Obserwuj nas na:

Nr 4/2021 (25)
Kwiecień 2021

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

PRZEKAZYWANIE DANYCH NA POTRZEBY BADAŃ STATYSTYCZNYCH

Przepisy z zakresu statystyki publicznej są podstawą do udostępnienia jedynie tych danych osobowych, które administrator może posiadać zgodnie z prawem dla realizacji ściśle wyznaczonych celów, przy zachowaniu określonych w RODO zasad, w tym proporcjonalności, minimalizacji czy ograniczenia czasowego.

Tę podstawową zasadę Prezes UODO przypomniał ostatnio, opiniując projekt rozporządzenia Rady Ministrów zmieniającego rozporządzenie w sprawie programu badań statystycznych statystyki publicznej na rok 2021.

Przewiduje on, że gminy na potrzeby badań statystycznych będą przekazywały GUS dane jednostkowe o właścicielach nieruchomości w rozumieniu ustawy o utrzymaniu czystości i porządku w gminach oraz ich współmałżonkach składających deklaracje (i ich korekty) o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie nieruchomości zamieszkałych, częściowo zamieszkałych oraz nieruchomości rekreacyjnych.

W opinii Prezesa UODO, nie ma podstaw, by gminy pozyskiwały, a następnie przekazywały GUS takie dane.

W przesłanym do Prezesa GUS stanowisku organ nadzorczy wskazał, że ustawa z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach w art. 2 ust. 1 pkt 4 za właściciela nieruchomości uznaje również współwłaściciela (współwłaścicieli), użytkownika wieczystego (użytkowników wieczystych) oraz jednostkę organizacyjną (jednostki organizacyjne) i osobę (osoby) posiadającą (posiadające) nieruchomości w zarządzie lub użytkowaniu, a także inny podmiot (podmioty) władający (władające) nieruchomością. Tylko zatem od osób wskazanych w powołanym przepisie rada gminy, na podstawie art. 6m ust. 1b tej ustawy, może domagać się podania: 1) imienia i nazwiska lub nazwy właściciela nieruchomości oraz adresu miejsca zamieszkania lub siedziby; 2) adresu nieruchomości; 3) danych stanowiących podstawę zwolnienia z opłaty za gospodarowanie odpadami komunalnymi; 4) numeru telefonu właściciela nieruchomości; 5) adresu poczty elektronicznej właściciela nieruchomości; 6) innych informacji niezbędnych do wystawienia tytułu wykonawczego; 7) informacji dotyczących posiadania kompostownika przydomowego i kompostowania w nim bioodpadów stanowiących odpady komunalne.

W powyższym wyliczeniu nie mieści się zaś współmałżonek właściciela nieruchomości (o ile nie jest współwłaścicielem, współużytkownikiem wieczystym, współzarządcą nieruchomości lub współużytkownikiem, współwładającym nieruchomością). Brak jest zatem podstaw, by – jak to przewidziano w pkt 3 lit. zzr załącznika do projektu rozporządzenia zmieniającego – urząd gminy pozyskiwał dane współmałżonków właścicieli nieruchomości składających deklaracje (i ich korekty) o wysokości opłaty za gospodarowanie odpadami komunalnymi w zakresie nieruchomości tylko po to, by następnie przekazać je do GUS na potrzeby prowadzenia badań statystycznych.

Prezes UODO zaznaczył, że taka konstrukcja powołanych przepisów stanowi w istocie próbę obejścia przez służby statystyki publicznej przepisów ustawy o utrzymaniu czystości i porządku w gminach normujących pozyskiwanie danych właścicieli nieruchomości i nie może być uznana za zgodną z zasadami ochrony danych osobowych, zwłaszcza z zasadą zgodności z prawem (legalizmu) i zasadą minimalizacji danych. Podkreślił, że żaden organ nie powinien być obligowany do zbierania nadmiarowych danych (danych, do których gromadzenia nie jest uprawniony stosownymi przepisami) jedynie dla potrzeb GUS.

Jednocześnie przypomniał, że przepisy o statystyce publicznej uprawniają GUS do pozyskiwania na potrzeby prowadzenia badań statystyki publicznej niezbędnych danych z różnych innych źródeł, w tym rejestrów publicznych.

Warto przypomnieć, że kwestie te były już sygnalizowane przez Prezesa UODO w 2019 r., a więcej informacji na ten temat jest dostępnych na stronie internetowej UODO w materiale „Pozyskiwanie danych na potrzeby statystyki musi być zgodne z ochroną danych osobowych". Ostatnio zaś wyjaśnienia dotyczące tej tematyki zamieszczone zostały w formie odpowiedzi na pytanie IOD „Czy GUS może zobowiązać gminy do przekazania mu innych danych niż te, które gmina może gromadzić?".

PODSTAWA PRAWNA PRZETWARZANIA DANYCH O STANIE ZDROWIA PRZEZ INSTYTUCJĘ FINANSOWĄ PROWADZĄCĄ I ZARZĄDZAJĄCĄ PPK

Ponieważ przepisy prawa krajowego określają sytuacje, w których uczestnik PPK przekazuje instytucji finansowej dane dotyczące poważnego zachorowania, to właśnie one wraz z art. 9 ust. 2 lit. b RODO stanowią podstawą uprawniającą instytucję finansową do przetwarzania danych o stanie zdrowia uczestnika PPK, jego współmałżonka lub dziecka.

Zgodnie z art. 101 ust. 1 ustawy z dnia 4 października 2018 r. o pracowniczych planach kapitałowych, uczestnik PPK w przypadku poważnego zachorowania zarówno swojego, jak i małżonka lub dziecka, może wnioskować o wypłatę do 25% środków zgromadzonych na swoim rachunku PPK. Artykuł 101 ust. 2 wymienionej ustawy stanowi zaś, że wniosek o wypłatę, o której mowa w ust. 1, uczestnik PPK składa wybranej instytucji finansowej. Do wniosku o wypłatę dołącza orzeczenie, o którym mowa w art. 2 ust. 1 pkt 23 lit. a-c, tj. orzeczenie lekarza orzecznika lub komisji lekarskiej Zakładu Ubezpieczeń Społecznych, albo orzeczenie zespołu do spraw orzekania o niepełnosprawności, lub zaświadczenie lekarza medycyny potwierdzające diagnozę wystąpienia poważnego zachorowania, o którym mowa w art. 2 ust. 1 pkt 23 lit. d lub e.

Biorąc pod uwagę tak ukształtowany stan prawny, podstawą przetwarzania danych o stanie zdrowia uczestnika PPK przez instytucję finansową jest art. 9 ust. 2 lit. b RODO, zgodnie z którym przetwarzanie szczególnych kategorii danych osobowych, w tym danych dotyczących zdrowia, jest dopuszczalne, gdy jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii Europejskiej lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą.

POZYSKIWANIE PRZEZ PCPR DANYCH OSOBOWYCH OD MOPS

W opinii Prezesa UODO, nie należy negować pozyskiwania przez PCPR na potrzeby prowadzenia konkretnego postępowania danych osobowych od MOPS. Natomiast zakres pozyskiwanych danych osobowych i informacji powinien być ograniczony jedynie do niezbędnego minimum, bez przetwarzania danych nadmiarowych bądź danych niemających znaczenia dla danej sprawy.

Czy powiatowe centrum pomocy rodzinie (PCPR) na potrzeby prowadzenia czynności monitorujących sytuację rodziny, w której osoba stosująca przemoc domową poddana była oddziaływaniom korekcyjno-edukacyjnym ma prawo pozyskiwać dane osobowe od miejskiego ośrodka pomocy społecznej (MOPS)? To kwestia, o wyjaśnienie której do Prezesa UODO zwrócił się jeden z podmiotów.

W odpowiedzi organ właściwy w sprawie ochrony danych osobowych wskazał, że w przypadku podmiotów publicznych co do zasady podstawę prawną przetwarzania danych osobowych (w tym udostępniania danych) powinno stanowić wykonanie obowiązku prawnego ciążącego na administratorze (art. 6 ust.1 lit. c RODO) lub też wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO). W przypadku zaś wniosku o udostępnienie dotyczy danych należących do kategorii szczególnych, o których mowa w art. 9 RODO, jak np. dane o stanie zdrowia, pamiętać należy, że są one objęte szczególnym reżimem przetwarzania.

Przepisy ustawy z dnia 12 marca 2004 r. o pomocy społecznej, ustawy z dnia 29 lipca 2005 r. o przeciwdziałaniu przemocy w rodzinie oraz rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 22 lutego 2011 r. w sprawie standardu podstawowych usług świadczonych przez specjalistyczne ośrodki wsparcia dla ofiar przemocy w rodzinie, kwalifikacji osób zatrudnionych w tych ośrodkach, szczegółowych kierunków prowadzenia oddziaływań korekcyjno-edukacyjnych wobec osób stosujących przemoc w rodzinie oraz kwalifikacji osób prowadzących oddziaływania korekcyjno-edukacyjne nie wskazują wprost na udostępnianie przez miejskie ośrodki pomocy społecznej (MOPS) informacji i danych powiatowemu centrum pomocy rodzinie (PCPR). Niemniej dokonując oceny przedstawionego zagadnienia, pod uwagę należy wziąć również pozostałe przepisy, które regulują przedmiotową materię.

Przepisy ustawy o pomocy społecznej z jednej strony stanowią, że w postępowaniu w sprawie świadczeń z pomocy społecznej należy kierować się przede wszystkim dobrem osób korzystających z pomocy społecznej i ochroną ich dóbr osobistych (art. 100 ust. 1), a dodatkowo regulują konieczność zachowania w tajemnicy wszelkich informacji i danych, które podmioty i osoby realizujące zadania w zakresie pomocy społecznej uzyskały przy wykonywaniu tych zadań (art. 100 ust. 7).

Jednocześnie wskazują, że w indywidualnych sprawach z zakresu pomocy społecznej należących do właściwości powiatu decyzje administracyjne wydaje starosta lub z jego upoważnienia kierownik powiatowego centrum pomocy rodzinie i inni pracownicy centrum upoważnieni na wniosek kierownika (art. 100 ust. 5). Tak więc przyjąć należy, że skoro m.in. kierownik PCPR ma ustawowe uprawnienie do wydawania decyzji administracyjnych, to dysponuje podstawą do zebrania dokumentów niezbędnych do jej wydania.

Pod uwagę wziąć również należy przepisy Kodeksu postępowania administracyjnego (k.p.a.), które wskazują, że w toku postępowania organy administracji publicznej współdziałają ze sobą w zakresie niezbędnym do dokładnego wyjaśnienia stanu faktycznego i prawnego sprawy, mając na względzie interes społeczny i słuszny interes obywateli oraz sprawność postępowania, przy pomocy środków adekwatnych do charakteru, okoliczności i stopnia złożoności sprawy (art. 7b k.p.a.). Oznacza to, że organy administracji publicznej mają obowiązek współpracowania, w tym również przekazywania informacji, które mają kluczowe znaczenie dla załatwienia danej sprawy (wydania decyzji). Dlatego też nie należy negować działań podejmowanych przez PCPR, które polegają na pozyskiwaniu danych od MOPS.

Natomiast zakres pozyskiwanych danych osobowych i informacji powinien być ograniczony jedynie do niezbędnego

minimum, bez przetwarzania danych nadmiarowych bądź danych niemających znaczenia dla danej sprawy. Dzięki temu przekazywanie określonych danych będzie służyło rozstrzygnięciu konkretnej sprawy i jednocześnie czyniło zadość zasadom przetwarzania danych określonych w art. 5 RODO. W każdym przypadku należy bowiem czynić zadość tym zasadom, w szczególności zasadzie zgodności z prawem, ograniczenia celu oraz minimalizacji danych, tak aby podejmowane działania służyły celowi, w którym dane są przetwarzane, a jednocześnie gwarantowały zachowanie prawa do prywatności i ochrony danych osobowych.

Prezes UODO wskazał również, że podczas toczących się postępowań prowadzonych przez PCPR, w czasie których PCPR samodzielnie próbuje uzyskać informacje od innych podmiotów, m.in. MOPS, to osoby, z udziałem których toczą się te postępowania, powinny również mieć możliwość przedłożenia stosownych dokumentów, a także oświadczeń niezbędnych do zbadania danej sprawy. Osoby te powinny być również informowane o pozyskiwaniu ich danych z innych źródeł. Pamiętać bowiem należy, że w przypadku pozyskiwania danych osobowych w sposób inny niż od osób, których one dotyczą, gdy źródłem danych są inne organy administracji publicznej lub osoby trzecie, wówczas PCPR ma obowiązek poinformować osobę, której dane dotyczą, o źródle pozyskania danych, chyba że przepis szczególny zwalnia PCPR z tego obowiązku.

CZY ANONIMIZACJĘ I PSEUDONIMIZACJĘ DANYCH MOŻNA STOSOWAĆ ZAMIENNIE?

Jednym z zadań administratora jest zapewnienie odpowiedniego bezpieczeństwa gromadzonych przez niego danych osobowych. Można to zrobić na wiele sposobów, używając różnych technik ochrony danych. Należy do nich np. anonimizowanie lub psedonimizowanie danych. Jednak technik tych administrator nie może stosować zamiennie w tym samym celu.

Jedna z fundamentalnych reguł ogólnego rozporządzenia o ochronie danych (RODO) głosi, że ochrona danych powinna dotyczyć wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Administrator, przetwarzając dane konkretnej osoby, musi zapewnić ochronę przed bezpośrednim lub pośrednim zidentyfikowaniem tej osoby na podstawie danych, które posiada. W każdym przypadku to administrator jest uprawniony i zobowiązany do wyboru takiego środka ochrony danych, który będzie zapewniał im należytą ochronę.

Jedną z metod ochrony danych, którą mogą zastosować administratorzy jest „pseudonimizacja" zdefiniowana w art. 4 pkt 5 RODO. Pojęcie to oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było przypisać konkretnej osobie bez użycia dodatkowych informacji. Muszą być one objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Ponieważ technika ta ogranicza możliwość powiązania zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą, to dzięki niej administrator może utrudnić identyfikację określonej osoby.

Pseudonimizacja zwiększa bezpieczeństwo przetwarzanych danych osobowych. To nic innego jak zmiana danych, które można np. zaszyfrować za pomocą specjalnego „klucza". Jednocześnie takie dodatkowe informacje powinny być przechowywane osobno. Urząd Ochrony Danych Osobowych od dawna przypomina, aby w sytuacji, gdy administrator przekazuje zaszyfrowane dane przy pomocy jakiegoś klucza, to klucz ten należy przekazać innym kanałem komunikacji niż zaszyfrowane dane. Trzeba pamiętać, że w przypadku użycia pseudonimizacji nadal istnieje prawdopodobieństwo pośredniego zidentyfikowania osoby fizycznej. Zgodnie z motywem 26 RODO spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej.

Trzeba mieć też na uwadze fakt, że pseudonimizacja nie jest metodą anonimizacji. Zgodnie z RODO spseudonimizowane dane osobowe poddane to wciąż dane osobowe. Pseudonimizacja polega na przekształceniu danych osobowych w sposób uniemożliwiający

przyporządkowanie poszczególnych informacji do określonej lub możliwej do zidentyfikowania osoby fizycznej. Co ważne, skoro administrator na skutek zastosowania anonimizacji uniemożliwi identyfikację danej osoby, to wówczas RODO nie będzie miało zastosowania do przetwarzania takich danych, bo te nie umożliwią już identyfikacji bezpośredniej lub pośredniej danej osoby.

Anonimizacja ma zastosowanie, gdy potrzeba trwale usunąć z nośników danych (papierowych lub elektronicznych) wszelkie informacje pozwalające na identyfikację osób, których dane osobowe dotyczą (np. imię, nazwisko, adres, numer telefonu).

Podsumowując, anonimizacja jest procesem nieodwracalnym. Z kolei pseudonimizacja umożliwia powrót do stanu sprzed zmiany. Zatem gdy administrator potrzebuje zabezpieczyć dane, to powinien wybrać takie narzędzie, które będzie zapewniało należytą ochronę danych.

Ponieważ wciąż pozostaje aktualna Opinia 05/2014 Grupy Roboczej Art. 29 z 10 kwietnia 2014 r. w sprawie technik anonimizacji, która wiele wyjaśnia także w temacie technik pseudonimizacji, warto się z nią zapoznać, aby bliżej przyjrzeć się konkretnym technikom depersonalizacji danych osobowych.

Zgodnie z ww. Opinią zanonimizowane dane nie są objęte zakresem przepisów dotyczących ochrony danych, ale osoby, których dane dotyczą, nadal mogą być upoważnione do ochrony na mocy innych przepisów (takich jak te chroniące poufność komunikacji). Administrator powinien uwzględniać, że zanonimizowane zbiory danych mogą nadal stanowić ryzyko szczątkowe dla osoby, której dane dotyczą. W praktyce z jednej strony anonimizacja i ponowna identyfikacja stanowią aktywne dziedziny badań i regularnie publikowane są nowe odkrycia w tym zakresie, z drugiej strony nawet zanonimizowane dane, takie jak statystyki, mogą być wykorzystywane w celu wzbogacenia istniejących profili poszczególnych osób fizycznych, co prowadzi do powstawania nowych problemów związanych z ochroną danych. Nie należy zatem uznawać anonimizacji za działanie jednorazowe, a administrator danych powinien regularnie przeprowadzać ponowną ocenę występującego ryzyka. Administrator powinien zwrócić uwagę, że to jakie narzędzie zastosuje wynikać będzie z przeprowadzonej analizy ryzyka w danej organizacji. Zasadność użycia danego sposobu bezpieczeństwa powinno być uwzględnione przez administratora już w fazie projektowania.

MIĘDZYNARODOWE

Prawa człowieka i wyzwanie cyfrowe a wkład Konwencji 108+

Konwencja 108+ i związane z nią prace Rady Europy w zakresie ochrony danych to jeden z elementów, który może przyczynić się do sprostania wyzwaniom związanym z prawami człowieka wynikającymi z rozwoju cyfrowego – to główne przesłanie sympozjum zorganizowanego 16 marca 2021 r. przez ICESCO we współpracy z Ministerstwem Stanu ds. Praw Człowieka i Stosunków z Parlamentem Maroka.

ICESCO (The Islamic World Educational, Scientific and Cultural Organisation) pracuje nad dostarczaniem innowacyjnych rozwiązań dla wyzwań związanych z prawami człowieka w technologii cyfrowej i opracowuje ramy prawne w celu ochrony tych praw w przestrzeni cyfrowej.

Więcej informacji o międzynarodowym sympozjum nt. „Prawa człowieka i cyfrowe wyzwania”:
https://www.icesco.org/en/2021/03/15/tomorrow-international-symposium-on-human-right-and-digital-challenge-at-icesco-headquarters/
Zapis sympozjum jest dostępne pod linkiem:
https://www.facebook.com/ICESCO.En/live

Źródło: https://www.coe.int/en/web/data-protection/-/human-rights-and-the-digital-challenge-the-contribution-of-convention-108-

Hiszpania: spółka ukarana m.in. za niezgodne z prawem przetwarzanie danych

Hiszpański organ ochrony danych (AEPD) nałożył na CAIXABANK S.A. łączną karę w wysokości 6 mln euro za niezgodne z prawem przetwarzanie danych osobowych klientów oraz niedostarczenie wystarczających informacji dotyczących przetwarzania danych osobowych.

AEPD uznała, że dokument opracowany w celu zapewnienia zgodności z informacjami nie zawierał wystarczających informacji na temat przedmiotowych kategorii danych osobowych ani informacji o celach przetwarzania, dla których dane osobowe są przeznaczone, jak również podstawy prawnej przetwarzania, zwłaszcza w odniesieniu do czynności przetwarzania opartych na uzasadnionym interesie firmy.

Wskutek tego hiszpański organ nadzorczy stwierdził, że CAIXABANK naruszył art. 13 i 14 RODO. Zgodnie z art. 83 ust. 5 lit. b RODO nałożono karę 2 mln euro. Podejmując decyzję o wysokości administracyjnej kary pieniężnej, AEPD wzięła pod uwagę jako czynniki obciążające, m.in. charakter, wagę i czas trwania naruszenia; nieumyślny charakter naruszenia, związek między działalnością firmy a przetwarzaniem danych osobowych, oraz fakt, że firma jest dużym przedsiębiorstwem.

Ponadto AEPD stwierdziła, że CAIXABANK nie zapewnił żadnego mechanizmu uzyskiwania zgody osoby, której dane dotyczą, a także, że udzielona zgoda nie spełniała wszystkich elementów do uznania jej ważności, a ponadto czynności przetwarzania prowadzone w oparciu o uzasadniony interes spółki nie były w istocie wystarczająco uzasadnione, w szczególności związek między działalnością spółki a przetwarzaniem danych osobowych. AEPD stwierdziła, że stanowiło to naruszenie art. 6 RODO i zgodnie z art. 83 ust. 5 lit. a RODO, co doprowadziło do nałożenia administracyjnej kary pieniężnej w wysokości 4 mln euro.

Oprócz administracyjnej kary pieniężnej, najwyższej, jaką kiedykolwiek nałożył hiszpański organ ochrony danych, AEPD nakazała CAIXABANK dostosować swoje operacje przetwarzania danych do art. 6, 13 i 14 RODO w ciągu najbliższych sześciu miesięcy.

Źródło: http://edpb.europa.eu/news/national-news/2021/spanish-data-protection-authority-aepd-imposes-fine-6000000-eur

Norwegia: działanie bez podstawy prawnej naraziło administratora na sankcję finansową

Norweski organ ochrony danych nałożył na Aquateknikk AS karę w wysokości 10 tys. euro (100 tys. koron norweskich) za przeprowadzenie oceny wiarygodności kredytowej wobec osoby fizycznej bez podstawy prawnej.

Sprawa ta została wszczęta w odpowiedzi na skargę osoby, która odkryła, że przedsiębiorstwo Aquateknikk przeprowadziło ocenę jej wiarygodności kredytowej, podczas gdy nie miała ona z nim żadnych relacji o charakterze konsumenckim ani powiązań z przedsiębiorstwem.

Ogólne rozporządzenie o ochronie danych (RODO) wymaga, aby każde przetwarzanie danych osobowych miało podstawę prawną. Oceny wiarygodności kredytowej są rodzajem danych osobowych podlegających szczególnej ochronie. Ocena wiarygodności kredytowej składa się z analizy danych osobowych pochodzących z wielu różnych źródeł w celu wykazania prawdopodobieństwa, że dana osoba będzie w stanie spłacić swoje zobowiązania. Ocena wiarygodności kredytowej zawiera również szczegółowe informacje na temat osobistej sytuacji finansowej danej osoby, takie jak stosunek zadłużenia do dochodów, uwagi dotyczące płatności oraz ewentualnie o kredycie hipotecznym.

Po zbadaniu tej sprawy organ ochrony danych stwierdził, że oceny zdolności kredytowej zostały przeprowadzone bez podstawy prawnej, z naruszeniem wymogów RODO. Przedsiębiorstwo nie miało uzasadnionego interesu w przeprowadzeniu oceny wiarygodności kredytowej skarżącego.

Źródło: https://edpb.europa.eu/news/national-news/2021/norwegian-dpa-issues-fine-aquateknikk_pl

Włochy: kara m.in. za brak wyznaczenia IOD

Włoski organ ochrony danych (Garante) nakazał Ministerstwu Rozwoju Gospodarczego uiszczenie kary w wysokości 75 tysięcy euro za to, że do 28 maja 2018 r. nie powołało inspektora ochrony danych (IOD), tj. dnia od którego RODO ma w pełni zastosowanie, oraz że udostępniło dane osobowe ponad 5 tys. menedżerów na instytucjonalnej stronie internetowej.

Po raz pierwszy Garante nałożył karę za brak wyznaczenia IOD w określonym terminie oraz za wyznaczenie IOD i przekazanie danych kontaktowych organowi ochrony danych z dużym opóźnieniem. Niemniej jednak od maja 2017 r. Garante rozpoczął kompleksową działalność informacyjną skierowaną do wszystkich ministerstw, wskazując dokładnie na wyznaczenie IOD jako jeden z trzech priorytetów, które należy uwzględnić w procesie dostosowywania się do nowych ram prawnych rozporządzenia.

Fakt niewyznaczenia IOD wyszedł na jaw w trakcie dochodzenia wszczętego przez Garante również na podstawie doniesień stwierdzających obecność na ministerialnej witrynie internetowej listy menedżerów, na której są widoczne i dostępne do pobrania dane osobowe ponad pięciu tysięcy specjalistów, w tym: imię i nazwisko, numer podatkowy, adres e-mail, życiorys z numerem telefonu komórkowego oraz, w niektórych przypadkach, kopia dokumentu tożsamości i karty zdrowia.

Włoski organ ochrony danych uznał ponadto, że publikacja pełnych życiorysów stanowi nieproporcjonalne przetwarzanie danych, niezgodne z zasadami RODO. Aby umożliwić skorelowanie zapotrzebowania przedsiębiorstw z ofertą doradztwa ze strony menedżerów, wystarczyłoby użyć mniej inwazyjnych narzędzi niż publikacja w Internecie danych i informacji o wszystkich menedżerach, unikając w ten sposób ryzyka narażenia ich na nieuzasadnione wykorzystanie ich danych przez osoby trzecie (np. kradzież tożsamości, niezgodne z prawem profilowanie, phishing itp.). Na przykład, można by przewidzieć selektywny dostęp do zastrzeżonych obszarów witryny instytucjonalnej poprzez przypisanie danych uwierzytelniających (np. nazwy użytkownika lub hasła) lub za pomocą narzędzi przewidzianych w Kodeksie administracji cyfrowej (CAD), które umożliwiłyby wgląd wyłącznie zainteresowanym MŚP.

Źródło: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556625

Włoski odpowiednik ZUS ukarany za niezgodne z RODO przetwarzanie danych

Niewskazanie kryteriów przetwarzania danych osobowych określonych kategorii wnioskodawców ubiegających się o „świadczenie w związku z COVID" (wł. „bonus COVID"), wykorzystanie informacji niekoniecznych do celów kontroli, wykorzystanie nieprawidłowych lub niekompletnych danych, nieodpowiednia ocena zagrożeń dla prywatności – to powody, dla których włoski organ ochrony danych nałożył karę na INPS.

Włoski organ ochrony danych (Garante) nakazał INPS (Narodowy Zakład Zabezpieczenia Społecznego) uiścić karę w wysokości 300 tys. euro w związku z naruszeniami popełnionymi w ramach prowadzonych przez INPS dochodzeń w sprawie zwalczania nadużyć finansowych dotyczących „świadczeń w związku z COVID" w odniesieniu do numerów identyfikacyjnych VAT.

Dochodzenie Garante zostało wszczęte na podstawie doniesień prasowych, dotyczących przetwarzania przez INPS danych wnioskodawców zajmujących stanowiska polityczne (szczególnie stanowiska parlamentarne, w administracji regionalnej lub lokalnej).

W toku dochodzenia włoski organ nadzorczy, uznając, że przeprowadzanie kontroli istnienia określonych przez prawo wymogów dotyczących wypłaty świadczeń jest związane z zadaniami leżącymi w istotnym interesie publicznym, stwierdził jednak szereg krytycznych punktów w metodach wykorzystywanych przez INPS w dochodzeniu.

Dochodzenie włoskiego organu ochrony danych wykazało, że INPS nie zaplanował odpowiednio przetwarzania danych osobowych i nie był w stanie wykazać, że przeprowadził kontrole zgodnie z rozporządzeniem, naruszając zasady uwzględniania ochrony prywatności w fazie projektowania i domyślnej ochrony danych oraz rozliczalności.

Po pierwsze, po uzyskaniu z otwartych źródeł danych dziesiątek tysięcy osób zajmujących stanowiska polityczne,

INPS dokonał opracowania i porównania danych wszystkich osób, które wystąpiły z wnioskiem o świadczenie, z danymi osób zajmujących wyżej wymienione stanowiska. Jednakże bez uprzedniego ustalenia, czy parlamentarzyści i samorządowcy regionalni lub lokalni są uprawnieni do tego świadczenia, również ze względu na różne cechy zajmowanych stanowisk. W ten sposób INPS naruszył zasady zgodności z prawem, prawidłowości i przejrzystości ustanowione w rozporządzeniu UE o ochronie danych osobowych.

INPS nie przestrzegał nawet zasady minimalizacji danych, ponieważ wszczął kontrole mające na celu odzyskanie świadczeń również w odniesieniu do wszystkich podmiotów, które, mimo że zwróciły się o nie, nie otrzymały ich, ponieważ ich wnioski został już odrzucone z powodów niezależnych od pełnionej funkcji.

Stwierdzono również, że INPS nie dokonał odpowiedniej oceny ryzyka związanego z przetwarzaniem tak wrażliwych danych, jak dane osób ubiegających się o korzyść ekonomiczną zaklasyfikowaną do społecznych środków osłonowych, nie przeprowadzając oceny wpływu na prawa i wolności zainteresowanych osób.

Z tych powodów Garante stwierdził, że przetwarzanie danych osobowych dokonywane przez INPS jest niezgodne z prawem i zastosował sankcję. Włoski organ ochrony danych nakazał również INPS usunięcie niepotrzebnych danych, które były do tej pory przetwarzane, i przeprowadzenie odpowiedniej oceny wpływu na prywatność.

Informacja w języku włoskim jest dostępna pod linkiem: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9556927

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 wobec osób z władz związku zawodowego trzeba spełniać obowiązek informacyjny?

Czy komornikowi należy udostępnić dane w postaci rachunku bankowego pracownika?

Jakie informacje publikować w BIP wz. z ustaleniem przebiegu granic działek ewidencyjnych?

URZĄD OCHRONY DANYCH OSOBOWYCH