Obserwuj nas na:

Nr 9/2021 (30)
Wrzesień 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

AKTUALNE WYZWANIA W PRACY INSPEKTORÓW OCHRONY DANYCH

Warto wspierać inspektorów ochrony danych w wykonywaniu ich funkcji i chronić ich niezależność. Kluczowe w tej pracy jest właściwe rozumienie roli inspektora i zapewnienie mu właściwych warunków funkcjonowania i gwarancji niezależności. Czy w przyszłości czeka nas jednak większa specjalizacja wśród inspektorów?

O kompetencjach i wyzwaniach stojących przed inspektorami ochrony danych wypowiedzieli się Monika Młotkiewicz, naczelnik Wydziału Współpracy z Inspektorami Ochrony Danych w UODO, oraz prof. Grzegorz Sibiga z Instytutu Nauk Prawnych Polskiej Akademii Nauk w rozmowie z Adamem Sanockim, rzecznikiem Prasowym UODO.

Adam Sanocki: Jakie są obecnie najistotniejsze kompetencje IOD?

Monika Młotkiewicz
Naczelnik Wydziału Współpracy z Inspektorami Ochrony Danych w UODO

Monika Młotkiewicz: Kompetencje inspektorów ochrony danych – odkąd zaczęliśmy stosować RODO – są niezmienne i wynikają one wprost z treści tej regulacji – są to fachowa wiedza i fachowe umiejętności, czyli znajomość prawa i praktyk w dziedzinie ochrony danych osobowych i umiejętność ich zastosowania w praktyce przy realizacji zadań inspektorów ochrony danych.

Przy czym ostatni czas był pod tym względem dość trudny. Pandemia przeniosła nas niemal z dnia na dzień prawie całkowicie w świat cyfrowy, narzuciła nam zupełnie nowe warunki funkcjonowania, za którymi zupełnie nie nadążały procesy prawne. Znaleźliśmy się tak naprawdę w sytuacji deficytu norm prawnych oraz braku jednoznacznych i niebudzących wątpliwości podstaw przetwarzania danych, w tym danych wrażliwych.

W takiej sytuacji bardzo trudno być doradcą, wskazywać w swoich organizacjach właściwe rozwiązania. I tutaj przewagę mieli ci inspektorzy, którzy mieli duże doświadczenie w swojej pracy, są biegli w wykonywaniu swoich zadań. Ci, którzy potrafili szybko reagować na tą nową sytuację, którzy mieli wiedzę w zakresie elektronicznych środków przekazu, funkcjonowania dużych platform internetowych, pracy zdalnej czy zagrożeń w cyberprzestrzeni. Dużą sztuką było szybkie dostosowanie obowiązujących procedur do nowej sytuacji i skuteczne zaznajomienie z nimi pracowników.

Grzegorz Sibiga: Inspektor ochrony danych potrzebuje różnego rodzaju kompetencji. Nie wystarczą tylko i wyłącznie kompetencje prawnicze, które były wymagane na początkowym etapie wdrożenia RODO i związane były przede wszystkim z nowym stanem prawnym. Natomiast wraz z upływem czasu okazuje się, że są potrzebne również innego rodzaju kompetencje – związane nie tylko z zarządzaniem bezpieczeństwem informacji, ale również kompetencje miękkie związane ze znajomością kultury organizacyjnej danej jednostki, jej specyfiki, związane ze znajomością zadań publicznych lub też biznesów, w ramach których dochodzi do przetwarzania danych osobowych.

Adam Sanocki: Jakie są najważniejsze aspekty związane z pracą IOD w administracji publicznej, a jakie w sektorze prywatnym?

prof. Grzegorz Sibiga
Instytut Nauk Prawnych
Polskiej Akademii Nauk

Grzegorz Sibiga: Faktycznie zauważalna jest różnica pomiędzy wykonywaniem funkcji IOD w sektorze publicznym i w szeroko rozumianym sektorze prywatnym. W sektorze publicznym wymaga się znajomości całej gamy różnego typu uregulowań dotyczących prawa administracyjnego oraz procedur, w jakich działa administracja publiczna. Natomiast gdy chodzi o działalność gospodarczą, występują tutaj pewne aspekty, które w sposób naturalny nie istnieją w administracji publicznej, takie jak choćby kwestia marketingu usług i produktów, czy też kwestia przekazywania danych wewnątrz grupy kapitałowej. Kwestie te są związane ze specyfiką działalności gospodarczej. Trzeba jednak podkreślić, że wspólnym mianownikiem dla pracy inspektora ochrony danych zarówno w sferze publicznej, jak i w sektorze prywatnym są przede wszystkim te przepisy ogólnego rozporządzenia o ochronie danych osobowych, a także ustawy o ochronie danych osobowych, które w takim samym stopniu dotyczą zarówno sektora publicznego, jak i sektora prywatnego.

Monika Młotkiewicz: Kwalifikacje inspektora ochrony danych są ściśle związane ze specyfiką administratora, z branżą, w której on funkcjonuje, niezależnie od tego, czy mówimy o sektorze publicznym, czy prywatnym. Praca inspektora ochrony danych wymaga bardzo dobrej orientacji w przepisach prawa, ale też w całym dorobku, który wiąże się z tymi przepisami. Chodzi tutaj o orzecznictwo sądowe, piśmiennictwo, rozstrzygnięcia organów nadzorczych. Czasem jest to bardzo rozległa specjalizacja branżowa, bo rzeczywiście w niektórych dziedzinach przepisy prawa, rekomendacje, wytyczne są bardzo szczegółowe. Mam na myśli takie dziedziny, jak działalność lecznicza, edukacja, sektor pracy, czyli takie dziedziny, które dotyczą zarówno podmiotów prywatnych, jak i publicznych. Takie szczegółowe, rozbudowane regulacje dotyczą również innych sektorów – sektora bankowego, ubezpieczeniowego, telekomunikacyjnego, farmaceutycznego, pomocy społecznej czy też sektora sądownictwa. Oczywiście sektor publiczny, posiada, co do zasady, np. odmienne podstawy przetwarzania danych, inne niż w sektorze prywatnym, czy też pewne specyficzne problemy specjalne wspólne zagadnienia, jak chociażby dostęp do informacji publicznej czy tworzenie narodowego zasobu archiwalnego. Niemniej jednak obserwujemy, że wiedza i doświadczenie sektorowe jest coraz bardziej cenione.

Adam Sanocki: Czy zatem warto rozdzielać te kompetencje na sektor publiczny i prywatny, czy może istotne są inne czynniki?

Grzegorz Sibiga: Bazując na swoim doświadczeniu uzyskanym z pracy naukowej, pracy kancelaryjnej jak i kierownika studiów podyplomowych dla inspektorów ochrony danych, przyznaję, że potrzebne są pewne specyficzne kompetencje dla każdego z rodzajów tych działalności. W administracji publicznej jest to przede wszystkim potrzeba znajomości szczególnych przepisów, czy też uregulowań dotyczących administracji publicznej, takich jak choćby prawo zamówień publicznych, znajomości procedur, które występują w administracji publicznej czy też znajomości archiwizacji, która jest bardzo specyficzna w administracji publicznej i różni się od tego, co występuje w przedsiębiorstwach. Natomiast gdy chodzi o sektor prywatny, kompetencje powinny podążać za biznesem, za samym przedmiotem działalności gospodarczej. W obu tych rodzajach działalności wydaje się, że potrzebne są też w coraz większym stopniu kompetencje miękkie, związane z potrzebą niezależności inspektora, komunikacji inspektora z pozostałymi osobami w jednostce organizacyjnej, jak również unikania konfliktów interesu. Miękkie kompetencje, które na początku obowiązywania RODO były mniej zauważalne, teraz w praktyce mają coraz większe znaczenie.

Monika Młotkiewicz: Na pewno warto wspierać inspektorów w wykonywaniu ich funkcji i chronić ich niezależność. Kluczowe jest właściwe rozumienie roli inspektora i zapewnienie mu właściwych warunków funkcjonowania i gwarancji niezależności. Niestety mimo że RODO stosujemy już od ponad 3 lat nie wszędzie jest to respektowane. Do UODO zgłaszane są problemy związane chociażby z powołaniem inspektora ochrony danych. Nie zawsze rozumie się, że musi to być fachowiec, że wiedza i bezpieczeństwo danych kosztuje, że nie można w tę rolę ubrać swojego pracownika zupełnie nieprzygotowanego do tej funkcji albo przeciążonego innymi obowiązkami albo też nowej wykwalifikowanej osoby, ale za najniższe możliwe wynagrodzenie.

Nie tylko polski organ do spraw ochrony danych osobowych, ale i inne organy nadzorcze w Unii Europejskiej pokazują w wydawanych decyzjach, że wysokie standardy, które są przyjęte w odniesieniu

do inspektora i jego niezależności muszą być respektowane. Organy reagują również wtedy, kiedy zadania inspektora nie są wykonywane w sposób prawidłowy, a odpowiedzialność za to ponosi administrator. Przykładem takiej reakcji była decyzja Prezesa Urzędu Ochrony Danych Osobowych w sprawie Szkoły Głównej Gospodarstwa Wiejskiego, gdzie naruszenie i kara dotyczyły m.in. niewłączania inspektora w sprawy ochrony danych osobowych i nieprawidłowe wykonywanie przez niego zadań. Innym przykładem decyzji jest nałożenie upomnienia na administratora, który przerzucał na inspektora swoje obowiązki.

Adam Sanocki: Jakie wyzwania w związku z tym czekają z jednej strony samych IOD, a jakie ich pracodawców?

Grzegorz Sibiga: Bardzo ważny jest wybór właściwego IOD przez administratora lub podmiot przetwarzający, bo to do nich należy obowiązek wybrania inspektora, który posiada właściwe kompetencje. Administrator czy podmiot przetwarzający powinni zwracać uwagę na doświadczenie i wiedzę inspektora ochrony danych osobowych w tym sektorze, w którym działają. Zatem, odnosząc się do podziału na sektor publiczny i prywatny, administrator z sektora publicznego, organ administracji publicznej, powinien poszukiwać przede wszystkim inspektorów ochrony danych osobowych, którzy mają doświadczenie i znają specyfikę administracji publicznej, bądź też są wyedukowani właśnie w tym kierunku. Natomiast pracodawcy w sektorze prywatnym, w przedsiębiorstwach, w naturalny sposób poszukują inspektorów, którzy mają doświadczenie w sektorze prywatnym, w biznesie, w działalności gospodarczej, a nawet w ściśle określonym rodzaju działalności gospodarczej, przykładowo w sektorze zdrowotnym, gdzie występuje bardzo duża specyfika. Z kolei ze strony inspektorów ochrony danych osobowych wymaga to jednak pewnej specjalizacji. Nie mówię, że jest to specjalizacja raz na zawsze w określonym sektorze, ale chcąc prawidłowo wykonywać swoją funkcję w administracji publicznej trzeba znać i rozumieć jej specyfikę, znać szczególne uregulowania prawne dotyczące sektora publicznego i tak samo w sektorze prywatnym. Bez tego, jak się wydaje niemożliwe jest już prawidłowe wykonywanie tej funkcji.

Monika Młotkiewicz: W pracy inspektora niezwykle ważna jest wiedza i wsparcie ze strony administratora oraz ze strony wszystkich osób, które przetwarzają dane w określonej organizacji. Takie osoby muszą współdziałać z inspektorem. Wiedza inspektora musi być ciągle aktualizowana. Co oznacza nie tylko stały wysiłek po stronie samych inspektorów w zakresie poszerzania tej wiedzy, korzystania z wiarygodnych źródeł informacji na temat prawa i praktyk, ale też stałe pozycje na ten cel w budżetach organizacji. W wiedzę inspektora trzeba systematycznie inwestować i taki obowiązek jest wprost zapisany w przepisach rozporządzenia ogólnego o ochronie danych osobowych.

Praca inspektora polega na tym, żeby informować o obowiązkach, wskazywać zauważone nieprawidłowości, zagrożenia związane z przetwarzaniem danych osobowych, ale ważne jest, aby za tymi rekomendacjami szły od strony pracodawców i zleceniodawców inspektorów ochrony danych konkretne decyzje, zarządzenia, przypisywanie odpowiednich zadań odpowiednim osobom w odpowiednich terminach i potem te decyzje muszą być egzekwowane. Tylko wtedy praca inspektora ma sens, przyczynia się do przestrzegania przepisów prawa i do rozwijania skutecznego systemu ochrony danych osobowych w takiej organizacji.

Zapis całej rozmowy z Moniką Młotkiewicz, naczelnik Wydziału Współpracy z Inspektorami Ochrony Danych w UODO, oraz prof. Grzegorzem Sibigą z Instytutu Nauk Prawnych Polskiej Akademii Nauk znajduje się w materiale wideo dostępnym pod linkiem:
https://video.uodo.gov.pl/video/rola-iod.mp4

WERYFIKOWANIE PRZEZ PRACODAWCĘ UPRAWNIEŃ PRACOWNIKA DO KIEROWANIA POJAZDAMI

Gdy do obowiązków pracownika należy prowadzenie służbowego pojazdu, celowe może być okresowe weryfikowanie przez pracodawcę jego uprawnień w tym zakresie. Pracodawca powinien jednak określić częstotliwość takiej kontroli, co powinno znaleźć swoje odzwierciedlenie w obowiązujących u niego regulaminach.

Podmiot zatrudniający pracowników, którzy na potrzeby wykonywania swoich obowiązków korzystają ze służbowych pojazdów, zwrócił się do Prezesa UODO o rozstrzygnięcie wątpliwości, czy obowiązujące przepisy uprawniają go do bieżącej weryfikacji uprawnień pracowników do kierowania pojazdami.

W odpowiedzi organ nadzorczy wskazał, że przepisy Kodeksu pracy dają pracodawcy podstawę do dokonywania takiej weryfikacji. Może on bowiem żądać od pracownika podania danych wskazanych zarówno w art. 22^1 § 1 Kodeksu pracy, a więc m.in. wykształcenia i kwalifikacji zawodowych, jak i w art. 22^1 § 3 Kodeksu pracy.

Artykuł 22^1 § 3 Kodeksu pracy wymienia bowiem informacje, jakich pracodawca żąda od pracownika dodatkowo w stosunku do tych wymienionych w art. 22^1 § 1 Kodeksu pracy. Oznacza to, że od osoby ubiegającej się o zatrudnienie nie można wymagać podania danych wymienionych w art. 22^1 § 3 Kodeksu pracy, a nie odwrotnie.

Wąskie rozumienie przepisu art. 22^1 § 3 Kodeksu pracy, polegające na uznaniu, że od osoby już zatrudnionej pracodawca nie może wymagać podania danych innych niż wymienione w tym przepisie, prowadziłoby do sytuacji, w której np. po zmianie zakresu obowiązków, która nie wiąże się z przeprowadzeniem nowego naboru, niemożliwa byłaby weryfikacja kwalifikacji lub uprawnień pracownika niezbędnych do wykonywania tych obowiązków.

Zgodnie zaś z art. 22^1 § 5 Kodeksu pracy, udostępnienie pracodawcy informacji, o których mowa w art. 22^1 § 1 i § 3 Kodeksu pracy następuje w formie oświadczenia osoby, której dane dotyczą, jednak pracodawca może żądać ich udokumentowania w zakresie niezbędnym do ich potwierdzenia. Zatem kiedy wykonywanie obowiązków służbowych wiąże się z prowadzeniem pojazdów, celowa wydaje się weryfikacja uprawnień pracownika w tym zakresie.

Pracodawca powinien jednak dokonać analizy odnoszącej się do częstotliwości dokonywania takiej weryfikacji, co powinno znaleźć swoje odzwierciedlenie w obowiązujących u niego regulaminach. Nie można bowiem zapomnieć, że bez względu na treść art. 22^1 Kodeksu pracy, administrator zobowiązany jest do przestrzegania zasad wymienionych w art. 5 ust. 1 RODO, w tym ograniczenia celu i minimalizacji danych.

DOPEŁNIANIE OBOWIĄZKU INFORMACYJNEGO PRZY WSZCZĘCIU POSTĘPOWANIA W DRUGIEJ INSTANCJI

Wojewódzki Sąd Administracyjny w Warszawie podzielił opinię Prezesa UODO, że w zakresie prowadzenia postępowania administracyjnego pierwszej i drugiej instancji, komendant wojewódzki oraz Komendant Główny Policji są odrębnymi administratorami, zobowiązanymi do dopełnienia obowiązku informacyjnego.

Przepisy RODO wprowadziły istotne zmiany dotyczące dopełniania tzw. obowiązku informacyjnego, w tym rozszerzyły jego zakres. Zmiana ta miała na celu zapewnienie osobom, których dane dotyczą, bardziej szczegółowej wiedzy o tym, co będzie się działo z ich danymi osobowymi.

O tym, że obowiązek informacyjny nie zawsze bywa realizowany prawidłowo może świadczyć sprawa zainicjowana skargą osoby będącej stroną postępowania administracyjnego prowadzonego przez policję.

O ile w toku postępowania pierwszej instancji komendant wojewódzki policji dopełnił obowiązku informacyjnego, o którym mowa w art. 13 RODO, o tyle Komendant Główny Policji, wszczynając postępowanie drugiej instancji, tego obowiązku nie zrealizował. Dlatego Prezes UODO w wydanej w tej sprawie decyzji (ZWOS.440.5927.2019) nakazał jego dopełnienie.

W uzasadnieniu organ nadzoru podniósł, że stosownie do art. 61 § 5 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (k.p.a.), „organ administracji publicznej przekazuje informacje, o których mowa w art. 13 ust. 1 i 2 RODO, przy pierwszej czynności skierowanej do strony, chyba że strona posiada te informacje, a ich zakres lub treść nie uległy zmianie, zaś zgodnie z art. 140 k.p.a., w sprawach nieuregulowanych w art. 136–139 k.p.a. w postępowaniu przed organami odwoławczymi mają odpowiednie zastosowanie przepisy o postępowaniu przed organami pierwszej instancji".

Organ nadzoru wskazał, że w zakresie prowadzenia postępowania administracyjnego pierwszej i drugiej instancji, komendant wojewódzki oraz Komendant Główny Policji są odrębnymi administratorami, zatem obaj byli zobowiązani do wypełnienia wobec skarżącego obowiązku informacyjnego w związku z – odpowiednio – wszczęciem postępowania pierwszej i drugiej instancji.

Komendant Główny Policji nie zgodził się jednak z tym stanowiskiem organu nadzoru i wniósł do WSA w Warszawie skargę na decyzję Prezesa UODO.

Po rozpoznaniu sprawy WSA w wydanym wyroku (sygn. akt II SA/Wa 1231/20) podzielił stanowisko Prezesa UODO, uznając, że komendant wojewódzki oraz Komendant Główny Policji są odrębnymi administratorami, zatem wszczynając odpowiednio postępowanie pierwszej i prowadzenie postępowania drugiej instancji, zobowiązani byli do wypełnienia obowiązku informacyjnego, o którym mowa w art. 13 ust. 1 i 2 RODO.

USŁUGI BANKOWE DLA PUP BEZ UMOWY POWIERZENIA

Powiatowy urząd pracy (PUP), przekazując bankowi listy bezrobotnych, którym mają być wypłacane świadczenia, nie powinien zawierać umowy powierzenia przetwarzania danych osobowych.

W takiej sytuacji mamy bowiem do czynienia z odrębnymi administratorami, których łączy jedynie umowa o świadczenie usług bankowych.

PUP przetwarza dane osób bezrobotnych w związku z realizacją własnych zadań określonych w przepisach prawa. Natomiast w związku z zawartą z bankiem umową o świadczenie usług bankowych udostępnia bankowi dane bezrobotnych w celu realizacji wypłaty należnych im świadczeń.

Z kolei bank w momencie otrzymania od PUP danych osób bezrobotnych, na rzecz których ma być zrealizowana określona w umowie usługa bankowa, staje się administratorem tych danych, który realizuje swoje zadania, samodzielnie określając cele i sposoby przetwarzania danych wynikające z przepisów ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe.

Z analogicznym podejściem mamy do czynienia w przypadku banku i pracodawcy, co zostało wskazane w tekście Czy pracodawca powinien zawierać umowy powierzenia z takimi podmiotami, jak ZUS czy bank? zamieszczonym na stronie internetowej UODO w zakładce IOD/Zadania IOD. Pracodawcę i bank w ramach realizowanych czynności bankowych wskazuje się jako przykład odrębnych administratorów również w Wytycznych EROD nr 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO (str. 15).

POTWIERDZANIE ODBYCIA ZABIEGU FIZJOTERAPII DOMOWEJ

W obecnym stanie prawnym dla potwierdzenia odbycia zabiegu fizjoterapii domowej nie można pobierać odcisku palca pacjenta.

Obowiązujące obecnie zarządzenie nr 195/2020/DSOZ Prezesa Narodowego Funduszu Zdrowia z 11 grudnia 2020 r. w sprawie określenia warunków zawierania i realizacji umów w rodzajach rehabilitacja lecznicza oraz programy zdrowotne w zakresie świadczeń – leczenie dzieci i dorosłych ze śpiączką stanowi (§ 12 ust. 14), że w ramach zakresu świadczeń – fizjoterapia ambulatoryjna oraz fizjoterapia domowa, świadczeniobiorca albo przedstawiciel ustawowy, opiekun prawny lub faktyczny pacjenta potwierdza każdego dnia realizację zabiegów fizjoterapeutycznych przez złożenie podpisu w dokumentacji medycznej.

Jeśli jednak pacjent nie może bądź w danym momencie nie potrafi nakreślić podpisu, ustawodawca w art. 17 ust. 2 ustawy z dnia 6 października 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta przewidział możliwość zastępstwa w postaci przedstawiciela ustawowego lub opiekuna faktycznego. Prezes NFZ w powołanym zarządzeniu umożliwił złożenie podpisu zastępczego również przez opiekuna prawnego. Dodatkowo art. 17 ust. 4 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta stanowi, że zgoda oraz sprzeciw, o których mowa w ust. 1–3 tej ustawy, mogą być wyrażone ustnie albo przez takie zachowanie się

osób wymienionych w tych przepisach, które w sposób niebudzący wątpliwości wskazuje na wolę poddania się czynnościom proponowanym przez osobę wykonującą zawód medyczny albo brak takiej woli. Możliwe jest zatem wyrażenie tzw. zgody dorozumianej.

Zgodnie z art. 5 ust. 1 lit. c) RODO, dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Powołane zarządzenie prezesa NFZ z 11 grudnia 2020 r. przewiduje konieczność potwierdzania każdego dnia realizacji zabiegów fizjoterapeutycznych przez złożenie podpisu w dokumentacji medycznej. Podpis ten może być złożony przez świadczeniobiorcę, jego przedstawiciela ustawowego, opiekuna prawnego lub faktycznego. Oznacza to, że administrator jest w posiadaniu wielu rozwiązań, które może zastosować w celu dopełnienia swoich obowiązków w zakresie wykonywania świadczeń zdrowotnych, lecz nie wynika z nich możliwość zbierania danych pacjentów w postaci odcisku palca.

Podkreślić należy, że ponieważ odcisk palca składany w sytuacji świadczącej jednocześnie o stanie zdrowia należy uznać za dane osobowe szczególnych kategorii, to aby mógł być on przetwarzany dla potwierdzenia odbycia zabiegu fizjoterapii domowej, musiałyby zostać stworzone szczególne gwarancje ustawowe, co wynika z art. 9 ust. 3 i 4 RODO.

Wcześniej pozyskiwanie takich danych legalizowało zarządzenie nr 13/2019/DSOZ Prezesa Narodowego Funduszu Zdrowia z 6 lutego 2019 r. w sprawie określenia warunków zawierania i realizacji umów w rodzajach rehabilitacja lecznicza oraz programy zdrowotne w zakresie świadczeń – leczenie dzieci i dorosłych ze śpiączką, ale zostało ono uchylone z dniem 1 stycznia 2020 r.

KLASYFIKACJA ZAWODÓW BEZ ABI

Z rozporządzenia w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy zniknie administrator bezpieczeństwa informacji (ABI).

To efekt uwag Prezesa UODO zgłoszonych w toku prac legislacyjnych nad projektem zmiany powołanego rozporządzenia. Organ nadzorczy, opiniując je, wskazał, że od 25 maja 2018 r. osobami zapewniającymi administratorom fachowe wsparcie w zakresie monitorowania przestrzegania przepisów o ochronie danych osobowych nie są już administratorzy bezpieczeństwa informacji (ABI), lecz inspektorzy ochrony danych (IOD). Wprost wynika to zarówno z przepisów RODO, jak i ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Prezes UODO podniósł zatem, że użycie w załączniku do analizowanego projektu rozporządzenia zatytułowanym „Klasyfikacja zawodów i specjalności na potrzeby rynku pracy" w sekcji „Struktura klasyfikacji zawodów i specjalności", w grupie 242 „Specjaliści do spraw administracji i zarządzania", w punkcie 242111 specjalizacji „Administrator bezpieczeństwa informacji (Inspektor ochrony danych)" jest nieuzasadnione. W odpowiedzi projektodawca zadeklarował skorygowanie projektu i wprowadzenie stosownej zmiany nazwy zawodu.

Holandia: TikTok ukarany za naruszenie prywatności dzieci

Holenderski organ ochrony danych nałożył na TikTok karę pieniężną w wysokości 750 tys. euro za naruszenie prywatności małych dzieci. Informacje dostarczane przez ten serwis społecznościowy podczas instalacji i korzystania z aplikacji były w języku angielskim, a zatem nie były łatwe do zrozumienia.

Nie oferując oświadczenia o ochronie prywatności w języku niderlandzkim, TikTok nie przedstawił odpowiedniego wyjaśnienia, w jaki sposób aplikacja zbiera, przetwarza i wykorzystuje dane osobowe. Jest to naruszenie przepisów dotyczących prywatności, które opierają się na zasadzie, że ludzie muszą zawsze mieć jasny obraz tego, co dzieje się z ich danymi osobowymi.

W zeszłym roku organ ochrony danych wszczął postępowanie w sprawie aplikacji z powodu obaw dotyczących prywatności dzieci, które zgodnie z prawem są traktowane jako kategoria osób szczególnie zagrożonych.

Dzieci są mniej świadome konsekwencji swoich działań, w tym skutków udostępniania danych osobowych w mediach społecznościowych. Z tego powodu dzieci otrzymują dodatkową ochronę na mocy przepisów o ochronie danych.

Przeniesienie postępowania w sprawie TikTok
Warto zauważyć, że w sprawie ostatecznie wypowie się irlandzki organ nadzorczy. Wynika to z faktu, że jeżeli przedsiębiorstwo nie ma siedziby w Europie, nadzór nad jej działalnością może sprawować każde państwo członkowskie UE. W przypadku przedsiębiorstw, które mają swoje siedziby w Europie, odpowiedzialność ta spadałaby głównie na kraj, w którym znajduje się jego siedziba. Początkowo TikTok nie miał swojej siedziby w Europie, a ponieważ sprawa dotyczyła holenderskich użytkowników serwisu, mógł się nią zająć się organ nadzorczy z Holandii. Jednak w trakcie holenderskiego postępowania TikTok rozpoczął działalność w Irlandii, dlatego zdecydowano o przekazaniu wyników postępowania irlandzkiej Komisji Ochrony Danych. Od tego momentu organ ochrony danych był upoważniony jedynie do oceny oświadczenia o ochronie prywatności TikTok, ponieważ samo naruszenie już się skończyło. Teraz to do irlandzkiej Komisji Ochrony Danych należy zakończenie tego postępowania i wydanie ostatecznego orzeczenia w sprawie innych możliwych naruszeń prywatności.

Większa kontrola dla rodziców
Na początku października zeszłego roku organ ochrony danych przedłożył TikTok raport z ustaleń swojego postępowania. Następnie TikTok wdrożył wiele zmian, aby jego aplikacja była bezpieczniejsza dla dzieci poniżej 16. roku życia.

Pozostałą kwestią jest to, że dzieci mogą nadal udawać, że są starsze, wpisując inny wiek podczas tworzenia konta. W ten sposób narażają się na większe ryzyko.

Jednak na skutek wprowadzonych zmian rodzice mają teraz większą kontrolę nad kontem swojego dziecka. Mogą zarządzać ustawieniami prywatności swojego dziecka za pośrednictwem własnego konta i funkcji „Family Pairing” („Kontrola rodzicielska”).

„Pomimo tych zmian zachęcamy rodziców do regularnych rozmów z dziećmi o tym, co robią w Internecie. Zainteresuj się filmami, które tworzą i porozmawiaj z nimi o tym, jak oni i inni użytkownicy odpowiadają sobie na TikTok”.

TikTok wniósł sprzeciw wobec kary pieniężnej.

Aby uzyskać więcej informacji o sprawie, kliknij: https://autoriteitpersoonsgegevens.nl/nl

Źródło: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_pl

Francja: MONSANTO ukarane za niepoinformowanie klientów o użyciu ich danych

Francuski organ nadzorczy CNIL ukarał MONSANTO – karą pieniężną w wysokości 400 tys. euro – za niepoinformowanie osób, których dane zostały zapisane w pliku dla celów lobbingu.

W 2019 roku media ujawniły, że MONSANTO jest w posiadaniu pliku zawierającego dane osobowe ponad 200 polityków lub m.in. dziennikarzy, działaczy ekologicznych, naukowców lub rolników, którzy mogliby wpłynąć na debatę lub opinię publiczną w sprawie odnowienia zezwolenia na stosowanie glifosatu w Europie. Jednocześnie CNIL otrzymała siedem skarg od osób, których dotyczyły te akta.

Kontrola CNIL ujawniła, że spis ten został przeprowadzony w imieniu MONSANTO przez kilka firm specjalizujących się w public relations i lobbingu, w ramach dużej kampanii reprezentacji interesów.

Przedmiotowe akta zawierały w odniesieniu do każdej z tych osób takie informacje, jak: organizacja, do której należały, stanowisko, które zajmowały, ich adres zawodowy, numer telefonu służbowego, numer telefonu komórkowego, służbowy adres e-mail oraz, w niektórych przypadkach, ich konto na Twitterze. Dodatkowo, każda osoba otrzymała ocenę od 1 do 5, która wskazywała na jej wpływ, wiarygodność i poparcie dla MONSANTO w różnych kwestiach, takich jak pestycydy czy organizmy genetycznie modyfikowane.

Zdaniem CNIL, spółka naruszyła przepisy, nie informując zainteresowanych osób o zapisaniu ich danych w tym pliku. Ponadto CNIL skrytykowała fakt, że przedsiębiorstwo nie wprowadziło gwarancji umownych, które w normalnych warunkach powinny regulować stosunki z podwykonawcą. Podkreśliła ona, że obowiązek informowania osób fizycznych jest głównym środkiem w ramach RODO, ponieważ umożliwia im wykonywanie ich praw, w szczególności prawa do sprzeciwu. Wreszcie Komisja zauważyła, że naruszenie zostało naprawione dopiero kilka lat po wdrożeniu przetwarzania, po tym jak media ujawniłyY jego istnienie.

Tworzenie plików kontaktowych przez przedstawicieli grup interesu do celów lobbingu nie jest samo w sobie nielegalne. Z drugiej strony, tylko osoby, co do których można w uzasadniony sposób oczekiwać, że ze względu na swoją reputację lub działalność będą przedmiotem kontaktów ze strony sektora, mogą zostać włączone do tej dokumentacji.

Chociaż nie jest konieczne uzyskanie zgody tych osób, dane w pliku muszą być gromadzone zgodnie z prawem, a osoby te muszą zostać poinformowane o istnieniu pliku, tak aby mogły skorzystać ze swoich praw, w tym prawa do sprzeciwu.

CNIL zauważyła, że osoby, których dane osobowe zostały zebrane, nie zostały poinformowane o istnieniu spornego pliku aż do 2019 roku i zostały poinformowane dopiero po ujawnieniu jego istnienia przez media. Jednakże żaden z wyjątków od obowiązku informowania osób fizycznych przewidzianych w RODO nie miał zastosowania w tym przypadku. Osoby, których dane dotyczą, powinny zatem zostać poinformowane o operacji przetwarzania. W tej kwestii CNIL zauważyła w szczególności, że MONSANTO posiadała informacje kontatowe (adres, numer telefonu lub adres e-mail) prawie wszystkich osób, które mogła z łatwością wykorzystać.

CNIL przypomniała również, że niepoinformowanie osób, których dane dotyczą, o istnieniu operacji przetwarzania nieuchronnie utrudnia korzystanie z praw przysługujących im na mocy RODO. Taka informacja jest podstawowym prawem, które warunkuje korzystanie z innych praw (dostępu, sprzeciwu, usunięcia itp.) przysługujących osobom fizycznym: w tym przypadku osoby te nie mogły z nich korzystać przez kilka lat.

Jako administrator danych, MONSANTO było zobowiązane do zapewnienia ram prawnych dla przetwarzania dokonywanego w jego imieniu przez podmiot przetwarzający, w szczególności w celu zapewnienia gwarancji dotyczących bezpieczeństwa danych. CNIL zauważyła jednak, że żaden z aktów zawartych między tymi dwoma przedsiębiorstwami nie zawierał informacji wymaganych na mocy art. 28 RODO.

Źródło: https://www.cnil.fr/fr/fichier-de-lobbying-sanction-de-400-000-euros-lencontre-de-la-societe-monsanto

RADA EUROPY

Urugwaj ratyfikował Konwencję 108+

Urugwaj dołączył do grona państw, które ratyfikowało zmodernizowaną Konwencję 108 (Konwencja 108+), tj. Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (CETS 223). Uroczystość przekazania dokumentu ratyfikującego odbyła się 5 sierpnia 2021 r. we Francji.

Urugwaj jest stroną konwencji nr 108 od 1 sierpnia 2013 r. Ta ratyfikacja, wraz z ratyfikacją Mauritiusa oraz Argentyny i Tunezji, pokazują zainteresowanie Konwencją 108+ poza granicami Europy oraz rolę, jaką ma ona do odegrania na całym świecie, aby chronić dane osobowe i wspierać główne wartości, które niesie.

Wejście w życie Konwencji 108+ ma kluczowe znaczenie w erze cyfrowej. Żeby jednak ten przełomowy dokument mógł w pełni odgrywać swoją rolę na arenie międzynarodowej, konieczne będzie ratyfikowanie go przez kolejne państw w tym roku i 2022 roku.

Źródło: nieoficjalne tłumaczenie ze strony https://www.coe.int/en/web/data-protection/-/uruguay-ratifies-convention-108-

EDUKACJA

Trwa nabór do XII edycji programu edukacyjnego „Twoje dane – Twoja sprawa"

Zapraszamy szkoły i placówki oświatowe do uczestnictwa w XII edycji ogólnopolskiego programu edukacyjnego „Twoje dane – Twoja sprawa".

W roku szkolnym 2021/2022 zaplanowaliśmy w programie wiele ciekawych i praktycznych działań, dostosowanych do zróżnicowanych potrzeb przedstawicieli społeczności szkolnych – przede wszystkim dyrektorów, nauczycieli oraz uczniów. Wśród planowanych działań znalazły się m.in.:

- konferencje,
- szkolenia oraz webinaria dla nauczycieli,
- rozmaite opracowania tematyczne o ochronie danych osobowych oraz o prywatności, które nauczyciele będą mogli wykorzystać podczas zajęć lekcyjnych czy pozalekcyjnych,
- cykl porad adresowany do nauczycieli, dzieci i młodzieży oraz rodziców na temat zasad bezpiecznego przetwarzania danych osobowych w różnych sytuacjach codziennych, a także podczas korzystania przez uczniów z nowych technologii.

Ponadto program edukacyjny UODO stwarza nauczycielom i uczniom możliwość realizacji autorskich inicjatyw edukacyjnych poświęconych ochronie danych osobowych. W minionych edycjach pojawiły się także i takie inicjatywy, które realizowano we współpracy

z inspektorami ochrony danych. Dzięki temu nauczyciele i uczniowie mogli uzyskać fachowe wsparcie i rzetelną wiedzą o ochronie danych osobowych i prywatności. Dodatkowo tego rodzaju współpraca pomaga poznać specyfikę pracy inspektora, co sprzyja lepszemu rozumieniu jego roli.

Uczestnictwo w programie to także okazja dla placówek oświatowych do tworzenia sieci wsparcia i samokształcenia dla nauczycieli.

Program jest realizowany pod honorowym patronatem Ministerstwa Edukacji i Nauki oraz Rzecznika Praw Dziecka.

Więcej informacji o programie znajduje się pod linkiem: https://uodo.gov.pl/pl/21/32

Żeby zgłosić uczestnictwo do programu, dyrektor szkoły lub placówki oświatowej powinien wypełnić formularz dostępny na stronie UODO: https://uodo.gov.pl/pl/21/31

NOWE ODPOWIEDZI NA PYTANIA INSPEKTORÓW

Znajdująca się na naszej stronie internetowej zakładka „Inspektor Ochrony Danych" w sekcji „Zadania IOD" została wzbogacona o kolejne zagadnienia.

Wyjaśnienia dotyczą takich kwestii, jak:

Czy broker ubezpieczeniowy ma status administratora?

Jaka jest podstawa przetwarzania danych w przypadku monitoringu karier zawodowych studentów?

Jakie rozwiązania są wystarczające w przypadku wykazu podmiotów podpowierzających?

URZĄD OCHRONY DANYCH OSOBOWYCH