Obserwuj nas na:

Nr 2/2021 (23)
Luty 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

ADMINISTRATOR NIE MOŻE PRZERZUCAĆ SWOICH OBOWIĄZKÓW NA IOD

Rolą IOD jest wpieranie administratora w przestrzeganiu i właściwym stosowaniu przepisów o ochronie danych osobowych, a nie wyręczanie go w realizacji jego zadań. Podmiotowi, który zobowiązał IOD do nadawania pracownikom upoważnień do przetwarzania danych osobowych, Prezes UODO udzielił upomnienia.

Inspektor ochrony danych to funkcja szczególna. Znajduje to odzwierciedlenie w brzmieniu przepisów RODO, które określają zarówno status IOD (art. 38), jak i jego obowiązki (art. 39).

Prezes UODO konsekwentnie wskazuje, że do zadań inspektora ochrony danych (IOD) należy m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk danego administratora, a także nadzorowanie prawidłowego wykonywania wynikających z nich obowiązków, doradzanie i podnoszenie świadomości w tym zakresie. Dlatego IOD nie powinien być osobą, która wyręcza administratora w realizacji należących do niego zadań. Mogłoby to prowadzić do powstania konfliktu interesów, którego występowania zakazuje w odniesieniu do inspektorów art. 38 ust. 6 RODO.

Wygodnictwo czy niska świadomość?

Niestety w praktyce zdarza się, że administratorzy, zawierając z IOD umowy o pracę lub świadczenie usług, do zakresu ich zadań wpisują swoje obowiązki.

Takie sytuacje często wynikają albo z wygodnictwa, albo z błędnego postrzegania inspektora jako osoby, która jako jedyna w organizacji odpowiedzialna jest za wykonywanie obowiązków z zakresu ochrony danych osobowych.

To działanie nieprawidłowe i naraża administratorów na odpowiedzialność z tytułu niezapewnienia zgodności z RODO. Podkreślić bowiem należy, że niezależnie od przyczyn takiego postępowania, to i tak ostatecznie administratorzy ponoszą odpowiedzialność za realizację obowiązków nałożonych na nich przepisami RODO.

Upomnienie dla szpitala

Niedawno przekonał się o tym szpital, który zobowiązywał swojego IOD do nadawania pracownikom upoważnień do przetwarzania danych osobowych. Prezes UODO udzielił mu za to upomnienia.

W wydanej w tej sprawie decyzji (ZWAD.405.31.331.2019) wskazał, że: „Podstawowy zakres zadań IOD, wśród których na próżno szukać jednak tych związanych z nadawaniem pracownikom administratora upoważnień do przetwarzania danych osobowych, określony został przez unijnego ustawodawcę w art. 39 ust. 1 rozporządzenia 2016/679, niemniej jednak zgodnie z art. 38 ust. 6 ww. rozporządzenia IOD może wykonywać też inne zadania i obowiązki, o ile administrator lub podmiot przetwarzający zapewni, aby te zadania i obowiązki nie powodowały konfliktu interesów.

Należy jednak przyjąć, że z uwagi na specyfikę zadań IOD ogniskujących się na doradzaniu oraz kontrolowaniu działalności administratora pod kątem zgodności operacji przetwarzania danych osobowych z przepisami o ochronie danych osobowych, administrator nie powinien przyznawać IOD uprawnień do nadawania w jego imieniu upoważnień do przetwarzania danych osobowych, pozostawiając IOD w procedurze wydawania upoważnień do przetwarzania danych osobowych sprawowanie funkcji doradczej i nadzorczej. Przyjęcie odmiennego założenia, w którym IOD byłby odpowiedzialny za przeprowadzenie tej procedury, a jednocześnie miałby monitorować jej zgodność z przepisami o ochronie danych osobowych, do czego zobowiązuje go unormowanie zawarte w art. 39 ust. 1 lit. b) rozporządzenia 2016/679, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów, czego wprost zakazuje art. 38 ust. 6 rozporządzenia 2016/679. Wyraźnego podkreślenia wymaga fakt, iż IOD, cechujący się szczególnym statusem w dziedzinie zapewniania właściwego przestrzegania przepisów o ochronie danych osobowych, musi mieć dla tego celu zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na efektywną, niezależną oraz prawidłową realizację obowiązków wynikających z przepisów prawa, co wynika z art. 38 ust. 2 i 3 rozporządzenia 2016/679. W tym kontekście za słuszny uznać należy pogląd, w którym nakładanie na IOD obowiązków prowadzących do powstania konfliktu interesów,

stawia pod znakiem zapytania nie tylko możliwość efektywnego wypełniania przez niego zadań, do realizacji których zobowiązuje go dyspozycja normy art. 39 rozporządzenia 2016/679, ale godzi w same fundamenty instytucji IOD, opartej w pierwszym rzędzie na niezależności jego funkcjonowania. (...)

IOD nie powinien być osobą, która realizuje obowiązki określone w art. 29 i art. 32 ust. 1 i 4 rozporządzenia 2016/679, tym bardziej, że adresatem norm zawartych w przytoczonych przepisach jest administrator danych lub podmiot przetwarzający. Jak już wyżej wskazano, przyjęcie odmiennego poglądu powodowałoby konflikt interesów, którego występowania zakazuje w odniesieniu do IOD art. 38 ust. 6 rozporządzenia 2016/679. Zatem uprawniony jest pogląd, zgodnie z którym dla celów zapewnienia właściwej skuteczności systemowi ochrony danych osobowych przyjętemu przez Szpital najkorzystniejszym rozwiązaniem jest to, w którym upoważnienia do przetwarzania danych osobowych wydawane są przez osobę pełniącą funkcję kierowniczą w ww. podmiocie, w tym np. kierownika działu kadr lub kierowników innych komórek organizacyjnych, a więc osoby będące w stanie w sposób najbardziej precyzyjny określać, komu oraz w jakim zakresie upoważnienie powinno zostać nadane oraz na bieżąco je aktualizować".

I choć praktyka szpitala została zmieniona, to jednak ze względu na to, że trwała ponad półtora roku, Prezes UODO uznał, że właściwym środkiem naprawczym będzie upomnienie. Jak wskazał w decyzji, „we wzmiankowanym, szerokim przedziale czasowym IOD zmuszony był do wykonywania obowiązków powodujących konflikt interesów, a zatem nie mógł należycie sprawować swojej funkcji, co w kontekście zadań IOD przewidzianych w art. 39 rozporządzenia 2016/679 sprawia, iż wagę tego naruszenia uznać należy za znaczną".

Przypadki powstawania konfliktu interesów

Na niewłaściwość takiej praktyki, jako powodującej konflikt interesów, Prezes UODO zwracał uwagę już dawniej. W zamieszczonym na stronie internetowej urzędu tekście „Czy IOD może nadawać upoważnienia?" wskazywał, że „Jeżeli administrator decyduje się na skorzystanie ze środka, jakim jest nadawanie upoważnień do przetwarzania danych (...), to może upoważnić inną osobę do nadawania upoważnień do przetwarzania danych w jego imieniu, ale osoba tą nie powinien być inspektor ochrony danych".

Z konfliktem interesów mielibyśmy do czynienia również wówczas, gdyby IOD miał w imieniu administratora sporządzać projekty umów powierzenia przetwarzania danych osobowych. Najpierw bowiem określałby, w jaki sposób ukształtowane będą relacje między administratorem i podmiotem przetwarzającym oraz prawa i zobowiązania stron umowy, a następnie, realizując swoje obowiązki, zobowiązany byłby jednocześnie ocenić prawidłowość i zgodność z przepisami podjętych w tym zakresie decyzji.

Na konieczność dokonywania oceny pod kątem występowania konfliktu interesów w związku z zawieraniem umów powierzenia przetwarzania danych Urząd wskazał m.in. udzielając odpowiedzi na jedno z pytań skierowanych do Prezesa UODO przez IOD, która została zamieszczona również na stronie internetowej UODO („Czy IOD może w imieniu administratora zawierać umowy powierzenia?"). Wskazano w niej, że: „Konflikt interesów następuje m.in. wtedy, gdy nie można pogodzić prawidłowego wykonywania zadań inspektora, przypisanych mu w art. 38 ust. 4 oraz art. 39 RODO, z realizacją innych zadań, gdyż pomiędzy zadaniami występuje sprzeczność, uniemożliwiająca odpowiednią ich realizację. W przypadku inspektora sprzeczność taka może wynikać z występowania przez niego jednocześnie w dwóch rolach lub podejmowania przez niego działań lub decyzji, które następnie muszą podlegać jego ocenie w zakresie zgodnie z art. 39 ust. 1 lit. a RODO. Może się tak stać zwłaszcza w sytuacji, gdy inspektor jest obciążany obowiązkami, które przepisy nakładają na administratora".

Ważna wskazówka

Kształtując zatem zakres obowiązków IOD warto pamiętać, że inspektor nie powinien realizować zadań, które mogą stać się następnie przedmiotem dokonywania przez niego czynności monitorowania ani podejmować decyzji w zakresie celów i środków dotyczących przetwarzania i zabezpieczania danych.

WERYFIKACJA PRZYNALEŻNOŚCI ZWIĄZKOWEJ PRACOWNIKA

Pracodawca ma prawo do zwracania się do zakładowej organizacji związkowej z pytaniem, czy konkretny pracownik korzysta z jej ochrony. Obowiązkiem związku zawodowego jest zaś przekazanie pracodawcy prawidłowej, aktualnej i rzetelnej informacji dotyczącej pracowników podlegających jego ochronie.

Kwestię wzajemnych relacji między związkami zawodowymi a pracodawcą określają przepisy ustawy z dnia 23 maja 1991 r. o związkach zawodowych oraz przepisy Kodeksu pracy.

Obustronnne obwiązki

W przypadku gdy pracodawca nosi się z zamiarem wypowiedzenia pracownikowi umowy o pracę zawartej na czas nieokreślony, to zgodnie z art. 38 § 1 Kodeksu pracy, zawiadamia o tym na piśmie reprezentującą pracownika zakładową organizację związkową, podając przyczynę uzasadniającą rozwiązanie umowy. Natomiast art. 30 ust. 3 ustawy o związkach zawodowych wskazuje, że pracodawca jest obowiązany zwrócić się do organizacji związkowej o informację o pracowniku korzystającym z jej obrony. Oznacza to, że obowiązek ustalenia, czy pracownik jest reprezentowany przez zakładową organizację związkową ciąży na pracodawcy.

Pracodawca powinien więc skierować do organizacji związkowej wniosek o potwierdzenie korzystania przez pracownika z ochrony związkowej, a prawnym obowiązkiem związku zawodowego jest przekazanie pracodawcy prawidłowej, aktualnej i rzetelnej informacji dotyczącej pracowników podlegających ochronie tego związku.

Orzecznictwo Sądu Najwyższego

Co istotne, Sąd Najwyższy w wyroku 14 marca 2012 r. (sygn. akt I PK 117/11), uznał, że jeśli pracodawca w trybie art. 30 ust. 2 ustawy o związkach zawodowych zwrócił się do zakładowej organizacji związkowej o informację, czy konkretny pracownik korzysta z jej ochrony, lecz w ciągu 5 dni nie otrzymał odpowiedzi, to jest zwolniony z obowiązku przewidzianego w art. 38 Kodeksu pracy, tj. zawiadamia jej o zamiarze wypowiedzenia umowy o pracę na czas nieokreślony, pod warunkiem że pomiędzy zasięgnięciem informacji a dokonaniem wypowiedzenia nie upłynął nadmiernie długi okres.

Uwaga na adekwatność

Mimo że przytoczone przepisy prawa pracy oraz ustawy o związkach zawodowych dają pracodawcy podstawę do wystąpienia do organizacji związkowej o informację, czy konkretny pracownik korzysta z ochrony związkowej, to jednak należy zwrócić uwagę, aby zakres danych osobowych pracownika przekazywany organizacji związkowej był adekwatny i wystarczający do celu, jakim jest uzyskanie informacji o jego przynależności do związku zawodowego. Takie postępowanie będzie zgodne z zasadami określonymi w art. 5 RODO, zwłaszcza zaś zasadą minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c.

Zgodnie z przepisami prawa

Warto podkreślić, że dane dotyczące przynależności związkowej - ze względu na swój charakter – są zgodnie z art. 9 ust. 1 RODO zaliczone do danych szczególnej kategorii, których przetwarzanie jest co do zasady zabronione, a dozwolone jedynie przy spełnieniu ściśle określonych warunków.

Pracodawca ma prawo przetwarzać dane osobowe pracowników w taki sposób i w takim zakresie, który wynika z przepisów prawa pracy.

Jeśli robi to w takim właśnie zakresie, pracownik nie może zastrzec swoich danych i żądać np., by nie były przekazywane organizacjom związkowym.

PRZEKAZYWANIE INFORMACJI O SKŁADKACH CZŁONKOWSKICH NA RZECZ SAMORZĄDU ZAWODOWEGO PIELĘGNIAREK I POŁOŻNYCH

Pracodawca, przekazując samorządowi zawodowemu pielęgniarek i położnych informacje dotyczące składek członkowskich odprowadzonych w imieniu poszczególnych osób, musi zachować ostrożność, by nie doszło przy tym do ujawnienia danych o wysokości ich zarobków.

Pielęgniarki i położne zatrudnione w placówkach leczniczych, zgodnie z obowiązującymi dla wymienionych zawodów przepisami, są zobligowane do płacenia składek na rzecz okręgowej izby pielęgniarek i położnych (OIPiP). Przed rozpoczęciem stosowania RODO pracodawcy przesyłali okręgowym izbom informacje zawierające numer prawa wykonywania zawodu wraz z przypisaną do niego kwotą odprowadzonej w imieniu danej osoby miesięcznej składki na rzecz OIPiP. Po 25 maja 2018 r. zaniechali tej praktyki i udostępniają jedynie informacje o globalnej miesięcznej kwocie odprowadzonych składek, bez informacji, od kogo indywidualnie one pochodzą.

Ponieważ takie postępowanie stanowi utrudnienie w działalności izb pielęgniarek i położnych, do Prezesa UODO kierowane były pytania, czy możliwe byłoby powrócenie do wcześniejszej praktyki.

Co stanowią przepisy

W udzielonych wyjaśnieniach Prezes UODO wskazał, że pielęgniarki i położne zatrudnione w placówkach leczniczych są zobligowane do przynależności do samorządu zawodowego i opłacenia na jego rzecz składek członkowskich. Przesądzają o tym przepisy ustawy z 1 lipca 2011 r. o samorządzie pielęgniarek i położnych (art. 2 ust. 3 oraz art. 11 ust. 2 pkt 11).

Ustawa ta w art. 20 pkt 11 wskazuje również, że Krajowy Zjazd, który jest najwyższym organem Naczelnej Izby Pielęgniarek i Położnych, w drodze uchwały określa wysokość i częstotliwość wpłat składki członkowskiej oraz zasady jej podziału.

W ocenie Prezesa UODO, powołane przepisy – ustanawiające obowiązek płacenia składki członkowskiej – stanowią podstawę do przetwarzania jedynie tych danych, które są niezbędne do realizacji tego konkretnego celu.

W zgodzie z zasadami z RODO

W sytuacji, kiedy przepisy szczególne nie wskazują dopuszczalnego zakresu przetwarzania danych osobowych, należy bowiem zastosować przepisy RODO, tak aby podejmowane działania nie naruszały ochrony danych osobowych oraz prawa do prywatności osób, których dane dotyczą. Istotne jest przestrzeganie m.in. zasad celowości oraz legalności, o których mowa w art. 5 ust. 1 RODO, ponieważ w tym przypadku przetwarzanie danych odbywa się w związku z realizacją obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą. Niezgodne z prawem byłoby więc np. przekazywanie innych danych osobowych pracowników, które wykraczają poza to, co niezbędne i adekwatne do osiągnięcia celu, w którym dane są przetwarzane.

Wysokość wynagrodzenia pod ochroną

Sam obowiązek płacenia składki członkowskiej nie stanowi dla pracodawcy podstawy do przekazywania informacji o zasadach wynagradzania oraz nie daje podstawy prawnej do wnioskowania przez okręgową izbę o informacje na temat wysokości wynagrodzenia poszczególnych pielęgniarek i położnych. Zaznaczyć należy, że jeżeli przepisy prawa powszechnego nie wskazują wprost na określone kompetencje samorządu pielęgniarek i położnych, to takiego uprawnienia nie można domniemywać.

Prezes UODO przypomina ponadto, że wynagrodzenie stanowi dobro osobiste pracownika oraz jego dane osobowe, które pracodawca ma obowiązek chronić przed nieuprawnionym dostępem.

Ważny sposób obliczania składki

Istotny dla przekazywania okręgowym izbom pielęgniarek i położnych informacji o odprowadzaniu składek

w imieniu konkretnego pracownika jest też sposób obliczania wysokości składki członkowskiej. Należy bowiem rozróżnić sytuację, w której składka pobierana jest kwotowo, tj. w kwocie stałej dla wszystkich członków, od tej, w której naliczana jest procentowo od wysokości wynagrodzenia.

Potrącanie z wynagrodzenia składki członkowskiej stałej dla wszystkich członków, oraz przekazywanie imiennej listy pracowników (czy też listy pracowników, która zamiast imienia i nazwiska będzie zawierała numer prawa wykonywania zawodu, który również identyfikuje danego pracownika) wraz z kwotą tej składki nie narusza przepisów o ochronie danych osobowych, ponieważ nie wskazuje na wysokość wynagrodzenia określonego pracownika.

Natomiast jeżeli wysokość składki stanowi określoną wartość procentową wynagrodzenia pracownika i jej wskazanie umożliwi określenie wysokości wynagrodzenia konkretnego pracownika, to w ocenie organu ochrony danych osobowych, przekazywanie takiej informacji jest sprzeczne z zasadami ochrony danych określonymi w art. 5 ust. 1 RODO oraz przepisami o ochronie danych osobowych, ponieważ w ten sposób pracodawca pośrednio ujawni informację o wysokości wynagrodzenia pracownika.

WYDAWANIE ZAŚWIADCZEŃ O DOCHODACH NA POTRZEBY UBIEGANIA SIĘ O DOFINANSOWANIE Z NARODOWEGO LUB WOJEWÓDZKIEGO FUNDUSZU OCHRONY ŚRODOWISKA – STATUS ADMINISTRATORA

W procesie wydawania zaświadczeń o wysokości przeciętnego miesięcznego dochodu przypadającego na jednego członka gospodarstwa domowego wydawanego osobom fizycznym, które zamierzają ubiegać się o dofinansowanie z narodowego lub wojewódzkiego funduszu ochrony środowiska, administratorem jest ten podmiot, do którego w całości należeć będzie nie tylko wydawanie zaświadczeń, ale także prowadzenie postępowań w tych sprawach, archiwizacja dokumentów, zapewnienie dostępu do informacji publicznej czy odpowiedniego bezpieczeństwa danych.

W ostatnim okresie jedna z gmin zwróciła się do Prezesa UODO z pytaniem, kto jest administratorem danych osobowych w przypadku, gdy wójt/burmistrz na podstawie art. 411 ust. 10r Prawa ochrony środowiska upoważnił kierownika ośrodka pomocy społecznej do wydawania zaświadczeń o wysokości przeciętnego dochodu przypadającego na jednego członka gospodarstwa domowego wydawanego na żądanie osób fizycznych, które zamierzają złożyć wniosek o przyznanie dofinansowania z narodowego lub wojewódzkiego funduszu ochrony środowiska.

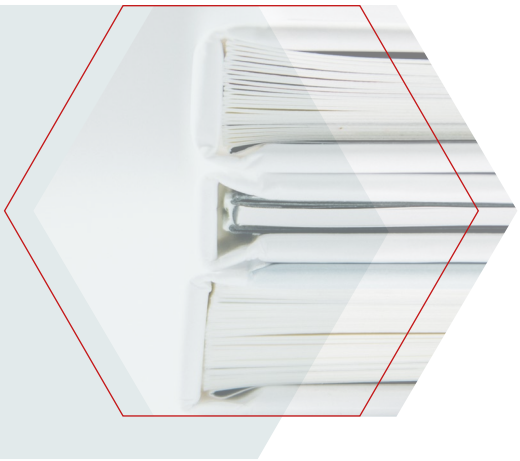
Wyjaśniając te kwestie, organ ds. ochrony danych osobowych przypomniał, że zgodnie z art. 4 pkt 7 RODO, administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

W przypadku podmiotów szeroko rozumianego sektora publicznego podmiot będący administratorem danych może być wskazany w konkretnym przepisie prawa, jednak najczęściej ma miejsce sytuacja, w której rola ta wynika z charakteru, kompetencji lub zakresu zadań publicznych, jakie przepisy temu przypisują. Wskazuje na to Grupa Robocza Art. 29 w opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169).

W przypadku podmiotów publicznych, cele, a czasem i sposoby przetwarzania, określone są w przepisach prawa. Podmioty te są zobowiązane do przetwarzania danych osobowych dla realizacji określonych prawem celów (zadań), zazwyczaj także przy użyciu wskazanych środków. Zatem o tym, czy dany organ, jednostka organizacyjna albo innego rodzaju podmiot jest administratorem danych osobowych, decyduje przede wszystkim rodzaj i charakter nadanych im przez prawo kompetencji z obszaru spraw publicznych oraz wyznaczone ustawowo zadania. Do uznania danego podmiotu za administratora danych potrzebna jest zatem zawsze analiza konkretnych przepisów regulujących działalność danego podmiotu.

Zgodnie z art. 411 ust. 10g ustawy z dnia 27 kwietnia 2001 r. – Prawo ochrony środowiska, osoba fizyczna, która zamierza złożyć wniosek o przyznanie dofinansowania z Narodowego Funduszu Ochrony Środowiska i Gospodarki Wodnej lub wojewódzkiego funduszu, może złożyć żądanie wydania zaświadczenia o wysokości przeciętnego miesięcznego dochodu przypadającego na jednego członka jej gospodarstwa domowego. Zaświadczenie to wydaje wójt, burmistrz lub prezydent miasta właściwy ze względu na miejsce zamieszkania wnioskodawcy (art. 411 ust. 10h ustawy). Zgodnie natomiast z art. 411 ust. 10r powołanej ustawy, wójt, burmistrz lub prezydent miasta może, w formie pisemnej, upoważnić swojego zastępcę, pracownika urzędu gminy albo kierownika ośrodka pomocy społecznej, a w przypadku przekształcenia ośrodka pomocy społecznej w centrum usług społecznych na podstawie przepisów ustawy z dnia 19 lipca 2019 r. o realizowaniu usług społecznych przez centrum usług społecznych – dyrektora centrum usług społecznych, lub kierownika innej jednostki organizacyjnej gminy, a także inną osobę na wniosek kierownika ośrodka pomocy społecznej, dyrektora centrum usług społecznych lub innej jednostki organizacyjnej gminy do prowadzenia postępowań w sprawach, o których mowa w ust. 10g, w tym do wydawania w tych sprawach zaświadczeń.

Administratorem jest ten podmiot, do którego w całości należeć będzie wykonywanie zleconego zadania, a więc nie tylko samo wydawanie zaświadczeń, ale także prowadzenie postępowań w tych sprawach, archiwizacja dokumentów, zapewnienie dostęp udo informacji publicznej czy odpowiedniego bezpieczeństwa danych. Jeśli więc całość zadań związanych z wydawaniem zaświadczeń zostanie przekazana kierownikowi OPS i to on będzie je faktycznie wykonywał, również on w stosunku do przetwarzanych w tym zakresie danych osobowych, będzie pełnił funkcję administratora.



SĄ WYMOGI AKREDYTACJI PODMIOTÓW MONITORUJĄCYCH PRZESTRZEGANIE POSTANOWIEŃ KODEKSÓW POSTĘPOWANIA

Prezes UODO, po konsultacjach z zainteresowanymi podmiotami i zaopiniowaniu przez Europejską Radę Ochrony Danych, przedstawił ostateczną wersję wymogów akredytacji podmiotu monitorującego. Oznacza to, że niebawem organ nadzoru będzie mógł zatwierdzić podmioty monitorujące kodeksy postępowania.

To istotne domknięcie systemu przyjmowania przewidzianych w RODO kodeksów postępowania, umożliwiające ich zatwierdzenie. Wskazanie w kodeksie postępowania akredytowanego podmiotu, który ma kontrolować jego przestrzeganie, jest bowiem warunkiem koniecznym do zatwierdzenia tego dokumentu.

Szczegółowe informacje na ten temat oraz przyjęte wymogi akredytacji podmiotów monitorujących kodeksy postępowania są dostępne na stronie internetowej UODO pod linkiem https://uodo.gov.pl/pl/138/1861.

Jednocześnie Prezes UODO zaprasza do udziału w organizowanym 15 lutego 2021 r. webinarium poświęconym wymogom akredytacji.

KARY

UODO: kary za brak współpracy oraz powiadomień o naruszeniu ochrony danych

Z początkiem nowego roku Prezes UODO zadecydował o ukaraniu administracyjnymi karami pieniężnymi dwóch podmiotów. O takie zakończenie postępowań złożyły się m.in. takie czynniki, jak: brak powiadomień o naruszeniu ochrony danych czy brak współpracy z organem ds. nadzoru.

Pierwsza z kara w wysokości 25 tys. zł polski organ nadzoru nałożył na Śląski Uniwersytet Medyczny, gdyż na uczelni doszło do naruszenia ochrony danych, o którym administrator powinien powiadomić nie tylko organ nadzoru, ale i osoby, których dotyczył ten incydent. Tymczasem w tym przypadku tak nie postąpił.

Z kolei druga kara dotyczyła braku współpracy z UODO poprzez nieudzielanie odpowiedzi na jego pisma oraz niezapewnienie dostępu do danych osobowych i innych informacji niezbędnych do realizacji jego zadań. Postępowanie UODO odnosiło się do spółki Smart Cities z Warszawy, a kara wyniosła 12 tys. zł.

Źródło:
1) kara dla Śląskiego Uniwersytetu Medycznego – https://uodo.gov.pl/pl/138/1825,
2) kara dla spółki Smart Cities – https://uodo.gov.pl/pl/138/1867.

Niemcy: ponad 10 mln euro kary za bezprawny monitoring pracowników

Rzecznik Ochrony Danych w Dolnej Saksonii nałożył na Notebooksbilliger.de karę pieniężną w wysokości 10,4 mln euro. Przedsiębiorstwo stosowało monitoring wideo wobec swoich pracowników przez co najmniej dwa lata bez uzasadnienia prawnego. Niektóre z obszarów zarejestrowanych przez kamery obejmowały przestrzenie robocze, hale handlowe, magazyny i pomieszczenia socjalne.

Przedsiębiorstwo twierdziło, że kamery wideo zostały zainstalowane w celu zapobiegania i ścigania przestępstw oraz śledzenia przepływu towarów w magazynach. Aby jednak zapobiec kradzieży, przedsiębiorstwo musi najpierw wdrożyć mniej surowe środki (np. wyrywkowe kontrole toreb przy opuszczaniu terenu przedsiębiorstwa). Ponadto nadzór wideo może być stosowany do badania przestępstw tylko wtedy, gdy istnieje uzasadnione podejrzenie o popełnienie takich przestępstw przez określone osoby. Ponadto przedsiębiorstwo wiele nagrań przechowywało przez 60 dni, czyli znacznie dłużej niż to konieczne.

Dodatkowo monitoring wideo dotknął także klientów przedsiębiorstwa, ponieważ niektóre kamery zostały skierowane na miejsca siedzące na hali sprzedaży, w obszarach, w których ludzie zwykle spędzają więcej czasu (np. wypróbowując zakupione urządzenia).

Sprawa, w której nałożono na przedsiębiorstwo karę pieniężną, oczekuje na postępowanie sądowe. Od tego czasu przedsiębiorstwo zorganizował nadzór wideo zgodnie z prawem i udowodniło to państwowemu Rzecznikowi Ochrony Danych w Dolnej Saksonii.

Źródło: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_pl

Holandia: technologia rozpoznawania twarzy pod lupą organu ds. ochrony danych

Holenderski organ ochrony danych wystosował formalne ostrzeżenie do supermarketu w związku z korzystaniem z technologii rozpoznawania twarzy.

Supermarket twierdzi, że używał technologii rozpoznawania twarzy, aby chronić swoich klientów i pracowników oraz zapobiegać kradzieżom w sklepach. Technologia została podłączona do kamer przy wejściu do sklepu

i skanowała twarze każdego, kto wszedł do sklepu. Następnie uzyskany obraz był porównywany z bazą danych osób, którym zakazano wchodzenia do sklepów. Twarze osób, których zakaz wchodzenia do sklepu nie dotyczył, były usuwane po kilku sekundach.

Po doniesieniach w mediach holenderski organ zażądał informacji od właściciela supermarketu. W grudniu 2019 roku supermarket wyłączył technologię rozpoznawania twarzy. Właściciel wskazał jednak w dostarczonych do organu nadzorczego dokumentach, że chciałby ją ponownie włączyć.

Dwa wyjątki

Technologia rozpoznawania twarzy wykorzystuje dane biometryczne do identyfikacji ludzi. Korzystanie z funkcji rozpoznawania twarzy w celu zapewnienia bezpieczeństwa jest zabronione w niemal wszystkich sytuacjach. Są jednak wyjątki:

1) sytuacja, gdy osoby wyraziły wyraźną zgodę na przetwarzanie ich danych;

W tym przypadku, chociaż właściciel supermarketu twierdzi, że klienci zostali ostrzeżeni, że sklep używa technologii rozpoznawania twarzy, to osoby te nie wyraziły na takie przetwarzanie danych wyraźnej zgody.

2) sytuacja, gdy technologia rozpoznawania twarzy jest niezbędna do celów uwierzytelniania lub bezpieczeństwa, ale tylko w zakresie, w jakim dotyczy to istotnego interesu publicznego.

Źródło: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_pl

XV DZIEŃ OCHRONY DANYCH OSOBOWYCH JUŻ ZA NAMI

Głównym wydarzeniem zorganizowanym w ramach obchodów XV Dnia Ochrony Danych Osobowych była w tym roku konferencja pt. „Realna ochrona danych osobowych w zdalnej rzeczywistości", zorganizowana 28 stycznia 2021 r. przez Urząd Ochrony Danych Osobowych w formule online.

W ramach trzech sesji merytorycznych przedstawiciele Urzędu, Komisji Europejskiej, prawnicy i praktycy omówili najbardziej aktualne kwestie dotyczące ochrony danych osobowych i prywatności, odnosząc się również do nowej rzeczywistości, jaką jest zdalna praca czy nauka, które stworzyły bezprecedensowe wyzwania w tym zakresie. Ponadto prelegenci dyskutowali o bieżących zadaniach i wyzwaniach, jakie stoją przed administratorami z sektora publicznego i prywatnego, w tym zwłaszcza sektora średnich i małych przedsiębiorstw, w związku ze stosowaniem przepisów o ochronie danych osobowych.

Zapraszamy do obejrzenia nagranie z konferencji, które jest dostępne pod linkiem: https://video.uodo.gov.pl/video/Konferencja_DODO.mp4

NOWE PYTANIA W ZAKŁADCE IOD

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 w przypadku PPE pracodawca powinien zawrzeć umowę powierzenia?
Czy IOD powinien sporządzić plan audytów?
Jak postępować, gdy dojdzie do zagubienia zwrotnego potwierdzenia odbioru?

URZĄD OCHRONY DANYCH OSOBOWYCH