Obserwuj nas na:

Nr 9/2020 (18)
Wrzesień 2020

URZĄD OCHRONY DANYCH OSOBOWYCH

NEWSLETTER

UODO DLA INSPEKTORÓW OCHRONY DANYCH

KOMORNIK NIE JEST ODBIORCĄ DANYCH

Przedsiębiorca nie musi informować dłużnika o udostępnieniu jego danych komornikowi mającemu przeprowadzić – zgodnie z wyrokiem sądu – egzekucję długów. Komornik nie jest bowiem odbiorcą danych w rozumieniu przepisów RODO.

Do takiego wniosku prowadzi analiza przepisów RODO oraz przepisów szczególnych regulujących prowadzenie czynności egzekucyjnych przez komorników sądowych.

Ogólna definicja odbiorcy

RODO w sposób ogólny określa, kogo należy uznać za odbiorcę danych. Zgodnie z definicją zawartą w art. 4 ust. 9 RODO, „odbiorca oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania”.

Motyw 31 RODO wskazuje, że „organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego”.

Komornik jako organ egzekucyjny egzekucji sądowej

Jednocześnie, jak wskazuje art. 758 ustawy z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (k.p.c.), sprawy egzekucyjne należą do właściwości sądów rejonowych i działających przy tych sądach komorników. Artykuł 759 § 1 powołanej ustawy stanowi, że czynności egzekucyjne są wykonywane przez komorników z wyjątkiem czynności zastrzeżonych dla sądów.

Z kolei przepisy ustawy z dnia 22 marca 2018 r. o komornikach sądowych (art. 3 ust. 1) przesądzają, że komornik jest organem władzy publicznej w zakresie wykonywania czynności w postępowaniu egzekucyjnym i zabezpieczającym. Jednocześnie stanowią, że komornik sądowy wykonuje czynności w zakresie swojej właściwości na wniosek. Szczegółowy zakres jego czynności określają zaś art. 9 i 10 powołanej ustawy.

W świetle tych regulacji komornika sądowego, będącego organem egzekucyjnym, którego działania są określone przepisami prawa, nie należy traktować jako odbiorcy danych w rozumieniu RODO.

O czym nie trzeba informować dłużnika

Zatem przedsiębiorca, który dysponuje prawomocnym wyrokiem sądu i z powodu braku wpływu należnych mu płatności przekazał dane osobowe dłużnika komornikowi sądowemu w celu prowadzenia przez niego ich egzekucji, realizując prawo dostępu osoby do dotyczących jej danych, o którym mowa w art. 15 RODO, nie musi wskazywać komornika jako podmiotu, któremu dane zostały ujawnione.

WYKAZANIE ISTNIENIA INTERESU PRAWNEGO LEGALIZUJE UDOSTĘPNIENIE DANYCH PRZEZ USC

Zobowiązanie sądu oraz wypis testamentu i oświadczenie, że określone dokumenty są niezbędne do przeprowadzenia postępowania spadkowego są wystarczające do uznania istnienia interesu prawnego i udostępnienia danych osobowych.

To sedno decyzji Prezesa UODO wydanej w sprawie skargi dwóch kobiet, które uważały, iż doszło do nieuprawnionego udostępnienia przez prezydenta miasta (Urząd Stanu Cywilnego) ich danych osobowych poprzez wydanie skróconego aktu urodzenia oraz skróconego odpisu aktu małżeństwa.

Złożone wnioski

Z informacji zebranych przez organ ds. ochrony danych osobowych w toku prowadzonego postępowania wynikało, że w Urzędzie Stanu Cywilnego został złożony wniosek o wydanie i bezpośrednie przesłanie do wskazanego sądu rejonowego odpisu skróconego aktu małżeństwa wskazanych w nim osób. Jako wykazanie istnienia interesu prawnego wnioskodawca przedłożył kopię protokołu z rozprawy dotyczącej stwierdzenia nabycia spadku, z którego wynikało, iż jako pełnomocnik osoby, która wniosła tę sprawę do sądu, został zobowiązany w terminie jednego miesiąca do przedłożenia odpisu aktu małżeństwa jednej ze skarżących pod rygorem zwrócenia się do stosownych instytucji i obciążenia kosztami związanymi z uzyskaniem tego dokumentu.

W odniesieniu do drugiej skarżącej złożony został wniosek o wydanie odpisu skróconego aktu urodzenia wskazanej osoby. W tym przypadku osoba składająca wniosek dla wykazania istnienia interesu prawnego przedłożyła wypis aktu notarialnego (testamentu) oraz złożyła oświadczenie, iż wnioskowany odpis jest potrzebny do przeprowadzenia postępowania spadkowego.

Wydanie i przekazanie odpisów

Kierownik urzędu stanu cywilnego uznał, iż w obu przypadkach interes prawny został przez wnioskodawców wykazany. Wydał zatem odpis skrócony aktu małżeństwa i przesłał zgodnie z wnioskiem bezpośrednio do sądu rejonowego, a także odpis skrócony aktu urodzenia, który został odebrany przez osobę działającą w imieniu wnioskodawcy.

Przepisy szczególne

Badając sprawę, Prezes UODO wziął pod uwagę przepisy, które regulują działanie urzędu stanu cywilnego, tj. ustawy z dnia 28 listopada 2014 r. – Prawo o aktach stanu cywilnego. Zgodnie z jej art. 45 ust. 1 i 3, odpis aktu stanu cywilnego i zaświadczenie o zamieszczonych lub niezamieszczonych w rejestrze stanu cywilnego danych dotyczących wskazanej osoby wydaje się osobie, której akt dotyczy, lub jej małżonkowi, wstępnemu, zstępnemu, rodzeństwu, przedstawicielowi ustawowemu, opiekunowi, osobie, która wykaże w tym interes prawny, sądowi, prokuratorowi, organizacjom społecznym, jeżeli jest to zgodne z ich celem statutowym i przemawia za tym interes społeczny, oraz organom administracji publicznej, w tym podmiotom, o których mowa w art. 5a ust. 1, Służbie Ochrony Państwa, Policji, Straży Granicznej i Służbie Więziennej, a także Żandarmerii Wojskowej, jeżeli jest to konieczne do realizacji ich ustawowych zadań.

Odpis skrócony aktu stanu cywilnego może być wydany z rejestru stanu cywilnego organom administracji publicznej, w tym podmiotom, o których mowa w art. 5a ust. 1, Zakładowi Ubezpieczeń Społecznych, Kasie Rolniczego Ubezpieczenia Społecznego, sądowi i prokuratorowi, do prowadzonych przez niepostępowań, za pośrednictwem usług sieciowych.

Orzecznictwo

Organ ds. ochrony danych osobowych wziął pod uwagę również orzecznictwo, m.in. wyrok Wojewódzkiego Sądu Administracyjnego w Szczecinie z 23 maja 2019 r. (sygn. akt II SA/Sz 343/19). Sąd orzekł w nim, że „co zaś tyczy się kwestii legalności udostępnia-

nia danych przez USC to samo wydawanie odpisów z aktów stanu cywilnego odbywa się na podstawie artykułu 45 ust. 1 ustawy z 28.11.2014 r. – Prawo o aktach stanu cywilnego (Dz.U. z 2020 r. poz. 463) określającego jako uprawnioną osobę, której akty dotyczą. W związku z faktem, iż wydawanie odpisów należałoby uznać za czynność prawną to zgodnie z artykułem 95 § 1 ustawy z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2019 r. poz. 1145) – dalej k.c. można jej dokonać również poprzez przedstawiciela. Umocowanie do działania w cudzym imieniu może opierać się na pełnomocnictwie (artykuł 96 k.c.)".

Odmowa uwzględnienia wniosku

Wobec powyższego Prezes UODO uznał, że w zakresie udostępnienia skróconego odpisu aktu małżeństwa, jeżeli żądanie udostępnienia danych nie wynika wprost z przepisów prawa materialnego, należy wskazać wiarygodną potrzebę posiadania odpisu poprzez dołączenie dokumentu, z którego wynika obowiązek jego posiadania. Takim dokumentem jest wezwanie sądu do dostarczenia odpisu dokumentu konkretnie wskazanego przez sąd.

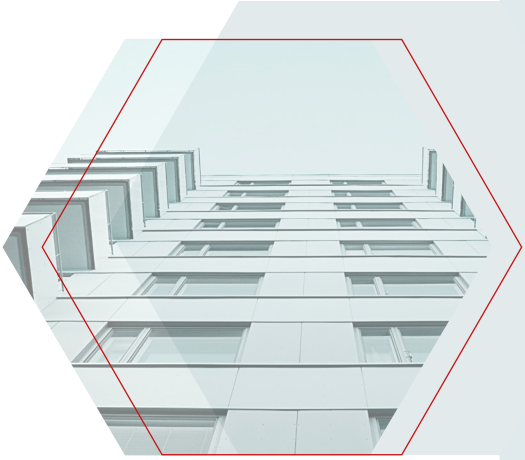
Co do przekazania skróconego aktu urodzenia, to w ocenie Prezesa UODO, również został wykazany interes prawny na mocy art. 45 Prawa o aktach stanu cywilnego. Dokument ten miał bowiem stanowić dowód w postępowaniu spadkowym.

W wydanej w tej sprawie decyzji organ ds. ochrony danych osobowych zaznaczył też, iż w obu przypadkach wystawione były stosowne upoważnienia do odbioru dokumentów.

Uznał więc, że kierownik USC działał w granicach i na podstawie prawa, przetwarzając dane osobowe w zakresie niezbędnym dla realizacji zadań i obowiązków wynikających z wiążących przepisów. Dlatego odmówił uwzględnienia wniosku skarżących.

PRÓBY DYSCYPLINOWANIA WŁAŚCICIELI DO PODAWANIA FAKTYCZNEJ LICZBY OSÓB MIESZKAJĄCYCH W DANYM LOKALU

Nieuprawnione jest umieszczenie na poszczególnych klatkach schodowych zbiorczej informacji o liczbie osób mieszkających w danym lokalu, która jest m.in. podstawą do obliczenia zaliczki na poczet opłaty za wywóz nieczystości.



W związku z tym, iż niektórzy właściciele zaniżają liczbę osób faktycznie mieszkających w danym lokalu, jedna ze wspólnot mieszkaniowych rozważała, czy możliwe jest wywieszenie na klatce schodowej zbiorczej listy, która nie zawiera niczyich imion i nazwisk, lecz jedynie numer lokalu i liczbę osób zgłoszonych jako w nim mieszkające. Taka praktyka byłaby jednak nieuprawniona.

Biorąc pod uwagę to, że zgodnie z art. 4 pkt 1 RODO, dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"), w ocenie organu ds. ochrony danych osobowych, wywieszenie listy zawierającej numer lokalu i liczbę mieszkających w nim osób zgłoszonych do obliczenia zaliczki na poczet opłaty za wywóz nieczystości stanowiłoby przetwarzanie danych osobowych naruszające jednocześnie prawo do prywatności.
Takie działanie nie znajdowało by też podstawy prawnej w przepisach prawa, na podstawie których działają wspólnoty mieszkaniowe (tj. ustawy z dnia 24 czerwca 1994 r. o własności lokali, a w zakresie w niej nieuregulowanym – ustawy z dnia 23 kwietnia 1964 r. Kodeks cywilny).

Urząd Ochrony Danych Osobowych od lat konsekwentnie prezentuje stanowisko, że brak jest podstaw prawnych do udostępniania (np. poprzez wywieszanie w gablotach informacyjnych na klatkach schodowych czy w innych miejscach dostępnych dla nieograniczonego kręgu osób) takich informacji, które wskazują na ewentualne zaległości w opłatach. Informacje

te stanowią dane osobowe i muszą być przetwarzane z poszanowaniem zasad określonych w RODO, w tym legalizmu, minimalizacji danych oraz ograniczenia celu przetwarzania.

Pierwsza z wymienionych zasad stanowi, że dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (art. 5 ust. 1 lit. a RODO). Zgodnie z zasadą minimalizacji danych (art. 5 ust. 1 lit. c RODO), administrator powinien przetwarzać tylko takiego rodzaju dane osobowe, które są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Zasada ograniczenia celu (art. 5 ust. 1 lit. b RODO) przesądza zaś, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami.

Zatem wspólnota mieszkaniowa powinna przetwarzać tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na wskazany cel zbierania danych. Nie powinna również podejmować działań, które w istocie polegają na weryfikacji posiadanych danych przez ogół lokatorów, z których nie wszyscy mogą być członkami wspólnoty mieszkaniowej uprawnionymi (na mocy art. 27 ustawy o własności lokali) do współdziałania w zarządzie nieruchomością wspólną.

PASZPORT DOZYMETRYCZNY BEZ MIEJSCA URODZENIA

Państwowa Agencja Atomistyki – na skutek uwag Prezesa UODO – rezygnuje z przetwarzania w paszporcie dozymetrycznym, czyli w dokumencie pracowników delegowanych wykonujących zadania na rzecz pracodawcy zewnętrznego w warunkach narażenia na promieniowanie jonizujące, danych w postaci miejsca urodzenia.

Wśród pracowników zawodowo narażonych na promieniowanie jonizujące szczególną grupę, która musi być objęta kontrolą dawek indywidualnych, stanowią tzw. pracownicy zewnętrzni. Są to osoby prowadzące działalność na własny rachunek lub zatrudnione przez pracodawcę zewnętrznego na terenie, do którego dostęp jest kontrolowany i objęty specjalnymi przepisami mającymi na celu ochronę przed promieniowaniem jonizującym lub rozprzestrzenianiem skażeń promieniotwórczych. To one muszą być wyposażone w indywidualny dokument narażenia na promieniowanie jonizujące – tzw. paszport dozymetryczny.

Projektowane zmiany w prawie krajowym

W ostatnim okresie, ze względu na konieczność wdrożenia do prawa krajowego postanowień dyrektywy Rady 2013/59/Euratom z dnia 5 grudnia 2013 r. ustanawiającej podstawowe normy bezpieczeństwa w celu ochrony przed zagrożeniami wynikającymi z narażenia na działanie promieniowania jonizującego, Prezes Państwowej Agencji Atomistyki zwrócił się do Prezesa UODO o zaopiniowanie wprowadzającego je projektu rozporządzenia Rady Ministrów w sprawie ochrony przed promieniowaniem jonizującym pracowników zewnętrznych narażonych podczas pracy na terenie kontrolowanym lub nadzorowanym.

W jego przepisach przewidywano, że paszport dozymetryczny, który pracownikowi zewnętrznemu wydaje Prezes Państwowej Agencji Atomistyki, będzie zawierał: imię i nazwisko, płeć, adres, datę i miejsce urodzenia oraz PESEL, a w przypadku cudzoziemca numer paszportu albo innego dokumentu potwierdzającego tożsamość pracownika.

Uwagi Prezesa UODO

Po analizie projektu Prezes UODO zwrócił uwagę, że w załączniku nr X dyrektywy został wskazany katalog danych, jakie powinien zawierać dokument poświadczający indywidualny monitoring radiologiczny.

Nie ma wśród nich danej w postaci miejsca urodzenia. Dlatego wskazał, że jej przetwarzanie stanowiłoby naruszenie zasady minimalizacji danych wyrażonej w art. 5 ust. 1 lit. c RODO i zwrócił się o stosowną zmianę projektowanych przepisów.

Nowa wersja projektu rozporządzenia

W najnowszej wersji projektu rozporządzenia postanowiono zrezygnować z umieszczania w paszporcie dozymetrycznym daty urodzenia. Tym samym Prezes UODO uznał opiniowany projekt rozporządzenia za uzgodniony.

JAK POSTĘPOWAĆ Z KORESPONDENCJĄ SKAZANYCH

Skazany funkcyjny nie powinien mieć dostępu do korespondencji innych skazanych przebywających w zakładzie karnym. Korespondencję adresowaną do skazanego doręcza mu wyznaczony funkcjonariusz lub pracownik, a jeżeli korespondencja podlega cenzurze lub nadzorowi, doręcza się ją po dokonaniu tych czynności.

Kwestię odbierania i dostarczania korespondencji skazanym należy rozpatrywać zarówno z uwzględnieniem przepisów ustawy z 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, jak i przepisów szczególnych, w tym rozporządzenia ministra sprawiedliwości z dnia 21 grudnia 2016 r. w sprawie regulaminu organizacyjno-porządkowego wykonywania kary pozbawienia wolności.

Korespondencję doręcza skazanemu wyznaczony funkcjonariusz lub pracownik

Rozdział 5 tego rozporządzenia określa m.in. organizację przyjmowania korespondencji. Wskazuje, że korespondencję skazanego administracja zakładu karnego przyjmuje w każdym dniu roboczym, a korespondencję urzędową – codziennie (§ 16 ust. 1). Przesądza, że w przypadku wysyłania przesyłki poleconej, wraz z korespondencją skazany przekazuje wypełniony druk „potwierdzenia nadania przesyłki poleconej", który po wysłaniu zwraca się skazanemu (§ 16 ust. 3). Stanowi też, że w zakładzie karnym typu zamkniętego skazany przekazuje korespondencję do wysłania w sposób umożliwiający jej cenzurę, a w zakładzie karnym typu półotwartego wówczas, gdy dyrektor zarządził cenzurowanie korespondencji (§ 16 ust. 4). Zgodnie natomiast z § 19 powołanego rozporządzenia, korespondencję adresowaną do skazanego doręcza mu wyznaczony funkcjonariusz lub pracownik, a jeżeli korespondencja podlega cenzurze lub nadzorowi, doręcza się ją po dokonaniu tych czynności (ust. 2).

Zadania skazanych funkcyjnych

Wymienione przepisy nie umocowują więc skazanego funkcyjnego do dostępu do korespondencji innych skazanych. Jak bowiem stanowi § 6 ust. 1 powołanego rozporządzenia ministra sprawiedliwości, dyrektor zakładu może wyznaczyć skazanych funkcyjnych do wykonywania zadań związanych z zatrudnieniem, zajęciami kulturalno-oświatowymi i sportowymi. Wśród tych zadań nie ma spraw związanych z korespondencją.

Tajemnica korespondencji i jej ograniczenia

Istotne dla takiego rozstrzygnięcia tej kwestii jest także to, że tajemnica korespondencji jest dobrem osobistym chronionym m.in. przepisami Konstytucji RP (art. 49), Kodeksu cywilnego (art. 23) czy ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (art. 41). Może ono zostać ograniczone przepisami rangi ustawowej.

Ich przykładem jest art. 8a § 1 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny wykonawczy (Kkw). Stanowi on, że korespondencja skazanego pozbawionego wolności podlega cenzurze i nadzorowi, chyba że ustawa stanowi inaczej. Przykładem wyjątków od tej zasady może być korespondencja prowadzona z obrońcą lub pełnomocnikiem będącym adwokatem lub radcą prawnym

czy prowadzona z organami ścigania, wymiaru sprawiedliwości i innymi organami państwowymi, organami samorządu terytorialnego, Rzecznikiem Praw Obywatelskich, Rzecznikiem Praw Dziecka, organami powołanymi na podstawie ratyfikowanych przez Rzeczpospolitą Polską umów międzynarodowych dotyczących ochrony praw człowieka oraz przedstawicielem niebędącym adwokatem ani radcą prawnym, który został zaaprobowany przez Przewodniczącego Izby Europejskiego Trybunału Praw Człowieka do reprezentowania skazanego przed tym Trybunałem (art. 8a § 2 i 3). Cenzurze nie podlega również korespondencja skazanych przebywających w zakładach typu otwartego (art. 92 pkt 13 Kkw), natomiast może zostać wprowadzona przez dyrektora w zakładzie typu półotwartego (art. 91 pkt 10 Kkw). Jest jednak obowiązkowa w zakładach zamkniętych (art. 90 pkt 8 Kkw). Jak wskazuje art. 242 Kkw, przez pojęcie nadzoru nad korespondencją rozumie się otwarcie listu i sprawdzenie jego zawartości, natomiast jej cenzura, to zapoznawanie się z treścią pisma oraz usunięcie części jego tekstu lub uczynienie go nieczytelnym.

Skazany nie zawsze może więc skorzystać z ochrony tajemnicy korespondencji, jednak dostęp do niej mogą mieć jedynie uprawnione osoby. Nie ma wśród nich skazanych funkcyjnych.

REALIZACJA AUTONOMICZNYCH UPRAWNIEŃ KONTROLNYCH RADNEGO

Radny, realizując swoje szczególne uprawnienia kontrolne, o których mowa w art. 24 ust. 2 ustawy o samorządzie gminnym, może uzyskać dostęp do danych osobowych jedynie w zakresie niezbędnym do realizacji celu określonego w tych przepisach.

Dla zapewnienia właściwej ochrony danych osobowych przetwarzanych w związku z realizacją autonomicznych uprawnień kontrolnych radnego istotne jest ustalenie, kto jest ich administratorem.

Zgodnie 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". Zatem dla ustalenia, czy dany podmiot można uznać za administratora, istotna jest więc jego samodzielność w podejmowaniu decyzji o celach i sposobach przetwarzania danych.

W przypadku podmiotów szeroko rozumianego sektora publicznego podmiot będący administratorem może być wskazany w konkretnym przepisie prawa. Jednak najczęściej ma miejsce sytuacja, w której rola ta wynika z charakteru, kompetencji lub i zakresu zadań publicznych, przyznanych mu tymi przepisami. Wskazuje na to Grupa Robocza Art. 29 w opinii 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający". Jednocześnie w dokumencie tym podkreśla się, że stosowanie pojęcia administratora staje się coraz bardziej złożone, ze względu na zróżnicowanie form prawnych oraz organizacyjnych różnych podmiotów, które faktycznie decydują o celach i środkach przetwarzania.

Radny też może być administratorem

Radny, realizując zadania na rzecz rady gminy, nie będzie administratorem. Jest wówczas bowiem częścią organu kolegialnego, jakim jest rada gminy. W takim przypadku to ona w związku z wykonywaniem swoich zadań ma status administratora.

Z inną sytuacją mamy do czynienia wówczas, gdy radny wykonuje swoje autonomiczne uprawnienia kontrolne, o których mowa w art. 24 ust. 2 ustawa z dnia 8 marca 1990 r. o samorządzie gminnym. Zgodnie z tym przepisem, „w wykonywaniu mandatu radnego radny ma prawo, jeżeli nie narusza to dóbr osobistych innych osób, do uzyskiwania informacji i materiałów, wstępu do pomieszczeń, w których znajdują się te informacje i materiały, oraz wglądu w działalność urzędu gminy, a także spółek z udziałem gminy, spółek handlowych z udziałem gminnych osób prawnych, gminnych osób prawnych, oraz zakładów, przedsiębiorstw i innych gminnych jednostek organizacyjnych, z zachowaniem przepisów o tajemnicy prawnie chronionej". Zatem realizując owe uprawnienia, radny będzie odrębnym administratorem, gdyż to on będzie ustalał cele i sposoby przetwarzania danych osobowych pozyskanych w związku z tego typu swoją aktywnością.

Ograniczenia w udostępnianiu informacji

Warto jednak podkreślić, że ustawodawca w art. 24 ust. 2 ustawy o samorządzie gminnym jednoznacznie ograniczył uzyskiwanie informacji i materiałów przez radnego do sytuacji, gdy nie narusza to dóbr osobistych innych osób. Prawo do ochrony danych osobowych bez wątpienia mieści się w tym pojęciu.

Administratorzy zobowiązani do udostępnienia informacji i materiałów radnemu muszą więc podjąć wszelkie czynności, by w takich przypadkach udostępnienie nie obejmowało informacji naruszających dobra osobiste osób fizycznych. Jedną z takich czynności może być m.in. anonimizacja danych osobowych zawartych w udostępnianych dokumentach.

Jednocześnie warto przypomnieć, że zgodnie z zasadą minimalizacji danych określoną w 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. Radny może więc uzyskać dostęp do danych osobowych jedynie w zakresie niezbędnym do wykonania celu realizowanego na podstawie art. 24 ust. 2 ustawy o samorządzie gminnym.

W czasie udostępniania radnemu pomieszczeń administratorzy muszą wprowadzić takie procedury, które pozwolą radnemu zrealizować jego uprawnienia, a jednocześnie zapewnią właściwą ochronę danych osobowych i dóbr osobistych osób fizycznych. Przykładowo, radny, któremu udostępniono pomieszczenia urzędu gminy, nie powinien mieć możliwości wglądu w ekrany komputerów urzędników przetwarzających dane osobowe interesantów.

Procedury dotyczące obsługi technicznej i bezpieczeństwa danych osobowych

W zakresie wykonywania swoich autonomicznych kompetencji radny jako administrator ma obowiązek realizować wszystkie obowiązki wynikające z RODO. Należy jednak podkreślić, że organ wykonawczy gminy, czyli wójt, burmistrz lub prezydent miasta, sprawując pieczę nad prawidłowością przetwarzania danych osobowych w gminie, będzie w zakresie obsługi technicznej i bezpieczeństwa danych osobowych ich administratorem. Organ ten powinien wypracować jednolite praktyki w tym zakresie także dla rady gminy oraz radnych, m.in. na potrzeby realizacji przez nich ich autonomicznych zadań, i wpisać je w ogólną koncepcję przetwarzania danych obowiązującą w danej gminie. Powinny znaleźć się w niej m.in. wskazówki dotyczące archiwizowania dokumentacji, która powstała w związku z wykonywaniem mandatu radnego (także tej wytworzonej w związku ze stosowaniem przez radnego art. 24 ust. 2 ustawy o samorządzie gminnym) czy też zalecenia korzystania przez radnych ze służbowych (a nie prywatnych) środków komunikacji (takich jak służbowy telefon lub służbowa poczta elektroniczna). Wypracowanie i wdrożenie tego typu rozwiązań powinno przyczynić się do zapewnienia lepszej ochrony danych osobowych (np. przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem lub zniszczeniem). W niektórych gminach, w związku z przyjętymi rozwiązaniami, administratorem w zakresie bezpieczeństwa przetwarzania danych może być również w pewnym zakresie rada gminy.

W zakresie wykonywania swoich autonomicznych kompetencji radny jako administrator ma obowiązek realizować wszystkie obowiązki wynikające z RODO.

Wsparcie IOD

W wypracowaniu i stosowaniu w danej gminie kompleksowej koncepcji przetwarzania danych ważną rolę ma do odegrania inspektor ochrony danych (IOD), którego zadaniem – zgodnie z art. 39 ust. 1 lit. a RODO – jest informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie. Do jego zadań, stosownie do art. 39 ust. 1 lit. b RODO, należy również monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

MIĘDZYNARODOWE

EIOD radzi, jak zapewnić bezpieczeństwo danych podczas pracy zdalnej/telepracy

Europejski Inspektor Ochrony Danych (EIOD) wydał wytyczne dla instytucji UE jako pracodawców, odpowiadając na ich problemy związane z zapewnieniem bezpieczeństwa podczas pandemii COVID-19.

W dokumencie podniesiono kwestie związane z narzędziami telepracy, zarządzaniem personelem czy danymi dotyczącymi zdrowia. Powstanie takich wytycznych jest uzasadnione tym bardziej ze względu na fakt, że telepraca prawdopodobnie pozostanie częścią „nowej rzeczywistości".

Zalecenia EIOD dotyczą m.in przetwarzania i minimalizacji danych, zatrzymywania i przekazywania danych, w szczególności w przypadku polegania na zewnętrznych dostawcach niektórych produktów lub usług. Ponadto EIOD dodaje, że zapewnienie bezpieczeństwa danych wymaga współpracy działów IT, inspektorów ochrony danych (IOD) i wszystkich użytkowników.

Poniżej przedstawiamy wybrane wskazówki dotyczące zapewnienia odpowiedniego stopnia ochrony danych podczas telepracy czy pracy zdalnej, na którą zapotrzebowanie wzrosło podczas pandemii COVID-19, np. połączeń konferencyjnych, współpracy zdalnej, wideokonferencji lub webinariów.

Proces podejmowania decyzji

Nie wolno lekceważyć wymogów ochrony danych i bezpieczeństwa tychże podczas poszukiwania odpowiednich narzędzi telepracy. Przy planowaniu wdrożenia takich narzędzi trzeba wziąć pod uwagę ryzyko naruszenia ochrony danych oraz możliwe do wprowadzenia zabezpieczenia. Trzeba dokonywać przeglądu używanych narzędzi, oceniać ich funkcje związane z bezpieczeństwem, poufnością i zapewnieniem prywatności. W ten proces należy zaangażować IOD oraz dział IT.

Urządzenia firmowe i prywatne

Zapewniając sprzęt firmowy, należy pamiętać o przestrzeganiu zasad przetwarzania danych osobowych oraz zapewnić odpowiedni poziom bezpieczeństwa związany m.in. z systemami IT.

Jednak przy świadczeniu pracy zdalnej wykorzystywane są także urządzenia prywatne. Zaleca się, aby przed rozpoczęciem korzystania przez pracownika z prywatnych urządzeń do telepracy (laptopów, tabletów itp.) skonsultowano się z działem IT w celu identyfikacji potencjalnych zagrożeń wynikających z użytkowania takiego sprzętu oraz odpowiednich pod kątem bezpieczeństwa ustawień systemowych. Tam, gdzie dane osobowe będą przetwarzane na urządzeniach osobistych, instytucja powinna przedstawić ich użytkownikom jasne zasady i instrukcje, jak postępować z tymi danymi osobowymi.

Role administratora i podmiotu przetwarzającego

Opierając się na zewnętrznych dostawcach nowych produktów lub usług, instytucje unijne powinny zawsze dążyć do uprzywilejowania najbardziej przyjaznych dla prywatności narzędzi i zapewnienia odpowiedniej kontroli nad sposobem, w jaki zewnętrzni dostawcy będą postępować z powierzonymi im danymi.

Przy podpisywaniu umowy z podmiotem przetwarzającym należy upewnić się, że role administratora i podmiotu przetwarzającego zostały precyzyjnie określone oraz że postanowienia umowne obejmują wszystkie obowiązkowe elementy wynikające z art. 29 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki

organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (dalej: rozporządzenia 2018/1725), np. posiadanie wszystkich niezbędnych informacji dotyczących podwykonawców, o których mowa w umowie.

Przetwarzanie danych w UE/EOG i przekazywanie danych

Jeśli instytucja współpracuje z zewnętrznym dostawcą, należy sprawdzić czy podmiot ten ma jednostkę organizacyjną w UE/EOG oraz, czy usługi oferowane przez ten podmiot wiążą się z przekazywaniem danych osobowych poza UE/EOG, w tym do celów, takich jak np. tworzenie kopii zapasowych itp. Jeśli tak jest, istotna jest weryfikacja, czy dostawca usług wdrożył odpowiednie zabezpieczenia. Jeśli dostawca zewnętrzny nie ma jednostki organizacyjnej w UE/EOG i nie podlega decyzji stwierdzającej odpowiedni stopień ochrony z art. 45 RODO, należy uzyskać odpowiednie zabezpieczenia zgodnie z art. 48 rozporządzenia 2018/1725.

Funkcjonalności monitorowania przez pracodawcę lub dostawcę usług

Praca zdalna i wykorzystywane do niej narzędzia, np. do wideokonferencji, często pozwalają na dodatkowe monitorowanie personelu. Domyślnie nie powinno dochodzić do takiego monitorowania.
W przypadku monitorowania przez dostawcę usług należy sprawdź opis jego usług i upewnić się, że nie jest prowadzony monitoring, a także – w razie konieczności – uzyskać dodatkowe zabezpieczenia umowne.

Jeśli wymagane jest monitorowanie przez pracodawcę, trzeba skonfigurować narzędzia w taki sposób, aby nie dochodziło do zbierania danych oraz w sposób przejrzysty zakomunikować to pracownikom. Trzeba ocenić, czy zastosowane środki są proporcjonalne do celu, który ma zostać osiągnięty. Należy pamiętać, że praca zdalna może być wykonywana przez pracownika przy użyciu prywatnego urządzenia. Wtedy przestrzeń domowa i prywatność pracowników nie powinny być naruszane.

Przykładowo, narzędzia wideokonferencyjne zwykle pozwalają na nagrywanie spotkań. Podczas nagrywania należy postępować tak samo, jak w przypadku spotkań osobistych: zwykle będzie to wymagało uzyskania zgody osób, które będą nagrywane.

Zatrzymywanie danych

Należy upewnić się, że wszelkie nowe narzędzia są skonfigurowane z odpowiednimi okresami zatrzymywania danych zgodnie z celem przetwarzania danych. W przypadku dostawców zewnętrznych należy uzyskać jasne i wiążące zobowiązanie, że informacje dotyczące instytucji są do niej zwracane lub usuwane po zakończeniu umowy.

Bezpieczeństwo danych

Pracodawca musi podjąć niezbędne środki w celu zapewnienia poufności, integralności i dostępności danych osobowych przetwarzanych za pomocą różnych narzędzi komunikacji elektronicznej: komunikatorów internetowych, narzędzi do współpracy online, poczty internetowej, narzędzi wideokonferencyjnych itp. Pracodawca musi na bieżąco zwiększać świadomość pracowników na temat typowych źródeł naruszeń danych, takich jak rosnąca liczba ataków typu „spoofing", ataków phishingowych oraz z wykorzystaniem inżynierii społecznej przy pomocy komunikatów związanych z COVID-19. Ponadto w ostatnim czasie pojawiły się doniesienia o atakowaniu narzędzi do konferencji online, w wyniku których hakerzy uzyskali nieautoryzowany dostęp do rozmów i wysyłali wiadomości phishingowe w celu kradzieży danych.

Źródło: https://edps.europa.eu/sites/edp/files/publication/20-07-15_edps_guidelines_remote_work_en.pdf

Belgowie nakładają karę za nieprzestrzeganie prawa do bycia zapomnianym

Belgijski organ nadzorczy (APD) nałożył na Google Belgium karę pieniężną w wysokości 600 tys. euro za nieprzestrzeganie prawa do bycia zapomnianym, po tym jak przedsiębiorstwo Google odrzuciło wniosek skarżącego obywatela o wyrejestrowanie przestarzałych artykułów, które szkodzą jego reputacji.

Kara nałożona na Google jest najwyższą w historii belgijskiego organu nadzorczego. Wcześniej najwyższa kara nałożona przez izbę ds. skarg wynosiła 50 tys. euro.

Wniosek o usunięcie odnośników do stron internetowych z Google Belgium

Skarżący, który ze względu na swoje stanowisko odgrywa rolę w życiu publicznym w Belgii, złożył w Google Belgium wniosek o usunięcie wyników wyszukiwania powiązanych z jego nazwiskiem w wyszukiwarce (tzw. de-referencing). Część stron, które chciałby w ten sposób usunąć, dotyczy ewentualnej politycznej przynależności, od której się odcina; druga część odnosiła się do skargi o molestowanie, którą wiele lat temu uznano za bezpodstawną.

Prawo do bycia zapomnianym

Jeżeli chodzi o strony dotyczące przynależności politycznej, izba ds. skarg belgijskiego organu nadzorczego uznała, że biorąc pod uwagę rolę skarżącego w życiu publicznym, utrzymanie ich odnośników jest konieczne w interesie publicznym i tym samym orzekła na korzyść Google.

W odniesieniu do stron dotyczących skargi o molestowanie przeciwko skarżącemu, APD uważa, że wniosek o usunięcie odniesienia jest uzasadniony i że Google wykazało poważne naruszenie, odrzucając go. Ponieważ fakty nie zostały ustalone, są stare i prawdopodobnie będą miały poważne reperkusje dla skarżącego, prawa i interesy osoby objętej postępowaniem muszą przeważać. Według izby ds. skarg Google dopuściło się szczególnego zaniedbania, ponieważ firma ta posiadała dowody, że fakty te były nieistotne i nieaktualne.

Hielke Hijmans, przewodniczący izby ds. skarg: „W prawie do bycia zapomnianym należy znaleźć właściwą równowagę między prawem dostępu społeczeństwa do informacji z jednej strony, a prawami i interesami zainteresowanej osoby z drugiej strony. Podczas gdy niektóre z artykułów przytoczonych przez skarżącego mogą być uznane za niezbędne dla prawa do informacji, inne, które odnoszą się do niepotwierdzonych aktów molestowania, sprzed około 10 lat, powinny być możliwe do zapomnienia. Utrzymując linki dostępne za pośrednictwem jego wyszukiwarki internetowej, powszechnie używane przez internautów, które mogą znacząco zaszkodzić reputacji skarżącego, Google wykazało wyraźne zaniedbanie”.

Kara pieniężna: 600 tys. euro

W związku z tym belgijski organ nadzorczy nałożył na Google karę pieniężną w wysokości 600 tys. euro: za brak usunięcia stron zgłaszających nieaktualną skargę przeciwko skarżącemu, za nieprzekazanie skarżącemu informacji uzasadniającej odmowę usunięcia oraz za brak przejrzystości w formularzu usunięcia zaproponowanym przez Google.

Nakazano również Google zaprzestać umieszczania odnośników do tych stron w Europejskim Obszarze Gospodarczym i dostosować swoje formularze wniosków o usunięcie z wykazu w celu zapewnienia większej jasności co do tego, które podmioty są odpowiedzialne za przetwarzanie danych.

Kompetencje APD w stosunku do Google Belgium

W tym przypadku Google argumentowało, że skarga jest bezpodstawna, ponieważ została wniesiona przeciwko Google Belgium, mimo że administratorem nie jest belgijski podmiot zależny Google, lecz Google LLC, z siedzibą w Kalifornii.

Izba ds. skarg nie przyjęła tego argumentu. Jej zdaniem działalność Google Belgium i Google LLC jest nierozerwalnie związana, i w związku z tym belgijski podmiot zależny może zostać pociągnięty do odpowiedzialności. Ma to kluczowe znaczenie dla zapewnienia skutecznej i wszechstronnej ochrony RODO, ponieważ nie jest łatwo krajowemu organowi w Europie sprawować skuteczną kontrolę i nakładać sankcje na przedsiębiorstwo znajdujące się w Stanach Zjednoczonych.

Z drugiej strony, izba ds. skarg przychyliła się do stanowiska Google, argumentującego, że główna jednostka organizacyjna w Europie (Google Ireland) nie jest odpowiedzialna za usuwanie danych ze strony.

Źródło: https://www.autoriteprotectiondonnees.be/publications/decision-quant-au-fond-n-37-2020.pdf

Włochy: niezamówiona korespondencja marketingowa jednym z powodów nałożenia kary

Włoski organ nadzorczy nałożył karę w wysokości prawie 17 mln euro na operatora telefonii Wind Tre SpA w związku z niezgodnym z prawem przetwarzaniem danych osobowych do celów marketingowych przedsiębiorstwa.

Do włoskiego organu nadzorczego wpłynęły skargi użytkowników w związku z niezamawianą komunikacją marketingową, przekazywaną bez zgody osób skarżących poprzez wiadomości tekstowe, e-maile, faksy i automatyczne połączenia telefoniczne. Ponadto skarżący oświadczali, że nie umożliwiono im wykonywania przysługujących im praw do wycofania zgody lub sprzeciwu wobec przetwarzania danych w celach marketingowych.

W innych przypadkach złożonych na podmiot skarg, dotyczyły one zamieszczania w publicznych wykazach telefonicznych danych osobowych użytkowników, którzy składali sprzeciw do przetwarzania danych.

Przeprowadzone postępowanie ujawniło, że aplikacje MyWind i My3 zostały skonfigurowane w taki sposób, by wymagać od użytkownika zgody na przetwarzanie danych do różnych celów w tym marketingu, profilowania, przekazywania danych stronom trzecim, wzbogacania danych i geolokalizacji przy każdym dostępie do aplikacji, a wycofanie takiej zgody było dozwolone po 24 godzinach.

Źródło: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9435901#english

Holenderski organ nadzorczy nałożył karę za pobieranie opłat za wykonywanie prawa dostępu do danych

Krajowy Rejestr Kredytowy (BKR) w Holandii nie może pobierać opłat od osób, które chcą uzyskać dostęp do swoich danych osobowych przetwarzanych w rejestrze. Za dotychczasową praktykę holenderski organ nadzorczy nałożył na BKR administracyjną karę pieniężną w wysokości 830 tys. euro.

BKR pobierał opłaty od osób, których dane dotyczą, w zamian za dostęp do ich danych w formacie cyfrowym. Co prawda mogły one uzyskać bezpłatną papierową kopię swoich danych, ale tylko raz w roku. Sytuacja ta stanowiła naruszenie przepisów ochrony danych osobowych.

W następstwie postępowania ukarany podmiot zmienił swoje procedury, które obecnie pozwalają na bezpłatne uzyskanie dostępu do przetwarzanych danych osobowych.

Źródło: https://edpb.europa.eu/news/national-news/2020/national-credit-register-bkr-fined-personal-data-access-charges_pl

EDUKACJA

Nabór do XI edycji programu edukacyjnego „Twoje dane - Twoja sprawa"

Zapraszamy szkoły i placówki oświatowe do uczestnictwa w XI edycji Ogólnopolskiego Programu Edukacyjnego „Twoje dane Twoja sprawa. Skuteczna ochrona danych osobowych. Inicjatywa edukacyjna skierowana do uczniów i nauczycieli", który odbywać się będzie w trakcie roku szkolnego 2020/2021.

Program „Twoje dane – Twoja sprawa" od wielu lat stanowi inspirację dla nauczycieli, uczniów i rodziców, którzy biorąc w nim udział, pokazują, w jaki sposób od najmłodszych lat można uczyć dzieci zasad ochrony danych osobowych, przekazując trudne treści podczas lekcji, pogadanek oraz przy wykorzystaniu gier i zabaw. Konkursy dla uczniów i szkół, specjalistyczne webinaria dla nauczycieli, wojewódzkie spotkania z cyklu "#RODO w Edukacji" czy poznawanie zasad ochrony danych osobowych poprzez podejmowanie inicjatyw edukacyjnych, w tym zwłaszcza tych, które realizowane są z okazji Dnia Ochrony Danych Osobowych – to doceniane przez szkoły i placówki edukacyjne działania.

W czasie trwania XI edycji uczniowie i nauczyciele będą systematycznie otrzymywać także porady nt. bezpieczeństwa danych osobowych w wirtualnym świecie, opracowane przez ekspertów UODO w formie pigułek wiedzy. Będą to krótkie i użyteczne wskazówki, podane w atrakcyjnej formie graficznej, dostarczającej wiedzy potrzebnej do świadomego korzystania z nowoczesnych urządzeń i programów komputerowych, a także aplikacji mobilnych, przeznaczonych do nauki i rozrywki.

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

Więcej informacji na temat Programu znajdą Państwo na stronie UODO: https://uodo.gov.pl/pl/21/32

Aby zgłosić uczestnictwo szkoły lub placówki oświatowej do Programu, należy 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 do pism w postępowaniu administracyjnym należy dołączać „rozdzielniki"?
Jaka jest podstawa do przetwarzania przez poradnie psychologiczne szczególnych kategorii danych?
Czy związek zawodowy może mieć dostęp do danych z wniosków o przyznanie świadczeń z ZFŚS?
Kto jest administratorem danych osobowych przetwarzanych w urzędzie wojewódzkim?
Jaki jest status WIOŚ w związku z wizyjnym systemem kontroli składowisk odpadów?
Czy w celu wytworzenia legitymacji należy skorzystać z powierzenia przetwarzania?