankową, bez jej zgody, co z kolei oznacza, że aby przetwarzać jej dane na warunkach określonych w ww. przepisie, bank musi dysponować dowodem, że osoba, której dane dotyczą, została poinformowana o zamiarze ich przetwarzania bez jej zgody.

Bank musi dysponować dowodem, że osoba, której dane dotyczą, została poinformowana o zamiarze ich przetwarzania. Wysłanie listu poleconego bez poświadczenia odbioru oraz wydruk z książki nadawczej nie są wystarczającymi dowodami spełnienia obowiązku informacyjnego.

Bank wyjaśnił, że skarżący został poinformowany za pomocą zawiadomienia przesłanego listem poleconym. Prezes UODO wskazał jednak, że wprawdzie przytoczone przepisy Prawa bankowego nie przewidują określonej formy dla spełnienia powyższego obowiązku informacyjnego, jednak jego realizacja za pomocą listu poleconego bez poświadczenia odbioru, pozbawia informującego dowodu skutecznego doręczenia takiej korespondencji. Zdaniem organu nadzorczego za taki dowód nie można również uznać wydruku z książki nadawczej, w której archiwizowane są pliki dotyczące zawiadomień wysyłanych listem poleconym przez bank, gdzie pod określoną pozycją widniały dane adresowe skarżącego.

Ciężar dowodu spoczywa na podmiocie udzielającym kredytu, a nie na kliencie

Biorąc powyższe pod uwagę Prezes UODO stwierdził, że powyższy dowód i wyjaśnienia przekazane organowi przez bank świadczą jedynie o przesłaniu skarżącemu ww. pisma z zawiadomieniem, nie stanowią one natomiast dowodu na okoliczność, iż korespondencja ta została skarżącemu skutecznie doręczona. Organ nadzorczy podkreślił również, powołując się, m. in. na wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 15 marca 2017 r., sygn. akt II SA/Wa 1695/16, że to na banku spoczywa ciężar udowodnienia, że poinformował skarżącego o zamiarze przetwarzania jego danych bez jego zgody i to w jego interesie powinno leżeć, aby poinformowanie, o którym mowa w art. 105a ust. 3 Prawa bankowego odbyło się w sposób, który umożliwi jego łatwe wykazanie w przypadku ewentualnego sporu.

3 WYBRANE DECYZJE UODO

Zdaniem Prezesa Urzędu Ochrony Danych Osobowych niedopuszczalna jest taka wykładnia art. 105a ust. 3 Prawa bankowego, że to na osobie fizycznej (w niniejszej sprawie na skarżącym) spoczywa ciężar udowodnienia, że nie został poinformowany o ww. zamiarze przetwarzania danych osobowych.

Prezes UODO stwierdził niniejszym, że bank nie spełnił warunków dla przetwarzania danych osobowych, o których mowa w art. 105a ust. 3 Prawa bankowego i tym samym dopuścił się naruszenia ochrony danych osobowych. Zgodnie z dyspozycją, obowiązującego jeszcze na gruncie ustawy o ochronie danych osobowych z 29 sierpnia 1997 r., art. 18 ust. 1 pkt 6 w zw. z art. 105a ust. 3 i ust. 5 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe organ nadzorczy nakazał więc zaprzestania przetwarzania danych skarżącego dotyczących umowy kredytowej w systemie Biura Informacji Kredytowej (BIK).

Administrator danych (bank) nie zgodził się jednak z takim rozstrzygnięciem i zaskarżył przedmiotową decyzję do Wojewódzkiego Sądu Administracyjnego w Warszawie. Po rozpatrzeniu skargi, Sąd I instancji uznał, że była ona zasadna i zasługiwała na uwzględnienie. Uzasadniając swoje stanowisko Sąd stwierdził m.in., że Prezes UODO dokonał błędnej wykładni art. 105a ust. 3 ustawy Prawo bankowe poprzez przyjęcie, że wykonanie obowiązku informacyjnego, o którym mowa w tym przepisie, polega na skutecznym doręczeniu klientowi banku informacji o zamiarze przetwarzania jego danych osobowych. Zdaniem Wojewódzkiego Sąd Administracyjnego w Warszawie prawidłowa interpretacja tego przepisu prowadzi do wniosku, że „poinformowanie" oznacza jedynie rzeczywiste umożliwienie klientowi banku zaznajomienie się ze wspomnianą informacją. Zdaniem Sądu I instancji organ nadzorczy dopuścił się również naruszenia przepisów procedury administracyjnej, błędnie przyjmując, że przedłożony przez bank wydruk z księgi nadawczej nie stanowi dowodu poinformowania klienta banku o zamiarze przetwarzania jego danych osobowych bez jego zgody, podczas gdy, w ocenie Sądu jest to dostateczny dowód przekazania wymaganej przez art. 105a ust. 3 informacji. W związku z powyższym Sąd I Instancji uchylił decyzję Prezesa UODO w zakresie, w jakim nakazywała ona zaprzestanie przetwarzania danych osobowych klienta banku w Biurze Informacji Kredytowej (BIK) na podstawie art. 105a ust. 3 i ust. 5 ustawy Prawo bankowe. Prezes UODO wniósł skargę kasacyjną od tego wyroku, podtrzymując swoje dotychczasowe stanowisko.

3 WYBRANE DECYZJE UODO

Naczelny Sąd Administracyjny rozpatrując skargę wskazał m.in., że prawodawca nie zdefiniował użytego w art. 105 ust. 3 Prawa bankowego pojęcia „poinformować" ani nie stworzył w tym zakresie żadnych szczególnych wymogów formalnych co do sposobu i treści takiego poinformowania. Jak dalej podkreślił Naczelny Sąd Administracyjny, prawidłowa wykładnia tego przepisu nie może jednak oznaczać całkowitej dowolności i powołując się na Słownik języka polskiego przytoczył, iż „poinformować" to tyle co „udzielić informacji, wskazówek, objaśnić, powiadomić o czymś, podać do wiadomości", czyli spowodować, że ktoś zaczyna o czymś wiedzieć. Sąd II instancji wskazał dalej, że w literaturze i orzecznictwie sądów administracyjnych zwraca się uwagę na materialny (ochronny), a nie formalny charakter tego przepisu. Dane osobowe są wartością chronioną ustawowo, a prawo do ich ochrony – jak przyjmuje się w piśmiennictwie, „stanowi swego rodzaju emanację ogólnego prawa gwarantowanego Konstytucją RP (art. 47).

Sąd II instancji wskazał dalej, że o ile nie powinno się abstrahować od istoty (celu) wprowadzenia instytucji przetwarzania danych osobowych dłużnika bez jego zgody tj. ochrony innych podmiotów przed wyłudzaniem kolejnych pożyczek przez nierzetelnych dłużników, czyli osoby, które pomimo zaciągnięcia określonego zobowiązania, nie wywiązują się z niego, to jednak pozycja dłużnika wobec podmiotu udzielającego pożyczki jest słabsza, a skutek w postaci przetwarzania danych osobowych bez jego zgody ma charakter publicznoprawny. Oznacza to, że wszelkie regulacje znoszące tę ochronę muszą być odczytywane i wykładane ściśle, z uwzględnieniem funkcji jakiej mają służyć. Przy takiej wykładni, sformułowanie użyte w przepisie art. 105a ust. 3 Prawa bankowego, odnoszące się do obowiązku informacyjnego musi więc oznaczać, że nie jest to tylko obowiązek formalny. Jakkolwiek ustawodawca w żaden sposób nie ograniczył sposobów i form takiego powiadomienia, to w każdym wypadku sposób ten powinien umożliwić zweryfikowanie faktu poinformowania klienta banku o zamierzonym przetwarzaniu jego danych osobowych. Co również istotne, przyjmując treść przepisu, ustawodawca posłużył się kategoryczną formą poinformować (czasownik przechodni dokonany) , a nie „informować".

Naczelny Sąd Administracyjny wskazał dalej, że określony w ustawie Prawo bankowe skutek ma nastąpić po upływie „30 dni od poinformowania tej osoby przez bank", a nie od – przykładowo – wysłania jej informacji. Takie „poinformowanie" może np. nastąpić osobiście w placówce banku lub innego podmiotu wymienionego w art. 105 ust.3, poprzez przesyłkę doręczoną listownie lub przez pracownika banku lub innego uprawnionego podmiotu, a nawet skierowania takiej informacji drogą elektroniczną (o ile strony w zawartej umowie taką korespondencję).

O ile więc sposób i forma poinformowania klienta mogą być różnorodne, to jednak w każdym wypadku sposób ten powinien umożliwić zweryfikowanie faktu poinformowania klienta banku o zamierzonym przetwarzaniu jego danych osobowych. Natomiast wybór formy poinformowania adresata, operatora pocztowego i sposobu przekazania informacji oraz związany z tym faktem obowiązek wykazania tego faktu obciążają bank lub inny zobowiązany podmiot, gdyż to one wywodzą z tego faktu skutki prawne. I jak podkreślił Sąd II instancji, taki sposób rozumienia obowiązku poinformowania zamieszczonego w art. 105a ust. 3 Prawa bankowego wynika nie tylko z gwarancyjnego charakteru tego przepisu dla kredytobiorcy, ale także z dobrze pojętego interesu podmiotów udzielających kredytów, aby w sposób skuteczny mogły zamieszczać w BIK stosowną informację o nierzetelnym kredytobiorcy. Wskazanie daty doręczenia przesyłki zawierającej stosowną informację umożliwia także prawidłowe wskazanie początku biegu trzydziestodniowego terminu.

Przenosząc obowiązek wykazania skutecznego poinformowania klienta na grunt badanej sprawy NSA przychylając się do wniosków Prezesa UODO wskazał, że wydruk z księgi nadawczej banku potwierdzał jedynie, że listem poleconym zostało wysłane pismo „Ostateczne wezwanie do zapłaty", które zawierało informacje o zamiarze skorzystania z prawa do przetwarzania informacji na podstawie art. 105a ust. 3 analizowanego przepisu. Nie wynika z niego natomiast, że przesyłka ta została skutecznie doręczona, a bank nie przedstawił żadnego innego dowodu jej doręczenia (wskazującego na datę doręczenia np. wydruk ze strony śledzenia przesyłek rejestrowanych).

Biorąc powyższe pod uwagę, Naczelny Sąd Administracyjny w oparciu o art. 151 oraz art. 188 ustawy z dnia 30 sierpnia 2002 r. Prawo o postępowaniu przed sądami administracyjnymi (p.p.s.a.) uwzględniając skargę kasacyjną wniesioną przez Prezesa UODO, uchylił zaskarżony wyrok i oddalił skargę wniesioną przez administratora danych.

Sygnatura sprawy:
decyzja Prezesa UODO ZSPR.440.700.2018,
wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie II SA/Wa 2037/19,
wyrok Naczelnego Sądu Administracyjnego III OSK 3233/21

WYTYCZNE W SPRAWIE WYKORZYSTANIA TECHNOLOGII ROZPOZNAWANIA TWARZY W OBSZARZE ŚCIGANIA PRZESTĘPSTW

Coraz więcej organów ścigania wykorzystuje technologię rozpoznawania twarzy (FRT). Umożliwia ona uwierzytelnienie lub identyfikację osoby i stosuje się ją na nagraniach wideo (np. CCTV) lub zdjęciach. Używana jest m.in. do wyszukiwania osób znajdujących się na policyjnych listach zagrożeń lub do monitorowania ruchów danej osoby w przestrzeni publicznej.

FRT opiera się na przetwarzaniu danych biometrycznych, a zatem obejmuje przetwarzanie szczególnych kategorii danych osobowych. Często wykorzystuje komponenty sztucznej inteligencji (AI) lub uczenia maszynowego, co umożliwia przetwarzanie danych na dużą skalę, ale stwarza również ryzyko dyskryminacji i błędnych wyników. FRT może być stosowana w kontrolowanych sytuacjach, ale również w przypadku tłumów i ważnych węzłów transportowych.

Technologia rozpoznawania twarzy jest narzędziem wrażliwym z punktu widzenia organów ścigania, które są organami wykonawczymi i posiadają suwerenne uprawnienia. Metoda ta może ingerować w prawa podstawowe – również wykraczać poza prawo do ochrony danych osobowych – i wpływać na społeczną i demokratyczną stabilność polityczną.

Wymogi dyrektywy 2016/680

W odniesieniu do ochrony danych osobowych w kontekście ścigania przestępstw należy spełnić wymogi dyrektywy 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych. Pewne ramy dotyczące korzystania z FRT określono w ww. dyrektywie, w szczególności w art. 3 ust. 13 dyrektywy (termin „dane biometryczne”), art. 4 (zasady dotyczące przetwarzania danych osobowych), art. 8 (zgodność przetwarzania z prawem), art. 10 (przetwarzanie szczególnych kategorii danych osobowych) i art. 11 dyrektywy (zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach).

4 NARUSZENIA I KONTROLE

FRT a prawa podstawowe

Zastosowanie technologii rozpoznawania twarzy może mieć również wpływ na inne prawa podstawowe. Dlatego też Karta praw podstawowych Unii Europejskiej ma zasadnicze znaczenie dla interpretacji dyrektywy 2016/680, w szczególności prawa do ochrony danych osobowych, o którym mowa w art. 8 Karty, ale także prawa do poszanowania życia prywatnego, o którym mowa w art. 7 Karty. Wszelkie ograniczenia w korzystaniu z praw podstawowych i wolności muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Zanim prawodawca krajowy stworzy nową podstawę prawną dla jakiejkolwiek formy przetwarzania danych biometrycznych z wykorzystaniem rozpoznawania twarzy, powinien skonsultować to z organem nadzorczym ds. ochrony danych.

Fakt, że fotografia została w sposób oczywisty upubliczniona przez osobę, której dane dotyczą (art. 10 dyrektywy 2016/680), nie oznacza, że związane z tym dane biometryczne, które można uzyskać z fotografii za pomocą określonych środków technicznych, zostały w sposób oczywisty upublicznione. Domyślne ustawienia usługi nie powinny być w żaden sposób interpretowane jako dane w sposób oczywisty upublicznione.

Obowiązki administratora

Administrator musi dokładnie rozważyć, w jaki sposób (lub czy może) spełnić wymogi dotyczące praw osoby, której dane dotyczą, przed rozpoczęciem jakiegokolwiek przetwarzania FRT, ponieważ stosowanie tej technologii często wiąże się z przetwarzaniem szczególnych kategorii danych osobowych bez widocznej interakcji z osobą, której dane dotyczą. Skuteczne wykonywanie praw osoby, której dane dotyczą, zależy od tego, czy administrator wypełnia swoje obowiązki informacyjne (art. 13 dyrektywy 2016/680). Oceniając, czy istnieje „konkretny przypadek" zgodnie z art. 13 ust. 2 dyrektywy 2016/680, należy wziąć pod uwagę kilka czynników, w tym to, czy dane osobowe są gromadzone bez wiedzy osoby, której dane dotyczą, ponieważ byłby to jedyny sposób, aby osoby, których dane dotyczą, mogły skutecznie wykonywać przysługujące im prawa. Jeżeli decyzje podejmowane są wyłącznie na podstawie zastosowania FRT, osoby, których dane dotyczą, muszą zostać poinformowane o funkcjach zautomatyzowanego podejmowania decyzji.

Więcej informacji znajduje się w Wytycznych EROD 5/2022 dostępnych na stronie organu.

PUBLICZNE ŁADOWANIE TELEFONU – RYZYKO CZY WYGODA?

W dzisiejszym świecie, gdzie nasze życie zawodowe i prywatne jest ściśle związane z urządzeniami elektronicznymi, korzystanie z publicznych portów USB może prowadzić do niebezpiecznych konsekwencji. Ładowanie telefonu czy tabletu, choć wydaje się być niegroźnym działaniem, może zostać wykorzystanie przez cyberprzestępców do ingerencji w system operacyjny urządzenia. Jednym z takich zagrożeń jest tzw. „juice jacking", który w ostatnich latach stał się coraz bardziej rozpowszechniony.

Czym jest „juice jacking"?

Juice jacking to szczególnie podstępny atak wykorzystujący naturalną potrzebę ładowania urządzenia poprzez podłączenie do publicznego, zewnętrznego źródła zasilania. Realizowany jest w taki sposób, że osoby atakujące modyfikują fabryczne ładowarki USB poprzez zainstalowanie dodatkowego modułu sprzętowego, co może doprowadzić do kradzieży danych lub zainstalowania złośliwego oprogramowania na urządzeniu użytkownika.

Zagrożenia związane z juice jackingiem

Publiczne porty USB, znajdujące się na lotniskach, w centrach handlowych, hotelach, kawiarniach czy w środkach transportu publicznego, mogą stać się miejscami potencjalnych ataków na nasze urządzenia. Oto kilka zagrożeń:

- **Kradzież danych:** Atakujący mogą wykorzystać juice jacking do kradzieży danych przechowywanych na urządzeniu, takich jak kontakty, pliki, hasła itp.
- **Zainstalowanie złośliwego oprogramowania:** Poprzez zainfekowanie urządzenia złośliwym oprogramowaniem, atakujący mogą uzyskać zdalny dostęp do urządzenia lub zgromadzić poufne informacje.
- **Ransomware:** Atakujący mogą zainstalować ransomware na urządzeniu, co prowadzi do zablokowania dostępu do danych na urządzeniu i żądania okupu za ich odblokowanie.
- **Podsłuchiwanie aktywności:** Atakujący mogą wykorzystać juice jacking do podsłuchiwania aktywności użytkownika na zainfekowanym urządzeniu, co może prowadzić do kradzieży poufnych informacji.

Istnieją jednak sposoby ochrony przed takim atakiem, które mogą pomóc użytkownikom zminimalizować ryzyko kradzieży danych podczas ładowania urządzeń mobilnych.
Dzięki odpowiednim środkom ostrożności można zabezpieczyć się przed tego rodzaju zagrożeniami.

5 NOWE TECHNOLOGIE

Co zatem należałoby zrobić, żeby nie paść ofiarą juice jackingu?

1. Przede wszystkim staraj się unikać korzystania z publicznych portów USB do ładowania urządzeń.
2. W razie konieczności korzystania z publicznych portów USB, należy pamiętać, żeby upewnić się, że nie mamy uruchomionego trybu „debugowanie USB”, gdyż może to stanowić potencjalne zagrożenie dla bezpieczeństwa danych, ponieważ umożliwia dostęp do zaawansowanych funkcji urządzenia. Dlatego zaleca się wyłączenie tej opcji, co pozwoli na zminimalizowanie ryzyka nieautoryzowanego dostępu do urządzenia.
3. Alternatywnie, można korzystać z zewnętrznych baterii przenośnych do ładowania urządzeń lub kabli „only charge”, które są przeznaczone wyłącznie do ładowania urządzenia i uniemożliwiają przesyłanie danych.
4. Zaleca się również regularnie sprawdzanie i instalowanie dostępnych aktualizacji systemu operacyjnego, aby zapewnić ochronę przed różnymi rodzajami ataków oraz utrzymać urządzenie w jak najbezpieczniejszym stanie.
5. Warto również zadbać o wyłączenie funkcji udostępniania danych na urządzeniu, gdy korzystamy z publicznych portów USB, aby ograniczyć ryzyko kradzieży danych. Ta prosta czynność może stanowić dodatkową warstwę ochrony dla użytkowników, którzy nie posiadają baterii przenośnych.
6. Ochronę urządzeń przed wirusami lub nieautoryzowanym pobraniem danych może zapewnić również tzw. bloker danych USB. Może być skuteczną formą ochrony nie tylko w przypadku juice jacking, ale również ataków typu badUSB (np. przy wykorzystaniu specjalnie spreparowanych pendrive’ów), zapobiegając podłączeniu zainfekowanego urządzenia do komputera, ograniczając w ten sposób ryzyko zainfekowania.

Publiczne porty USB mogą stanowić poważne zagrożenie dla bezpieczeństwa naszych danych i urządzeń, jednak świadomość tych zagrożeń oraz stosowanie odpowiednich środków ostrożności, takich jak unikanie publicznych portów USB i korzystanie z zabezpieczeń fizycznych, jest kluczowe dla ochrony naszych danych.

TSUE: PARLAMENTARNA KOMISJA ŚLEDCZA MUSI PRZESTRZEGAĆ RODO

Trybunał Sprawiedliwości Unii Europejskiej w swoim wyroku postanowił, że parlamentarna komisja śledcza musi co do zasady przestrzegać ogólnego rozporządzenia o ochronie danych. Inaczej jest w sytuacji, gdy wykonuje ona działalność mającą na celu ochronę bezpieczeństwa narodowego.

Ponadto, jeżeli w państwie członkowskim funkcjonuje tylko jeden organ nadzoru, jest on co do zasady właściwy do kontrolowania przestrzegania RODO przez komisję śledczą. Natomiast w sytuacji, gdy komisja śledcza wykonuje w rzeczywistości działalność mającą na celu ochronę bezpieczeństwa narodowego, nie podlega ona RODO, a w konsekwencji kontroli organu nadzoru.

Skarga do austriackiego regulatora

Nationalrat, izba poselska austriackiego parlamentu, powołała komisję śledczą do zbadania możliwości wywierania nacisków politycznych na federalny urząd ochrony konstytucji i zwalczania terroryzmu[1].
Na przesłuchaniu z udziałem przedstawicieli mediów komisja śledcza przesłuchała świadka. Protokół z tego przesłuchania został opublikowany na stronie internetowej austriackiego parlamentu. Protokół zawierał pełne imię i nazwisko świadka, mimo jego wniosku o ich utajnienie.

Według świadka opublikowanie jego pełnego imienia i nazwiska odbyło się z naruszeniem przepisów RODO. Złożył on wobec tego skargę do austriackiego organu ochrony danych. Na poparcie skargi wyjaśnił, że pracował jako tajny funkcjonariusz policyjnej grupy zajmującej się zwalczaniem przestępczości na drogach publicznych. Organ ochrony danych oddalił jego skargę, twierdząc, że zasada podziału władz sprzeciwia się temu, by ów organ, wchodzący w skład władzy wykonawczej, mógł kontrolować przestrzeganie RODO przez komisję śledczą, która jest częścią władzy ustawodawczej. Świadek nie zgodził się z tym poglądem i zaskarżył decyzję organu do austriackich sądów.

1 W dniu 1 grudnia 2021 r. urząd ten został zastąpiony przez dyrekcję ds. bezpieczeństwa państwa i służb wywiadowczych.

Austriacki trybunał administracyjny zwrócił się do Trybunału Sprawiedliwości o ustalenie, czy komisja śledcza, reprezentująca władzę ustawodawczą i prowadząca dochodzenie w sprawie działalności dotyczącej bezpieczeństwa narodowego, podlega RODO i kontroli organu ochrony danych.

Przychylny skarżącemu wyrok TSUE

Trybunał orzekł, że komisja śledcza powołana przez parlament państwa członkowskiego w ramach wykonywania jego uprawnień z zakresu kontroli władzy wykonawczej musi, co do zasady, przestrzegać RODO.

Nie ulega wątpliwości, że RODO nie stosuje się do przetwarzania danych osobowych dokonywanego przez organy państwowe w ramach działalności mającej na celu ochronę bezpieczeństwa narodowego. Mimo to, z zastrzeżeniem weryfikacji tego stwierdzenia przez austriacki trybunał administracyjny, wydaje się, że przedmiotowe dochodzenie jako takie nie ma na celu ochrony bezpieczeństwa narodowego. Komisja śledcza została bowiem powołana w celu zbadania możliwości wywierania nacisków politycznych na organ należący do władzy wykonawczej, który odpowiadał za ochronę konstytucji i zwalczanie terroryzmu.

Niezależnie od powyższego, wymóg dotyczący ochrony bezpieczeństwa narodowego może uzasadnić ograniczenie obowiązków i praw wynikających z RODO pod warunkiem, że zostało ono wprowadzone w drodze aktu prawnego. Z akt sprawy nie wynika, aby omawiana komisja śledcza twierdziła, iż ujawnienie nazwiska świadka było konieczne dla ochrony bezpieczeństwa narodowego i oparte na przewidzianym w tym celu krajowym akcie prawnym. Dokonanie właściwych ustaleń w tym zakresie należy jednak do austriackiego trybunału administracyjnego.

Ponieważ Austria zdecydowała się na utworzenie tylko jednego organu nadzoru, w rozumieniu RODO, czyli organu ochrony danych, organ ten jest co do zasady właściwy również w sprawach z zakresu kontroli przestrzegania RODO przez komisję śledczą taką jak omawiana w rozpatrywanej sprawie, i to niezależnie od zasady podziału władz. Jest to konsekwencją bezpośredniego skutku RODO i zasady prymatu prawa Unii, które ma pierwszeństwo przed normami krajowymi, nawet rangi konstytucyjnej.

Źródło: Wyrok TSUE

TSUE: WYROK W SPRAWIE PRZETWARZANIA SZCZEGÓLNYCH KATEGORII DANYCH I ODSZKODOWAŃ NA MOCY RODO

W dniu 21 grudnia 2023 r. Trybunał Sprawiedliwości Unii Europejskiej wydał wyrok w sprawie Krankenversicherung Nordrhein (C-667/21), w którym wyjaśnił zasady przetwarzania szczególnych kategorii danych osobowych oraz charakter odszkodowania przyznanego na gruncie art. 82 RODO.

Sprawa dotyczyła przetwarzania danych osobowych niezdolnego do pracy pracownika, w tym danych zdrowotnych, przez jego pracodawcę – dostawcę usług medycznych kasy chorych (MDK) w Niemczech.

Zgodnie z obowiązującym prawem MDK sporządza raporty dotyczące zdolności do pracy osób ubezpieczonych w kasie chorych, również te dotyczące stanu zdrowia pracowników MDK. Pracownik MDK po powzięciu informacji o sporządzeniu raportu dotyczącego jego osoby, uznawszy, że dane dotyczące jego zdrowia były przetwarzane przez pracodawcę niezgodnie z prawem, wystąpił o odszkodowanie na podstawie art. 82 RODO.

W swoim wyroku TSUE orzekł m.in., że aby przetwarzać szczególne kategorie danych zgodnie z RODO, musi istnieć zarówno podstawa prawna na mocy art. 6 RODO, jak i mający zastosowanie wyjątek na mocy art. 9 RODO. W sprawie wykładni art. 82 RODO TSUE orzekł, że RODO ustanawia system odpowiedzialności opartej na winie, w którym wina administratora jest domniemana, chyba że jest on w stanie udowodnić, że nie jest w żaden sposób odpowiedzialny za zdarzenie powodujące szkodę. W odniesieniu do charakteru odszkodowania należnego osobie, której dane dotyczą, na mocy art. 82 RODO, TSUE wyjaśnił, że ma ono charakter czysto kompensacyjny, a nie karny.

Źródło: Wyrok TSUE

FRANCJA: KARA W WYSOKOŚCI 105 TYS. EURO DLA NS CARDS FRANCE

W wyniku przeprowadzonych przez organ nadzorczy pod koniec 2021 r. dwóch dochodzeń w sprawie spółki, stwierdzono naruszenia dotyczące czasu przechowywania danych kont użytkowników, informacji przekazywanych osobom fizycznym, bezpieczeństwa danych oraz metod umieszczania plików cookies i znaczników na terminalach użytkowników.

NS Cards France jest spółką, która tworzy i publikuje stronę internetową neosurf.com i aplikację mobilną "Neosurf", która umożliwia dokonywanie płatności online po zarejestrowaniu się w serwisie.

Francuski organ nadzorczy po przeprowadzonych dochodzeniach stwierdził kilka naruszeń RODO, tj. nieprzestrzeganie obowiązku przechowywania danych przez okres nie dłuższy, niż jest to niezbędne do celów, dla których zostały zebrane (art. 5 ust. 1 lit. e RODO), nieprzestrzeganie obowiązku informowania osób fizycznych (art. 12 i 13 RODO), niedopełnienie obowiązku zapewnienia bezpieczeństwa przetwarzanych danych osobowych (art. 32 RODO) oraz jedno naruszenie francuskiej ustawy o ochronie danych: nieprzestrzeganie obowiązków związanych z korzystaniem z plików cookies i trackerów (art. 82).

Źródło: Komunikat EROD

FRANCJA: POWSTAŁ PORADNIK WS. OCENY SKUTKÓW TRANSFERU DANYCH

Francuski organ nadzorczy (CNIL) opublikował projekt przewodnika do konsultacji publicznych w sprawie oceny skutków transferu danych. Przewodnik ten oferuje metodologię i tzw. checklistę, które mają pomóc w przeprowadzeniu oceny skutków transferu, zgodnie z sześciostopniowym procesem zalecanym przez Europejską Radę Ochrony Danych.

Jego celem jest stworzenie wskazówek dla przeprowadzania analizy przekazywania danych z EOG do państwa trzeciego, koncentrując się na zgodności z narzędziami ujętymi w art. 46 RODO. Przewodnik nie stanowi natomiast oceny przepisów i praktyk obowiązujących w kraju trzecim ani związanych z nimi zagrożeń.

Przewodnik składa się z sześciu kroków, które należy wykonać w celu przeprowadzenia oceny skutków dla ochrony danych:

1. Zidentyfikowanie i określenie transferów danych do państw trzecich
2. Udokumentowanie zastosowanego narzędzia transferu
3. Ocena ustawodawstwa i praktyk w kraju docelowym oraz skuteczności narzędzia przekazywania danych
4. Określenie i przyjęcie środków uzupełniających
5. Wdrożenie środków uzupełniających i niezbędnych kroków proceduralnych
6. Ponowna ocena stopnia ochrony danych w odpowiednich odstępach czasu i monitorowanie potencjalnych zmian, które mogą mieć wpływ na stopień tej ochrony

Źródło: komunikat CNIL

HISZPANIA WERYFIKUJE WIEK UŻYTKOWNIKÓW W CELU OCHRONY NIELETNICH PRZED DOSTĘPEM DO TREŚCI DLA DOROSŁYCH W INTERNECIE

W grudniu 2023 r. hiszpański organ nadzorczy (AEPD) przedstawił praktyczną propozycję systemu weryfikacji wieku i ochrony nieletnich w Internecie przed treściami przeznaczonymi dla dorosłych. Celem tej inicjatywy było wykazanie, że technicznie możliwe jest zabezpieczenie nieletnich przed dostępem do nieodpowiednich treści, przy jednoczesnym zapewnieniu anonimowości osób dorosłych podczas przeglądania Internetu.

System przedstawiony przez AEPD składa się z dekalogu zawierającego zasady, jakie musi spełniać system weryfikacji wieku, notatki technicznej ze szczegółami projektu oraz trzech praktycznych filmów pokazujących działanie systemu na różnych urządzeniach. Uzupełnienie stanowi grafika przedstawiająca ryzyko związane z obecnie stosowanymi systemami weryfikacji wieku.

Zadania dekalogu to: zapewnienie anonimowości online dla nieletnich; koncentracja na dostępie dozwolonym ze względu na wiek; zachowanie anonimowości u dostawców usług internetowych; ograniczenie weryfikacji dostępu do nieodpowiednich treści; zapewnienie braku konieczności ujawniania konkretnego wieku; zapobieganie profilowaniu na podstawie nawyków przeglądania; brak łączenia aktywności użytkownika między usługami; zapewnienie możliwości realizacji władzy rodzicielskiej; przestrzeganie praw podstawowych; ustanowienie ram zarządzania.

Źródło: komunikat AEPD

META IGNORUJE PRAWO UŻYTKOWNIKÓW DO ŁATWEGO WYCOFANIA ZGODY

Podczas gdy jedno kliknięcie użytkownika wystarczy, aby wyraził zgodę na śledzenie, wycofanie zgody wiąże się ze skomplikowanym procesem przejścia na płatną subskrypcję. Jak wskazuje NOYB jest to niezgodne z prawem, ponieważ RODO wyraźnie stanowi, że wycofanie zgody musi być równie łatwe, jak jej udzielenie.

Od początku listopada użytkownicy Instagrama i Facebooka, którzy nie chcą być śledzeni, muszą uiszczać tzw. opłatę za prywatność w wysokości do 251,88 euro rocznie. Po skardze NOYB odnoszącej się do fazy zgody w systemie „pay or okay", organizacja złożyła kolejną skargę do austriackiego organu ochrony danych w celu uwzględnienia sytuacji wycofania zgody.

Minęło zaledwie sześć miesięcy, odkąd Europejski Trybunał Sprawiedliwości (TSUE) orzekł, że przetwarzanie danych użytkowników przez Metę było niezgodne z prawem. Pomimo to, gigant mediów społecznościowych podjął trzecią próbę obejścia europejskich przepisów dotyczących prywatności. Zamiast pytać użytkowników o zgodę, Meta pobiera teraz opłaty za wybór ustawień przyjaznych prywatności. Użytkownicy, którzy nie chcą płacić, muszą zaakceptować śledzenie w celu uzyskania ukierunkowanych reklam. Skargę na tę praktykę NOYB złożył w listopadzie 2023 roku.

Kosztowne wycofanie zgody

Niezgodne z prawem podejście firmy Meta do bezpłatnej zgody nie jest jednak jedynym problemem. Gdy użytkownicy wyrażą zgodę na śledzenie, nie mogą jej w łatwy sposób wycofać w późniejszym terminie. Pomimo, że zgodnie z art. 7 RODO „wycofanie zgody powinno być równie łatwe jak jej udzielenie", w praktyce jedyną opcją wycofania zgody (jednym kliknięciem) jest wykupienie subskrypcji w wysokości 251,88 euro. Ponadto, jak wskazuje skarżący, użytkownik musi przejść przez kilka okien i banerów, aby znaleźć stronę, na której może faktycznie cofnąć zgodę. NOYB przypomina, że Europejska Rada Ochrony Danych za nieprzestrzeganie zasady art. 7 RODO może nałożyć na podmiot karę finansową.

Massimiliano Gelmi, prawnik ds. ochrony danych w NOYB: „Prawo jest jasne, wycofanie zgody musi być tak łatwe, jak jej udzielenie w pierwszej kolejności. Jest boleśnie oczywiste, że płacenie 251,88 euro rocznie za wycofanie zgody nie jest tak łatwe, jak kliknięcie przycisku "OK" w celu zaakceptowania śledzenia”.

Skarga do austriackiego regulatora

NOYB złożył skargę do austriackiego organu ochrony danych (DSB) w imieniu jednego skarżącego. Organ ten powinien nakazać firmie Meta dostosowanie operacji przetwarzania danych do europejskich przepisów o ochronie danych oraz zapewnienie użytkownikom łatwego sposobu na wycofanie zgody – bez konieczności uiszczania opłaty. Ponadto NOYB sugeruje, że regulator powinien nałożyć na Meta karę, aby zapobiec jej dalszym naruszeniom. Sprawa zostanie prawdopodobnie przekazana przez austriacki DSB do irlandzkiego DPC, który jest organem wiodącym dla Mety w UE.

Źródło: NOYB

PRAWO NOWYCH TECHNOLOGII – NAJWAŻNIEJSZE ZMIANY LEGISLACYJNE W 2024 (POLSKA I UE)

Xawery Konarski
Prezes Stowarzyszenia Prawa Nowych Technologii

W 2024 r. czeka nas wiele zmian prawnych w zakresie cyberbezpieczeństwa, nowych technologii i ochrony danych osobowych.

W obszarze cyberbezpieczeńtwa na wdrożenie do krajowego porządku prawnego czeka dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148, czyli dyrektywa NIS 2. Jej transpozycja do prawa krajowego ma nastąpić do 17 października 2024 r.

Ochrona przed cyberzagrożeniami

Dyrektywa ta rozszerza zakres podmiotów, które będą podlegały regulacjom. Określone w tych regulacjach podmioty kluczowe i ważne będą miały obowiązek wdrożenia środków zarządzania ryzykiem w cyberbezpieczeństwie oraz zgłaszania poważnych incydentów. W dyrektywie przewidziano też środki nadzoru nad podmiotami objętymi obowiązkami przewidzianymi w tej regulacji oraz kary, jakie będą nakładane za niestosowanie się do tych wymagań.

Również do 17 października 2024 r. powinna zostać implementowana dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2557 z dnia 14 grudnia 2022 r. w sprawie odporności podmiotów krytycznych i uchylająca dyrektywę Rady 2008/114/WE (dyrektywa CER), tzw. dyrektywę o odporności podmiotów krytycznych. Dotyczy ona zarówno podmiotów publicznych, jak i prywatnych i wraz z dyrektywą NIS 2 tworzy komplementarne, zharmonizowane ramy prawne w zakresie zapewniania ciągłości usług kluczowych dla państwa oraz odporności (fizycznej i w cyberprzestrzeni) podmiotów je świadczących.
Zgodnie z postanowieniami dyrektywy CER do 17 lipca 2026 r. każde państwo członkowskie ma zidentyfikować podmioty krytyczne dla sektorów i podsektorów określonych w załączniku do tej dyrektywy. A uznanie za podmiot krytyczny nastąpi w drodze decyzji administracyjnej.

Podmioty krytyczne będą musiały wprowadzić odpowiednie i proporcjonalne środki techniczne, bezpieczeństwa i organizacyjne, które mają zapewnić im odporność na wszelkiego rodzaju incydenty. Państwa członkowskie mają zaś wyznaczyć co najmniej jeden właściwy organ odpowiedzialny za prawidłowe stosowanie i egzekwowanie przepisów określonych w tej dyrektywie.
W 2024 r. planowane jest stworzenie projektu Rozporządzenia Parlamentu Europejskiego w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020 (Cyber Resilience Act), tzw. Rozporządzenie o cyberodporności.
Jest to pierwszy, horyzontalny akt prawny w Unii Europejskiej, który wprowadza obowiązkowe wymogi w zakresie cyberbezpieczeństwa dla produktów posiadających elementy cyfrowe. Ma mieć zastosowanie do wszystkich produktów, które są bezpośrednio lub pośrednio połączone z innym urządzeniem lub siecią (np. Internet rzeczy, IoT).
Celem tych rozwiązań jest zapewnienie podstawowego poziomu bezpieczeństwa produktów z elementami cyfrowymi, tak aby skutecznie chronić firmy i konsumentów przed cyberzagrożeniami. Oznacza to, że producenci lub dystrybutorzy takich urządzeń będą musieli w odpowiedni sposób projektować swoje produkty czy wdrożyć procedury reagowania na wypadek wykrycia podatności przez cały cykl życia takich wyrobów.

SI i nowe technologie

W pierwszym kwartale 2024 r. możemy spodziewać się uchwalenia rozporządzenia Parlamentu Europejskiego i Rady ustanawiające zharmonizowane przepisy dotyczące sztucznej inteligencji (Akt w sprawie sztucznej inteligencji). Rozwiązania te maja być stosowane u dostawców wprowadzających do obrotu lub oddających do użytku systemy sztucznej inteligencji w UE, niezależnie od tego, czy dostawcy ci mają siedzibę w Unii czy w państwie trzecim.
Rozporządzenie będzie miało też wpływ na użytkowników systemów sztucznej inteligencji, którzy znajdują się w Unii.
Podstawowym celem przepisów Aktu o sztucznej inteligencji jest ograniczenie ryzyk związanych ze stosowaniem systemów sztucznej inteligencji. Przyjęte zostało podejście do SI oparte na ocenie ryzyka. Założono bowiem, że systemy niosące za sobą wyższy poziom ryzyka powinny podlegać szerszym i bardziej restrykcyjnym wymogom, niż systemy których wykorzystywanie wiąże się jedynie z ograniczonym lub niskim ryzykiem.

7 WSPÓŁPRACA Z UODO

W projekcie Aktu wprowadzono listę zakazanych systemów SI (np. systemy tworzące lub rozszerzające bazy danych rozpoznawania twarzy poprzez nieukierunkowane pobieranie obrazów twarzy z Internetu lub nagrań z kamer przemysłowych), czy też nałożono dodatkowe obowiązki na dostawców i systemów generatywnej inteligencji. Ich działalność ma być przejrzysta dla użytkowników, a wiec mają np. informować, że treści zostały wygenerowane przez SI, a także informacje jak działa dany system sztucznej inteligencji.
Na rozwiązania związane z SI ma mieć też wpływ projektowana dyrektywa UE w sprawie dostosowania przepisów dotyczących pozaumownej odpowiedzialności cywilnej do sztucznej inteligencji (tzw. dyrektywa w sprawie odpowiedzialności za sztuczną inteligencję). Trudno jednak ocenić czy proponowane rozwiązania zostaną uchwalone w tym roku.
Dyrektywa ta ma zastosowanie do pozaumownych roszczeń cywilnoprawnych z tytułu szkód wyrządzonych przez system sztucznej inteligencji, w przypadku gdy są one wnoszone w ramach systemów odpowiedzialności na zasadzie winy. W związku z tym wprowadzona ona szczególne regulacje dotyczące ujawniania dowodów dotyczących systemów sztucznej inteligencji (SI) wysokiego ryzyka, aby umożliwić powodowi uzasadnienie pozaumownego cywilnoprawnego roszczenia odszkodowawczego opartego na zasadzie winy.

Regulacje dotyczące internetu

Dostawcy usług cyfrowych od 17 lutego 2024 r. będą musieli spełnić wymogi Aktu o usługach cyfrowych. Wobec największych podmiotów tj. bardzo dużych platform internetowych i wyszukiwarek internetowych, akt ten ma już zastosowanie od 25 sierpnia 2023 r., a teraz spełnienie owych wymagań czeka mniejszych graczy.
Zgodnie z tymi regulacjami dostawcy usług pośrednich, a więc dostawcy usług hostingu (np. centra danych), serwisy społecznościowe, internetowe platformy handlowe, internetowe sklepy z aplikacjami, platformy wymiany treści przez użytkowników oraz serwisy online umożliwiające np. zakup usług turystycznych będą podlegać pod nowe zasady moderowania treści w Internecie, w tym w zakresie zwalczania treści nielegalnych i szkodliwych. A użytkownicy, kwestionujący podejmowane w stosunku do nich decyzje przez pośredników internetowych.
W pierwszym półroczu 2024 r. planowane jest uchwalenie projektu Rozporządzenia UE w sprawie przejrzystości i targetowania reklamy politycznej. Projektowane rozwiązania zakładają wprowadzone szeregu obowiązków dotyczących transparentności reklamy politycznej oraz zgłaszania przypadków reklamy niezgodnej z prawem. Projekt ten przewiduje ustanowienie zakazu targetowania reklamy politycznej w oparciu o dane „ujawniające poglądy polityczne”, o ile adresat reklamy nie wyrazi na to zgody.

7 WSPÓŁPRACA Z UODO

W pierwszym kwartale 2024 roku ma zostać uchwalona ustawa – Prawo komunikacji elektronicznej, która wdraża do polskiego systemu prawnego przepisy dyrektywy nr 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. Nowa ustawa uchyli obecnie obwiązujące Prawo telekomunikacyjne i rozszerzy zarazem zakres podmiotowy obecnych regulacji. Obejmie ona nie tylko tradycyjnych przedsiębiorców telekomunikacyjnych, ale również podmioty świadczące usługi poczty elektronicznej, komunikatorów internetowych czy czaty internetowe.

Zarządzanie danymi

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 2022/868 w sprawie europejskiego zarządzania danymi (Akt w sprawie zarządzania danymi) obowiązuje na terytorium całej Unii Europejskiej od 24 września 2023 r. Regulacje te miały być uzupełnione tzw. ustawą wprowadzającą, między innymi określającą kompetencje organu odpowiedzialnego za wykonanie przepisów rozporządzenia. Polska uchybiła temu wymogowi, w szczególności w poprzedniej kadencji Sejmu nie został uchwalony projekty ustawy w sprawie zarządzania danymi.

Akt w sprawie zarzadzania danymi poszerza możliwości ponownego wykorzystywania informacji sektora publicznego przez podmioty prywatne. Określa też zasady świadczenia usług pośrednictwa danych pomiędzy podmiotami prywatnymi. Ponadto tworzy ramy prawne promujące nowy model biznesowy wymiany danych, jakim są regulowane usługi pośrednictwa danych pomiędzy podmiotami prywatnymi.

Kolejny akt prawny dotyczący danych, a mianowicie Rozporządzenie UE w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania (tzw. Akt w sprawie danych) wejdzie w życie 11 stycznia 2024 r., a jego przepisy zaczną obowiązywać po upływie 20 miesięcy. Zakres tej regulacji obejmie m.in. producentów produktów i usług, które wytwarzają dane, posiadaczy danych, odbiorców danych w UE, czy podmioty publiczne, które zwracają się o udostępnienie danych.

Akt w sprawie danych ustanawia zharmonizowane przepisy dotyczące udostępniania danych generowanych w wyniku korzystania z produktu lub powiązanej usługi, użytkownikom tego produktu lub tej usługi. Rozporządzenie zwiększa też dostęp do danych, m.in. poprzez przyznanie użytkownikom prawa do żądania wydania danych wygenerowanych przez produkty lub powiązane z nimi usługi z których korzystają. Akt w sprawie danych zawiera również przepisy dotyczące zapewnienia łatwości przenoszenia danych w celu m.in. ułatwienia zmiany dostawców usług przetwarzania danych w chmurze.

URZĄD OCHRONY DANYCH OSOBOWYCH

www.uodo.gov.pl