URZĄD OCHRONY DANYCH OSOBOWYCH

BIULETYN UODO
NUMER SPECJALNY

Materiały z archiwalnej strony UODO

z okresu 31.08.2018 r. – 12.05.2022 r.

https://uodo.gov.pl/

SPIS TREŚCI

WSTĘP 8

WYZNACZENIE I STATUS IOD 10

Czy zastępca IOD powinien być wyznaczony na stałe? 10

Czy dane kontaktowe IOD muszą być łatwo dostępne? 12

Czy administrator musi podać imię i nazwisko IOD na stronie internetowej? 13

Czy funkcję IOD można łączyć z wykonywaniem zawodu adwokata lub radcy prawnego? 14

Czy istnieje możliwość wyznaczenia osoby prawnej do sprawowania funkcji IOD? 15

Wyznaczenie IOD w straży gminnej (miejskiej) umiejscowionej w strukturze urzędu 16

Czy IOD musi odbyć szkolenie dla IOD oraz posiadać certyfikat potwierdzający jego odbycie? 16

Czy osoba spokrewniona z osobą zarządzającą może być IOD? 17

Brak jednostki organizacyjnej w UE a zgłoszenie IOD 17

Kto może, a kto musi wyznaczyć IOD na podstawie RODO? 18

Czy należy wyznaczyć IOD w niepublicznym zakładzie opieki zdrowotnej mając około 2 000 pacjentów? 22

W jaki sposób należy oceniać kwalifikacje osoby kandydującej do pełnienia funkcji IOD? 23

Czy IOD powinien być wyznaczany na podstawie takich samych kwalifikacji jak było w przypadku ABI? 25

Czy IOD może być pracownikiem administratora? 26

Czy członek zarządu stowarzyszenia może być w nim jednocześnie inspektorem ochrony danych? 26

Czy IOD może jednocześnie pełnić funkcję pełnomocnika do spraw ochrony informacji niejawnych? 27

Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji? 28

Czy możliwe jest łączenie funkcji IOD z obowiązkami administratora systemu informatycznego (ASI)? 29

Czy funkcję IOD może pełnić obcokrajowiec? 31

Czy funkcję IOD może pełnić osoba spoza organizacji administratora/podmiotu przetwarzającego? 31

Czy można powołać więcej niż jednego IOD? 32

Czy po wejściu stosowania RODO CUW może powołać jednego IOD dla wszystkich obsługiwanych jednostek? 32

Ile maksymalnie podmiotów będzie mógł obsługiwać jeden IOD? 33

Czy różni przedsiębiorcy niewchodzący w skład tej samej grupy mogą powołać jednego IOD? 34

Czy podmioty publiczne mogą powołać jednego IOD poza sytuacją uregulowaną w art. 37 ust. 3 RODO? 35

Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO? 36

Kto wysyła powiadomienie o odwołaniu inspektora ochrony danych w przypadku likwidacji administratora 41

Czy kierownik urzędu stanu cywilnego jest administratorem i czy musi wyznaczyć IOD? 42

Czy praca IOD może być kontrolowana? 44
Czy administrator jest zobowiązany na podstawie RODO do zapewnienia inspektorowi zespołu IOD? 45
Czy z zewnętrznym IOD należy zawrzeć umowę powierzenia? 47
Czy z zewnętrznym IOD wykonującym zadania dla banku należy zawrzeć umowę powierzenia? 52
Czy obowiązek z art. 38 ust. 2 RODO dotyczy administratora korzystającego z usług zewnętrznego IOD? 53
Czy można łączyć funkcję IOD z zadaniami związanymi z obsługą wniosków od sygnalistów? 55
Wyznaczenie IOD na podstawie ustawy wdrażającej dyrektywę policyjną (DODO) 58
Wyznaczenie IOD w sądach powszechnych 60
ZAWIADOMIENIA PREZESA UODO ZWIĄZANE Z IOD 63
Jak prawidłowo zawiadomić o wyznaczeniu/odwołaniu/zmianie danych IOD (zastępcy IOD)? 63
W jakim terminie należy dokonać zawiadomienia o wyznaczeniu/odwołaniu/zmianie danych IOD (zastępcy)? 64
Jaki formularz zawiadomienia wybrać? 64
Formularze zawiadomień IOD 65
Jak złożyć kwalifikowany podpis elektroniczny pod zawiadomieniem dotyczącym IOD? 66
Dlaczego (na biznes.gov.pl) przy wgrywaniu podpisanego pliku xml otrzymuję komunikaty o błędach? 66
Czy Urząd Ochrony Danych Osobowych potwierdza otrzymanie zawiadomienia? 66
Co zrobić w przypadku problemów technicznych związanych ze złożeniem zawiadomienia dotyczącego IOD? 66
Jak podpisać zawiadomienie dotyczące IOD przez więcej niż jedną osobę? 67
Czy można zawiadomić o IOD przez pełnomocnika? 67
Czy do zawiadomienia trzeba dołączyć pełnomocnictwo? 68
Jak powinno wyglądać pełnomocnictwo dla osoby zgłaszającej IOD? 68
W jakiej formie administrator/podmiot przetwarzający powinien udzielić pełnomocnictwa? 68
Co należy rozumieć przez formę elektroniczną pełnomocnictwa? 69
Jak skutecznie podpisać pełnomocnictwo w formie elektronicznej? 69
Czy od zawiadomienia składanego przez pełnomocnika należy uiścić opłatę? 69
Czy pełnomocnik powinien dołączyć do zawiadomienia potwierdzenie dokonania opłaty skarbowej? 70
Czy pełnomocnik ujawniony w CEIDG, może w imieniu tego podmiotu dokonać zawiadomienia? 70
Czy notariusz może uwierzytelnić elektronicznie pełnomocnictwo upoważniające do zawiadomienia? 70
Czy pełnomocnik powinien weryfikować prawidłowość przesłanego przez niego zawiadomienia? 71
Jak ocenić, czy przesłane zawiadomienie dotyczące IOD (zastępcy IOD) jest poprawne? 71
Jakie są najczęściej popełniane błędy w zawiadomieniach dotyczących IOD? 72
Kiedy należy ponownie przesłać zawiadomienie dotyczące IOD? 72

Do którego organu kierować zawiadomienie, jeśli podmiot nie posiada jednostki organizacyjnej w UE? 73
Kto powinien zawiadomić o odwołaniu IOD w przypadku likwidacji/przejęcia administratora? 74
Czy należy zawiadamiać o zmianie, gdy następuje zmiana osób uprawnionych do reprezentacji? 75
Czy złożone przeze mnie zgłoszenie ABI zostało już rozpatrzone? 76

ZADANIA IOD 77

Jakie zadania ma IOD? 77
Czy prowadzenie rejestru czynności powinno być zaliczane do zadań IOD? 80
Czy po wejściu stosowania RODO CUW może powołać jednego IOD dla wszystkich obsługiwanych jednostek? 81
Na czym polega wykonywanie zadań przez IOD z należytym uwzględnieniem ryzyka? 82
Kto powinien opracować wewnętrzną politykę ochrony danych osobowych? Administrator czy IOD? 83
Czy IOD jest zobowiązany wykonywać swoje zadania również na rzecz zakładowej organizacji związkowej? 83
Czy rejestr czynności prowadzony na podstawie art. 30 ust. 1 RODO musi być udostępniany publicznie? 84
Czy naruszenie przepisów odnoszących się do IOD może skutkować administracyjnymi karami pieniężnymi? 84
Czy pracodawca powinien zawierać umowy powierzenia z takimi podmiotami, jak ZUS czy bank? 86
Co należy zrobić, jeśli zawiadomienie o naruszeniu nie zostało odebrane przez adresata? 87
Jak identyfikować podopiecznych Domu Pomocy Społecznej w związku z podawaniem leków? 88
Czy żłobek jest administratorem danych stażysty skierowanego na staż przez Powiatowy Urząd Pracy 88
Jak długo powinny być udostępniane w BIP oświadczenia majątkowe, np. radnego, wójta? 89
Czy prywatny numer telefonu sołtysa stanowi informację publiczną? 90
Kiedy administrator może pobrać opłatę za udzielenie informacji osobie, której dane dotyczą? 91
Czy w przypadku dożywiania dzieci szkoła musi zawrzeć umowę powierzenia danych z OPS? 92
Czy administrator musi kontrolować podmiot przetwarzający? 93
Czy komendant straży miejskiej musi posiadać odrębną politykę ochrony danych? 94
Czy biegli rewidenci mają status administratora w związku ze świadczeniem swoich usług? 96
Czy rzecznik praw konsumentów jest administratorem danych osobowych? 97
Czy administrator powinien udzielać upoważnień do przetwarzania danych? 98
Czy administrator powinien nadawać upoważnienia np. sędziom? 100
Czy IOD może nadawać upoważnienia? 101
Czy elektroniczna postać upoważnienia spełnia wymogi „pisemnego upoważnienia”? 103
Jak należy wywiązać się z obowiązku informacyjnego przy zastosowaniu fotopułapek? 104
Czy szkoła może udostępnić dane na temat liczby uczniów i innych mieszkających pod danym adresem? 106
Czy w przypadku kierowania studenta na praktyki zawodowe konieczne jest powierzenie? 107

Czy w przypadku kierowania ucznia na praktyki zawodowe konieczne jest powierzenie? 109
Jaka jest podstawa prawna przetwarzania danych osób upoważnionych do odbioru dziecka? 110
Czy przekazanie dokumentacji do fumigacji powoduje konieczność zawarcia umowy powierzenia? 111
Jakie informacje o pracownikach można udostępnić jako informację publiczną 112
Czy należy odbierać zgodę na przetwarzanie od osób będących na kwarantannie? 117
Czy szczególny obowiązek upubliczniania decyzji administracyjnej zwalnia z anonimizacji danych? 120
W jaki sposób identyfikować osoby, które zwracają się do IOD jako punktu kontaktowego? 122
Na jakiej podstawie gmina może udostępniać obraz z kamer Policji? 124
Który podmiot należy uznać za administratora danych przetwarzanych poza systemem EKSMON? 127
Czy z laboratorium należy zawrzeć umowę powierzenia? 131
Czy wojewoda może utworzyć bazę wyników badań w kierunku wirusa SARS-CoV-2? 133
Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych? 135
Czy lekarzom należy nadawać upoważnienia? 137
Jaka jest podstawa przetwarzania danych członków rodziny pracownika korzystającego z ZFŚS? 141
Czy z dokumentacji pracowniczej należy usuwać dane nadmiarowe? 144
Czy z sołtysem należy zawierać umowę powierzenia? 145
Kto jest administratorem w przypadku PKZP działającej przy pracodawcy? 148
Czy do pism w postępowaniu administracyjnym należy dołączać „rozdzielniki”? 150
Jaka jest podstawa do przetwarzania przez poradnie psychologiczne szczególnych kategorii danych? 154
Czy związek zawodowy może mieć dostęp do danych z wniosków o przyznanie świadczeń z ZFŚS? 157
Kto jest administratorem danych osobowych przetwarzanych w urzędzie wojewódzkim? 160
Jaki jest status WIOŚ w związku z wizyjnym systemem kontroli składowisk odpadów? 161
Czy w celu wytworzenia legitymacji należy skorzystać z powierzenia przetwarzania? 163
Czy mediator jest administratorem danych? 164
Kto jest administratorem danych przetwarzanych w celu wydania karty seniora? 169
Obowiązek informacyjny w związku z Rejestrem Danych Kontaktowych 171
Czy przesłanką przetwarzania przez organy publiczne może być art. 6 ust. 1 lit. f RODO? 174
Czy trzeba precyzyjnie określać okres przechowywania danych? 176
Czy trzeba dopełniać obowiązku informacyjnego wobec rodziny pracownika korzystającego z ZFŚS? 178
Jaki jest status projektanta w związku z wykonywaniem prac projektowych? 179
Czy z firmą szkoleniową trzeba zawrzeć umowę powierzenia? 180
Czy izba wytrzeźwień musi wypełniać obowiązek informacyjny z art. 14 RODO? 182

Na jakiej podstawie OPS przetwarza dane wolontariuszy w akcji „Wspieraj Seniora”? 183
Czy kilku administratorów może mieć jedną dokumentację ochrony danych osobowych? 184
Jaki jest status geodetów w postępowaniu rozgraniczeniowym? 186
Czy Policja może udostępnić poszkodowanemu dane sprawcy wypadku? 189
Czy IOD może w imieniu administratora zawierać umowy powierzenia? 192
Czy w przypadku PPE pracodawca powinien zawrzeć umowę powierzenia 193
Czy IOD powinien sporządzić plan audytów? 195
Jak postępować, gdy dojdzie do zagubienia zwrotnego potwierdzenia odbioru? 196
Czy pracownik działu kadr urzędu gminy może przetwarzać dane kierowników jednostek organizacyjnych? 197
Jaki jest status komisji antymobbingowej? 200
Czy inspektorowi ochrony danych należy nadawać upoważnienie do przetwarzania danych? 202
Czy GUS może zobowiązać gminy do przekazania mu innych danych niż te, które gmina może gromadzić? 203
Czy wobec osób z władz związku zawodowego trzeba spełniać obowiązek informacyjny? 205
Czy komornikowi należy udostępnić dane w postaci nr rachunku bankowego pracownika? 207
Jakie informacje można publikować w BIP wz. z ustaleniem przebiegu granic działek ewidencyjnych? 210
Która przesłanka jest podstawą przetwarzania danych przez pracodawcę stosującego monitoring? 211
Czy w jedn. organizacyjnych samorządu terytorialnego funkcjonuje kilku odrębnych administratorów? 215
Jaka jest podstawa przetwarzania danych studentów, którym udziela się pomocy materialnej? 222
Jaka powinna być podstawa prawna przetwarzania danych osobowych osób wystawiających referencje? 223
Czy uczelnia może udostępnić dane studentów wyłącznie w oparciu o ustawę o Straży Granicznej? 226
Jak prawidłowo usuwać dane pozyskane dla przyznania Karty Dużej Rodziny? 227
Czy broker ubezpieczeniowy ma status administratora? 228
Jaka jest podstawa przetwarzania danych w przypadku monitoringu karier zawodowych studentów? 231
Jakie rozwiązania są wystarczające w przypadku wykazu podmiotów podpowierzających? 232
Czy ze związkiem powiatowo-gminnym należy zawrzeć umowę powierzenia? 233
Czy przedsiębiorstwo wodociągowe może udostępnić gminie dane na temat ilości zużytej wody? 235
Jaki jest status rodziny sprawującej pieczę zastępczą? 237
Jaka jest podstawa przetwarzania przez szkołę danych uczniów w celu wydania mLegitymacji? 241
Jakie dokumenty i przez jaki okres powinny być publikowane w BIP? 243
Czy przedstawiciel związku zawodowego może mieć dostęp do danych we wnioskach o przyznanie świadczeń 249
Jaki jest okres retencji danych zebranych w związku z rekrutacją na uczelnię wyższą? 251
Czy pracodawca może pozyskiwać od pracownika informacje na temat powodów odejścia z pracy? 253

Czy art. 2 ust. 1 ust. o ochronie danych osobowych jest podstawą udostępnienia danych przez urząd? 256
Czy należy podpisać umowę powierzenia z firmą sprzątającą? 258
W jakim zakresie należy ujawniać dane przedsiębiorców prowadzących ośrodki szkolenia kierowców? 260
Jak postępować w przypadku otrzymywania tzw. niechcianych danych? 262
Jak należy określać czas przechowywania upoważnień do przetwarzania danych byłego pracownika? 263
Czy wz. ze zmianą przepisów można udostępnić związkom zawodowym informację o wys. składki członkowskiej? 264
Czy OPS może weryfikować źródła ogrzewania z CEEB przy rozpatrzeniu wniosku o dodatek osłonowy? 266
Czy członkom wspólnoty mieszkaniowej można udostępnić dane innych jej członków? 269
Czy prawo dostępu do danych osobowych można realizować przez pełnomocnika? 271
Czy szkoła może udostępnić CUW kopię rejestru czynności przetwarzania? 273
W jakim języku należy wypełnić obowiązek informacyjny? 275
Czy administrator może przerzucać swoje obowiązki na IOD? 276
Czy okręgowa izba inżynierów budownictwa może udostępnić inwestorowi dane projektanta? 279
Na co zwrócić szczególną uwagę przy powierzeniu danych osobowych w sektorze medycznym? 280

WSTĘP

Szanowni Państwo,

archiwalna strona internetowa UODO, ze względów bezpieczeństwa musi zostać wyłączona. Będzie ona dostępna do końca marca 2025 roku. Cały materiał który się tam znajduje zostanie poddany archiwizacji i będzie dostępny w ramach dostępu do informacji publicznej. Zdecydowaliśmy się jednak na udostępnienie części materiałów. Chcemy ułatwić dostęp do pytań i odpowiedzi IOD z lat 2018-2022 i w tym celu przygotowaliśmy numer specjalny „Biuletynu UODO". Jest to zbiór pytań i odpowiedzi dla IOD – łącznie 168 pytań, które na archiwalnej stronie Urzędu znajdowały się w podzakładkach:

- Wyznaczenie i status IOD,
- Zawiadomienia Prezesa UODO związane z IOD,
- Zadania IOD.

Wśród nich jest 36 pytań (cała zawartość podzakładki Wyznaczenie i status IOD), które są dostępne na aktualnej stronie Urzędu jednak zależy nam na tym aby zestawienia które państwo przedstawiamy było kompletne i zawierało wszystkie 168 pytań z lat 2018-2022. W Biuletynie publikujemy też materiały starsze, które wciąż stanowią – szczególnie dla Inspektorów Ochrony Danych – ważny punkt odniesienia.

Publikowane przez UODO pytania i odpowiedzi IOD wskazywały kierunek i zasady interpretacji przepisów dotyczących ochrony danych osobowych i służyły jako sugestie dla rozstrzygania nowych, pojawiających się wątpliwości.

Na stronach „Biuletynu UODO" wciąż sukcesywnie publikujemy nowe materiały dotyczące IOD, w tym odpowiedzi na pytania inspektorów. Pytania i odpowiedzi IOD opublikowane po 2022 roku opublikujemy w następnym numerze specjalnym Biuletynu UODO. Dodatkowo na koniec roku będziemy zbierać i publikować pytania i odpowiedzi IOD z danego roku w jednym wydawnictwie

analogicznym do tego które właśnie przekazujemy na Państwa ręce. Liczymy na to, że ten pomysł zostanie przez Państwa dobrze przyjęty.

Dlaczego zdecydowaliśmy się na numer specjalny?

Jesteśmy zmuszeni zamknąć stronę archiwalną ze względów bezpieczeństwa, ale też z powodów porządkowych. Zależy nam na tym, aby dostępne na stronie internetowej UODO materiały były aktualne i zgodne z obowiązującym stanem prawnym. Nie będą już Państwo mogli korzystać ze stron: archiwum.uodo.gov.pl oraz archiwum.giodo.gov.pl.

Numer specjalny zawiera archiwalne materiały w wersji oryginalnej. Zdecydowaliśmy się tylko na niewielkie zmiany, jedną z nich jest aktualizacja linków do formularzy zawiadomień IOD, które są dziś na aktualnej stronie UODO. Drugą zmianą, jest to, że tam, gdzie jest taka możliwość, zamiast linków zamieściliśmy tekst źródłowy ze strony archiwalnej UODO.

Pod każdym materiałem zamieściliśmy datę wytworzenia informacji. To ważne dla oceny aktualności danego materiału, które odnoszą się do stanu prawnego z dniach ich publikacji w tej dacie.

Powrót formularzy zawiadomień IOD na aktualną stronę UODO

Zachęcamy do składania zawiadomień przez platformę biznes.gov.pl.

Mamy jednak świadomość, że formularze zawiadomień dotyczących IOD są dla naszych interesantów ułatwieniem. Wychodząc naprzeciw Państwa oczekiwaniom, opublikowaliśmy je na aktualnej stronie UODO. Formularze dostępne są w zakładce zawiadomienie na podstawie RODO oraz zawiadomienie na podstawie DODO.

Formularze mają stanowić jedynie pomoc w przypadku wystąpienia problemów technicznych na tym portalu, stanowiąc alternatywny sposób zawiadomienia Prezesa UODO dla podmiotów zobowiązanych do zawiadomień dotyczących inspektorów

Mirosław Wróblewski
Prezes UODO

WYZNACZENIE I STATUS IOD

Czy zastępca IOD powinien być wyznaczony na stałe?

Jak należy rozumieć słowo „wyznaczyć" użyte w art. 11a ustawy o ochronie danych osobowych? Zgodnie z tym przepisem administrator, który wyznaczył IOD, może wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności. W związku z tym w niektórych komentarzach do przepisów o ochronie danych osobowych wskazuje się, że osoba zastępująca inspektora ochrony danych nie powinna być wyznaczana na stałe, a jedynie na czas jego nieobecności. Jednak czy właściwe rozumienie przepisu nie powinno być inne? Czy nie powinno się ustanowić w strukturze organizacyjnej stanowiska zastępcy? Czy zatrudnienie na stanowisku zastępcy nie powinno być stałe, choćby dlatego, że taka osoba musi posiadać stosowne kwalifikacje zawodowe? Za takim podejściem przemawiałoby ponadto to, że nieobecność IOD może być planowa, ale częściej jest nieplanowa, i trudno sobie wyobrazić każdorazowe zawiadamianie Prezesa UODO o tych faktach (wyznaczony, odwołany). Taka praktyka wprowadza dużo zamieszania, podważa znaczenie inspektorów i jest krytycznie odbierana przez pracowników.

Tak jak wskazaliśmy w odpowiedzi na pytanie: **Czy administrator jest zobowiązany na podstawie RODO do zapewnienia inspektorowi zespołu IOD?**, RODO nakłada na administratora konkretne obowiązki wobec funkcjonującego w jego organizacji inspektora ochrony danych, a sposób ich realizacji zależy od specyfiki danego administratora (m.in. jego wielkości, struktury, rodzaju działalności) i prowadzonego przez niego przetwarzania danych (m.in. charakteru, zakresu, kontekstu i celów przetwarzania). W zależności od tych czynników administrator musi zapewnić IOD właściwe warunki funkcjonowania, które umożliwią mu skuteczne i prawidłowe wykonywanie zadań.

Udzielanie IOD wsparcia w wypełnianiu przez niego zadań, w tym zapewnianie mu niezbędnych do tego zasobów, to jeden z obowiązków administratora, wyrażony wprost w 38 ust. 2 RODO. Jak wyjaśnia Grupa Robocza Art. 29 w swoich Wytycznych dotyczących inspektora ochrony danych, w zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych (IOD i jego pracowników).

W skład zespołu IOD wchodzić może osoba (osoby) zastępujące inspektora w czasie jego nieobecności. Możliwość powołania takiej osoby stwarza administratorowi art. 11a ust. 1 ustawy o ochronie danych osobowych. Przepis ten odczytywany literalnie wskazuje, że administrator może w każdym czasie wyznaczyć zastępcę IOD, który będzie pełnił tę funkcję podczas nieobecności IOD. W gestii administratora jest zatem decyzja, czy wyznaczyć stałego zastępcę

(bez konieczności wyznaczania i odwoływania podczas poszczególnych nieobecności IOD), czy będzie wyznaczał zastępcę doraźnie jedynie na czas faktycznej nieobecności inspektora.

Niemniej kolejne ustępy tego artykułu wskazują, że osoba zastępująca inspektora musi spełniać kryteria kwalifikacyjne wynikające z art. 37 ust. 5 i 6 RODO, czyli analogiczne jak IOD. W związku z wykonywaniem obowiązków inspektora w czasie jego nieobecności do osoby go zastępującej stosuje się odpowiednio przepisy dotyczące inspektora (art. 11a ust. 2). Ponadto zgodnie z art. 11a ust. 3 ustawy o ochronie danych osobowych, do wyznaczenia osoby zastępującej inspektora stosuje się art. 10 i art. 11 tej ustawy. Oznacza to, że administrator lub podmiot przetwarzający, który zdecyduje się na wyznaczenie zastępcy IOD, zobowiązany jest zawiadomić Prezesa UODO o jego wyznaczeniu oraz dokonywać innych zawiadomień dotyczących zmiany danych lub odwołania zastępcy, a także zobowiązany jest do publikowania jego imienia, nazwiska oraz adresu poczty elektronicznej lub numeru telefonu na swojej stronie internetowej (a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności).

Rozwiązanie polegające na wyznaczeniu stałego zastępcy IOD nie tylko pozwala zapewnić ciągłość wykonywania zadań IOD, ale też - ze względu na to, że osoba taka musi mieć odpowiednie, takie jak IOD przygotowanie merytoryczne (zgodnie z art. 11a ust. 1 ustawy o ochronie danych osobowych) - może stanowić realne i ciągłe wsparcie administratora (i obsługującego go IOD). W tym zakresie słuszne są przedstawione w przytoczonym pytaniu IOD zapatrywanie i argumentacja, że warto zmierzać do rozwiązań o stałym, długookresowym charakterze. Wskazują na to nie tylko potrzeba przyjmowania efektywnych rozwiązań w celu rzetelnego przestrzegania zasad ochrony danych osobowych, ale też względy pragmatyczne związane ze sposobem ukształtowania przez polskiego ustawodawcę przepisów dotyczących osoby zastępującej IOD, w tym z obowiązkiem zawiadamiania Prezes UODO o osobie wyznaczonej do zastępowania IOD.

Powołanie na stałe „zastępcy" posiadającego odpowiednią wiedzę i przygotowanie służyłoby zapewnieniu ciągłości działania IOD podczas jego nagłej lub planowanej nieobecności (np. choroba, urlop). W czasie obecności IOD „osoba zastępująca" mogłaby np. na bieżąco współpracować z inspektorem ochrony danych w celu omówienia istotnych spraw, dzięki czemu znałaby specyfikę aktualnych działań administratora i inspektora.

Warto nadmienić, że w opinii UODO dopuszczalne jest, by administrator wyznaczył dwie osoby zastępujące inspektora ochrony danych. Jedna realizowałaby zadania IOD podczas jego nieobecności, a druga wówczas, gdyby w pracy nie było zarówno IOD, jak i tej pierwszej, zastępującej go osoby (więcej informacji w tym zakresie znajduje się w wydaniu 10 newslettera UODO dla IOD (październik 2020) str. 2) – **tekst w ramce poniżej**.

Informacja ze strony archiwalnej UODO

IOD MOŻE MIEĆ DWÓCH ZASTĘPCÓW – Administrator może wyznaczyć dwie osoby zastępujące inspektora ochrony danych. Należy jednak zadbać o to, by przejrzyście określić nie tylko system zastępstw IOD, ale również podział obowiązków wszystkich osób, tak by wówczas, gdy jednocześnie będą one obecne w pracy, nie było wątpliwości, kto za jakie zadania jest odpowiedzialny.

W opinii organu ds. ochrony danych osobowych dopuszczalne jest, by administrator wyznaczył dwie osoby zastępujące inspektora ochrony danych. Jedna realizowałaby zadania IOD podczas jego nieobecności, a druga wówczas, gdyby w pracy nie było zarówno IOD, jak i tej pierwszej, zastępującej go osoby. Przyjęcie takiego rozwiązania jest racjonalne, umożliwia bowiem zapewnienie ciągłości wykonywania zadań IOD, a tym samym podnosi standard ochrony danych. Określenie kwestii zastępstwa IOD (np. w wewnętrznym zarządzeniu) sprzyja dobrej organizacji pracy IOD i uniknięcia sytuacji, w której nie było osoby, która mogłaby wykonywać zadania IOD podczas jego nieobecności. Ważne jest jednak, aby kierownictwo jednostki zadbało nie tylko o przejrzyste określenie systemu zastępstw IOD, ale również jasno określiło podział obowiązków między IOD i jego „zastępców", tak aby nie doprowadzić do ewentualnych konfliktów na tym tle i by wówczas, gdy jednocześnie w pracy będzie obecny inspektor i osoby go zastępujące, nie było wątpliwości, kto za jakie zadania jest odpowiedzialny. Dla wszystkich, zarówno wewnątrz podmiotu będącego administratorem danych, jak w relacjach zewnętrznych musi być jasne, kto w danym momencie jest odpowiedzialny za monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa.

Data wytworzenia informacji: 29.07.2021 r.

Czy dane kontaktowe IOD muszą być łatwo dostępne?

Czy dane kontaktowe IOD muszą być łatwo dostępne dla osób, których dane dotyczą? W jaki sposób powinny one zostać opublikowane na stronie internetowej administratora?

Celem obowiązku publikowania przez administratora na swojej stronie internetowej imienia i nazwiska oraz adresu poczty elektronicznej lub numeru telefonu inspektora ochrony danych jest zapewnienie, aby osoby, których dane dotyczą, mogły mieć łatwy i bezpośredni kontakt z inspektorem, bez konieczności kontaktowania się z innymi jednostkami podmiotu [Wytyczne Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (WP 243), str. 13.

Jeśli administrator prowadzi własną stronę internetową, dane o wyznaczonym IOD powinny znaleźć się w łatwo dostępnym miejscu strony, np. w zakładce: „Kontakt", „Inspektor ochrony danych", „RODO" czy „Ochrona danych osobowych". Za niewłaściwe należy natomiast uznać publikowanie tych danych w miejscach wymagających długiego przeszukiwania, takich jak „Aktualności" czy „Polityka prywatności".

Zgodnie z RODO jednym z zadań inspektora ochrony danych (IOD) jest pełnienie roli punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym

a osobami, których dane dotyczą. Unijny prawodawca w art. 38 ust. 4 RODO uprawnił osoby, których dane dotyczą, do kontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Ta rola inspektora jest mocno powiązana z obowiązkami administratora oraz podmiotu przetwarzającego określonymi w art. 12-22 RODO i ma przyczyniać się do skuteczniejszego ich wykonywania.

Przykładem może tu być sytuacja, gdy dochodzi do naruszenia ochrony danych, które może powodować wysokie ryzyko naruszenia praw i wolności. W takim przypadku znaczenie praw osób oraz roli inspektora uwydatnia się w sposób szczególny. Jak należy wnioskować z art. 34 ust. 2 RODO, w przypadkach takich naruszeń, osoby, których to naruszenie dotyczy, powinny mieć możliwość zwrócenia się do IOD lub innego punktu kontaktowego w celu uzyskania dodatkowych informacji, wykraczających poza zakres przekazany im w zawiadomieniu o naruszeniu.

Data wytworzenia informacji: 26.11.2020 r.

Czy administrator musi podać imię i nazwisko IOD na stronie internetowej?

Czy obowiązkowe jest opublikowanie imienia i nazwiska IOD na stronie internetowej administratora? Z jakich przepisów prawa wynika ten obowiązek?

Podanie imienia i nazwiska inspektora ochrony danych na stronie internetowej podmiotu, który go wyznaczył, jest obowiązkowe. Obowiązek ten wynika wprost z przepisów prawa.

Zgodnie z art. 37 ust. 7 RODO, administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych. Sposób realizacji tego obowiązku doprecyzowany został w art. 11 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych. W przepisie tym wskazano, że podmiot, który wyznaczył inspektora, **udostępnia dane inspektora w zakresie: imię i nazwisko oraz adres poczty elektronicznej lub nr telefonu inspektora,** niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Jednocześnie należy przypomnieć, że podmiot, który wyznaczył inspektora ochrony danych powinien zadbać o to, by **informacja o danych kontaktowych IOD była łatwo dostępna dla osób, których dane dotyczą.**

Więcej na ten temat w odpowiedzi na pytanie: Czy dane kontaktowe IOD muszą być łatwo dostępne?

Data wytworzenia informacji: 26.11.2020 r.

Czy funkcję IOD można łączyć z wykonywaniem zawodu adwokata lub radcy prawnego?

Kwestia dopuszczalności jednoczesnego pełnienia funkcji inspektora ochrony danych i wykonywania zawodu radcy prawnego i adwokata w świetle przepisów regulujących wykonywanie tych zawodów stała się w 2018 r. przedmiotem skierowanych do obu samorządów wystąpień Prezesa UODO. Na prośbę Prezesa UODO oba samorządy przedstawiły swoje opinie, a z korespondencją dotyczącą tego zagadnienia można zapoznać się pod następującym linkiem: https://www.giodo.gov.pl/pl/1520282/10461 – **tekst w ramce poniżej**.

Informacja ze strony archiwalnej GIODO

Samorządy adwokatów i radców prawnych o dopuszczalności jednoczesnego wykonywania zawodu i pełnienia funkcji IOD

GIODO wystąpił do samorządu radców prawnych i samorządu adwokatów z prośbą o przedstawienie stanowiska w sprawie możliwości wykonywania tych zawodów i jednoczesnego pełnienia funkcji administratora bezpieczeństwa informacji lub inspektora ochrony danych. Wskazał, że opinia samorządów w tej sprawie będzie istotną pomocą dla wszystkich podmiotów przygotowujących się obecnie do stosowania od 25 maja 2018 r. przepisów RODO i będzie odpowiedzią na wiele wątpliwości, które były sygnalizowane Generalnemu Inspektorowi.

W opinii Naczelnej Rady Adwokackiej wykonywanie zawodu adwokata nie wyklucza jednoczesnego pełnienia funkcji inspektora ochrony danych (IOD) bowiem przepisy RODO gwarantują IOD niezależność, co jest również podstawą wykonywania zawodu adwokata. W przypadku inspektora ochrony danych niezależność gwarantują mu podległość najwyższemu kierownictwu danego podmiotu, zakaz wydawania IOD instrukcji oraz zakaz zwolnienia z powodu wykonywania przez niego czynności przewidzianych przepisami.

Krajowa Rada Radców Prawnych przekazała opinię, zgodnie z którą wykonywanie zadań IOD/ABI nie może być kwalifikowane jako podkategoria pojęcia świadczenia pomocy prawnej, chociaż te obszary mają pewne wspólne zakresy. Radcy prawni, jako profesjonaliści w zakresie świadczenia pomocy prawnej, po uzyskaniu dodatkowych kwalifikacji wymaganych dla wykonywania zadań IOD, mogą podejmować się pełnienia tej funkcji, choć zaznaczyć należy, że rzetelne wykonywanie zadań IOD może wymagać znacznej ilości czasu. Ponadto ze względu na określone ryzyka związane z konfliktem interesów, w szczególności związane z potencjalnym naruszeniem zasad etyki zawodowej oraz rozbieżnymi charakterystykami funkcji radcy prawnego oraz IOD, rekomenduje się niełączenie wykonywania tych ról w ramach jednego podmiotu (administratora danych/klienta).

Generalny Inspektor dziękuje samorządom za przekazanie stanowisk zawierających cenne zalecenia i wskazówki, a wszystkich zainteresowanych zaprasza do zapoznania się z treścią wystąpień GIODO i przedstawionych przez samorządy stanowisk.

W opinii Naczelnej Rady Adwokackiej (NRA) wykonywanie zawodu adwokata nie wyklucza jednoczesnego pełnienia funkcji inspektora ochrony danych (IOD), bowiem przepisy RODO gwarantują IOD niezależność, co jest również podstawą wykonywania zawodu adwokata. Zadania powierzone IOD nie uwłaczają godności adwokata, nie ograniczają jego niezawisłości oraz nie podważają zaufania do adwokatury. W przypadku inspektora ochrony danych niezależność gwarantuje mu m.in. podległość najwyższemu kierownictwu, zakaz wydawania IOD instrukcji oraz zakaz odwołania IOD z powodu wykonywania przez niego jego zadań. Z uwagi na brzmienie art. 1 ust. 3 ustawy z dnia 26 maja 1982 r. Prawo o adwokaturze (Dz. U. z 2018 r. poz. 1184 ze zm.) dopuszczalne jest pełnienie funkcji IOD przez adwokata na podstawie umowy cywilnoprawnej (art. 37 ust. 6 RODO). W swojej opinii NRA podkreśliła, że niezbędnym warunkiem jest poosiadanie przez adwokata wiedzy z zakresu ochrony danych osobowych zgodnie art. 37 ust. 5 RODO.

Krajowa Rada Radców Prawnych (KRRP) przekazała opinię, zgodnie z którą wykonywanie zadań IOD nie może być kwalifikowane jako podkategoria pojęcia świadczenia pomocy prawnej, chociaż te obszary mają pewne wspólne zakresy. Ze względu na określone ryzyka, w szczególności związane z potencjalnym naruszeniem zasad etyki zawodowej oraz rozbieżnymi charakterystykami funkcji radcy prawnego oraz IOD, **KRRP rekomenduje niełączenie wykonywania tych ról w ramach jednego podmiotu (administratora danych/klienta).** KRRP wskazała również na konieczność posiadania przez IOD odpowiednich kwalifikacji , w szczególności w zakresie zadań leżących poza zakresem pojęcia świadczenia pomocy prawnej np. znajomości aspektów technicznych, funkcjonowania systemów informatycznych, bezpieczeństwa IT, oceny ryzyka, prowadzenia audytów.

Dostarczone przez samorządy opinie potwierdzają, że rzetelna analiza co do możliwości powierzenia IOD dodatkowych obowiązków powinna obejmować wiele aspektów związanych z regulacjami danego zawodu oraz statusem, zdaniami i wymaganiami w zakresie kwalifikacji stawianymi IOD. Należy podkreślić, że na administratorze spoczywa obowiązek zapewnienia, by powierzenie IOD dodatkowych zadań i obowiązków nie powodowało konfliktu interesów (art. 38 ust. 6 RODO).

Data wytworzenia informacji: 28.06.2019 r.

Czy istnieje możliwość wyznaczenia osoby prawnej do sprawowania funkcji IOD?

Nie. Do pełnienia funkcji IOD musi być zawsze wyznaczona konkretna osoba fizyczna. Przepisy ustawy o ochronie danych osobowych wymagają, aby administrator i podmiot przetwarzający, którzy wyznaczyli IOD, udostępnili imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora na swojej stronie internetowej, lub gdy administrator nie posiada własnej

strony, w sposób ogólnie dostępny w miejscu prowadzenia działalności (art. 11). Imię i nazwisko konkretnej osoby pełniącej funkcję IOD należy też podać Prezesowi UODO, powiadamiając go o wyznaczeniu takiej osoby (art. 10 ust. 1 ustawy o ochronie danych osobowych).

IOD jest punktem kontaktowym dla osób, których dane dotyczą i organu nadzorczego zgodnie z art. 38 ust. 4 i art. 39 ust. 1 lit. e RODO. Zatem zarówno wewnątrz podmiotu będącego administratorem, jak i w relacjach zewnętrznych, dla wszystkich musi być jasne, jaka konkretna osoba fizyczna pełni tę funkcję.

Data wytworzenia informacji: 28.06.2019 r.

Wyznaczenie IOD w straży gminnej (miejskiej) umiejscowionej w strukturze urzędu

Czy straż gminna (miejska), która jest umiejscowiona w strukturze urzędu gminy jest zobowiązana do wyznaczenia IOD na podstawie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczeniem przestępczości?

Zgodnie z art. 10a ust. 2 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z 2018 r., poz. 928 z późn. zm.) administratorem danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r., poz. 125) przez straż gminną jest komendant straży.

Przepis art. 46 ust. 1 ustawy z dnia 14 grudnia 2018 r. wskazuje, że administrator (w rozumieniu jej art. 4 pkt 1) wyznacza inspektora ochrony danych. Zatem do wyznaczenia inspektora ochrony danych (IOD) zobowiązani są komendanci straży gminnej i miejskiej, niezależnie od tego, czy są oni umiejscowieni w strukturze urzędu gminy, czy nie.

Data wytworzenia informacji: 03.06.2019 r.

Czy IOD musi odbyć szkolenie dla IOD oraz posiadać certyfikat potwierdzający jego odbycie?

Czy IOD jest zobowiązany odbyć szkolenie dla IOD oraz posiadać certyfikat potwierdzający jego odbycie?

Zgodnie z art. 37 ust. 5 RODO inspektor ochrony danych (IOD) wyznaczany jest na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych wskazuje, że

wymagany poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki.

Ogólne rozporządzenie o ochronie danych bardzo mocno akcentuje wymóg wiedzy i fachowości IOD, nie reguluje jednak zasad czy trybu weryfikacji spełnienia tego wymogu. Niemniej certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie inspektora niewątpliwie w większości przypadków będą ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej przez danego administratora do pełnienia tej funkcji.

Data wytworzenia informacji: 03.06.2019 r.

Czy osoba spokrewniona z osobą zarządzającą może być IOD?

Czy funkcję IOD w określonym podmiocie może pełnić osoba spokrewniona z osobami, które kierują lub zarządzają tym podmiotem?

Przepisy prawa nie zawierają zakazu odnoszącego się do takiej sytuacji. Niemniej w każdym przypadku należy starannie przeanalizować i ocenić, czy określone relacje rodzinne nie będą miały wpływu na wykonywanie zadań i obowiązków IOD w sposób niezależny i nie będą powodować konfliktu interesów (art. 38 ust. 6 RODO). Istotą funkcji IOD jest obiektywne i niezależne wykonywanie zadań określonych w RODO(art. 39 ust. 1, Motyw 97 RODO).

IOD powinien w swoich działaniach opierać się na rzeczywistym stanie faktycznym badanej sprawy, nie powinien ulegać żadnym naciskom i podporządkowywać swoich opinii innym osobom. Jego nadrzędnym celem w każdej sytuacji powinno być zapewnienie, że przetwarzanie danych będzie następowało zgodnie z prawem.

Data wytworzenia informacji: 03.06.2019 r.

Brak jednostki organizacyjnej w UE a zgłoszenie IOD

Do którego organu nadzorczego należy kierować zawiadomienie o wyznaczeniu IOD w przypadku podmiotów nieposiadających jednostki organizacyjnej w UE?

Zawiadomienie organu nadzorczego o wyznaczeniu inspektora ochrony danych przez podmioty wskazane w art. 3 ust. 2 RODO powinno nastąpić do organu nadzorczego w państwie członkowskim, w którym przedstawiciel administratora w UE ma jednostkę organizacyjną.

Do podmiotów (administratorów i podmiotów przetwarzających) nieposiadających jednostki organizacyjnej w UE RODO może mieć zastosowanie, również w zakresie obowiązku wyznaczenia

inspektora ochrony danych osobowych, wówczas, gdy prowadzone przez nie czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w UE - niezależnie od tego, czy wymaga się od tych osób zapłaty; lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE.

Takie podmioty mają obowiązek wyznaczenia swojego przedstawiciela w UE, chyba że przetwarzanie ma charakter sporadyczny, nie obejmuje na dużą skalę przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych, lub jeżeli administrator jest organem lub podmiotem publicznym. Wyznaczenie przedstawiciela nie wpływa na obowiązki lub odpowiedzialność prawną administratora lub podmiotu przetwarzającego wynikającą z RODO (art. 27 ust. 5 RODO, Motyw 80).

Do jakiego organu podmioty takie powinny kierować zawiadomienie o wyznaczeniu IOD? Stosując analogię do obowiązku zgłaszania naruszeń i wskazówek przekazanych w kontekście tego obowiązku w odniesieniu do podmiotów, które nie posiadają jednostki organizacyjnej w UE w Wytycznych dotyczących zgłaszania naruszeń ochrony danych (WP 250) zgłoszenia związane z inspektorem ochrony danych powinny być kierowane do organu nadzorczego w państwie członkowskim, w którym przedstawiciel administratora w UE ma jednostkę organizacyjną. W przypadku zgłoszeń naruszeń ochrony danych osobowych Gr. Robocza wypowiedziała się następująco: „ (…) *w przypadku, gdy naruszenie odnotuje administrator niemający jednostki organizacyjnej w UE, który podlega przepisom art. 3 ust. 2 lub 3, na administratorze tym wciąż spoczywają obowiązki zgłaszania określone w art. 33 i 34. W art. 27 ustanowiono wymóg zobowiązujący administratora (i podmiot przetwarzający) do wyznaczenia przedstawiciela w UE w przypadku, gdy zastosowanie ma art. 3 ust. 2. W takich przypadkach Grupa Robocza Art. 29 zaleca, aby zgłoszenia były kierowane do organu nadzorczego w państwie członkowskim, w którym przedstawiciel administratora w UE ma jednostkę organizacyjną. Podobnie w przypadku gdy podmiot przetwarzający podlega przepisom art. 3 ust. 2, spoczywają na nim obowiązki dotyczące podmiotów przetwarzających, a w szczególności obowiązek zgłaszania naruszenia administratorowi na podstawie art. 33 ust. 2.”* (str. 21)

Data wytworzenia informacji: 03.06.2019 r.

Kto może, a kto musi wyznaczyć IOD na podstawie RODO?

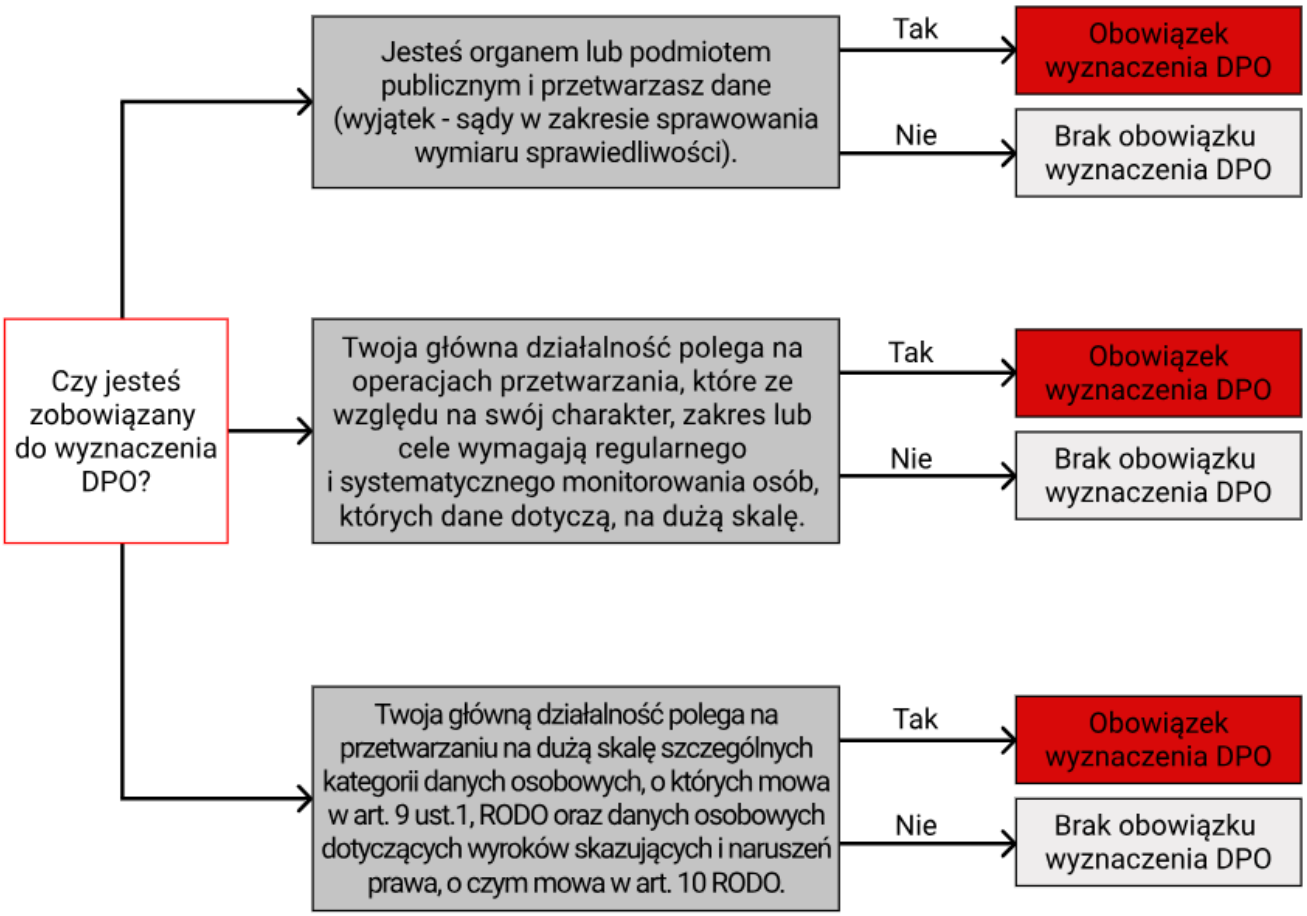
Ogólne rozporządzenie o ochronie danych w art. 37 ust. 1 RODO przewiduje obowiązek wyznaczenia inspektora dla administratorów i podmiotów przetwarzających wówczas, gdy:

1. przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości.

Przez organy i podmioty publiczne obowiązane do wyznaczenia IOD, o których mowa w art. 37 ust. 1 lit. a RODO, rozumie się jednostki sektora finansów publicznych (np. jednostki samorządu terytorialnego, uczelnie publiczne), instytuty badawcze oraz Narodowy Bank Polski (art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych).

1. główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę.
2. główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 RODO.

W interpretacji terminów użytych w art. 37 ust. 1 lit. b i c RODO („główna działalność", „regularne i systematyczne monitorowanie" i „na dużą skalę") pomocne mogą być motywy RODO oraz Wytyczne Grupy Roboczej art. 29 dotyczące inspektora ochrony danych



W pozostałych przypadkach wyznaczenie inspektora będzie fakultatywne. Jednakże nawet w sytuacji, gdy z przepisów nie wynika obowiązek wyznaczenia IOD, Grupa Robocza art. 29 w swoich wytycznych dotyczących inspektora ochrony danych zaleca administratorom i podmiotom przetwarzającym udokumentowanie wewnętrznej procedury, przeprowadzonej w celu ustalenia i uwzględnienia poszczególnych przesłanek z art. 37 ust. 1 RODO istnienia lub braku tego obowiązku.

Kwalifikacje do pełnienia funkcji IOD

Zgodnie z art. 37 ust. 5 RODO inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO. Poziom wiedzy inspektora powinien być ustalany w kontekście konkretnych potrzeb administratora danych i procesora (motyw 97 RODO). Jak wskazuje Grupa Robocza art. 29 wymagany poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki.

Wobec czego wybór inspektora ochrony danych powinien być dokonany z zachowaniem należytej staranności i z uwzględnieniem charakteru przetwarzania danych osobowych w ramach jednostki.

IOD powinien posiadać:

- fachową wiedzę z zakresu krajowych i europejskich przepisów o ochronie danych osobowych;
- fachową wiedzę z zakresu praktyk w dziedzinie ochrony danych osobowych;
- dogłębną znajomość przepisów RODO;
- wiedzę biznesową i sektorową dotycząca działalności administratora;
- odpowiednią wiedzę na temat procesów przetwarzania danych, systemów informatycznych oraz zabezpieczeń stosowanych u administratora i jego potrzeb w zakresie ochrony danych;
- w przypadku organów i podmiotów publicznych IOD powinien również wykazywać się znajomością procedur administracyjnych i funkcjonowania jednostki.

W odniesieniu do wypełnienia zadań IOD Grupa Robocza wskazała, że priorytetem DPO powinno być zapewnienie przestrzegania rozporządzenia. Inspektor ma zatem odgrywać kluczową rolę w zakresie wspierania „kultury ochrony danych" oraz pomagać w implementacji niezbędnych elementów RODO tj.:

- zasady przetwarzania danych osobowych;
- prawa osób, których dane dotyczą;
- ochrony danych w fazie projektowania oraz domyślnej ochrony danych;
- prowadzenia rejestru czynności przetwarzania;
- wymogów bezpieczeństwa przetwarzania;
- zgłaszanie naruszeń.

Jeśli chodzi o osobiste cechy inspektora kwalifikujące go do wykonywania funkcji, to są to: rzetelne podejście do wykonywania swoich obowiązków i wysoki poziom etyki zawodowej.

Forma zatrudnienia IOD

Zgodnie z art. 37 ust. 6 RODO inspektorem ochrony danych może zostać zarówno pracownik administratora lub podmiotu przetwarzającego, jak i osoba spoza grona pracowników ww. podmiotów (outsourcing).

Data wytworzenia informacji: 07.01.2019 r.

Czy należy wyznaczyć IOD w niepublicznym zakładzie opieki zdrowotnej mając około 2 000 pacjentów?

Zgodnie z przepisami RODO (art. 37 ust. 1) obowiązek wyznaczenia IOD występuje gdy:

- przetwarzania dokonują organ lub podmiot publiczny,
- główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, **na dużą skalę,**
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu **na dużą skalę** szczególnych kategorii danych osobowych albo danych osobowych dotyczących wyroków skazujących i czynów zabronionych.

Sposób sformułowania przepisu określającego obowiązek wyznaczenia inspektora jest mało precyzyjny, ale takie sformułowanie zostało użyte celowo, właśnie po to, aby administrator danych samodzielnie dokonywał analizy sytuacji i ocenił, czy taki obowiązek w jego przypadku istnieje.

Co więcej – w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243) zaleca się, aby przeprowadzenie oceny w zakresie istnienia obowiązku wyznaczenia inspektora udokumentować, a nawet powtarzać taką ocenę w razie potrzeby, co jakiś czas. Sytuacja danego podmiotu może się bowiem zmieniać. Na przykład mała przychodnia może stopniowo rozszerzać swoją działalność, obejmując o nowe usługi i świadczenia i po jakimś czasie stać się dużym podmiotem przetwarzającym dane wrażliwe na dużą skalę.

W celu ułatwienia administratorowi dokonania oceny, czy jest zobowiązany do wyznaczenia IOD, Grupa Robocza Artykułu 29 w powołanych wyżej wytycznych zawarła wskazówki, jak należy rozumieć „główną działalność" czy „dużą skalę", a także wiele praktycznych, konkretnych przykładów sytuacji spełniających te kryteria. Wskazówki oparte są na założeniu, że wraz z rozwojem praktyki ukształtują się standardy, które umożliwią bardziej szczegółowe i/lub kwantytatywne zidentyfikowanie „dużej skali" w odniesieniu do określonych rodzajów przetwarzania.

W Wytycznych zaznaczono, że w przypadku placówek medycznych główną działalnością jest wprawdzie zapewnianie opieki zdrowotnej, ale ta działalność nie byłaby możliwa bez przetwarzania danych w formie dokumentacji medycznej. Jako przykład „działalności głównej polegającej na przetwarzaniu na dużą skalę wrażliwych danych osobowych" jest tam podana działalność szpitali. Natomiast jako przykład przetwarzania nie mieszczący się w definicji dużej skali - zgodnie z motywem 91 RODO - należy wskazać przetwarzanie danych pacjentów przez pojedynczego lekarza lub innego pracownika służby zdrowia (pielęgniarkę, położną).

Warto dodać, że na podstawie tych samych przesłanek RODO przewiduje obowiązek wyznaczenia IOD przez tzw. podmioty przetwarzające, czyli podmioty, które przetwarzają dane osobowe na zlecenie placówek medycznych w związku ze specjalistycznymi usługami, jakie dla nich świadczą, na przykład przechowują dokumentację medyczną lub serwisują sprzęt informatyczny czy diagnostyczny.

Data wytworzenia informacji: 07.01.2019 r.

W jaki sposób należy oceniać kwalifikacje osoby kandydującej do pełnienia funkcji IOD?

IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.

Wymagany od inspektora poziom wiedzy fachowej nie jest jednoznacznie określony, ale zgodnie z Wytycznymi dotyczącymi IOD musi być on współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Wyższy poziom wiedzy powinien być wymagany np. w przypadku:

- wyjątkowo skomplikowanych procesów przetwarzania,
- przetwarzania dużej ilości danych szczególnych kategorii,
- podmiotów regularnie przekazujących dane do państw trzecich.

IOD powinien mieć odpowiednią wiedzę z zakresu krajowych, europejskich oraz sektorowych przepisów i praktyk w zakresie ochrony danych osobowych, a także dogłębną znajomość RODO. Jednocześnie powinien posiadać odpowiednią wiedzę na temat:

- procesów przetwarzania, systemów informatycznych oraz zabezpieczeń stosowanych u administratora,
- sektora, w którym działa administrator,
- procedur administracyjnych i funkcjonowania jednostki.

Jeśli chodzi o osobiste cechy IOD kwalifikujące go do wykonywania funkcji, to są to: rzetelne podejście i wysoki poziom etyki zawodowej.

Ocena kompetencji osoby do wykonywania zadań wymaga uwzględnienia charakteru i zakresu zadań inspektora. Zgodnie z przepisami RODO, inspektor będzie miał m.in. obowiązek identyfikowania poszczególnych obowiązków ciążących na mocy RODO na administratorze (w tym kierownictwie i wszystkich osobach przetwarzających dane) oraz podmiocie przetwarzającym (w tym kierownictwie i wszystkich osobach przetwarzających dane osobowe), informowania

o nich oraz doradzania w zakresie tych obowiązków. Specjalnego merytorycznego przygotowania wymaga udzielanie administratorowi i podmiotowi przetwarzającemu zaleceń co do oceny skutków dla ochrony danych (więcej na temat roli inspektora w ocenie skutków dla ochrony danych w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (DPO) oraz w Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych). Ważnym zadaniem IOD jest obowiązek pełnienia roli punktu kontaktowego dla organu nadzorczego i punktu kontaktowego dla osób, których dane dotyczą (art. 38 ust. 4 RODO).

Grupa Robocza Art. 29 w Wytycznych dotyczących inspektorów ochrony danych (DPO) w odniesieniu do umiejętności wykonywania zadań inspektora wskazuje, że priorytetem dla niego powinno być zapewnienie przestrzegania RODO. IOD ma zatem odgrywać kluczową rolę w zakresie wspierania „kultury ochrony danych" oraz pomagać w implementacji niezbędnych elementów RODO, tj.:

- zasad przetwarzania danych osobowych,
- praw osób, których dane dotyczą,
- ochrony danych w fazie projektowania oraz domyślnej ochrony danych,
- rejestru czynności przetwarzania,
- wymogów bezpieczeństwa przetwarzania,
- zgłaszania naruszeń.

Znaczenie fachowej wiedzy w zakresie prawa i praktyki zostało dodatkowo podkreślone przez zobowiązanie administratorów i podmiotów przetwarzających do zapewnienia IOD zasobów niezbędnych do utrzymania wysokiego i aktualnego poziomu wiedzy (art. 38 ust. 2 RODO). Wymóg uaktualniania wiedzy i zapewnienia na to środków finansowych jest uzasadniony wobec zmieniającego się stale stanu wiedzy technicznej, rozwoju technologicznego i postępu wielkoskalowych metod przetwarzania danych.

IOD powinien kształcić się, rozwijać swoje doświadczenia i umiejętności w różnych formach edukacyjnych, a możliwość powołania się na wskazany art. 38 ust. 2 RODO może być mu bardzo pomocny w uzyskaniu niezbędnych na to środków finansowych.

Mimo, iż RODO bardzo mocno akcentuje wymóg wiedzy i fachowości IOD, nie reguluje zasad czy trybu weryfikacji spełnienia tego wymogu. Niemniej certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie inspektora niewątpliwie w większości przypadków będą ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej do pełnienia tej funkcji.

Data wytworzenia informacji: 07.01.2019 r.

Czy IOD powinien być wyznaczany na podstawie takich samych kwalifikacji jak było w przypadku ABI?

Wymogi stawiane inspektorom ochrony danych przez przepisy RODO są podobne do tych stawianych wcześniej ABI, ale nie są identyczne. Zgodnie z art. 36a ust. 5 pkt 2 ustawy o ochronie danych osobowych, osoba powoływana na stanowisko ABI powinna była posiadać odpowiednią wiedzę w zakresie ochrony danych osobowych. RODO zaś w art. 37 ust. 5 stanowi, iż inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 ogólnego rozporządzenia.

Wymagany od inspektora poziom wiedzy fachowej nie jest nigdzie jednoznacznie określony, ale zgodnie z Wytycznymi Grupy Roboczej Art. 29 dotyczącymi inspektorów ochrony danych (WP 243) musi być on współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Wyższy poziom wiedzy powinien być wymagany np. w przypadku wyjątkowo skomplikowanych procesów przetwarzania, przetwarzania dużej ilości danych szczególnych kategorii, podmiotów regularnie przekazujących dane do państw trzecich.

Inspektor ochrony danych powinien mieć odpowiednią wiedzę z zakresu krajowych, europejskich oraz sektorowych przepisów i praktyk w zakresie ochrony danych osobowych, a także dogłębną znajomość RODO. Jednocześnie powinien posiadać odpowiednią wiedzę na temat: procesów przetwarzania, systemów informatycznych oraz zabezpieczeń stosowanych u administratora, sektora w którym działa administrator, procedur administracyjnych i funkcjonowania jednostki.

Ocena umiejętności wykonywania zadań wymaga uwzględnienia charakteru i zakresu zadań inspektora, spośród których kilka stanowi nowość w stosunku do wymogów stawianych ABI. Zgodnie z przepisami RODO, inspektor będzie miał m.in. obowiązek identyfikowania poszczególnych obowiązków ciążących na mocy RODO na administratorze (w tym kierownictwie i wszystkich osobach przetwarzających dane) oraz podmiocie przetwarzającym (w tym

kierownictwie i wszystkich osobach przetwarzających dane osobowe), informowania o nich oraz doradzania w zakresie tych obowiązków. Specjalnego merytorycznego przygotowania wymagać będzie udzielanie administratorowi i podmiotowi przetwarzającemu zaleceń co do oceny skutków dla ochrony danych (więcej na temat roli inspektora w ocenie skutków dla ochrony danych w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243) oraz w Wytycznych Grupy Roboczej Art. 29 dotyczących oceny skutków dla ochrony danych). Nowym, ważnym zadaniem będzie obowiązek pełnienia roli punktu kontaktowego dla organu nadzorczego i punktu kontaktowego dla osób, których dane dotyczą (art. 38 ust. 4 RODO).

Grupa Robocza Art. 29 w Wytycznych dotyczących inspektorów ochrony danych w odniesieniu do umiejętności wykonywania zadań inspektora wskazuje, że priorytetem dla niego powinno być zapewnienie przestrzegania rozporządzenia. DPO ma zatem odgrywać kluczową rolę w zakresie wspierania „kultury ochrony danych" oraz pomagać w implementacji niezbędnych elementów RODO, w tym zwłaszcza nowych obowiązków tj., np. ochrony danych w fazie projektowania oraz domyślnej ochrony danych, rejestru czynności przetwarzania, zgłaszania naruszeń.

Znaczenie fachowej wiedzy w zakresie prawa i praktyk zostało dodatkowo podkreślone przez zobowiązanie administratorów danych i podmiotów przetwarzających do zapewnienia inspektorowi ochrony danych zasobów niezbędnych do utrzymania wysokiego i aktualnego poziomu wiedzy (art. 38 ust. 2 RODO). Mimo iż ogólne rozporządzenie o ochronie danych bardzo mocno akcentuje wymóg wiedzy i fachowości DPO, nie reguluje zasad czy trybu weryfikacji spełnienia tego wymogu. Niemniej certyfikaty, dyplomy oraz inne dokumenty poświadczające wiedzę i doświadczenie inspektora niewątpliwie w większości przypadków będą ważnym kryterium kwalifikacyjnym i argumentem przemawiającym na korzyść osoby wyznaczanej do pełnienia tej funkcji.

Data wytworzenia informacji: 15.01.2019 r.

Czy IOD może być pracownikiem administratora?

Zgodnie z art. 37 ust. 6 RODO inspektorem ochrony danych może zostać zarówno pracownik administratora lub podmiotu przetwarzającego, jak i osoba spoza grona pracowników ww. podmiotów (outsourcing).

Data wytworzenia informacji: 15.01.2019 r.

Czy członek zarządu stowarzyszenia może być w nim jednocześnie inspektorem ochrony danych?

Niedopuszczalne jest powołanie na IOD osoby będącej kierownikiem (zarządzającym) podmiotem posiadającym status administratora lub podmiotu przetwarzającego, takich jak np. członka zarządu stowarzyszenia, dyrektora szkoły, wójta, członka zarządu spółki. Przyjęcie odmiennego stanowiska prowadziłoby do sytuacji, w których IOD w zakresie przestrzegania przepisów o ochronie danych osobowych - oceniałby i monitorował samego siebie.

Zgodnie z art. 38 ust. 3 RODO, IOD ma podlegać bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego, nie zaś być członkiem organu zarządzającego tym podmiotem.

Data wytworzenia informacji: 07.01.2019 r.

Czy IOD może jednocześnie pełnić funkcję pełnomocnika do spraw ochrony informacji niejawnych?

RODO nie zakazuje wprost łączenia obu tych funkcji. W każdym konkretnym przypadku konieczne jest jednak dokonanie rzetelnej oceny pod kątem spełnienia wszystkich warunków gwarantujących IOD niezależne i prawidłowe wykonywanie swoich zadań.

Po pierwsze, powyższe rozwiązanie nie może wpływać na prawidłowe umiejscowienie IOD w strukturze administratora i wykonywanie jego zadań w sposób niezależny. W zakresie zapewniania przestrzegania przepisów o ochronie danych osobowych, IOD nie może podlegać ani otrzymywać poleceń od jakichkolwiek innych osób niż kierownika jednostki organizacyjnej lub osoby fizycznej będącej administratorem. Analogiczny wymóg dotyczy pełnomocnika ds. ochrony informacji niejawnych, który zgodnie z art. 14 ust. 2 ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych, powinien podlegać bezpośrednio kierownikowi jednostki organizacyjnej, w której wykonuje swoje obowiązki.

Po drugie, łączenie tych funkcji nie może prowadzić do konfliktu interesów (art. 38 ust. 6 RODO). Wystąpienie sprzecznych priorytetów skutkować mogłoby zaniedbaniem obowiązków pełnionych przez IOD. W każdej konkretnej sytuacji należy zatem starannie przeanalizować (podobnie zresztą jak w przypadku łączenia funkcji IOD z jakimikolwiek innymi zadaniami), czy IOD jest w stanie wykonywać swoje zadania w sposób prawidłowy przy pełnieniu obu funkcji jednocześnie. Należy zatem przemyśleć ilość czasu potrzebnego na wykonywanie poszczególnych obowiązków (w tym na współpracę z innymi służbami kontrolnymi), stopień skomplikowania i ważności zadań, rezerwę czasową na nieplanowane zadania, ilość i rodzaj danych osobowych oraz procesów i systemów informatycznych służących do ich przetwarzania, obszary ryzyka, związane z tymi procesami. Pod rozwagę należy brać również wiele innych czynników, takich jak np. struktura, wielkość i zasoby kadrowe danego podmiotu (w tym również pod kątem obowiązku prowadzenia szkoleń personelu). W szczególności, w przypadku IOD zatrudnionego w niepełnym wymiarze czasu pracy, albo łączącego obowiązki IOD z innymi zadaniami, priorytetem powinno być zapewnienie IOD odpowiedniej ilości czasu na wykonywanie powierzonych zadań.

Zdaniem Grupy Roboczej art. 29 dobrą praktyką byłoby wskazanie czasu, który należy poświęcić na obowiązki IOD. Takiego samego uwzględnienia i analizy wymagają obowiązki związane z pełnieniem funkcji pełnomocnika do spraw informacji niejawnych. Starannie należy rozważyć ilość informacji niejawnych oraz ich rodzaj, a także czas i możliwości wykonywania wszystkich zadań określonych w art. 15 ustawy o ochronie informacji niejawnych, do których należy m.in. zapewnienie ochrony informacji niejawnych, w tym stosowanie środków bezpieczeństwa fizycznego, zapewnienie ochrony systemów teleinformatycznych, w których są przetwarzane informacje niejawne, zarządzanie ryzykiem bezpieczeństwa, w szczególności szacowanie ryzyka, kontrola ochrony informacji niejawnych oraz przestrzegania przepisów o ochronie tych informacji.

W świetle art. 38 ust. 2 RODO administrator oraz podmiot przetwarzający zapewniają inspektorowi zasoby niezbędne do wykonywania zadań wskazanych w art. 39 RODO oraz zasoby niezbędne do utrzymania jego fachowej wiedzy. Obowiązek ten oznacza, że IOD powinien posiadać takie środki organizacyjne, techniczne, technologiczne oraz finansowe, aby móc efektywnie realizować ciążące na nim obowiązki związane z pełnioną funkcją.

Ustawa o ochronie informacji niejawnych przewiduje natomiast w art. 15 ust. 2, że pełnomocnik ds. informacji niejawnych realizuje swoje zadania przy pomocy wyodrębnionej i podległej mu komórki organizacyjnej do spraw ochrony informacji niejawnych, jeżeli jest ona utworzona w jednostce organizacyjnej. Komórką taką może być też kancelaria tajna zgodnie z art. 42 ust. 4 ustawy o ochronie informacji niejawnych. W przypadku utworzenia takiej komórki, pełnomocnik ds. informacji niejawnych może dysponować pomocą i wsparciem pracowników „pionu ochrony" przy realizacji swoich zadań w związku z pełnioną funkcją, co w konkretnych, uzasadnionych przypadkach może pozytywnie wpłynąć na ocenę możliwości łączenia obu omawianych funkcji. IOD również może być wspierany przez zespół IOD.

Warto zaznaczyć, że zadania IOD dotyczą wszystkich danych osobowych przetwarzanych przez administratora, natomiast zadania pełnomocnika ds. informacji niejawnych koncentrują się na szczególnej kategorii informacji, jakimi są informacje niejawne. Niemniej zadania przypisywane obu funkcjom wykazują pewne podobieństwa, a wiedza i doświadczenie potrzebne do pełnienia jednej z tych funkcji mogą być pomocne w pełnieniu drugiej.

Data wytworzenia informacji: 07.01.2019 r.

Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji?

Zgodnie z art. 38 ust. 6 RODO IOD może wykonywać inne zadania i obowiązki przy czym administrator lub podmiot przetwarzający powinni zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Oznacza to, że IOD nie może zajmować w organizacji stanowiska, na którym określa się sposoby i cele przetwarzania danych.

W Wytycznych Grupy Roboczej Art. 29 dotyczące inspektorów ochrony danych (DPO) wskazane zostały przykłady takich stanowisk. Należą do nich: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli sprawujące je osoby biorą udział w określaniu celów i sposobów przetwarzania danych (Wytyczne Grupy Roboczej art. 29).

Powołanie na IOD kierownika komórki w organizacji, np. dyrektora departamentu IT, który jako kierownik decydowałby o sposobach zabezpieczeń systemów informatycznych, projektowałby systemy służące przetwarzaniu danych osobowych, bądź dyrektora działu kadr, który decydowałby np. jakie dane są zbierane od potencjalnych kandydatów do pracy, a z drugiej strony – jako IOD badałby zgodność przetwarzania danych z przepisami o ochronie danych osobowych spowoduje, że osoba taka będzie sama kontrolowała procesy przetwarzania danych, o których jako kierownik danej komórki będzie jednocześnie decydować. Warto zaznaczyć, że nawet jeśli osoba ta osobiście nie tworzyłaby wskazanych systemów, ale np. projektowałby je pracownik danej komórki, to fakt ten byłby bez znaczenia, ponieważ to kierownik odpowiada za całość działań komórki, w tym podległych mu pracowników.

Ponadto administrator, rozważając wyznaczenie na IOD kierownika komórki w organizacji, powinien uwzględnić, co najmniej trzy kryteria:

- organizacyjne (IOD powinien podlegać bezpośrednio najwyższemu kierownictwu jednostki organizacyjnej),
- merytoryczne (inne obowiązki nie powinny negatywnie wpływać na niezależne wykonywanie zadań IOD),
- czasowe (IOD powinien dysponować czasem wystarczającym do wykonywania swoich zadań, przy uwzględnieniu m.in. liczby obowiązków czy stopnia ich skomplikowania).

Uwzględnienie kryterium czasowego powinno obejmować analizę, czy IOD pełniący jednocześnie inną funkcję, będzie w stanie wykonywać swoje obowiązki we właściwy sposób, biorąc pod uwagę w szczególności stopień skomplikowania i liczbę innych zadań. IOD powinien dysponować czasem pozwalającym mu na prawidłowe realizowanie wszystkich zadań.

Reasumując, jednoczesne pełnienie funkcji IOD i funkcji kierownika komórki w organizacji nie jest w RODO wprost zakazane, lecz nieprzeprowadzenie analizy w tym zakresie przez administratora oraz nieuwzględnienie wskazanych kryteriów może w konsekwencji spowodować naruszenie przepisów o ochronie danych osobowych.

Data wytworzenia informacji: 07.01.2019 r.

Czy możliwe jest łączenie funkcji IOD z obowiązkami administratora systemu informatycznego (ASI)?

W większości przypadków zakres obowiązków związanych z pełnieniem funkcji ASI jest uregulowany jedynie w sferze wewnętrznej danego administratora, np. w polityce bezpieczeństwa lub wynika z zakresu obowiązków pracownika bądź z umowy o świadczenie usług zawartej z osobą spoza określonej organizacji. Zdarza się, że zadania ASI w odniesieniu do

konkretnych systemów wskazane są w szczególnych przepisach prawa, np. art. 10 ust. 2 ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego; art. 2 pkt 2 ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia. Pełnienie funkcji ASI jest najczęściej powierzane informatykowi lub kierownikowi działu IT, a do jego głównych zadań należy: administrowanie serwerami służącymi przetwarzaniu danych, wdrożenie zabezpieczeń systemów informatycznych, wykrycia nieautoryzowanego dostępu do systemu, zachowanie ciągłości ich funkcjonowania, konfigurowanie kont użytkowników. Z tego powodu, łączenie funkcji IOD i ASI w konkretnych przypadkach może być uznane za niezgodne z RODO. Oceny w tym zakresie należy dokonywać z punktu widzenia spełnienia wymogów, jakie w RODO wskazano w odniesieniu do IOD, w tym w szczególności jego niezależności, właściwego umiejscowienia w strukturze organizacyjnej administratora oraz realnej możliwości prawidłowego wykonywania wyznaczonych mu zadań. Z tej perspektywy konsolidacja funkcji IOD z funkcją ASI może powodować zagrożenia dla bezpieczeństwa przetwarzania danych osobowych. Osoba odpowiadająca za bieżące prowadzenie przetwarzania danych osobowych i bezpieczeństwo danych w systemach informatycznych będzie bowiem sprawować jednocześnie nadzór nad zgodnością z prawem wykonywanych przez siebie działań. Sytuacja taka powoduje zatem faktyczny brak nadzoru nad zgodnością przetwarzania danych z przepisami prawa, w tym przepisami określającymi wymogi co do bezpieczeństwa danych osobowych.

IOD nie może podlegać jakimkolwiek innym osobom niż najwyższe kierownictwo (art. 38 ust. 3 RODO), co ma mu gwarantować niezależne, prawidłowe i skuteczne wykonywanie funkcji. Najwyższym kierownictwem jednostki organizacyjnej - w zależności od jej rodzaju – może być osoba lub osoby (np. wchodzące w skład organu), które kierują jej pracami (np. ministrowie kierujący działami administracji rządowej, dyrektorzy szkół), prowadzą jej sprawy (np. zarząd spółki) albo podejmują zarobkową działalność (np. przedsiębiorcy jednoosobowi), działając jako administrator. W przypadku jednoczesnego pełnienia funkcji IOD i ASI wykluczone jest rozwiązanie, w którym osoba taka podlegałaby np. dyrektorowi ds. informatycznych, kierownikowi działu IT lub jakiejkolwiek innej osobie (np. dyrektorowi generalnemu urzędu publicznego), która nie jest najwyższym kierownictwem w rozumieniu art. 38 ust. 3 RODO.

Zgodnie z art. 38 ust. 6 RODO IOD może wykonywać inne zadania i obowiązki przy czym administrator lub podmiot przetwarzający powinni zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. RODO nie precyzuje w jakich sytuacjach będzie zachodził, wskazany w art. 38 ust. 6 RODO, konflikt interesów. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Oznacza to, że IOD nie może zajmować w organizacji stanowiska, na którym określa się sposoby i cele przetwarzania danych.

Za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu

marketingu, kierownik działu HR, kierownik działu IT) oraz niższe stanowiska, jeśli osoby je piastujące biorą udział w określaniu celów i sposobów przetwarzania danych.

Dlatego też ww. konflikt interesów może obejmować również stanowiska związane z bezpieczeństwem w organizacji, o ile z ich piastowaniem wiąże się decydowanie - w jakikolwiek sposób o sposobach i celach przetwarzania danych osobowych w organizacji.

Podsumowując, ocena czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana indywidualnie z uwzględnieniem konkretnych okoliczności. Oznacza to, że możliwość zaistnienia konfliktu powinna być stale monitorowana, ponieważ przyczyny zaistnienia takiego konfliktu mogą występować również w późniejszym czasie, po rozpoczęciu pełnienia funkcji przez IOD.

Data wytworzenia informacji: 07.01.2019 r.

Czy funkcję IOD może pełnić obcokrajowiec?

Funkcja inspektora ochrony danych osobowych może być w Polsce pełniona przez obcokrajowca. Należy jednak podkreślić, iż jednym z ważnych zadań IOD jest pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą (art. 38 ust. 4 RODO) oraz dla organu nadzorczego (art. 39 ust. 1 lit. e RODO). Grupa Robocza art. 29 ds. ochrony danych w Wytycznych dotyczących inspektorów ochrony danych (str. 11) wskazuje, że IOD „powinien mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą i współpracy z właściwymi organem nadzorczym. Oznacza to również, że komunikacja musi odbywać się w języku lub językach używanych przez organy nadzorcze i osoby, których dane dotyczą."

W konsekwencji należy uznać, że administrator zobowiązany jest zapewnić sprawną i efektywną komunikacją pomiędzy IOD a organem nadzorczym oraz osobami, których dane dotyczą, w języku polskim.

Data wytworzenia informacji: 07.01.2019 r.

Czy funkcję IOD może pełnić osoba spoza organizacji administratora/podmiotu przetwarzającego?

Zgodnie z art. 37 ust. 6 RODO inspektorem ochrony danych może zostać zarówno pracownik administratora lub podmiotu przetwarzającego, jak i osoba spoza grona pracowników ww. podmiotów. Możliwe będzie więc nadal pełnienie funkcji inspektora ochrony danych w modelu outsourcingu, na podstawie umowy o świadczenie usług. Podkreślenia wymaga jednak, że osoba wykonująca funkcję IOD na podstawie umowy o świadczenie usług musi spełniać wszystkie wymogi stawiane przez przepisy RODO, np. wymogi dotyczące unikania konfliktu interesów,

gwarancji niezależności, łatwości nawiązania z nim kontaktu, właściwego i terminowego włączania go we wszystkie sprawy dotyczące ochrony danych osobowych.

Podkreślenia wymaga fakt, iż konieczne będzie zawiadomienie organu nadzorczego przez każdego z administratorów/podmiotów przetwarzających o wyznaczeniu konkretnej osoby oraz jak wynika z art. 10 ust. 1 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, podania następujących informacji tj.: imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora.

Data wytworzenia informacji: 15.01.2019 r.

Czy można powołać więcej niż jednego IOD?

Przepisy o ochronie danych osobowych nie przewidują możliwości wyznaczenia więcej niż jednego IOD. Zarówno wewnątrz podmiotu będącego administratorem danych, jak w relacjach zewnętrznych, dla wszystkich musi być jasne, kto pełni tę ważną funkcję i jest odpowiedzialny za monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa. Innymi słowy: osoba ta powinna być wyraźnie wskazana przez kierownictwo jednostki zarówno wszystkim zatrudnionym przy przetwarzaniu danych osobowych, jak i - na zewnątrz organizacji - osobom, których dane dotyczą oraz organowi nadzorczemu. Dla osób, których dane dotyczą, oraz dla organu nadzorczego IOD jest punktem kontaktowym zgodnie z art. 38 ust. 4 i art. 39 ust. 1 lit. e RODO. Przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 11) zobowiązują administratora i podmiot przetwarzający, którzy wyznaczyli IOD, by udostępnili imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora na swojej stronie internetowej. Jeżeli administrator lub podmiot przetwarzający nie prowadzi własnej strony, udostępnia informacje o IOD w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Dane inspektora w powyższym zakresie muszą być przekazane również Prezesowi UODO (art. 10 tej ustawy).

Data wytworzenia informacji: 07.01.2019 r.

Czy po wejściu stosowania RODO CUW może powołać jednego IOD dla wszystkich obsługiwanych jednostek?

Centra Usług Wspólnych (CUW) są tworzone jako osobne podmioty, a domeną ich działań są najczęściej działania pomocnicze, wykonywane zarówno w odniesieniu do organów wykonawczych, jak i uchwałodawczych samorządu terytorialnego, jak również do obsługi poszczególnych jednostek organizacyjnych, między innymi urzędów, zakładów i jednostek

budżetowych. Ostateczną decyzję, zarówno co do powołania samorządowego centrum usług wspólnych, jak i jego kształtu oraz zakresu realizowanych przez niego zadań, podejmuje organ stanowiący danej jednostki samorządu terytorialnego.

CUW nie jest administratorem danych przekazanych przez jednostki obsługiwane. Może je przetwarzać w zakresie i celu niezbędnym do wykonywania zadań w ramach wspólnej obsługi tych jednostek (zgodnie z art. 10d ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, art. 6d ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym i art. 8f ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa). W zależności od różnych możliwych rozwiązań stosowanych przez konkretne samorządy, CUW może być natomiast administratorem danych np. swoich pracowników.

Na gruncie ogólnego rozporządzenia o ochronie danych obowiązek wyznaczenia inspektora ochrony danych w sektorze publicznym dotyczyć będzie wszystkich organów i podmiotów publicznych (art. 9 u.o.d.o.), zarówno tych będących administratorami danych, jak i podmiotami przetwarzającymi.

Niemniej nawet w sytuacji, gdyby miał być nim pracownik jednej z tych jednostek, np. pracownik CUW, konieczne jest osobne wyznaczenie IOD przez każdą z tych jednostek, np. każdą szkołę, dom kultury – jako osobnych administratorów. Zatem nawet jeżeli CUW świadczy obsługiwanym podmiotom usługi związane z szeroko rozumianą ochroną danych osobowych, nie jest uprawniony do wyznaczania inspektora ochrony danych w tych podmiotach. Obowiązek wyznaczania inspektora ochrony danych nie może być przeniesiony, np. w drodze uchwały czy porozumienia, na inną jednostkę organizacyjną, np. na CUW.

Każdy z podmiotów zobowiązanych do wyznaczenia inspektora ochrony danych (niezależnie, czy będzie to jedna, ta sama osoba, czy różne osoby) będzie również zobowiązany - zgodnie z art. 37 ust. 7 RODO - do opublikowania danych kontaktowych inspektora i zawiadomienia o nich organu nadzorczego. Tak jak o danych kontaktowych dotyczy zatem każdej jednostki samorządu terytorialnego, o której mowa w art. 37 ust. 1 lit. a RODO.

Data wytworzenia informacji: 15.01.2019 r.

Ile maksymalnie podmiotów będzie mógł obsługiwać jeden IOD?

Ani przepisy rozporządzenia ogólnego, ani ich interpretacje wydawane np. przez Grupę Roboczą Art. 29 w postaci wytycznych, nie dają odpowiedzi na takie pytanie. Stosowanie tego rozwiązania będzie mogło jednak następować jedynie w uzasadnionych przypadkach, a liczba obsługiwanych podmiotów musi się mieścić w racjonalnych granicach. Ocena tej kwestii zależna jest od wielu czynników, w tym m.in. od: efektywnej dostępności inspektora, możliwości uzyskania przez niego szczegółowej wiedzy na temat funkcjonowania podmiotu, dysponowania przez niego

odpowiednią do zakresu zadań i specyfiki procesów przetwarzania danych ilością czasu, konieczności unikania konfliktu interesów oraz wielkości i struktury organizacyjnej jednostki będącej administratorem danych. Na powyższe pytanie konkretnie będzie można zatem odpowiedzieć jedynie w kontekście konkretnych sytuacji. Niemniej tak jak każda decyzja dotycząca przyjmowanych rozwiązań w zakresie ochrony danych osobowych, również decyzja w zakresie wyboru odpowiedniej osoby do pełnienia funkcji inspektora, musi być podejmowana z pełną świadomością ciążącej na administratorze danych odpowiedzialności za prawidłowe przestrzeganie przepisów prawa.

Data wytworzenia informacji: 15.01.2019 r.

Czy różni przedsiębiorcy niewchodzący w skład tej samej grupy mogą powołać jednego IOD?

Art. 37 ust. 2 RODO wyraźnie przewiduje możliwość powołania jednego inspektora ochrony danych przez administratorów tworzących grupę przedsiębiorstw, np. grupę kapitałową, o ile będzie można nawiązać z nim kontakt z każdej jednostki organizacyjnej. Grupa przedsiębiorstw została zdefiniowana w przepisach rozporządzenia jako przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane.

Prawodawca europejski w art. 37 ust. 2 RODO przyjął model niejako „wspólnego wyznaczenia inspektora ochrony danych" przez grupę przedsiębiorstw, ze względu na wzajemne powiązania tych przedsiębiorstw, wspólne regulacje wewnętrzne, podobne zasady i sposoby postępowania z danymi osobowymi.

Każde z przedsiębiorstw, wyznaczając na swojego inspektora tę samą osobę, będzie miało możliwość pozostawania jednocześnie w zgodzie nie tylko z warunkiem wskazanym w tym przepisie (łatwości nawiązania kontaktu z inspektorem), ale też ze wszystkimi innymi wymaganiami określonymi w przepisach prawa co do inspektorów ochrony danych. Co bardzo ważne - w takiej sytuacji możliwe będzie np. racjonalne i wspólne określenie zasad dotyczących zapewnienia takiemu inspektorowi wystarczającej ilości czasu na wypełnianie jego obowiązków, pomoc w stworzeniu planu jego pracy, a w razie potrzeby wsparcie jego funkcjonowania

zespołem odpowiednich specjalistów. Inspektor obsługujący grupę podobnie funkcjonujących podmiotów ma możliwość rzetelnego poznania szczegółów ich funkcjonowania oraz obowiązujących je przepisów. Z powyższych powodów rozwiązanie przyjęte w art. 37 ust. 2 wydaje się racjonalne i uzasadnione, i można przypuszczać, że grupy przedsiębiorstw będą chciały z niego korzystać.

Regulacja przyjęta w tym przepisie nie oznacza jednak, że nie jest dopuszczalne wyznaczenie jednej osoby przez kilku administratorów danych poza wskazanym przypadkiem, czyli poza grupą

przedsiębiorstw. Przepisy RODO nie zawierają bowiem zakazu w tym zakresie. W każdym przypadku skorzystania z takiego rozwiązania bezwzględnym warunkiem jest to, żeby ta osoba była w stanie autentycznie wypełniać swoje obowiązki wobec każdej obsługiwanej przez niego organizacji i to w sposób w pełni odpowiadający przepisom prawa i potrzebom konkretnego administratora danych (zobacz też odpowiedź na pytanie „Czy podmioty publiczne mogą powołać jednego IOD poza sytuacją uregulowaną w art. 37 ust. 2 RODO?").

Data wytworzenia informacji: 06.02.2019 r.

Czy podmioty publiczne mogą powołać jednego IOD poza sytuacją uregulowaną w art. 37 ust. 3 RODO?

Zgodnie z art. 37 ust. 3 RODO jednego inspektora będzie mogło powołać - przy uwzględnieniu ich struktury organizacyjnej i wielkości - kilku administratorów danych będących podmiotami publicznymi, np. publiczne placówki oświatowe, muzea. Podmioty takie, np. ze względu na realizowanie zadań publicznych w tym samym obszarze, mogą przyjmować podobne rozwiązania organizacyjne i korzystać z tych samych procedur.

Przepisy RODO nie zawierają wyrażonego wprost zakazu wyznaczania przez kilka podmiotów publicznych tej samej osoby na inspektora ochrony danych poza sytuacją wskazaną w art. 37 ust. 3. Skorzystanie z takiego rozwiązania wymaga dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora danych.

Trzeba mieć przy tym świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył oraz tzw. „efektywnej dostępności" inspektora dla osób z danej organizacji. Do zadań IOD należy np. bieżące monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa oraz udzielanie informacji i rad w zakresie obowiązków wynikających z tych przepisów. Zwłaszcza w pierwszych latach stosowania nowych przepisów inspektorzy będą odgrywać ważną rolę we wspieraniu „kultury ochrony danych" i pomagać w zrozumieniu i implementacji wszystkich elementów unijnego rozporządzenia, spośród których wiele jest w naszym systemie prawa nowością.

Trudno będzie również wykonywać równolegle w wielu podmiotach zadania w zakresie punktu kontaktowego dla osób, których dane dotyczą oraz punktu kontaktowego dla organu nadzorczego. Na mocy rozporządzenia każda osoba w każdej sprawie dotyczącej jej danych ma prawo kontaktować się z wyznaczonym dla danej organizacji inspektorem. Organ nadzorczy będzie natomiast mógł wymagać od inspektora gotowości do współpracy w związku z realizacją

zadań i uprawnień organu w zakresie prowadzonych postępowań, a także tzw. „uprzednich konsultacji".

Każda osoba pełniąca funkcję DPO musi unikać konfliktu interesów. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Zatem z pełnieniem funkcji inspektora wiążą się bardzo konkretne wymagania prawne i wymagań tych trzeba będzie sumiennie przestrzegać.

Data wytworzenia informacji: 15.01.2019 r.

Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?

Inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora, czy też nie – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny (motyw 97 RODO).

W celu zapewnienia niezależności inspektorowi ochrony danych ogólne rozporządzenie o ochronie danych, wprowadza kilka szczegółowych rozwiązań, które pozwalają na osiągnięcie ww. celu, a mianowicie:

a) **bezpośrednia podległość IOD najwyższemu kierownictwu,**

b) **wspieranie IOD w wypełnianiu jego zadań,**

c) **zapewnienie udziału IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych,**

d) **zakaz wydawania instrukcji IOD co do wykonywania przez niego zadań,**

e) **unikanie konfliktu interesów IOD,**

f) **zakaz odwoływania i karania IOD,**

g) **obowiązek zachowania tajemnicy lub poufności co do wykonywania zadań przez IOD.**

Jako dobrą praktykę Grupa Robocza art. 29 w swoich wytycznych dotyczących IOD, wskazuje wprowadzenie wewnętrznych regulacji (regulaminów, statutów) gwarantujących inspektorowi ochrony danych niezależność w wykonywaniu przez niego zadań.

a) bezpośrednia podległość IOD najwyższemu kierownictwu

Jednym ze szczegółowych rozwiązań służących niezależności IOD jest umieszczenie go pod najwyższym kierownictwem. Zgodnie z art. 38 ust. 3 RODO IOD podlega bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

Podległość najwyższemu kierownictwu jest jedną z gwarancji niezależnej, wysokiej pozycji inspektora ochrony danych w strukturze administratora danych, a ponadto skraca drogę raportowania, co ma istotne znaczenie w razie konieczności podejmowania szybkich działań naprawczych w sytuacji naruszenia ochrony danych osobowych.

Bezpośrednia podległość oznacza, że w ramach podejmowanych przez siebie czynności IOD nie może podlegać jakimkolwiek innym osobom lub jednostkom organizacyjnym wchodzącym w skład struktury administratora danych (art. 38 ust. 3 RODO).

Sposób rozumienia terminu najwyższe kierownictwo na pewno zależy od typu podmiotu jakim jest administrator lub podmiot przetwarzający. Tytułem przykładu wskazać można, że „najwyższym kierownictwem" będzie osoba lub osoby wchodzące w skład organu, które kierują jej pracami (ministrowie kierujący działami administracji rządowej, dyrektorzy szkół), albo prowadzą jej sprawy (zarząd spółki, wspólnicy spółki jawnej, właściciel jednoosobowej działalności gospodarczej).

b) wspieranie IOD w wypełnianiu jego zadań

Administrator danych i podmiot przetwarzający są zobowiązani do wspierania inspektora ochrony danych poprzez m.in. zapewnienie mu zasobów niezbędnych do wykonania tych zadań.

Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych opowiada się za szerokim rozumieniem zasobów:

- wsparcie IOD ze strony kadry kierowniczej (np. na poziomie zarządu),
- wymiar czasu umożliwiający IOD wykonywanie zadań,
- odpowiednie wsparcie finansowe, infrastrukturalne (pomieszczenia, sprzęt, wyposażenie) i kadrowe, gdy to właściwe,
- oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia IOD i jego zadaniach,
- umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT itd.
- ciągłe szkolenie. DPO powinien mieć możliwość ciągłego aktualizowania wiedzy z zakresu ochrony danych osobowych. Celem powinno być zwiększanie wiedzy DPO i zachęcanie go do udziału w szkoleniach, warsztatach, forach poświęconych ochronie danych etc.;
- wsparcie kadrowe, np. powołanie zespołu inspektora ochrony danych.

c) zapewnienie udziału IOD we wszystkich zagadnieniach związanych z ochroną danych osobowych

Artykuł 38 RODO zobowiązuje administratora oraz podmiot przetwarzający do zapewnienia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych

osobowych. Norma ta ma zapobiegać próbom ograniczania inspektorowi dostępu do niezbędnych dla realizacji jego zadań informacji, a tym samym sprzyja zachowaniu jego niezależności.

Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektora ochrony danych niezwykle istotne jest, by IOD był zaangażowany od najwcześniejszego etapu we wszystkie kwestie związane z przetwarzaniem danych osobowych, ponieważ ułatwi to zapewnienie zgodności z RODO. Przepisy ogólnego rozporządzenia o ochronie danych w określonych przypadkach wprost nakazują administratorowi angażowanie IOD w podejmowanie określonych czynności i decyzji, np. nakazują administratorowi konsultowanie się z IOD przy okazji dokonywania takiej oceny skutków. W związku z tym angażowanie inspektora ochrony danych we wszelkie kwestie związane z ich przetwarzaniem powinno być standardową procedurą w organizacji.

Ponadto IOD powinien być postrzegany jako partner w dyskusji i powinien być włączany w prace grup roboczych poświęconych procesom związanym z przetwarzaniem danych osobowych w ramach organizacji. Należy zapewnić mu między innymi: udział w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji, uczestnictwo przy podejmowaniu kluczowych decyzji dotyczących przetwarzania danych osobowych wraz z odpowiednio wcześniejszym udostępnieniem IOD informacji umożliwiających zajęcie mu stanowiska, natychmiastowe konsultowanie się z nim w przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi, określenie przez administratora lub podmiot przetwarzający innych przypadków, które wymagają konsultacji z IOD.

Ponadto stanowisko IOD powinno być zawsze brane pod uwagę przez kierownictwo oraz pracowników danego podmiotu. Grupa Robocza art. 29 zaleca, aby w ramach dobrych praktyk, dokumentować przypadki i powody postępowania niezgodnego z zaleceniem IOD.

d) zakaz wydawania instrukcji IOD co do wykonywania przez niego zadań

Istotną gwarancją w zakresie niezależności inspektora ochrony danych jest niewątpliwie wprowadzenie zakazu wydawania przez administratora lub podmiotu przetwarzającego instrukcji

(poleceń) dla IOD dotyczących wykonywania przez niego zadań (art. 38 ust. 3 RODO). Zakaz wydawania instrukcji inspektorowi ochrony danych, oznacza, że w ramach wypełniania swoich zadań inspektor ochrony danych, nie może otrzymywać poleceń dotyczących sposobu załatwienia sprawy, środków jakie mają zostać podjęte, czy też celu jaki powinien zostać osiągnięty. Ponadto, administrator nie powinien uniemożliwiać, bądź ograniczać inspektorowi ochrony danych kontaktu z Prezesa Urzędu Ochrony Danych Osobowych.

W Wytycznych dotyczących inspektora ochrony danych Grupa Robocza art. 29 wskazuje, że IOD nie może również zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, w tym określonej wykładni przepisów.

Z drugiej strony Grupa Robocza art. 29 podkreśla, że niezależność IOD (w tym również w kontekście zakazu do wydawania instrukcji, co do wykonywania zadań IOD) nie oznacza, iż IOD posiada uprawnienia decyzyjne wykraczające poza zadania z art. 39 RODO. Nie zmienia to faktu, że za zapewnienie zgodności z przepisami o ochronie danych osobowych i wykazanie zgodności odpowiedzialni są administrator i podmiot przetwarzający. W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami IOD, inspektor ochrony danych powinien mieć możliwość jasnego przedstawienia swojego stanowiska osobom podejmującym decyzję.

Respektowanie powyższego zakazu może być szczególnie problematyczne na styku wykonywania wewnętrznego audytu różnych sfer działalności podmiotu będącego administratorem danych. Szczególnie ważne, zwłaszcza na początku funkcjonowania omawianego przepisu, może być dokonanie wnikliwej analizy zakresu i celów poszczególnych stanowisk związanych z wewnętrznym audytem, tak aby inne osoby wewnątrz organizacji np. prawnicy, audytorzy mogli realizować swoje zadania, nie naruszając przedmiotowego zakazu.

e) unikanie konfliktu interesów IOD

Zgodnie z art. 38 ust. 6 RODO, istnieje możliwość nakładania na inspektora ochrony danych innych zadań i obowiązków, ale administrator i podmiot przetwarzający muszą zapewnić by nie powodowało to konfliktu interesów. Zatem jak wyjaśnia Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych oznacza to m.in., że IOD nie może zajmować w organizacji stanowiska związanego z określaniem sposobów i celów przetwarzania danych. Aspekt ten powinien być analizowany osobno i indywidualne dla każdego podmiotu. Powierzając inspektorowi ochrony danych inne zadania, w celu uniknięcia konfliktu interesów administrator danych lub podmiot przetwarzających, powinni w swojej organizacji zidentyfikować stanowiska niekompatybilne z pełnieniem funkcji IOD.

Cenną podpowiedzią w tym zakresie jest wskazanie, że co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych. Ponadto konflikt interesów może powstać wówczas, gdy zewnętrzny IOD zostanie poproszony o reprezentowanie administratora lub podmiotu przetwarzającego przed sądem w sprawie dotyczącej ochrony danych osobowych.

Wskazane byłoby też opracowanie wewnętrznej polityki określającej stanowiska będące w konflikcie interesów oraz opracowanie generalnego dokumentu dotyczącego konfliktu interesów. Ponadto administrator lub podmiot przetwarzający powinni wprowadzić odpowiednie zabezpieczenia do wewnętrznych zasad organizacji celem zapewnienia, by ogłoszenia o rekrutacji

na stanowisko inspektora ochrony danych były sformułowane w jasny, precyzyjny sposób i niwelowały ryzyko powstania konfliktu interesów.

f) zakaz odwoływania i karania IOD

Zachowanie niezależności przez inspektora ochrony danych wspiera również art. 38 ust. 3 RODO, stanowiący, że administrator lub podmiot przetwarzający nie może odwołać ani karać IOD za wypełnianie przez niego zadań. Oczywiście przepis ten należy odnosić do obiektywnie prawidłowego wykonywania zadań. Nie chodzi tu o ochronę inspektora, który nie wywiązuje się należycie ze swoich zadań. Jest to jedyny przepis w ogólnym rozporządzeniu o ochronie danych dotyczący odwołania IOD.

Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektora ochrony danych inspektor nie może zostać odwołany ani ukarany za udzielenie określonego zalecenia, nawet jeśli jest ono niezgodne ze stanowiskiem reprezentowanym przez administratora lub podmiot przetwarzający. Grupa Robocza art. 29 wyjaśnia, że chodzi tu o kary w różnych formach, bezpośrednie albo pośrednie, np. brak albo opóźnienie awansu, utrudnienie rozwoju zawodowego, ograniczenie dostępu do korzyści oferowanych pozostałym pracownikom. Zakaz odwoływania inspektora ochrony danych, nie oznacza natomiast, że IOD nie może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie swoich obowiązków (np. z powodu kradzieży). Grupa Robocza art. 29 zaleca stosowanie polityki, że im stabilniejsza podstawa zatrudnienia i szerszy zakres ochrony inspektora ochrony danych przed odwołaniem, tym większa szansa na wykonywanie przez IOD zadań w sposób niezależny.

g) obowiązek zachowania tajemnicy lub poufności co do wykonywania zadań przez IOD

IOD jest zobowiązany do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań zgodnie z prawem Unii lub państwa członkowskiego (art. 38 ust. 5 RODO).

Jeśli chodzi o IOD, to w związku z wykonywaniem swoich zadań będzie on miał niewątpliwie dostęp do danych osobowych, w tym danych osobowych, o których mowa w art. 9 ust. 1 RODO oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o których mowa w art. 10 RODO, jak również informacji dotyczących środków technicznych i organizacyjnych zapewniających przetwarzanie zgodne z przepisami RODO, w tym polityk ochrony danych. IOD będzie również zobowiązany do przestrzegania wszystkich przepisów prawa krajowego i unijnego, które będą miały do niego zastosowanie i na mocy których, określone informacje objęte są prawnie chronionymi tajemnicami. Zobowiązanie inspektora ochrony danych do przestrzegania tajemnicy jest w pełni uzasadnione i służyć będzie nie tylko bezpieczeństwu danych osobowych, ale i wzmocnieniu zaufania do inspektorów ze strony administratorów danych i podmiotów przetwarzających. Co ważne - w Wytycznych dotyczących inspektora ochrony danych Grupa Robocza art. 29 podkreśla, że obowiązek zachowania tajemnicy

oraz poufności nie uniemożliwia IOD kontaktu z Prezesem Urzędu Ochrony Danych Osobowych i zasięgania jego opinii.

Data wytworzenia informacji: 11.02.2019 r.

Kto wysyła powiadomienie o odwołaniu inspektora ochrony danych w przypadku likwidacji administratora

Kto powinien zawiadomić Prezesa UODO o odwołaniu inspektora ochrony danych w przypadku likwidacji/przejęcia administratora, który wyznaczył tego inspektora (np. w przypadku likwidacji gimnazjum)?

Powiadomienia Prezesa Urzędu Ochrony Danych Osobowych o odwołaniu dotychczasowego inspektora ochrony danych powinien dokonać podmiot, który go wyznaczył. Obowiązek ten wynika z art. 10 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

W sytuacji zaś, gdy administrator nie zawiadomił Prezesa UODO o odwołaniu IOD, może to zrobić podmiot, który jest jego następcą prawnym, a zatem przejął prawa i obowiązki likwidowanego podmiotu, wstępując tym samym w jego prawa.

Na przykładzie gimnazjów wskazać można, że obowiązku zawiadomienia o odwołaniu IOD powinna była zatem dokonać placówka, która została zlikwidowana na mocy tzw. reformy systemu edukacji przeprowadzonej na podstawie przepisów Prawa oświatowego oraz ustawy z dnia 14 grudnia 2016 roku – Przepisy wprowadzające ustawę – Prawo oświatowe (Dz.U. z 2017 r. poz. 60, ze zm.), dalej jako ustawa zmieniająca. Art. 117 ust. 4 ustawy zmieniającej wskazuje na podjęcie tzw. uchwał deklaratoryjnych, stanowiących akt przekształcenia placówki oświatowej. Należy wziąć pod uwagę także, czy gimnazjum zostało przekształcone w szkołę podstawową, czy zostało włączone do szkoły podstawowej, zgodnie z art. 129 ust. 1 ustawy zmieniającej.

Natomiast, zgodnie z art. 89 ust. 6 Prawa oświatowego, dokumentację zlikwidowanej szkoły publicznej przekazuje się organowi prowadzącemu szkołę, z wyjątkiem dokumentacji przebiegu nauczania, którą przekazuje się organowi sprawującemu nadzór pedagogiczny, w terminie jednego miesiąca od dnia zakończenia likwidacji.

Zatem w przypadku, gdy gimnazjum nie zawiadomiło o odwołaniu IOD, za wysłanie takiego zawiadomienia IOD odpowiedzialny jest ten podmiot, który jest następcą prawnym zlikwidowanego gimnazjum.

Data wytworzenia informacji: 27.02.2020 r.

Czy kierownik urzędu stanu cywilnego jest administratorem i czy musi wyznaczyć IOD?

W jednostce samorządu, w której pełnię funkcję IOD, burmistrz zatrudnił inną osobę na stanowisku kierownika urzędu stanu cywilnego. Czy w takiej sytuacji kierownik urzędu stanu cywilnego jest administratorem przetwarzanych przez siebie danych osobowych? Jeśli kierownik USC jest administratorem, to nasuwa mi się kolejne pytanie, czy jest on zobowiązany do wyznaczenia inspektora ochrony danych? Moja wątpliwość wynika z faktu, że ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych w art. 9 wskazuje, że przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa w art. 37 ust. 1 lit. a RODO, rozumie się: jednostki sektora finansów publicznych, instytuty badawcze, Narodowy Bank Polski. Kolejne pytanie dotyczy formy w jakiej powinno nastąpić wyznaczenie inspektora przez kierownika USC?

Odpowiadając na pierwsze pytanie zauważyć należy, że ustawa z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego określa wprost, kto realizuje cele z zakresu ustawy, w związku z tym, iż do dokonywania czynności z zakresu rejestracji stanu cywilnego został z mocy ustawy zobowiązany kierownik urzędu stanu cywilnego (art. 9 ustawy z dnia 28 listopada 2014 r. Prawo o aktach stanu cywilnego). Z tego względu należy uznać, iż to kierownik urzędu stanu cywilnego jest administratorem danych osobowych, niezależnie od tego, czy w określonej sytuacji faktycznie stanowisko to będzie piastować organ gminy – wójt (burmistrz, prezydent miasta) – czy inna osoba wyznaczona na to stanowisko przez wójta (burmistrza, prezydenta miasta) na podstawie art. 6 ust. 4 lub 5 ustawy Prawo o aktach stanu cywilnego.

Odnosząc się natomiast do pytania dotyczącego ewentualnego obowiązku wyznaczenia inspektora ochrony przez kierownika urzędu stanu cywilnego, w pierwszej kolejności stwierdzić należy, że wobec brzmienia art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, który to przepis prawa krajowego ustala kierunek interpretacji w polskim systemie prawnym, użytego w art. 37 ust. 1 lit. a RODO, pojęcia „organ lub podmiot publiczny", nie można przyjąć, aby obowiązek wyznaczenia inspektora ochrony danych dla kierownika USC wynikał z przesłanki wymienionej w art. 37 ust. 1 lit. a RODO. Warto mieć jednak na uwadze, że nawet w sytuacji braku takiego obowiązku, administrator – kierownik urzędu stanu cywilnego – może dobrowolnie takiego inspektora wyznaczyć.

Jednocześnie należy przypomnieć, że art. 37 ust. 3 RODO dopuszcza możliwość wyznaczenia przez kilku administratorów jednego inspektora ochrony danych, przy uwzględnieniu jednak ich struktury organizacyjnej i wielkości. Zaznaczyć jednak należy, że skorzystanie z takiego rozwiązania wymaga dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora danych. Ocena tej kwestii zależna jest od wielu czynników, w tym m.in. od: dysponowania przez niego

odpowiednią do zakresu zadań i specyfiki procesów przetwarzania danych ilością czasu, konieczności unikania konfliktu interesów oraz wielkości i struktury organizacyjnej jednostki będącej administratorem danych. Trzeba mieć przy tym świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył oraz tzw. „efektywnej dostępności" inspektora dla osób z danej organizacji. Do zadań IOD należy bowiem np. bieżące monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa oraz udzielanie informacji i rad w zakresie obowiązków wynikających z tych przepisów, a także pełnienie punktu kontaktowego dla osób, których dane dotyczą oraz dla organu nadzorczego. Wobec tego decyzja w zakresie wyboru odpowiedniej osoby do pełnienia funkcji inspektora, musi być podejmowana przez administratora z pełną świadomością ciążącej na nim odpowiedzialności za prawidłową realizację ciążących na nim obowiązków wynikających z przepisów prawa. (więcej informacji na ten temat znaleźć można w Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243) oraz na stronie internetowej Urzędu w zakładce Inspektor Ochrony Danych.

Zatem w przypadku, gdyby burmistrz i kierownik USC wyznaczyli na swojego inspektora tę samą osobę powinni wspólnie określić zasady dotyczące zapewnienia takiemu inspektorowi wystarczającej ilości czasu na wypełnianie jego obowiązków, pomocy w stworzeniu planu jego pracy, a w razie potrzeby wsparcie jego funkcjonowania zespołem odpowiednich specjalistów.

Informujemy, że wyznaczenie do piastowania stanowiska kierownika urzędu stanu cywilnego innej osoby niż wójt (burmistrz, prezydent), który jest odrębnym administratorem, nie musi oznaczać konieczności stworzenia procedur i polityk ochrony danych dotyczących przetwarzania w tym obszarze w odrębnym dokumencie. Jedna dokumentacja może bowiem regulować kwestie ochrony danych dotyczące administratorów istniejących w ramach tej samej jednostki. Więcej informacji na ten temat znaleźć można w odpowiedzi na pytanie CZY KOMENDANT STRAŻY MIEJSKIEJ MUSI POSIADAĆ ODRĘBNĄ POLITYKĘ OCHRONY DANYCH?.

Warto także pamiętać, że jeśli kierownik USC decydowałby się na wyznaczenie inspektora, to on jako administrator powinien dokonać tego wyznaczenia, a także zawiadomić Prezesa UODO o jego wyznaczeniu.

Odnosząc się zaś do pytania dotyczącego formy czynności polegającej na wyznaczeniu inspektora, wskazać należy przede wszystkim, że przepisy RODO oraz ustawy o ochronie danych osobowych nie zwierają szczegółowych uregulowań w tym zakresie. Wobec tego decyzja w tej kwestii należy do administratora. Biorąc jednak pod uwagę zasadę rozliczalności, zgodnie z którą administrator musi być w stanie wykazać przestrzeganie przepisów w zakresie ochrony danych osobowych, co w praktyce najczęściej oznacza dokumentowanie wszelkich procesów związanych z ochroną danych osobowych, administrator powinien wybrać taką formę, która umożliwi mu wykazanie w szczególności: kiedy i kogo wyznaczył do pełnienia takiej funkcji.

Data wytworzenia informacji: 27.02.2020 r.

Czy praca IOD może być kontrolowana?

Czy działania podejmowane przez IOD w związku z wykonywaniem przez niego jego zadań mogą podlegać kontroli przeprowadzanej przez administratora bezpośrednio lub za pośrednictwem podmiotów, którym zleca on taką kontrolę, np. wewnętrznych lub zewnętrznych audytorów? Czy w jednostkach sektora finansów publicznych audytor może inspektorowi wydać zalecenia na gruncie przepisów dotyczących audytu wewnętrznego?

Niezależność IOD, o której mowa w motywie 97 RODO oraz w art. 38 RODO, jest jedną z najważniejszych gwarancji skutecznego i prawidłowego wykonywania jego zadań, a tym samym realnego zapewnienia zgodności przetwarzania danych osobowych z przepisami prawa.

Jednocześnie to administrator ponosi pełną odpowiedzialność za zgodne z przepisami ochrony danych osobowych przetwarzanie danych. Inspektor ochrony danych podlega bezpośrednio administratorowi i w związku z tym sposób wykonywania funkcji przez IOD musi podlegać jego kontroli, przy czym może to być kontrola wewnętrzna lub zlecona przez administratora podmiotowi zewnętrznemu. W jednym i drugim przypadku taka kontrola (audyt) musi uwzględniać niezależne funkcjonowanie (gwarancje niezależności) IOD, tak wyraźnie podkreślane w RODO. Dotyczy to również wdrożonych w danej organizacji systemów wewnętrznej kontroli (systemy oceny zgodności). Systemy te nie mogą w jakikolwiek sposób ograniczać możliwości wykonywania przez IOD jego zadań, w tym dokonywania kompleksowej, bieżącej oceny zgodności przetwarzania danych osobowych z przepisami prawa.

Administratorzy będący jednostkami sektora finansów publicznych w celu zapewnienia zgodnego z prawem przetwarzania danych osobowych i właściwej organizacji bezpieczeństwa informacji korzystają z pomocy zarówno audytorów, jak i inspektorów ochrony danych. Audytor wewnętrzny dokonuje systematycznej oceny kontroli zarządczej, obejmując zasięgiem swojego działania wszystkie obszary jednostki, w tym działania podejmowane przez IOD. Sposób przeprowadzania audytu wewnętrznego został określony w przepisach prawa (m.in. w rozporządzeniu Ministra Finansów z dnia 4 września 2015 r. w sprawie audytu wewnętrznego oraz informacji o pracy i wynikach tego audytu), ale musi on uwzględniać przepisy RODO, w tym m.in. w art. 38 ust. 3 RODO.

Gdy audyt (kontrola) dotyczy pracy IOD, respektowanie niezależnego wykonywania jego zadań oznacza zakaz wydawania IOD przez osoby kontrolujące jakichkolwiek bezpośrednich poleceń/zaleceń odnośnie tych zadań. Ostateczne decyzje co do oceny wyników audytu dotyczącego prawidłowości wykonywania ciążących na IOD obowiązków podejmuje kierownik jednostki, a inspektor musi mieć możliwość przedstawienia swojego stanowiska. Racje obu stron

powinny zostać uzasadnione i udokumentowane. Materiał ten może być przydatny w celach dowodowych w przypadkach oceny prawidłowości wykonywania funkcji IOD w kontekście jego odpowiedzialności na gruncie przepisów prawa pracy lub Kodeksu cywilnego (odpowiedzialności kontraktowej) albo odpowiedzialności karnoprawnej.

Data wytworzenia informacji: 12.11.2020 r.

Czy administrator jest zobowiązany na podstawie RODO do zapewnienia inspektorowi zespołu IOD?

Jestem inspektorem ochrony danych w dużym szpitalu o bardzo złożonej strukturze organizacyjnej zatrudniającej personel liczący ponad 2000 pracowników. W mojej codziennej pracy w związku z wykonywaniem zadań IOD spotykam się z ogromną ilością zagadnień dotyczących ochrony danych osobowych wymagających mojej analizy i udzielenia wsparcia administratorowi, bądź jego pracownikom. Istotnym wsparciem w wykonywaniu przeze mnie zadań IOD byłoby wyznaczenie przez administratora zespołu IOD. Czy przepisy RODO nakazują administratorowi wyznaczenie zespołu?

RODO nakłada na administratora (kierownictwo podmiotu będącego administratorem) określone, bardzo konkretne obowiązki wobec funkcjonującego w jego organizacji inspektora ochrony danych, a sposób ich realizacji zależy od specyfiki danego administratora (m.in. jego wielkości, struktury, rodzaju działalności) i prowadzonego przez niego przetwarzania danych (m.in. charakter, zakres, kontekst i cele przetwarzania). W zależności od tych czynników administrator musi zapewnić IOD właściwe warunki funkcjonowania i to administrator odpowiedzialny jest za skuteczne i prawidłowe wykonywanie przez inspektora jego zadań.

Takim konkretnym obowiązkiem nałożonym na administratora, jest udzielanie IOD **wsparcia w wypełnianiu przez niego zadań** (o których mowa w art. 39 RODO), **zapewniając mu zasoby niezbędne do wykonania tych zadań** oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej zgodnie z art. 38 ust. 2 RODO.

Grupa Robocza art. 29 w Wytycznych dotyczących inspektora ochrony danych WP243 rev.01 opowiada się za szerokim rozumieniem zasobów, do których zalicza m.in.: **wsparcie kadrowe, np. powołanie zespołu inspektora ochrony danych.** Dodać należy, że przez zasoby, które powinien zapewnić administrator można rozumieć również:

- wsparcie IOD ze strony kadry kierowniczej (np. na poziomie zarządu),
- wymiar czasu umożliwiający IOD wykonywanie zadań,
- odpowiednie wsparcie finansowe, infrastrukturalne (pomieszczenia, sprzęt, wyposażenie)

- oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia IOD i jego zadaniach,
- umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT itd.
- ciągłe szkolenie. IOD powinien mieć możliwość ciągłego aktualizowania wiedzy z zakresu ochrony danych osobowych. Celem powinno być zwiększanie wiedzy IOD i zachęcanie go do udziału w szkoleniach, warsztatach, forach poświęconych ochronie danych etc.

Administrator wyznaczając na inspektora daną osobę powinien wspólnie z nią określić zasady dotyczące zapewnienia takiemu inspektorowi wystarczającej ilości czasu na wypełnianie jego obowiązków, pomocy w stworzeniu planu jego pracy, a **w razie potrzeby wsparcie jego funkcjonowania zespołem odpowiednich specjalistów.** W celu realizacji wyrażonej w art. 5 ust. 2 RODO zasady rozliczalności, konieczne jest dokonanie starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec administratora danych. Ocena tej kwestii zależna jest od wielu czynników, w tym m.in. od: dysponowania przez nią odpowiednią do zakresu zadań i specyfiki procesów przetwarzania danych ilością czasu, konieczności unikania konfliktu interesów oraz wielkości i struktury organizacyjnej jednostki będącej administratorem danych. Trzeba mieć przy tym świadomość, że **wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania** oraz tzw. „efektywnej dostępności" inspektora dla osób z danej organizacji. Do zadań IOD należy bowiem np. bieżące monitorowanie zgodności przetwarzania danych osobowych z przepisami prawa oraz udzielanie informacji i rad w zakresie obowiązków wynikających z tych przepisów, a także pełnienie punktu kontaktowego dla osób, których dane dotyczą oraz dla organu nadzorczego.

W skład zespołu IOD wchodzić może osoba (osoby) osoby zastępujące inspektora w czasie jego nieobecności. Możliwość powołania takiej osoby przewiduje art. 11a ust. 1 ustawy o ochronie danych osobowych. W opinii UODO dopuszczalne jest, by administrator wyznaczył dwie osoby zastępujące inspektora ochrony danych. Jedna realizowałaby zadania IOD podczas jego nieobecności, a druga wówczas, gdyby w pracy nie było zarówno IOD, jak i tej pierwszej, zastępującej go osoby.

Warto również odnotować pogląd zawarty w Podręczniku Inspektora Ochrony Danych Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasipublicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym, str. 123, dotyczący powołania zespołu IOD w podmiotach publicznych: *„W organach publicznych faktycznie zalecane byłoby stworzenie zespołu. W małych podmiotach publicznych w skład takiego zespołu mogą wchodzić po prostu obecni pracownicy regularnie spotykający się z inspektorem ochrony danych w celu omówienia istotnych spraw i opracowania polityki. W większych - część pracowników może zostać formalnie przypisana do pełnienia funkcji wspierających inspektora ochrony danych na część etatu. W innych konieczne może okazać się mianowanie pełnoetatowych pracowników wspierających inspektora*

ochrony danych. Jak jasno wynika z wszystkich wytycznych, decyzje w tych sprawach należy podejmować, biorąc pod uwagę (i) złożoność lub wrażliwość operacji przetwarzania danych osobowych oraz (ii) rozmiar i zasoby danego podmiotu. Jednak w końcu zgodnie z RODO zasoby przydzielone inspektorowi ochrony danych (i zespołowi) muszą być odpowiednie do wykonywanych obowiązków."

Wiele informacji na temat obowiązków administratora określonych w art. 37 i 38 RODO można znaleźć w zakładce IOD na stronie internetowej UODO. Cennych wskazówek dostarczają też rozstrzygnięcia Prezesa UODO (decyzja Prezesa UODO o sygn. ZSOŚS.421.25.2019 decyzja Prezesa UODO) i innych organów nadzorczych UE, których zadaniem jest monitorowanie i egzekwowanie przestrzegania ww. przepisów (m.in. poprzez nakładanie na administratorów administracyjnych kar pieniężnych na podstawie art. 83 ust. 4 lit a RODO, CZY NARUSZENIE PRZEPISÓW ODNOSZĄCYCH SIĘ DO IOD MOŻE SKUTKOWAĆ ADMINISTRACYJNYMI KARAMI PIENIĘŻNYMI?).

Data wytworzenia informacji: 18.05.2021 r.

Czy z zewnętrznym IOD należy zawrzeć umowę powierzenia?

Z uwagi na liczne różne interpretacje prawne, zwracam się z prośbą o wyjaśnienie na stronie UODO następującej kwestii, czy w przypadku zawierania umowy z zewnętrznym inspektorem ochrony danych należy posłużyć się konstrukcją powierzenia przetwarzania danych określoną w art. 28 RODO?

Wykonywanie zadań IOD przez osobę, która nie jest członkiem personelu administratora powinno następować na podstawie umowy o świadczenie usług niebędącej umową powierzenia danych.

Art. 37 ust. 6 RODO wskazuje wprost, iż inspektor ochrony danych może wykonywać swoje zadania na podstawie umowy o świadczenie usług, czyli nie musi być on pracownikiem administratora. Dopuszczalny jest zatem outsourcing tej funkcji, przy czym przedmiotem umowy z inspektorem nie są zadania administratora, a zadania wskazane w art. 39 ust. 1 RODO.

Umowa o świadczenie usług, której przedmiotem jest wykonywanie zadań IOD nie będzie umową powierzenia przetwarzania. Konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator w celu realizacji swoich celów (zadań) związanych z przetwarzaniem danych posługuje się innym, zewnętrznym podmiotem. Innymi słowy powierzenie przetwarzania powinno mieć miejsce w przypadkach, gdy administrator prowadzący działalność w określonej dziedzinie, ma potrzebę skorzystać z pomocy zewnętrznych specjalistów, których usługi będą miały charakter pomocniczy, nierzadko techniczny, wspierający działalność główną administratora. Podmiot przetwarzający jest zobowiązany do stosowania się do instrukcji przekazanych przez administratora co najmniej w odniesieniu do celu przetwarzania oraz istotnych elementów sposobu przetwarzania. Najczęściej występujące **przykładowe** usługi

świadczone w modelu powierzenia wskazujemy w Poradniku Wskazówki i wyjaśnienia dotyczące obowiązku z art. 30 ust. 1 i 2 RODO (dostępne pod linkiem: https://uodo.gov.pl/pl/383/214) jako:

1) przechowywanie danych klienta (administratora) rozumiane jako udostępnienie zamawiającemu określonej przestrzeni dyskowej w infrastrukturze przetwarzającego na przechowywanie danych, którymi zlecający (administrator) sam zarządza i decyduje o tym, jakie dane tam przechowuje – np. wykonuje kopie zapasowe danych elektronicznych;
2) udostępnianie klientowi (administratorowi) mocy obliczeniowej procesorów, przestrzeni pamięci operacyjnej i dyskowej lub innych usług na potrzeby instalacji i eksploatacji usług przetwarzania, którymi zamawiający w pełni zarządza – dostarczanie infrastruktury informatycznej;
3) udostępnienie klientowi (administratorowi) określonej platformy programistycznej (np. serwera www wraz z odpowiednim oprogramowaniem do prowadzenia własnej strony internetowej);
4) wykonywanie na zamówienie klienta (zamawiającego) określonych usługi w zakresie konfiguracji sprzętowej, programowej, w tym zabezpieczeń udostępnionych mu serwerów, innych urządzeń komputerowych oraz oprogramowania – usługi administracyjne i konserwacyjne;
5) wykonywanie na zamówienie klienta (zamawiającego) usług programistycznych, w tym aktualizacji oprogramowania na okoliczność zmieniających się przepisów prawnych lub wymagań klienta – usługi programistyczne itp.
6) samo przechowywanie dokumentacji podatkowej, księgowej, kadrowej i medycznej;
7) prowadzenie dokumentacji podatkowej, księgowej, kadrowej;
8) archiwizacja danych elektronicznych;
9) skanowanie i digitalizacja danych;
10) niszczenie nośników informacji. Inne przykłady przypadków uzasadniających skorzystanie z konstrukcji powierzenia przetwarzania danych można znaleźć np. w odpowiedzi na pytanie:

CZY PRZEKAZANIE DOKUMENTACJI DO FUMIGACJI POWODUJE KONIECZNOŚĆ ZAWARCIA UMOWY POWIERZENIA?, CZY W CELU WYTWORZENIA LEGITYMACJI NALEŻY SKORZYSTAĆ Z POWIERZENIA PRZETWARZANIA?, CZY PO WEJŚCIU STOSOWANIA RODO CUW MOŻE POWOŁAĆ JEDNEGO IOD DLA WSZYSTKICH OBSŁUGIWANYCH JEDNOSTEK?

Czy świadczenie usługi kolokacji implikuje konieczność zawarcia umowy powierzenia? (Newsletter UODO dla IOD Wydanie 3 (marzec 2020, str. 5) – **tekst w ramce poniżej**.

Informacja ze strony archiwalnej UODO

CZY ŚWIADCZENIE USŁUGI KOLOKACJI IMPLIKUJE KONIECZNOŚĆ ZAWARCIA UMOWY POWIERZENIA?

Centra danych w dobie postępu technologicznego i globalizacji są ważnym elementem zgodności z przepisami RODO, gdyż są właścicielami zasobów fizycznych, z użyciem których może dochodzić do przetwarzania danych osobowych na dużą skalę oraz ułatwiają ich przepływ. Należy pamiętać, że zgodnie z definicją zawartą w art.4 pkt.2 rozporządzenia RODO pojęcie przetwarzania obejmuje nie tylko potocznie rozumiane aktywne podejmowanie działań (takie jak zbieranie, porządkowanie czy usuwanie), ale również zachowanie bierne (jak przechowywanie). W tym sensie bardzo często podmioty takie będą uważane za podmioty przetwarzające, a umowy z podmiotami świadczącymi usługi hostingowe, chmurowe czy kolokacyjne powinny uwzględniać regulacje dotyczące powierzenia przetwarzania danych osobowych.

Czym jest kolokacja?

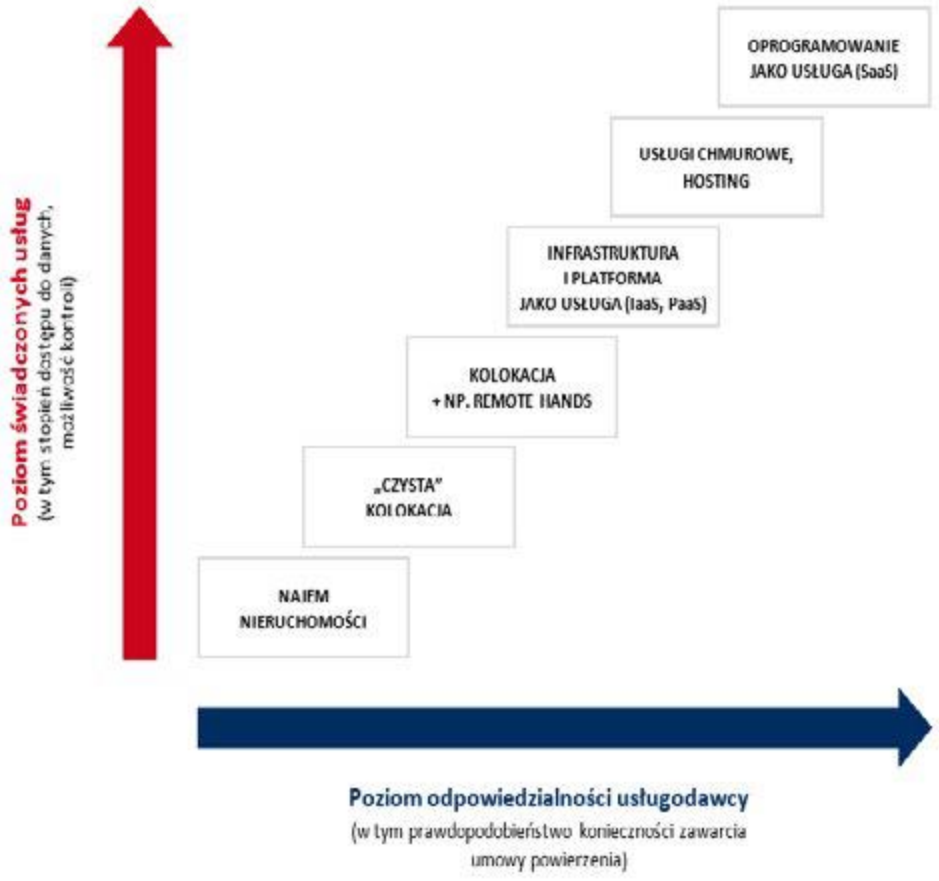
Ograniczenie się wyłącznie do tego zakresu usług, w którym istotą świadczonej usługi nie jest uprawnienie do operacji na danych osobowych a jedynie udostępnienie nieruchomości i odpowiedniej infrastruktury a usługodawca nie ma dostępu do pomieszczeń, w którym znajdują się serwery klienta, w większości przypadków nie będzie implikowała konieczności uwzględnienia w umowie regulacji dotyczących powierzenia przetwarzania.

W przypadku umowy, której zapisy przewidują możliwość uzyskania dostępu do pomieszczeń znacznie wzrasta prawdopodobieństwo konieczności uwzględnienia w umowie elementów powierzenia. W ramach stosownych umów, usługa kolokacji może obejmować wsparcie przy rozwiązywaniu problemów, monitorowanie, serwisowanie czy modernizowanie sprzętu klienta (służącego do przetwarzania danych) co jest utożsamiane w branży IT jako tzw. „remote hands". Należy pamiętać, że istotą konstrukcji powierzania przetwarzania jest zlecenie przez administratora wybranemu podmiotowi dokonania określonych czynności przetwarzania, w imieniu i na rzecz administratora, tj. czynności o których mowa w art. 4 pkt. 2 rozporządzenia RODO. Najczęściej administrator podejmuje decyzję o powierzeniu przetwarzania, gdy uzna, że podmiot, któremu powierzy te czynności, wykona je szybciej, taniej bądź skuteczniej. Podmiot świadczący usługę kolokacji, w zależności od treści umowy, może uzyskiwać fizyczny dostęp do nośników, na których znajdują się dane osobowe i na polecenie administratora wykonywać na nich operacje (np. tworzenia kopii zapasowych, usuwania danych, niszczenia danych poprzez niszczenie fizycznych nośników). W takich wypadkach konieczne jest uwzględnienie w umowie regulacji dotyczących powierzenia przetwarzania.

Jeśli nie dochodzi do powierzenia przetwarzania danych osobowych, stosowna umowa usługi kolokacyjnej powinna zawierać wymagania związane z prawidłowym zabezpieczeniem infrastruktury, gdyż to na administratorze, jako podmiocie decydującym o środkach przetwarzania danych osobowych, ciąży obowiązek zapewnienia właściwych środków technicznych i organizacyjnych, a co za tym idzie – obowiązek doboru środków adekwatnych do zagrożeń.

Konkluzja

Aby uznać czy w ramach przedmiotowych rozważań zachodzi konieczność zawarcia umowy powierzenia za każdym razem administrator musi dokonać oceny czy relacja z wybranym podwykonawcą nie jest przetwarzaniem danych osobowych w imieniu administratora (czyli dochodzi do powierzenia przetwarzania). W tym celu powinien dokonać analizy celu, sposobów i środków oraz skonsultować się z inspektorem ochrony danych (jeśli został wyznaczony). Aby móc stwierdzić czy może zachodzić sytuacja, w której podmiot świadczący usługę kolokacji jest podmiotem przetwarzającym w rozumieniu rozporządzenia 2016/679, warto odpowiedzieć sobie na kilka pytań, tj. czy usługodawca: - ma dostęp do danych osobowych, czy może je na polecenie klienta odczytywać, dokonywać na nich zmian bądź udostępniać? - jest odpowiedzialny za takie procesy podejmowane w imieniu klienta jak przechowywanie, szyfrowanie, udostępnianie, analizowanie, usuwanie bądź niszczenie danych? - czy w imieniu klienta może ingerować w zasoby fizyczne, tj. dyski twarde będące nośnikami danych osobowych, np. poprzez ich fizyczne usunięcie? - czy ma fizyczny dostęp do maszyn klienta, może je w jego imieniu przenosić, wyłączać/włączać? - czy w imieniu klienta podejmuje inne działania poza podstawowym zapewnieniem środowiska niezbędnego do prawidłowego działania zasobów sprzętowych? Przynamniej jedna odpowiedź twierdząca może implikować konieczność zawarcia umowy powierzenia, jednakże każdą sytuację należy ocenić indywidualnie i poprzedzić stosowną, wyżej wymienioną analiząW branży IT, pojęcie kolokacji (bądź hotelingu) utożsamiane jest z usługą polegającą na zapewnieniu klientowi możliwości umieszczenia własnego sprzętu informatycznego i/lub telekomunikacyjnego zapewniającego przetwarzanie jego danych (bądź jego klientów) w niezbędnych warunkach zapewniających ww. urządzeniom prawidłowe działanie, tj. dostarczenie energii elektrycznej, ochrona fizyczna, usługi telekomunikacyjne, chłodzenie, zapewnienie stałej temperatury, czystości powietrza itp. Immamentną cechą usługi kolokacji jest więc przechowywanie sprzętu. Jest to więc też najmniej inwazyjna forma wpływu na dane osobowe przez podmiot świadczący usługę kolokacji (centra danych).Odpowiedź na to pytanie, jak na każde poruszające problematykę konieczności zawarcia umowy powierzenia, zależy od zakresu świadczonych usług i znajomości wszystkich okoliczności faktycznych w relacji między usługodawcą a klientem. Tak więc status podmiotu przetwarzającego powinien być przypisywany podmiotowi biorącemu rzeczywisty, nie jedynie formalny udział w zleconych na zasadzie outsourcingu operacjach przetwarzania



Rys. 1. Poziom świadczonych usług a odpowiedzialność usługodawcy w kontekście powierzenia przetwarzania

Natomiast przedmiotem umowy o świadczenie usług, o której mowa w art. 37 ust. 6 RODO, powinny być zadania wskazane w art. 39 ust. 1 RODO, realizowane przy spełnieniu warunków określonych w przepisach tego aktu, w sposób gwarantujący inspektorowi niezależność. Administrator i podmiot przetwarzający mają m.in. obowiązek zapewnić, aby inspektor nie otrzymywał instrukcji dotyczących wykonywania swoich zadań (art. 38 ust. 4 RODO).

Dostęp do danych osobowych niezbędnych (zewnętrznemu) IOD do wykonywania jego zadań wynika z przepisów prawa. Art. 38 ust. 2 RODO stanowi, że administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu m.in. dostęp do danych osobowych i operacji przetwarzania. W kontekście dostępu do danych należy podkreślić, że ust. 5 ww. tego artykułu zobowiązuje IOD do zachowania tajemnicy lub poufności co do wykonywania swoich zadań - zgodnie z prawem Unii lub prawem państwa członkowskiego.

W kontekście przedstawionego zagadnienia warto pamiętać, że możliwość wykonywania przez osobę, z którą zawierana jest umowa o świadczenie usług, zadań innych niż określone w RODO ograniczona jest zakazem występowania w tym zakresie konfliktu interesów (art. 38 ust. 6 RODO).

Warto również nadmienić, że Grupa Robocza art. 29 w Wytycznych dotyczących inspektorów ochrony danych (WP 243) podkreśla, że w przypadku gdy funkcję IOD pełni osoba spoza organizacji administratora- biorąc pod uwagę fakt, iż IOD posiada wiele zadań - administrator albo podmiot przetwarzający musi mieć pewność, że jeden IOD, z zespołem, jeśli jest to niezbędne**, pozytywnie wypełni swoje obowiązki pomimo wyznaczenia go dla kilku podmiotów i organów publicznych** (str. 11 – 12 Wytycznych).

W odpowiedzi na pytanie Czy podmioty publiczne mogą powołać jednego IOD poza sytuacją uregulowaną w art. 37 ust. 3 RODO? wyjaśniamy, że skorzystanie z rozwiązania określonego w art. 37 ust. 3 RODO wymaga dokonania starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora danych. Trzeba mieć przy tym świadomość, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył oraz tzw. „efektywnej dostępności" inspektora dla osób z danej organizacji.

Data wytworzenia informacji: 18.05.2021 r.

Czy z zewnętrznym IOD wykonującym zadania dla banku należy zawrzeć umowę powierzenia?

Czy w przypadku, gdybyśmy zdecydowali się na zawarcie umowy na świadczenie usługi Inspektora Ochrony Danych w banku przez podmiot zewnętrzny, należy również zawrzeć umowę powierzenia przetwarzania danych z tym podmiotem?

W przypadku gdy administratorem jest bank, w pierwszej kolejności należy mieć na uwadze, że prawidłowe wykonywanie zadań przez IOD wiąże się z zapewnieniem mu dostępu do danych objętych tajemnicą bankową. Zgodnie z RODO, administrator zobowiązany jest zapewnić, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych. Musi on również wspierać inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania (art. 38 ust. 1 i 2 RODO).

A zatem do prawidłowego wykonywania zadań IOD niezbędny jest dostęp do informacji dotyczących przetwarzania danych osobowych, do samych danych osobowych, jak i operacji przetwarzania. Dlatego też warto rozważyć, czy najlepszym rozwiązaniem nie byłoby wyznaczenie do pełnienia funkcji IOD pracownika banku. Jeśli miałaby to być osoba wykonująca obowiązki na podstawie umowy o świadczenie usług, to do umowy takiej zastosowanie powinien mieć art. 6a

ust. 1 pkt 2 ustawy Prawo bankowe który umożliwi zapoznanie się przez IOD z informacjami objętymi tajemnicą bankową. Jak wskazuje bowiem art. 104 ust. 2 pkt 2 lit. a Prawa bankowego, obowiązek zachowania tajemnicy bankowej, o którym mowa w art. 104 ust. 1 Prawa bankowego, nie dotyczy przypadków, w których bank, zgodnie z art. 6a ust. 1 i art. 6b-6d, powierzył wykonywanie, stale lub okresowo, czynności związanych z działalnością bankową. Przy czym podmioty oraz osoby w nich zatrudnione, którym, zgodnie z m.in. przepisem art. 104 ust. 2 pkt 2 lit. a Prawa bankowego udzielono lub ujawniono informacje objęte tajemnicą bankową, mogą wykorzystać te informacje wyłącznie w celu zawarcia i wykonania umów, o których mowa m.in. w ust. 2 pkt 2 lit. a Prawa bankowego (art. 104 ust. 5 Prawa bankowego). Ponadto zgodnie art. 38 ust. 5 RODO, inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań zgodnie z prawem Unii lub prawem państwa członkowskiego.

Wykonywanie zadań IOD przez osobę, która nie jest członkiem personelu administratora, powinno następować na podstawie umowy o świadczenie usług niebędącej umową powierzenia danych. Art. 37 ust. 6 RODO wskazuje wprost, iż inspektor ochrony danych może wykonywać swoje zadania na podstawie umowy o świadczenie usług, czyli nie musi być on pracownikiem administratora (banku). Dopuszczalny jest zatem outsourcing tej funkcji, przy czym przedmiotem umowy z inspektorem nie są zadania administratora, a zadania wskazane w art. 39 ust. 1 RODO. Szerzej na ten temat pisaliśmy na naszej stronie w zakładce Inspektor Ochrony Danych/Wyznaczenie i status IOD, w odpowiedzi na pytanie Czy z zewnętrznym IOD należy zawrzeć umowę powierzenia?

Data wytworzenia informacji: 28.06.2021 r.

Czy obowiązek z art. 38 ust. 2 RODO dotyczy administratora korzystającego z usług zewnętrznego IOD?

Czy obowiązek określony w art. 38 ust. 2 RODO dotyczący „zapewnienia inspektorowi ochrony danych zasobów niezbędnych do utrzymania jego wiedzy fachowej", odnosi się jedynie do inspektorów zatrudnionych na etacie, czy też do tych, którzy wykonują swoje zadnia na podstawie umowy o świadczenie usług?

Funkcja IOD to specjalizacja wymagająca ciągłego zaangażowania w rozwój zawodowy. Metody i technologie wykorzystywane do przetwarzania i zapewniania bezpieczeństwa danym osobowym, a także przyrastająca liczba regulacji prawnych oraz ich zmiany powodują, że wiedzę w zakresie prawa i praktyk w dziedzinie ochrony danych osobowych trzeba ciągle aktualizować.

Zadania nałożone w RODO na inspektorów są trudne, a ich wykonywanie wymaga specjalnego merytorycznego przygotowania. Jak wskazuje Grupa Robocza Art. 29 w Wytycznych dotyczących inspektora ochrony danych WP243 rev.01, inspektor odgrywa kluczową rolę w zakresie

wspierania „kultury ochrony danych" w ramach podmiotu oraz pomaga w implementacji niezbędnych elementów RODO, w tym zasad przetwarzania danych osobowych, praw osób, których dane dotyczą, ochrony danych w fazie projektowania oraz domyślnej ochrony danych, rejestru czynności przetwarzania, wymogów bezpieczeństwa przetwarzania i zgłoszenia naruszeń.

Z powyższych względów prawodawca unijny nałożył na administratora i podmiot przetwarzający w art. 38 ust. 2 RODO obowiązek stałego wspierania IOD poprzez dostarczanie mu niezbędnych zasobów do wykonania jego zadań oraz dostępu do danych osobowych i operacji przetwarzania, a także zasobów niezbędnych do utrzymania jego wiedzy fachowej. Obowiązek ten odnosi się zarówno do sytuacji, gdy inspektor jest członkiem personelu administratora, jak i do inspektorów wykonujących swoje zadania na podstawie zawieranych przez nich umów o świadczenie usług.

RODO nie przesądza, jakie konkretnie środki i w jaki konkretnie sposób administrator (podmiot przetwarzający) - korzystający ze wsparcia IOD – powinien zapewnić, aby wywiązać się z obowiązku określonego w art. 38 ust. 2 RODO. W świetle RODO kwalifikacje zawodowe IOD obejmują nie tylko wiedzę fachową na temat prawa i praktyk w dziedzinie ochrony danych, ale też umiejętności wypełnienia zadań, o których mowa w art. 39. Warto zatem, aby ocena, jakie zasoby są niezbędne dla utrzymania kwalifikacji IOD uwzględniała oba powyższe elementy.

W Podręczniku Inspektora Ochrony Danych Wytyczne dla inspektorów ochrony danych w sektorze publicznym i quasi-publicznym dotyczące sposobu zapewnienia zgodności z europejskim ogólnym rozporządzeniem o ochronie danych, str. 116, wskazano, że „*organizacja powinna zapewnić swojemu IOD możliwość utrzymania i dalszej poprawy swoich kompetencji, także po nominacji poprzez udział w stosownych kursach i seminariach".*

Grupa Robocza Art. 29 w Wytycznych dotyczących inspektora ochrony danych WP243 rev.01 wskazała, że poziom wiedzy inspektora musi być współmierny do charakteru, skomplikowania i ilości danych przetwarzanych w ramach jednostki. Dla przykładu, w przypadku wyjątkowo skomplikowanych procesów przetwarzania danych osobowych lub w przypadku przetwarzania dużej ilości danych szczególnych kategorii, inspektor może potrzebować wyższego poziomu wiedzy i wsparcia. Dlatego Grupa Robocza Art. 29 opowiedziała się za szerokim rozumieniem zasobów i wskazała m.in. na potrzebę ciągłego szkolenia IOD, zapewniającego mu możliwość ciągłego aktualizowania wiedzy z zakresu ochrony danych osobowych. Inspektorów należy zachęcać do udziału w szkoleniach, warsztatach, forach poświęconych ochronie danych osobowych, by mogli zwiększać swoją wiedzę. Co do zasady im bardziej skomplikowane procesy przetwarzania danych, tym więcej środków należy przeznaczyć na IOD. Ochrona danych musi być skuteczna i wymaga wystarczających zasobów odpowiednich do zakresu przetwarzania danych.

Motyw 97 RODO wyjaśnia, że niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają przetwarzane dane osobowe. Jeżeli zatem poziom wiedzy fachowej inspektora musi być

odpowiedni do „prowadzonych operacji przetwarzania oraz ochrony, której wymagają przetwarzane dane osobowe" i ma być utrzymywany na tym poziomie (art. 38 ust. 1 RODO), to ilość i rodzaj zasobów przeznaczanych na zapewnienie właściwych kwalifikacji inspektora musi być dobierany indywidualnie i z uwzględnieniem powyższych kryteriów.

W przedstawionej sprawie tzn. w sytuacji, gdy inspektor wykonuje zadania na podstawie umowy o świadczenie usług, kwestie związane z zapewnianiem zasobów na utrzymanie wiedzy fachowej IOD powinny być starannie ustalane przez strony umowy przy zawieraniu (lub ewentualnie renegocjonowaniu umowy), tak aby zapewnić zgodność z przywołanym wyżej art. 38 ust. 2 RODO i zasadą rozliczalności (administrator powinien móc wykazać, że prawidłowo zrealizował ciążący na nim obowiązek). Ustalenia te powinny odnosić się do tego, jakiego rodzaju będą to środki, w jaki sposób zostaną zapewnione. Takie staranne ukształtowanie postanowień umowy dotyczących obowiązków jej stron przyczynia się do osiągniecia celów umowy i jej realnego wykonania.

Przy konstruowaniu treści umowy obowiązuje zasada swobody stron w określaniu wzajemnych praw i obowiązków, niemniej jest ona ograniczona wymogami wynikającymi z przepisów o ochronie danych osobowych. Przyjęte przez strony rozwiązania związane z zapewnianiem zasobów na utrzymanie wiedzy fachowej IOD powinny uwzględniać wiele kryteriów, takich jak: aktualny stan wiedzy IOD i dotychczasowe sposoby jej aktualizowania, specyfika prowadzonego przez administratora przetwarzania związanego z rodzajem i zakresem jego działalności, złożoność i liczba procesów przetwarzania danych, stosowane środki techniczne i stopień ich zaawansowania oraz bieżące potrzeby dotyczące dostosowania się do wymogów prawnych i praktyk w dziedzinie ochrony danych osobowych.

Dokształcanie inspektora przekłada się na coraz wyższy poziom fachowości oraz jakości i efektywności jego pracy. Niesie to niewątpliwie korzyści dla kierownictwa i osób przetwarzających dane osobowe u administratora (podmiotu przetwarzającego), którzy - wspierani przez odpowiednio wykwalifikowanego inspektora – są w stanie sprostać wymogom, jakie nakładają na nich przepisy prawa i regulacje wewnętrzne oraz zminimalizować popełniane błędy.

Data wytworzenia informacji: 28.06.2021 r.

Czy można łączyć funkcję IOD z zadaniami związanymi z obsługą wniosków od sygnalistów?

Oczekujemy na wejście w życie krajowych regulacji wdrażających tzw. dyrektywę o ochronie sygnalistów nr 2019/1937. Pytanie dotyczy osoby, która miałaby przyjmować ewentualne zgłoszenia sygnalistów oraz prowadzić postępowania wyjaśniające dotyczące zgłaszanych

nieprawidłowości. Czy funkcję taką firma może powierzyć osobie pełniącej funkcję IOD? Czy nie będziemy mieli w takim przypadku do czynienia z konfliktem interesów?

Organizowanie procesu przyjmowania i rozpatrywania zgłoszeń o nieprawidłowościach reguluje dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1937 z dnia 23 października 2019 r. w sprawie ochrony osób zgłaszających naruszenia prawa Unii. Obecnie w Polsce trwają prace nad projektem ustawy wdrażającej tę dyrektywę, wobec tego **nie znamy ostatecznego kształtu przyjętych w niej rozwiązań**, w tym tych dotyczących zadań i statusu członków personelu odpowiedzialnych za rozpatrywanie zgłoszeń naruszenia prawa.

Jeśli chodzi o uregulowanie tych kwestii w dyrektywie, to odnosi się ona do nich w szczególności w wymienionych niżej przepisach i motywach.

W motywie 74 dyrektywy wskazano, że w celu rozpatrywania zgłoszeń oraz w celu zapewnienia komunikacji z osobą dokonującą zgłoszenia, a także w celu prowadzenia we właściwy sposób działań następczych w związku ze zgłoszeniem, członkowie personelu właściwych organów, którzy są odpowiedzialni za rozpatrywanie zgłoszeń, **powinni być specjalnie przeszkoleni, między innymi w kwestii mających zastosowanie przepisów o ochronie danych.**

Natomiast w motywie 77 wskazano, że konieczne jest, aby członkowie personelu właściwego organu, którzy są odpowiedzialni za rozpatrywanie zgłoszeń, oraz członkowie personelu właściwego organu, którzy mają prawo dostępu do informacji przekazanych przez osobę dokonującą zgłoszenia, **przestrzegali obowiązku zachowania tajemnicy zawodowej i poufności przy przekazywaniu danych zarówno w ramach właściwego organu, jak i poza ten organ.**

Z kolei w art. 12 ust. 4 dyrektywy wskazano, że państwa członkowskie zapewniają, aby właściwe organy **wyznaczyły członków personelu odpowiedzialnych za rozpatrywanie zgłoszeń, a w szczególności odpowiedzialnych za:**

a) przekazywanie wszystkim zainteresowanym osobom informacji na temat procedur dokonywania zgłoszeń;

b) przyjmowanie zgłoszeń i podejmowanie działań następczych w związku z tymi zgłoszeniami;

c) utrzymywanie kontaktu z osobą dokonującą zgłoszenia w celu przekazywania jej informacji zwrotnych i zwracania się, w razie potrzeby, o dalsze informacje.

Przepisy dyrektywy nie regulują natomiast kwestii łączenia zadań osób zajmujących się obsługą zgłoszeń z innymi zadaniami.

W takiej sytuacji administrator przed powierzeniem osobie pełniącej funkcję IOD innych zadań lub obowiązków (w tym przypadku polegających na przyjmowaniu zgłoszeń sygnalistów oraz prowadzeniu postępowań wyjaśniających) powinien dokonać starannej analizy w zakresie zapewnienia IOD właściwych warunków dla zachowania jego niezależności i prawidłowego wykonywania zadań. Ocena ta powinna być dokonana przy uwzględnieniu stosownych przepisów

RODO oraz Wytycznych Grupy Roboczej Art. 29 dotyczących inspektorów ochrony danych (WP 243).

Zgodnie bowiem z art. 38 ust. 6 RODO IOD może wykonywać „inne zadania i obowiązki". W dalszej części przepisu występuje jednak zastrzeżenie, iż „administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów".

Konflikt interesów następuje, jeśli nie można pogodzić prawidłowego wykonywania zadań IOD z realizacją innych zadań, gdyż pomiędzy zadaniami występuje sprzeczność, uniemożliwiająca odpowiednią ich realizację. Konflikt interesów może być również rezultatem nadmiaru obowiązków przydzielonych do wykonania IOD, jeśli IOD musi wybrać między obowiązkami, jakie będzie realizował, a tymi, którym nie podoła z powodu braku czasu koniecznego na ich wykonanie.

Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Oznacza to, że IOD nie może zajmować w organizacji stanowiska, na którym określa się sposoby i cele przetwarzania danych. W powołanych wyżej Wytycznych dotyczących IOD wskazane zostały przykłady takich stanowisk. Należą do nich: stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli sprawujące je osoby biorą udział w określaniu celów i sposobów przetwarzania danych.

Ocena, czy w przypadku konkretnej osoby i wykonywanych przez nią zadań nie występuje konflikt interesów, powinna być dokonywana indywidualnie z uwzględnieniem konkretnych okoliczności. Oznacza to, że możliwość zaistnienia konfliktu powinna być stale monitorowana, ponieważ przyczyny zaistnienia takiego konfliktu mogą występować również w późniejszym czasie, po rozpoczęciu pełnienia funkcji przez IOD.

Administrator powinien przy tym uwzględnić m.in. następujące kryteria:

- organizacyjne (IOD powinien podlegać bezpośrednio najwyższemu kierownictwu jednostki organizacyjnej),
- merytoryczne (inne obowiązki nie powinny negatywnie wpływać na niezależne wykonywania zadań IOD),
- czasowe (IOD powinien dysponować czasem wystarczającym do wykonywania swoich zadań, przy uwzględnieniu m.in. liczby obowiązków czy stopnia ich skomplikowania).

Odnosząc się do kryterium organizacyjnego należy zauważyć, że w przypadku jednoczesnego pełnienia funkcji IOD i wykonywania innych zadań wykluczone jest rozwiązanie, w którym osoba taka podlegałaby np. dyrektorowi departamentu, kierownikowi działu lub jakiejkolwiek innej

osobie (np. dyrektorowi generalnemu urzędu publicznego), która nie jest najwyższym kierownictwem w rozumieniu art. 38 ust. 3 RODO.

Podsumowując należy wskazać, że administrator przed powierzeniem IOD wykonywania innych zadań powinien dokonać analizy, czy IOD będzie w stanie wykonywać prawidłowo swoje obowiązki. Nieprzeprowadzenie analizy w tym zakresie może w konsekwencji spowodować naruszenie przepisów o ochronie danych osobowych.

Na zakończenie warto zwrócić uwagę, że przewidziana w RODO zasada rozliczalności wymaga w szczególności, aby administratorzy wykazywali logikę, na której oparli swoje decyzje, i potrafili uzasadnić, dlaczego przyjęli określone rozwiązania.

Wiele informacji na temat obowiązków administratora określonych w art. 37 i 38 RODO, a także na temat kryteriów oceny, czy osoba pełniąca funkcję IOD może pełnić również inne funkcje i obowiązki można znaleźć w zakładce IOD na naszej stronie internetowej. Cennych wskazówek dostarczają też decyzje Prezesa UODO i innych organów nadzorczych UE, jako organów zobowiązanych do egzekwowania przestrzegania ww. przepisów (m.in. mowa o tym w art. 83 ust. 4 lit. a RODO).

Więcej informacji dotyczących tego zagadnienia można znaleźć w rozdziale IOD **Wyznaczenie i status IOD**, w tym m.in. w odpowiedzi na pytania:

Jakie gwarancje niezależności zostały przyznane IOD w przepisach RODO?

Czy IOD może być osoba pełniąca funkcję kierownika komórki w organizacji?

Czy IOD może jednocześnie pełnić funkcję pełnomocnika do spraw ochrony informacji niejawnych?

Czy możliwe jest łączenie funkcji IOD z obowiązkami administratora systemu informatycznego (ASI)?

Data wytworzenia informacji: 03.11.2021 r.

Wyznaczenie IOD na podstawie ustawy wdrażającej dyrektywę policyjną (DODO)

Większość podmiotów podlegających ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości było zobowiązanych od 25 maja 2018 r. do wyznaczenia inspektora ochrony danych (IOD) na podstawie RODO. Wskazuje na to - odnoszący się do organów i podmiotów publicznych – art. 37 ust. 1 lit. a RODO oraz art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

Co prawda RODO nie ma zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed

zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, jednak ze względu na przetwarzanie przez te organy i podmioty publiczne danych osobowych w innych celach, np. realizacji zadań pracodawców, były one zobowiązane do wyznaczenia IOD już na gruncie RODO.

Dlatego też w związku z ww. ustawą z dnia 14 grudnia 2018 r. wdrażającą dyrektywę 2016/680, która obowiązuje od 6 lutego 2019 r., w większości przypadków administratorzy danych nie musieli wyznaczać nowego IOD. Wymóg ten mieli zaś ci, którzy wcześniej nie wyznaczyli inspektora.

Jakie podmioty zobowiązane są do wyznaczenia IOD na podstawie ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości?

Podmiotami zobowiązanymi do wyznaczenia IOD na podstawie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości są przede wszystkim: sądy, prokuratury, Policja, Straż Graniczna, Służba Więzienna, Żandarmeria Wojskowa, Służba Ochrony Państwa. Obowiązek ten mają również Generalny Inspektor Informacji Finansowej, Krajowa Administracja Skarbowa. Także komendanci straży gminnej i miejskiej musza wyznaczyć IOD, niezależnie od tego, czy są oni umiejscowieni w strukturze urzędu gminy czy nie. Ponadto wymóg wyznaczenia inspektora spoczywa także na się Głównym Inspektorem Transportu Drogowego, Straży Ochrony Kolei, Ministerstwie Środowiska, Głównym Inspektorze Ochrony Środowiska, Straży Rybackiej, Głównym Inspektorze Straży Leśnej, Państwowej Straży Łowieckiej, Urzędzie Żeglugi Śródlądowej, urzędach morskich, Państwowej Inspekcji Sanitarnej, Państwowej Straży Pożarnej, Inspektorze Nadzoru Wewnętrznego (MSWiA). Nowe regulacje określają, że podmioty odpowiedzialne za bezpieczeństwo imprez masowych oraz przewoźnicy lotniczy również są w grupie administratorów, którzy muszą powołać IOD.

Sposób i termin zawiadomienia Prezesa UODO o wyznaczeniu IOD

Zgodnie z art. 46 ust. 9 ustawy z 14 grudnia 2018 r. zawiadomienie sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem zaufanym ePUAP osoby uprawnionej do reprezentowania administratora. Więcej informacji o tym, jak można uzyskać profil zaufany ePUAP można znaleźć pod następującym linkiem https://pz.gov.pl/pz/index

W zawiadomieniu należy podać imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora ochrony danych. Warto skorzystać z właściwego formularza elektronicznego dostępnego na stronie www.uodo.gov.pl. (więcej informacji w odpowiedzi na pytanie: Jaki formularz zawiadomienia wybrać?)

Zawiadomienie należy złożyć w terminie 14 dni od dnia wyznaczenia. Ten sam termin dotyczy zawiadomienia o każdej zmianie w zakresie danych (czyli imię, nazwisko, adres poczty

elektronicznej lub numer telefonu inspektora ochrony danych oraz nazwy i adresu podmiotu, który wyznaczył IOD) oraz o odwołaniu inspektora ochrony danych (termin liczy się od dnia zaistnienia zmiany lub odwołania).

Zawiadomienie może zostać dokonane przez pełnomocnika. Do zawiadomienia dołącza się pełnomocnictwo udzielone w formie elektronicznej (więcej informacji znaleźć można w odpowiedziach na pytania dotyczących zgłaszania IOD przez pełnomocnika).

Zastępca IOD

Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przewiduje możliwość wyznaczenia osoby zastępującej inspektora ochrony danych w czasie jego nieobecności (art. 46 ust. 4). W przypadku zawiadamiania Prezesa UODO o zastępcy IOD, należy postąpić w sposób opisany powyżej, wybierając jeden z formularzy dotyczących zastępcy IOD (więcej w odpowiedzi na pytanie: JAKI FORMULARZ ZAWIADOMIENIA WYBRAĆ?).

Data wytworzenia informacji: 08.04.2022 r.

Wyznaczenie IOD w sądach powszechnych

Obowiązek wyznaczenia IOD w sądach powszechnych wynika zarówno z RODO i z ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, jak i z ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Sądy powszechne już od 25 maja 2018 r., czyli od momentu wejścia do stosowania RODO, były zobowiązane do wyznaczenia inspektora ochrony danych. Obowiązek taki przewidziany został w art. 37 ust. 1 lit a RODO oraz w art. 9 ustawy o ochronie danych osobowych.

Od 6 lutego 2019 r. sądy powszechne podlegają też ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, przyjętej w związku z obowiązkiem wdrożenia w Polsce dyrektywy 2016/680 (tzw. dyrektywy policyjnej). Ustawa ta w art. 46 ust. 1 zobowiązuje administratorów do wyznaczenia inspektora ochrony danych realizującego zadania na jej podstawie.

Ponadto, od 6 lutego – na mocy tej ustawy – weszły w życie zmiany w ustawie z dnia 27 lipca 2001 r. – Prawo o ustroju sądów powszechnych. Artykuły 175a § 1 i art. 175db wskazują obecnie prezesa sądu, dyrektora sądu oraz sąd jako odrębnych administratorów.

Prezesi i dyrektorzy właściwych sądów – każdy w zakresie realizowanych zadań – są administratorami danych osobowych:

1. sędziów i sędziów w stanie spoczynku oraz asesorów sądowych,

2. referendarzy sądowych, asystentów sędziów, dyrektorów sądów oraz ich zastępców, kuratorów sądowych, aplikantów aplikacji sądowej, aplikantów kuratorskich, urzędników oraz innych pracowników sądów,
3. biegłych sądowych, lekarzy sądowych, mediatorów oraz ławników,
4. kandydatów na stanowiska wymienione w pkt 1 i 2.

Sądy zaś są administratorami danych osobowych przetwarzanych w postępowaniach sądowych w ramach sprawowania wymiaru sprawiedliwości albo realizacji zadań z zakresu ochrony prawnej. Stosownie do art. 175 dd § 1 Prawa o ustroju sądów powszechnych nadzór nad przetwarzaniem danych osobowych, których administratorami są sądy, zgodnie z art. 175da i art. 175db, wykonują w zakresie działalności sądu rejonowego, okręgowego apelacyjnego właściwe organy. Ponadto sądy są administratorami innych danych osobowych, wobec których ustalają cele i sposoby przetwarzania (np. gromadzonych w związku z zawieraniem przez sąd umów cywilnoprawnych).

Jeden IOD dla trzech administratorów

Każdy z wyżej wskazanych administratorów (prezesi i dyrektorzy właściwych sądów oraz sądy) zobowiązany jest do wyznaczenia IOD. Od rodzaju zadań, które każdy z nich realizuje zależy, czy obowiązek ten wynika z RODO i ustawy o ochronie danych osobowych, czy też - jak w przypadku sądu – zarówno z RODO i ustawy o ochronie danych osobowych, jak i ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.

Przekładając to na praktykę, należy przewidywać, że w większości przypadków prezes sądu i dyrektor sądu wyznaczą do pełnienia funkcji IOD tę samą osobę, która pełni tę funkcję dla sądu jako administratora. Przy czym sąd jest administratorem danych przetwarzanych na podstawie RODO i ustawy z dnia 14 grudnia 2018 r. Możliwość wyznaczenia jednej, tej samej osoby, dla kilku podmiotów publicznych przewiduje art. 37 ust. 3 RODO oraz art. 46 ust. 3 ustawy z dnia 14 grudnia 2018 r.

W takim przypadku trzeba pamiętać, że inspektor obsługujący trzech administratorów musi realizować zadania zarówno na podstawie RODO, jak i na podstawie ustawy z dnia 14 grudnia 2018 r. Wymienione akty prawne przewidują pewne odrębności w zakresie zadań inspektorów, np. do zadań IOD wynikających z ustawy z dnia 14 grudnia 2018 r. należy przeprowadzanie na zlecenie Prezesa UODO sprawdzeń stosowania przepisów tej ustawy przez administratora.

Ponadto IOD pełniący funkcję zarówno na podstawie RODO, jak i ustawy wdrażającej tzw. dyrektywę policyjną powinien spełniać wymagania dla inspektorów przewidziane w obu aktach prawnych, np. ustawa z dnia 14 grudnia 2018 r. przewiduje dla inspektorów wymóg posiadania pełnej zdolności do czynności prawnych oraz korzystania z pełni praw publicznych, a także braku skazania prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione umyślnie (art. 46 ust. 2 pkt. 1 i 3).

Zakres działania IOD

W przypadku sądów ze względu na ochronę niezawisłości sędziowskiej z zakresu kompetencji inspektora wyłączone są operacje przetwarzania danych mieszczące się w czynnościach orzeczniczych (sprawowania wymiaru sprawiedliwości). Jednakże w zakresie całej pozostałej działalności sądu związanej z przetwarzaniem danych (np. realizowania uprawnień osób, których dane dotyczą, prowadzenia rejestrów i wykazów czynności przetwarzania, właściwego zabezpieczania danych osobowych, zgłaszania naruszeń ochrony danych) inspektor powinien służyć swoim merytorycznym wsparciem zarówno kierownictwu sądu, jak i jego pracownikom. Oznacza to także, że większość praktyk, procedur, sposobów zabezpieczeń danych osobowych wypracowanych przez sądy na podstawie RODO i ustawy o ochronie danych osobowych powinno być rozwijane i kontynuowane z uwzględnieniem zarówno wymogów RODO, jak i ustawy wdrażającej dyrektywę policyjną.

Poinformowanie osób, których dane dotyczą oraz UODO o wyznaczeniu IOD

O wyznaczeniu inspektora (zarówno na podstawie RODO, jak i ustawy z dnia 14 grudnia 2018 r.) oraz o zakresie i podstawach jego działania na rzecz trzech administratorów powinni dowiedzieć się zarówno wszystkie osoby przetwarzające dane osobowe w sądzie, jak i osoby, których dane dotyczą oraz organ nadzorczy. Dla osób, których dane dotyczą, oraz dla organu nadzorczego IOD jest bowiem punktem kontaktowym zgodnie z art. 38 ust. 4 i art. 39 ust. 1 lit. e RODO oraz art. 47 ust. 1 pkt 7 i 8 ustawy z dnia 14 grudnia 2018 r.

W związku z tym zarówno ustawa o ochronie danych osobowych (art. 11), jak i ustawa z dnia 14 grudnia 2018 r. (art. 46 ust. 11) zobowiązują administratorów by udostępnili imię i nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora na swojej stronie internetowej. Jeżeli administrator lub podmiot przetwarzający nie prowadzi własnej strony, udostępnia informacje o IOD w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Dane inspektora w powyższym zakresie muszą być przekazane również Prezesowi UODO.

Obowiązujące od 6 lutego 2019 r. przepisy oznaczają, że prezes sądu i dyrektor sądu jako administratorzy, w celu powiadomienia Prezesa UODO o wyznaczeniu inspektora powinni skorzystać z elektronicznej formy zawiadomienia zgodnie z art. 10 ust. ust. 6 ustawy o ochronie danych osobowych. Oznacza to, że zawiadomienie należy opatrzyć kwalifikowanym podpisem elektronicznym albo podpisem zaufanym.

Natomiast zawiadomienie o wyznaczeniu IOD przez sąd jako administratora danych działającego na podstawie ustawy z dnia 14 grudnia 2018 r. powinno również nastąpić w postaci elektronicznej, ale na podstawie art. 46 ust. 9 ustawy z dnia 14 grudnia 2018 r.

Wyznaczenie IOD na podstawie ustawy wdrażającej dyrektywę policyjną (DODO).

Data wytworzenia informacji: 08.04.2022 r.

ZAWIADOMIENIA PREZESA UODO ZWIĄZANE Z IOD

Jak prawidłowo zawiadomić o wyznaczeniu/odwołaniu/zmianie danych IOD (zastępcy IOD)?

Aby prawidłowo zawiadomić **o wyznaczeniu/odwołaniu/zmianie** danych IOD (zastępcy IOD) należy pamiętać o poniższych określonych prawem wymaganiach:

1. Zawiadomienie dotyczące IOD lub jego zastępcy musi mieć postać elektroniczną.

Jedynym prawidłowym i skutecznym sposobem zawiadomienia **Prezesa UODO** o wyznaczeniu inspektora ochrony danych jest zawiadomienie **w postaci elektronicznej** (zgodnie z art. 10 ust. 6 ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz z art. 46 ust. 9 ustawy z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości).

Analogiczny sposób dotyczy także zawiadomień dotyczących zastępcy inspektora ochrony danych (art. 11a ust. 3 ustawy z 10 maja 2018 r. o ochronie danych osobowych oraz art. 46 ust. 6 ustawy z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości) .

Oznacza to, że należy skorzystać z właściwego formularza elektronicznego(dotyczącego IOD bądź zastępcy IOD) odpowiedniego do podstawy ich powołania. Administratorzy wyznaczający IOD/zastępcę IOD na podstawie RODO oraz ustawy z dnia 10 maja 2018 r. powinni bowiem skorzystać z formularzy oznaczonych jako RODO, natomiast administratorzy wyznaczający IOD/zastępcę IOD na podstawie ustawy z dnia 14 grudnia 2018 r., powinni skorzystać z formularzy DODO.

Podkreślić też należy, że niektórzy administratorzy są zobowiązani do wyznaczenia IOD zarówno na podstawie RODO, jak i ustawy z dnia 14 grudnia 2018 r. (np. Policja), a wówczas muszą oni przesłać osobne zawiadomienia, korzystając przy tym z właściwych formularzy.

Odpowiednie elektroniczne formularze znajdziecie Państwo na dole naszej strony internetowej pod belką: Formularze zawiadomień IOD - załatw online na www.biznes.gov.pl. Zawiadomienie musi zostać podpisane podpisem elektronicznym

2. Wypełniony formularz musi zostać opatrzony kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP osoby uprawnionej do reprezentowania administratora.
3. W zawiadomieniu należy podać wszystkie wymagane przepisami prawa informacje.

W zawiadomieniu należy podać wszystkie wymagane przepisami prawa informacje. W ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych są one określone **w art. 10 ust. 1 i 3. Natomiast w ustawie z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości wymagane informacje wskazane zostały w art. 46 ust. 9.**

4. **Do zawiadomienia składanego przez pełnomocnika należy załączyć pełnomocnictwo udzielone w formie elektronicznej oraz opłatę skarbową** od pełnomocnictwa (chyba że przepisy zwalniają od jej uiszczenia).

Więcej na ten temat znaleźć można w materiałach dotyczących zgłaszania IOD przez pełnomocnika.

Data wytworzenia informacji: 31.08.2018 r.

W jakim terminie należy dokonać zawiadomienia o wyznaczeniu/odwołaniu/zmianie danych IOD (zastępcy)?

Zawiadomienia należy dokonać w ciągu 14 dni od dnia wyznaczenia/odwołania/lub zmiany danych IOD lub zastępcy IOD (art. 10 ust. 1 i 4 oraz art. 11 ust. 3 w związku z art. 10 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, a także art. 46 ust. 9 i 10 oraz art. 46 ust. 6 w związku z art. 46 ust. 10 ustawy z dnia 14 grudnia 2018 r. o ochronie danych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości).

Ponadto, zgodnie z art. 10 ust. 4 ustawy z dnia 10 maja 2018 r. ochronie danych osobowych, należy dokonać zawiadomienia o zmianach dotyczących danych administratora lub podmiotu przetwarzającego, o których mowa w art. 10 ust. 3 tej ustawy, w terminie 14 dni od dnia zaistnienia danej zmiany. Pomocne informacje na temat tego obowiązku można znaleźć w pytaniu CZY NALEŻY ZAWIADAMIAĆ O ZMIANIE, GDY NASTĘPUJE ZMIANA OSÓB UPRAWNIONYCH DO REPREZENTACJI?

Data wytworzenia informacji: 08.01.2019 r.

Jaki formularz zawiadomienia wybrać?

Obowiązek wyznaczenia inspektora ochrony danych przewiduje zarówno:

1) ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 8) w zawiązku z art. 37 ust. 1 RODO,
2) jak i ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (art. 46 ust. 1) wdrażająca tzw. dyrektywę policyjną (DODO).

Dla realizacji obowiązków wynikających z każdej z powyższych ustaw przygotowane zostały odrębne formularze.

Wobec powyższego zawiadamiając Prezesa UODO o wyznaczeniu IOD lub dokonując innych zgłoszeń dotyczących IOD administrator/podmiot przetwarzający powinien w zależności od tego, z której z powyższych ustaw wynika realizowany przez niego obowiązek, wybrać formularz z odpowiedniej kategorii, tj.

- Zawiadomienia na podstawie RODO

lub

- Zawiadomienia na podstawie DODO (tj. na podstawie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości).

Przepisy każdej z wymienionych ustaw przewidują możliwość powołania zastępcy IOD – zawiadomienia dotyczące zastępcy mają odrębne formularze.

Warto też zwrócić uwagę, czy zawiadomienie wysyłamy w związku z wyznaczeniem IOD lub jego zastępcy, czy też odwołaniem tych osób lub też zmianą zgłaszanych informacji (dla każdej z tych sytuacji jest inny formularz – RODO lub DODO). Gdy chcemy poinformować, że z funkcji IOD (zastępcy IOD) została odwołana jedna osoba, a na jej miejsce powoływana jest inna, wówczas należy skorzystać z formularza:

- odwołanie dotychczasowego i wyznaczenie nowego inspektora ochrony danych (RODO lub DODO) lub
- odwołanie dotychczasowego zastępcy inspektora ochrony danych i wyznaczenie nowego (RODO lub DODO).

Jeśli zawiadomienie zostało przesłane na niewłaściwym formularzu konieczne jest jego ponowne przesłanie.

Data wytworzenia informacji: 08.04.2022 r.

Formularze zawiadomień IOD

Alternatywnym sposobem zawiadomienia Prezesa UODO o danych kontaktowych inspektora ochrony danych oraz w przypadku niedających się rozwiązać problemów z wysłaniem zawiadomienia przez platformę biznes.gov.pl, jest zawiadomienie, które można wysłać przez platformę epuap.gov.pl (użytkownik po zalogowaniu i wybraniu formularza przekierowywany jest na portal obywatel.gov.pl), załączając właściwy formularz Materiały do pobrania

Data wytworzenia informacji: 07.01.2019 r.

Jak złożyć kwalifikowany podpis elektroniczny pod zawiadomieniem dotyczącym IOD?

https://www.biznes.gov.pl/pl/portal/0075#4

Data wytworzenia informacji: 07.01.2019 r.

Dlaczego (na biznes.gov.pl) przy wgrywaniu podpisanego pliku xml otrzymuję komunikaty o błędach?

Podpisując plik na platformie biznes.gov.pl, powinni Państwo zweryfikować, czy oprogramowanie do składania podpisu, z którego Państwo korzystają, jest prawidłowo skonfigurowane.

Przykładowe instrukcje znajdą Państwo na stronie biznes.gov.pl

Składanie podpisu elektronicznego

Data wytworzenia informacji: 07.01.2019 r.

Czy Urząd Ochrony Danych Osobowych potwierdza otrzymanie zawiadomienia?

Dostarczone do UODO zawiadomienie jest potwierdzane Urzędowym Poświadczeniem Przedłożenia generowanym automatycznie w postaci pliku UPP.xml przez biznes.gov.pl lub portal epuap.gov.pl. Ocena, czy przesłane zawiadomienie o wyznaczeniu/odwołaniu/zmianie danych IOD lub zastępcy IOD jest poprawne, należy do zgłaszającego (pełnomocnika, jeżeli zawiadomienie jest składane przez pełnomocnika).

Więcej na ten temat znaleźć można w odpowiedzi na pytanie: JAK ocenić, czy przesłane zawiadomienie dotyczące IOD (zastępcy IOD) jest poprawne?

Data wytworzenia informacji: 08.04.2022 r.

Co zrobić w przypadku problemów technicznych związanych ze złożeniem zawiadomienia dotyczącego IOD?

Co zrobić w przypadku problemów technicznych związanych ze złożeniem zawiadomienia dotyczącego IOD?

Co zrobić w przypadku problemów technicznych związanych ze złożeniem zawiadomienia dotyczącego inspektora ochrony danych (IOD) lub w sytuacji nieotrzymania pliku UPP (Urzędowe Poświadczenie Przedłożenia)?

W przypadku problemów technicznych związanych ze złożeniem zawiadomienia dotyczącego IOD lub jego zastępcy (np. złożeniem podpisu) bądź z uzyskaniem UPP należy kontaktować się odpowiednio z pomocą techniczną:

- platformy biznes.gov.pl (https://www.biznes.gov.pl/pl/centrum-pomocy),
- centrum pomocy użytkowników ePUAP (https://epuap.gov.pl/wps/wcm/connect/epuap2/PL/Strefa+Klienta_Pomoc/Kontakt/).

Pod tymi linkami znajdą Państwo w szczególności numery telefonów do infolinii oraz informacje na temat innych form komunikacji z pomocą techniczną.

Data wytworzenia informacji: 16.03.2022 r.

Jak podpisać zawiadomienie dotyczące IOD przez więcej niż jedną osobę?

Pomocne informacje oraz instrukcje znajdują się na platformie biznes.gov.pl w materiale. Jak na Biznes.gov.pl podpisać wnioski/Jak dwie i więcej osób może podpisać wniosek?

Na platformie ePUAP znajduje się również instrukcja jak podpisać zawiadomienie przez dwie osoby za pośrednictwem ePUAP. W tym celu została przygotowana przez tę platformę instrukcja „Opatrywanie dokumentu elektronicznego więcej niż jednym podpisem zaufanym Wersja 1.0 zdnia 8 lutego 2019". Dostępna jest ona na stronie https://epuap.gov.pl/ w zakładce pt. „Instrukcja podwójnego podpisywania".

Data wytworzenia informacji: 07.01.2019 r.

Czy można zawiadomić o IOD przez pełnomocnika?

O wyznaczeniu (zmianie danych lub odwołaniu) IOD lub zastępcy IOD administratorzy/podmioty przetwarzające mogą zawiadomić przez pełnomocnika. Taką możliwość przewidują zarówno przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (art. 10 ust. 2), jak i przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych **przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości** (art. 46 ust. 9).

Jednak, aby takie zawiadomienie było skuteczne, pełnomocnik musi pamiętać o spełnieniu warunków związanych z **elektroniczną postacią zawiadomienia** oraz **elektroniczną formą**

pełnomocnictwa, a także o przesłaniu wraz z zawiadomieniem pełnomocnictwa i dowodu uiszczenia opłaty skarbowej od pełnomocnictwa (chyba że przepisy zwalniają od jej uiszczenia). Przed przystąpieniem do wysłania zawiadomienia warto przygotować sobie pełnomocnictwo oraz dowód dokonania opłaty skarbowej.

Data wytworzenia informacji: 07.01.2019 r.

Czy do zawiadomienia trzeba dołączyć pełnomocnictwo?

Jeśli zawiadomienia dokonuje pełnomocnik wtedy do każdego zawiadomienia musi być dołączone pełnomocnictwo udzielone w formie elektronicznej.

Wyjątek stanowi sytuacja gdy pełnomocnik jest ujawniony w CEIDG. Wtedy nie musi przesyłać pełnomocnictwa, wystarczające bowiem jest to, że widnieje on w CEIDG.

Natomiast przesłanie jedynie pełnomocnictwa bez załączenia stosownego zawiadomienia jest nieprawidłowe.

Data wytworzenia informacji: 08.04.2022 r.

Jak powinno wyglądać pełnomocnictwo dla osoby zgłaszającej IOD?

Urząd Ochrony Danych Osobowych nie narzuca konkretnego wzoru pełnomocnictwa udzielonego osobie zgłaszającej IOD (zastępcę IOD). Ważne jest, aby z treści pełnomocnictwa wynikało upoważnienie do wykonania takiej czynności. Pełnomocnictwo może mieć charakter ogólny i obejmować wiele różnych czynności dokonywanych przed organem lub dotyczyć tej konkretnej czynności (przesłania zawiadomienia dot. IOD lub jego zastępcy). W każdym przypadku musi być ono udzielone przez osobę uprawnioną do reprezentowania administratora/podmiotu przetwarzającego.

Data wytworzenia informacji: 07.01.2019 r.

W jakiej formie administrator/podmiot przetwarzający powinien udzielić pełnomocnictwa?

Jeżeli zawiadomienie dotyczące IOD ma być dokonane przez pełnomocnika, to pełnomocnictwo powinno zostać udzielone w formie elektronicznej.

Data wytworzenia informacji: 07.01.2019 r.

Co należy rozumieć przez formę elektroniczną pełnomocnictwa?

Pełnomocnictwa należy udzielić w formie elektronicznej, co oznacza, że powinno być ono (np. dokument w formacie DOC.) opatrzone kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP złożonym przez osobę lub osoby udzielające pełnomocnictwa (zgodnie z reprezentacją administratora/podmiotu przetwarzającego).

Możliwe jest także dołączanie pełnomocnictwa uwierzytelnionego elektronicznie przez notariusza. W takim przypadku do zawiadomienia należy załączyć pełnomocnictwo poświadczone za zgodność przez notariusza i opatrzone jego kwalifikowanym podpisem elektronicznym (zgodnie z art. 97 § 2 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie).

Co istotne, dokument podpisany własnoręcznie i zeskanowany nie jest uznany za prawidłową formę pełnomocnictwa. Sam skan pełnomocnictwa nieopatrzony podpisem w powyżej wskazany sposób, nie będzie miał właściwej, tj. elektronicznej, formy.

Data wytworzenia informacji: 07.01.2019 r.

Jak skutecznie podpisać pełnomocnictwo w formie elektronicznej?

Plik zawierający treść pełnomocnictwa, np. w formacie DOC, należy opatrzyć podpisem potwierdzonym profilem zaufanym ePUAP lub **kwalifikowanym podpisem elektronicznym**.

Data wytworzenia informacji: 07.01.2019 r.

Czy od zawiadomienia składanego przez pełnomocnika należy uiścić opłatę?

Jeżeli zawiadomienia dokonuje pełnomocnik, należy uiścić opłatę skarbową. Zgodnie z art. 1 ust. 1 pkt 2 ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej (Dz. U. z 2021 r. poz. 1923 ze zm.), **opłacie skarbowej podlega** w sprawach indywidualnych z zakresu administracji publicznej **złożenie dokumentu stwierdzającego udzielenie pełnomocnictwa** lub prokury albo jego odpisu, wypisu lub kopii w sprawie z zakresu administracji publicznej lub w postępowaniu sądowym.

Opłatę skarbową uiszcza się na numer konta bankowego **Urzędu Miasta Stołecznego Warszawy** Centrum Obsługi Podatnika (dostępny pod linkiem: https://bip.warszawa.pl/Menu_podmiotowe/dzielnice/Srodmiescie/default.html).

W tytule wpłaty, wraz z treścią – opłata skarbowa za pełnomocnictwo - należy zamieścić skrót PUODO, zaś dowód uiszczenia tej należności przesłać do Urzędu Ochrony Danych Osobowych jako załącznik do formularza.

Opłaty od złożonego pełnomocnictwa nie uiszcza się między innymi w przypadku, gdy mocodawcą jest podmiot określony w art. 7 pkt. 1-5 ustawy o opłacie skarbowej, np. jednostki budżetowe, jednostki samorządu terytorialnego, organizacje pożytku publicznego.

Data wytworzenia informacji: 07.01.2019 r.

Czy pełnomocnik powinien dołączyć do zawiadomienia potwierdzenie dokonania opłaty skarbowej?

Jeśli zgłoszenia dotyczącego IOD dokonuje pełnomocnik, do zawiadomienia - poza pełnomocnictwem w formie elektronicznej - należy załączyć dowód uiszczenia opłaty skarbowej w postaci dokumentu wykonania zlecenia przelewu przez system bankowości elektronicznej lub w postaci skanu otrzymanego dowodu wpłaty (w przypadku wpłaty za pośrednictwem poczty lub w kasie urzędu).

Wyjątki:

Opłaty od złożonego pełnomocnictwa nie uiszcza się m.in. w przypadku, gdy mocodawcą jest podmiot określony w art. 7 pkt. 1-5 ustawy z dnia 16 listopada 2006 r. o opłacie skarbowej, a więc np. jednostki budżetowe, jednostki samorządu terytorialnego, organizacje pożytku publicznego.

Data wytworzenia informacji: 07.01.2019 r.

Czy pełnomocnik ujawniony w CEIDG, może w imieniu tego podmiotu dokonać zawiadomienia?

Tak, pełnomocnik ujawniony w CEIDG może dokonać zawiadomienia o wyznaczeniu inspektora ochrony danych**.** Taki pełnomocnik nie musi przesyłać pełnomocnictwa z uwagi na ww. wpis w CEIDG.

Data wytworzenia informacji: 07.01.2019 r.

Czy notariusz może uwierzytelnić elektronicznie pełnomocnictwo upoważniające do zawiadomienia?

Tak, osoba działająca w imieniu administratora/podmiotu przetwarzającego, może do zawiadomienia o wyznaczeniu inspektora ochrony danych załączyć pełnomocnictwo, które będzie uwierzytelnione elektronicznie przez notariusza. W takim przypadku do zawiadomienia należy załączyć pełnomocnictwo poświadczone za zgodność przez notariusza i opatrzone jego

kwalifikowanym podpisem elektronicznym (art. 97 § 2 ustawy z dnia 14 lutego 1991 r. Prawo o notariacie, t.j. Dz. U. z 2017 r. poz. 2291 z późn. zm.).

Data wytworzenia informacji: 07.01.2019 r.

Czy pełnomocnik powinien weryfikować prawidłowość przesłanego przez niego zawiadomienia?

Oceny poprawności zawiadomienia powinien dokonać samodzielnie zgłaszający, w tym pełnomocnik.

Jeśli zawiadomienie złożone przez pełnomocnika nie spełniało powyższych warunków konieczne jest jego ponowne przesłanie.

Należy też pamiętać, że wraz z ponownym zgłoszeniem i przedstawieniem do niego prawidłowego dokumentu pełnomocnictwa, należy ponownie wnieść opłatę skarbową. Art. 1 ust. 1 pkt 2 ustawy o opłacie skarbowej nie wiąże powstania obowiązku podatkowego w opłacie skarbowej z faktem ustanowienia pełnomocnika ani istnienia już w obrocie ważnego umocowania, ale z faktem złożenia tego dokumentu (jego odpisu, wypisu lub kopii). A zatem ustawa podatkowa jednoznacznie stanowi, że obowiązek ten powstaje „z chwilą złożenia dokumentu" (patrz wyrok WSA w Szczecinie z 6.02.2013 r., sygn. akt I SA/Sz 737/12).

Data wytworzenia informacji: 08.04.2022 r.

Jak ocenić, czy przesłane zawiadomienie dotyczące IOD (zastępcy IOD) jest poprawne?

Ocena, czy zawiadomienie zostało sporządzone i wysłane poprawnie należy do zgłaszającego (pełnomocnika, jeżeli zawiadomienie jest składane przez pełnomocnika). Jeśli zawiadomienie nie spełnia wymagań, trzeba je ponowić.

Zawiadomienie jest poprawne, jeżeli:

1) ma postać elektroniczną;
2) zostało podpisane kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP przez osobę/osoby uprawnione do reprezentowania administratora;
3) zgłaszający przekazał w zawiadomieniu wszystkie wymagane przepisami prawa informacje;

4) pełnomocnik spełnił warunki związane z elektroniczną postacią zawiadomienia oraz elektroniczną formą pełnomocnictwa, a także przesłał opłatę skarbową od pełnomocnictwa (chyba że przepisy zwalniają od jej uiszczenia).

Szczegółowe informacje co do poprawności przesyłanego zawiadomienia zostały zamieszczone w materiale JAK PRAWIDŁOWO ZAWIADOMIĆ O WYZNACZENIU/ODWOŁANIU/ZMIANIE DANYCH IOD (ZASTĘPCY IOD)? oraz materiałach dotyczących zgłaszania IOD przez pełnomocnika.

Data wytworzenia informacji: 08.04.2022 r.

Jakie są najczęściej popełniane błędy w zawiadomieniach dotyczących IOD?

Najczęściej popełnianymi błędami związanymi z zawiadomieniami IOD są:

- przesłanie zawiadomienia w postaci papierowej np. drogą listowną zamiast w postaci elektronicznej, która jest jedyną prawidłową postacią zawiadomienia zgodnie z przepisami o ochronie danych osobowych,
- przesłanie pisma przewodniego bez formularza zawiadomienia,
- przesłanie zawiadomienia na niewłaściwym formularzu (np. szkoła przesyła zawiadomienie na formularzu przeznaczonym dla organów przetwarzające dane na podstawie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości),
- przesłanie zawiadomienia dotyczącego zastępcy IOD na niewłaściwym formularzu (np. przesłanie zawiadomienia na formularzu dotyczącym IOD),
- nieprzedstawienie pełnomocnictwa bądź załączenie do zawiadomienia pełnomocnictwa bez zachowania jego formy elektronicznej, np. scan pełnomocnictwa nieopatrzony kwalifikowanym podpisem elektronicznym, podpisanie pełnomocnictwa przez jednego członka zarządu, gdy z reprezentacji w KRS wynika reprezentacja dwuosobowa.

Jeśli zawiadomienie zawiera błędy konieczne jest jego ponowne przesłanie.

Data wytworzenia informacji: 08.04.2022 r.

Kiedy należy ponownie przesłać zawiadomienie dotyczące IOD?

Zawiadomienie dotyczące IOD należy ponownie przesłać w przypadku, gdy:

1) nie otrzymali Państwo potwierdzenia UPP (tj. Urzędowego Poświadczenia Przedłożenia generowanego automatycznie przez portale biznes.gov.pl i epuap.gov.pl w postaci pliku UPP.xml),
2) przesłane zawiadomienie nie spełnia warunków określonych przepisami prawa (np. nie zostało opatrzone podpisem/podpisami elektronicznymi osób uprawnionych do reprezentowania administratora, zostało przesłane na niewłaściwym formularzu).

Odpowiednie formularze związane z zawiadomieniami dotyczącymi IOD mogą Państwo znaleźć na dole naszej strony internetowej pod belką: Formularze zawiadomień IOD - załatw online na biznes.gov.pl.

Informacje i wyjaśnienia w zakresie zawiadomień dotyczących IOD mogą Państwo znaleźć na stronie internetowej UODO w zakładce Zawiadomienia Prezesa UODO związane z IOD.

Data wytworzenia informacji: 08.04.2022 r.

Do którego organu kierować zawiadomienie, jeśli podmiot nie posiada jednostki organizacyjnej w UE?

Do którego organu nadzorczego należy kierować zawiadomienie dotyczące IOD, jeśli administrator nie posiada jednostki organizacyjnej w UE?

Zawiadomienie organu nadzorczego o wyznaczeniu inspektora ochrony danych przez podmioty wskazane w art. 3 ust. 2 RODO (tj. administratora lub podmiot przetwarzający niemający jednostek organizacyjnych w Unii) powinno nastąpić do organu nadzorczego w państwie członkowskim, w którym przedstawiciel administratora/podmiotu przetwarzającego w UE ma jednostkę organizacyjną.

Do podmiotów (administratorów i podmiotów przetwarzających) nieposiadających jednostki organizacyjnej w UE RODO może mieć zastosowanie, również w zakresie obowiązku wyznaczenia inspektora ochrony danych, wówczas, gdy prowadzone przez nie czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w UE - niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE.

Takie podmioty mają obowiązek wyznaczenia swojego przedstawiciela w UE, chyba że przetwarzanie ma charakter sporadyczny, nie obejmuje na dużą skalę przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych, i jest mało prawdopodobne, by ze względu na swój charakter,

kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych, lub jeżeli administrator jest organem lub podmiotem publicznym. Wyznaczenie przedstawiciela nie wpływa na obowiązki lub odpowiedzialność prawną administratora lub podmiotu przetwarzającego wynikającą z RODO (art. 27 ust. 5 RODO, Motyw 80).

Stosując analogię do obowiązku zgłaszania naruszeń i wskazówek przekazanych w kontekście tego obowiązku w odniesieniu do podmiotów, które nie posiadają jednostki organizacyjnej w UE w Wytycznych dotyczących zgłaszania naruszeń ochrony danych (WP 250) zgłoszenia związane z inspektorem ochrony danych powinny być kierowane do organu nadzorczego w państwie członkowskim, w którym przedstawiciel administratora w UE ma jednostkę organizacyjną.

W przypadku zgłoszeń naruszeń ochrony danych osobowych Grupa Robocza Art. 29 wypowiedziała się następująco: „(…) w przypadku, gdy naruszenie odnotuje administrator niemający jednostki organizacyjnej w UE, który podlega przepisom art. 3 ust. 2 lub 3, na administratorze tym wciąż spoczywają obowiązki zgłaszania określone w art. 33 i 34. W art. 27 ustanowiono wymóg zobowiązujący administratora (i podmiot przetwarzający) do wyznaczenia przedstawiciela w UE w przypadku, gdy zastosowanie ma art. 3 ust. 2. W takich przypadkach Grupa Robocza Art. 29 zaleca, aby zgłoszenia były kierowane do organu nadzorczego w państwie członkowskim, w którym przedstawiciel administratora w UE ma jednostkę organizacyjną. Podobnie w przypadku gdy podmiot przetwarzający podlega przepisom art. 3 ust. 2, spoczywają na nim obowiązki dotyczące podmiotów przetwarzających, a w szczególności obowiązek zgłaszania naruszenia administratorowi na podstawie art. 33 ust. 2.” (str. 21)

Data wytworzenia informacji: 08.04.2022 r.

Kto powinien zawiadomić o odwołaniu IOD w przypadku likwidacji/przejęcia administratora?

Kto powinien zawiadomić Prezesa UODO o odwołaniu inspektora ochrony danych w przypadku likwidacji/przejęcia administratora, który wyznaczył tego inspektora?

Zgodnie z art. 10 ust. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych podmiot, który wyznaczył inspektora ochrony danych, ma obowiązek zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego odwołaniu.

W sytuacji zaś, gdy administrator nie zawiadomił Prezesa UODO o odwołaniu IOD, może to zrobić podmiot (np. zgodnie ze sposobem reprezentacji określonym w KRS), który jest jego następcą prawnym, a zatem przejął prawa i obowiązki likwidowanego podmiotu. W przypadkach, gdy żaden podmiot nie będzie następcą prawnym likwidowanego administratora, zawiadomienia

o odwołaniu IOD powinny dokonać osoby upoważnione do reprezentowania administratora podczas jego likwidacji.

Data wytworzenia informacji: 08.04.2022 r.

Czy należy zawiadamiać o zmianie, gdy następuje zmiana osób uprawnionych do reprezentacji?

Czy należy przesłać zawiadomienie dotyczące IOD w sytuacji zmiany osoby/osób uprawnionych do reprezentacji podmiotu, który wyznaczył IOD?

Przepisy ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (dalej: u.o.d.o.) nie zobowiązują do zawiadamiania organu nadzoru o zmianach danych osoby (osób) uprawnionych do reprezentacji podmiotu, który wyznaczył IOD.

Zgodnie art. 10 ust. 4 u.o.d.o. podmiot, który wyznaczył inspektora ochrony danych, ma obowiązek zawiadomić Prezesa UODO o każdej zmianie danych wskazanych w ustępach 1 i 3 art. 10 powołanej ustawy. A zatem Prezesa UODO trzeba powiadomić o zmianach, które dotyczą takich danych, jak:

- imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora,
- imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna,
- firma przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą,
- pełna nazwa oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w dwóch powyższych punktach,
- numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.

Organ nadzorczy trzeba również zawiadomić o odwołaniu IOD. Analogiczne rozwiązania dotyczące powiadamiania Prezesa UODO odnoszą się do sytuacji, w której podmiot wyznaczył osobę zastępującą inspektora (stosownie do art. 11a ust. 3 u.o.d.o.).

Ponieważ przepisy u.o.d.o. nie zobowiązują administratora do zawiadamiania organu nadzoru o zmianach danych osoby (osób) uprawnionych do reprezentacji podmiotu, który wyznaczył IOD, nie ma potrzeby informowania Prezesa UODO o takich zmianach.

Warto nadmienić, że również przepisy ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, nie zobowiązują administratora do zawiadamiania organu nadzoru o zmianach danych osoby (osób) uprawnionych do reprezentacji podmiotu, który wyznaczył IOD.

Data wytworzenia informacji: 08.04.2022 r.

Czy złożone przeze mnie zgłoszenie ABI zostało już rozpatrzone?

Wraz z uchyleniem z dniem 25 maja 2018 r. ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922z późn. zm.) przestały obowiązywać przepisy w zakresie rejestracji administratorów bezpieczeństwa informacji (ABI). Jest to związane z rozpoczęciem stosowania od tego dnia RODO.

W związku z uchyleniem powyższych przepisów Prezes Urzędu Ochrony Danych Osobowych (dawniej GIODO) nie prowadzi już ogólnokrajowego, jawnego rejestru ABI, zaś postępowania w sprawie rejestracji ABI zostały umorzone (art. 160 i art. 175 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych Dz.U. z 2018 r. poz. 1000).

Obecne przepisy dotyczące ochrony danych osobowych przewidują wyznaczenie IOD. Więcej informacji na temat wyznaczenia IOD oraz formy zawiadomienia Prezesa Urzędu o jego wyznaczeniu można znaleźć na naszej stronie w sekcji Inspektor Ochrony Danych.

Data wytworzenia informacji: 07.01.2019 r.

ZADANIA IOD

Jakie zadania ma IOD?

Do zadań inspektora ochrony danych zgodnie z art. art. 39 ust. 1 oraz 38 ust. 4 RODO należą:

1. **informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.**

Niewątpliwie prawidłowe wykonywanie powyższego zadania przez IOD bezpośrednio przekłada się na podejmowanie przez administratorów i podmioty przetwarzające świadomych i trafnych decyzji.

Aby kompetentnie edukować i doradzać innym IOD musi być do tego dobrze przygotowany merytorycznie, musi sam bardzo dobrze znać obowiązki administratorów i podmiotów przetwarzających oraz powiązane z nimi uprawnienia podmiotów danych. Dbanie o edukację osób podejmujących działania i decyzje w zakresie ochrony danych osobowych jest działaniem ciągłym i powtarzalnym, wymagającym umiejętności interpersonalnych i dydaktycznych.

2. **monitorowanie przestrzegania niniejszego rozporządzenia, 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.**

Aktywność inspektora ochrony danych w tym zakresie nie powinna mieć charakteru jednorazowego, a charakter ciągły i długofalowy. Zgodnie z Wytycznymi Grupy Roboczej art. 29 dotyczącymi inspektorów ochrony danych monitorowanie to:

- zbieranie informacji w celu identyfikacji procesów przetwarzania;
- analizowanie i sprawdzanie zgodności przetwarzania;
- informowanie, doradzanie i rekomendowanie określonych działań.

Wykonując ten obowiązek inspektor ochrony danych powinien dostosować sposób i rodzaj przekazywanych informacji do grupy docelowej, tak aby zadanie to było realizowane w sposób efektywny i skuteczny.

3. **udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35.**

Zgodnie z art. 35 ust. 2 RODO administrator dokonując oceny skutków konsultuje się z IOD, jeżeli został wyznaczony, w celu wydania przez niego zaleceń.

RODO określa, kiedy i jak należy dokonywać oceny skutków dla ochrony danych, natomiast nie zawiera konkretnych wskazówek, w jaki sposób oceny takiej należałoby dokonać. Pomocne w tym zakresie mogą być Wytyczne Grupy Roboczej art. 29, zgodnie z nimi administrator dokonując ww. oceny powinien konsultować się z IOD w następujących kwestiach:

- czy należy przeprowadzić ocenę skutków dla ochrony danych;
- metodologii przeprowadzenia oceny skutków dla ochrony danych;
- czy należy przeprowadzić wewnętrzną ocenę czy też zlecić ją podmiotowi zewnętrznemu;
- zabezpieczeń (w tym środków technicznych i organizacyjnych) stosowanych do łagodzenia wszelkich zagrożeń praw i interesów osób, których dane dotyczą;
- prawidłowości przeprowadzonej oceny skutków dla ochrony danych i zgodności jej wyników z RODO (czy należy kontynuować przetwarzanie, czy też nie oraz jakie zabezpieczenia należy zastosować).

Jeśli administrator nie zgadza się z zaleceniami IOD w wyżej wymienionych przypadkach, dokumentacja oceny skutków dla ochrony danych powinna zawierać pisemne uzasadnienie nieuwzględnienia zaleceń IOD.

4. **współpraca z Prezesem Urzędu Ochrony Danych Osobowych.**

Zgodnie z artykułem 39 ust. 1 lit. d RODO, IOD powinien współpracować z organem nadzorczym w kwestiach związanych z przetwarzaniem danych osobowych oraz w stosownych przypadkach zwracać się do niego.

5. **pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.**

Pełnienie przez IOD funkcji punktu kontaktowego należy traktować jako pełnienie przez niego roli pośrednika pomiędzy administratorem lub podmiotem przetwarzającym, a organem nadzorczym.

IOD z jednej strony udziela fachowego wsparcia administratorowi w zakresie sposobu wykonania obowiązków nałożonych na administratora wynikających z RODO, z drugiej strony wspomaga go przed organem nadzorczym w wykazaniu zasadności wybranych rozwiązań w ramach prowadzonych przez organ postępowań.

Obowiązek pełnienia roli punktu kontaktowego przez IOD dla organu nadzorczego, wynika z art. 39 ust. 1 lit. e RODO. Wobec czego, jeżeli organ nadzorczy zwróci się do IOD o udzielenie mu informacji w określonych przypadkach (w tym dostępu do dokumentów), inspektor powinien się z tego obowiązku należycie wywiązać.

Poniżej przykłady sytuacji, w których IOD będzie pełnił funkcję punktu kontaktowego.

1) punkt kontaktowy w zakresie naruszeń (art. 33 RODO);

W przypadku zgłoszenia naruszenia ochrony danych przez administratora Prezesowi Urzędu Ochrony Danych Osobowych, administrator jest zobowiązany do podania danych kontaktowych IOD w celu uzyskania przez organ wszelkich ważnych w tej sprawie informacji. Przepis ten zobowiązuje jednocześnie inspektora ochrony danych do współpracy oraz przekazywania wszelkich niezbędnych informacji Prezesowi Urzędu.

2) punkt kontaktowy w zakresie uprzednich konsultacji (art. 36 RODO).

Zgodnie z art. 35 RODO na administratora danych nałożony jest obowiązek dokonywania oceny skutków dla ochrony danych oraz konsultowania się w tej sprawie z powołanym IOD. Ponadto, w przypadku, gdy zmienia się ryzyko wynikające z operacji przetwarzania administrator powinien dokonać przeglądu, by stwierdzić czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych. Jeżeli ocena ta wykaże, że przetwarzanie może powodować wysokie ryzyko przy braku zastosowania przez administratora środków dla zminimalizowania tego ryzyka, to zgodnie z art. 36 RODO administrator konsultuje się w tej sprawie z Prezesem Urzędu Ochrony Danych Osobowych. Zasadne jest założenie, że IOD jako doradca administratora, powinien w tej sprawie ściśle współpracować z Prezesem Urzędu, przedstawiając wszystkie istotne aspekty mogące mieć wpływ na treść przyszłego zalecenia.

Warto zwrócić uwagę, że powołany inspektor ochrony danych zgodnie z Wytycznymi Grupy Roboczej art. 29 powinien, komunikować się w języku używanym przez Prezesa Urzędu.

6. **pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia.**

Osoby, których dane dotyczą, zgodnie z art. 38 ust. 4 RODO, powinny mieć możliwość skontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy niniejszego rozporządzenia. W związku z tym, na stronie internetowej administratora lub podmiotu przetwarzającego powinny się znaleźć dane kontaktowe inspektora ochrony danych, umożliwiające kontakt z nim zainteresowanym podmiotom. W dużej organizacji, ilość pytań wpływających do IOD może być tak duża, że mogłoby to powodować trudności w wykonywaniu przez niego innych zadań. W związku z powyższym pożądane byłoby w takim przypadku, wyznaczenie pracowników lub

powołanie zespołu osób, które wspierałyby inspektora ochrony danych w zakresie wykonywania tego zadania.

Zadania inspektora ochrony danych w RODO zostały sformułowane w sposób ogólny, bez wskazania trybu oraz terminów ich realizacji. Taki sposób ujęcia obowiązków inspektora jest wyrazem nowego podejścia do ochrony danych osobowych opartego na analizie ryzyka i zasadzie rozliczalności, zapisanej w art. 5 ust. 2 RODO. Wyznaczenie IOD roli doradczej i weryfikacyjnej wobec działań administratora danych i podmiotu przetwarzającego (oraz ich pracowników) sprawia, że zarówno zadania IOD, jak i sposób ich realizacji są ściśle powiązane nie tylko z obowiązkami administratorów danych lub podmiotów przetwarzających, ale też z nowym sposobem podejścia do ich realizacji.

Należy pamiętać, że podmiotem, który faktycznie podejmuje decyzje i odpowiada za wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających odpowiedni stopień bezpieczeństwa oraz wykazanie, że przetwarzanie odbywa się zgodnie z przepisami ochrony danych osobowych jest administrator lub podmiot przetwarzający. Na podstawie art. 24 RODO administratorzy i podmioty przetwarzające są zobowiązani uwzględniać: charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, i odpowiednio do nich - dobierać i wdrażać środki techniczne i organizacyjne, tak, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te powinny być w razie potrzeby poddawane przeglądom i uaktualniane. Ponadto zarówno przy określaniu ilości zbieranych danych osobowych, jak i zakresu ich przetwarzania, okresu przechowywania, dostępności oraz sposobów przetwarzania konieczne jest stosowanie mechanizmów takich jak zapewnienie ochrony danych osobowych na etapie projektowania oraz domyślnej ochrony danych („privacy by design” oraz „privacy by default”), zarówno przed przystąpieniem do przetwarzania danych, jak i w czasie prowadzonego przetwarzania (art. 25 RODO).

Data wytworzenia informacji: 15.01.2019 r.

Czy prowadzenie rejestru czynności powinno być zaliczane do zadań IOD?

Zgodnie z art. 30 ust. 1 i 2 RODO, do administratora należy obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, za które odpowiada, a do podmiotu przetwarzającego - prowadzenie rejestru kategorii czynności przetwarzania dokonywanych w imieniu administratora. **To te podmioty są odpowiedzialne za efektywne wykonanie tego obowiązku i pozostawanie w gotowości do wykazania tego na żądanie organów ochrony danych.** Tym samym są one zobowiązane określić, kto konkretnie w danej organizacji ma

wykonywać określone czynności składające się na spełnienie wymogów określonych w art. 30 RODO, uwzględniając konkretne okoliczności, m.in. takie jak wielkość i struktura organizacyjna danego podmiotu oraz skala przetwarzania danych. Zgodnie z jedną z najważniejszych zasad, na których oparta jest nowa regulacja – zasadą rozliczalności, odpowiedni dobór rozwiązań zapewniających zgodność z przepisami o ochronie danych osobowych należy do administratorów danych i podmiotów przetwarzających.

Ze względu na swoją zawartość i cele, rejestry czynności oraz rejestry kategorii czynności mogą być również przydatnym instrumentem monitorowania zgodności dla inspektorów ochrony danych. Wprawdzie z art. 30 rozporządzenia ogólnego bezsprzecznie wynika, że obowiązek prowadzenia rejestrów należy do administratorów i podmiotów przetwarzających, nie zaś do inspektora ochrony danych, niemniej trudno sobie wyobrazić, że inspektor ochrony danych - jako osoba dysponująca odpowiednią wiedzą i umiejętnościami w dziedzinie ochrony danych osobowych - nie będzie angażowała się w tworzenie i prowadzenie rejestrów, a następnie wykorzystywała ich w swojej pracy.

Inspektor ochrony danych jako fachowiec **może wspomagać administratora w tworzeniu i prowadzeniu rejestrów** na przykład poprzez doradzanie mu w kwestiach związanych z wykonaniem tego obowiązku.

Data wytworzenia informacji: 15.01.2019 r.

Czy po wejściu stosowania RODO CUW może powołać jednego IOD dla wszystkich obsługiwanych jednostek?

Centra Usług Wspólnych (CUW) są tworzone jako osobne podmioty, a domeną ich działań są najczęściej działania pomocnicze, wykonywane zarówno w odniesieniu do organów wykonawczych, jak i uchwałodawczych samorządu terytorialnego, jak również do obsługi poszczególnych jednostek organizacyjnych, między innymi urzędów, zakładów i jednostek budżetowych. Ostateczną decyzję, zarówno co do powołania samorządowego centrum usług wspólnych, jak i jego kształtu oraz zakresu realizowanych przez niego zadań, podejmuje organ stanowiący danej jednostki samorządu terytorialnego.

CUW nie jest administratorem danych przekazanych przez jednostki obsługiwane. Może je przetwarzać w zakresie i celu niezbędnym do wykonywania zadań w ramach wspólnej obsługi tych jednostek (zgodnie z art. 10d ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, art. 6d ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym i art. 8f ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa). W zależności od różnych możliwych rozwiązań stosowanych przez konkretne samorządy, CUW może być natomiast administratorem danych np. swoich pracowników.

Na gruncie ogólnego rozporządzenia o ochronie danych obowiązek wyznaczenia inspektora ochrony danych w sektorze publicznym dotyczyć będzie wszystkich organów i podmiotów publicznych (art. 9 u.o.d.o.), zarówno tych będących administratorami danych, jak i podmiotami przetwarzającymi.

Niemniej nawet w sytuacji, gdyby miał być nim pracownik jednej z tych jednostek, np. pracownik CUW, konieczne jest osobne wyznaczenie IOD przez każdą z tych jednostek, np. każdą szkołę, dom kultury – jako osobnych administratorów. Zatem nawet jeżeli CUW świadczy obsługiwanym podmiotom usługi związane z szeroko rozumianą ochroną danych osobowych, nie jest uprawniony do wyznaczania inspektora ochrony danych w tych podmiotach. Obowiązek wyznaczania inspektora ochrony danych nie może być przeniesiony, np. w drodze uchwały czy porozumienia, na inną jednostkę organizacyjną, np. na CUW.

Każdy z podmiotów zobowiązanych do wyznaczenia inspektora ochrony danych (niezależnie, czy będzie to jedna, ta sama osoba, czy różne osoby) będzie również zobowiązany - zgodnie z art. 37 ust. 7 RODO - do opublikowania danych kontaktowych inspektora i zawiadomienia o nich organu nadzorczego. Tak jak obowiązek wyznaczenia inspektora, tak i obowiązek powiadomienia o danych kontaktowych dotyczy zatem każdej jednostki samorządu terytorialnego, o której mowa w art. 37 ust. 1 lit. a RODO.

Data wytworzenia informacji: 15.01.2019 r.

Na czym polega wykonywanie zadań przez IOD z należytym uwzględnieniem ryzyka?

Przepis dotyczący zadań inspektora ochrony danych (art. 39 ust. 2 RODO) wyraźnie wskazuje na konieczność dostosowania trybu i metod pracy do specyfiki przetwarzania danych oraz związanego z tym przetwarzaniem ryzyka. Inspektor ma wypełniać swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Chodzi tu o ogólną, zdroworozsądkową zasadę, którą IOD może odnieść do wielu aspektów swojej codziennej pracy. Wypełnianie zadań „z należytym uwzględnieniem ryzyka" wymaga od IOD ustalania priorytetów w swojej pracy i koncentrowania się na aspektach pociągających za sobą większe ryzyko.

Zdaniem Grupy Roboczej Art. 29, takie podejście powinno ułatwić IOD doradzenie administratorowi, m.in.:

- które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi,
- jakie szkolenia dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych należy przeprowadzić,

- na które operacje przetwarzania należy przeznaczyć więcej czasu i zasobów.

IOD wykonując swoje zadania (art. 39 ust. 2 RODO), powinien zatem stosować rozwiązania dostosowane do potrzeb podmiotów, w których pełni swoją funkcję, a także cech konkretnego przetwarzania danych i związanego z tym przetwarzaniem ryzyka. Konieczność realizacji obowiązków w powyższy sposób w konsekwencji ma prowadzić do skuteczniejszej ochrony danych.

Data wytworzenia informacji: 15.01.2019 r.

Kto powinien opracować wewnętrzną politykę ochrony danych osobowych? Administrator czy IOD?

Zgodnie z art. 24 RODO administrator, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Treść powyższego artykułu wskazuje jednoznacznie, że wdrożenie odpowiednich środków technicznych i organizacyjnych (które mogą obejmować również wdrożenie przez administratora odpowiednich polityk ochrony danych) należy do obowiązków administratora (osób przez niego wyznaczonych).

Rolą IOD jest natomiast dokonywanie oceny przyjętych przez administratora środków (w tym wewnętrznych polityk) pod kątem ich zgodności z przepisami prawa i skuteczności. Do zadań inspektora ochrony danych należy też monitorowanie przestrzegania przyjętej w dziedzinie ochrony danych osobowych polityki przez osoby upoważnione do przetwarzania danych (art. 39 ust. 1 lit. b RODO).

W trakcie tworzenia polityk dotyczących ochrony danych wskazane jest, aby administrator zasięgał opinii i wskazówek u swojego inspektora ochrony danych (IOD), który posiada fachową wiedzę na temat prawa i praktyk w dziedzinie ochrony danych, zgodnie z treścią art. 39 ust. 1 lit. a RODO

Data wytworzenia informacji: 07.01.2019 r.

Czy IOD jest zobowiązany wykonywać swoje zadania również na rzecz zakładowej organizacji związkowej?

Zakładowa organizacja związkowa jest w zakresie swoich kompetencji określonych w prawie pracy i ustawie o związkach zawodowych odrębnym administratorem danych, niezależnym od

pracodawcy, u którego działa. W związku z tym - jeżeli nie istnieją w tym zakresie odrębne uzgodnienia - IOD nie jest zobowiązany do wykonywania zadań określonych w art. 39 RODO, na rzecz innych administratorów, w tym np. komisji zakładowej jako odrębnego administratora danych.

Data wytworzenia informacji: 07.01.2019 r.

Czy rejestr czynności prowadzony na podstawie art. 30 ust. 1 RODO musi być udostępniany publicznie?

Żaden przepis prawa nie nakazuje publikowania rejestru czynności lub kategorii czynności na stronie internetowej administratora danych lub podmiotu przetwarzającego**.** We wskazówkach i wyjaśnieniach dotyczących obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO, wskazujemy, że celem i funkcją obowiązku określonego w art. 30 RODO jest zachowanie przez administratora i podmiot przetwarzający zgodności z RODO oraz umożliwienie organowi nadzorczemu monitorowanie prowadzonego przetwarzania (str. 4). Zgodnie z art. 30 ust. 4 takie rejestry udostępniane są jedynie na żądanie organu nadzorczego. Biorąc pod uwagę, że zgodnie z art. 30 ust. 1 lit. g i art. 30 ust. 2 lit. d RODO zawierają one ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, nie powinny być one udostępniane osobom trzecim.

Data wytworzenia informacji: 07.01.2019 r.

Czy naruszenie przepisów odnoszących się do IOD może skutkować administracyjnymi karami pieniężnymi?

Czy naruszenie przepisów odnoszących się do inspektora ochrony danych może skutkować administracyjnymi karami pieniężnymi nakładanymi na administratora danych lub podmiot przetwarzający?

Stosownie do art. 83 ust. 4 lit. a RODO, naruszenia przepisów bezpośrednio odnoszących się do IOD (art. 37–39 RODO) podlegają administracyjnej karze pieniężnej do 10 mln euro, a w przypadku przedsiębiorstwa – do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego. Karami administracyjnymi obwarowane są zatem zarówno poszczególne obowiązki administratorów danych i podmiotów przetwarzających dotyczące wyznaczania IOD i zapewnienia mu określonych warunków wykonywania funkcji, jak i wykonywanie zadań przez IOD. Jednocześnie, należy mieć na uwadze, iż organ nadzorczy nakłada kary pieniężne zgodnie z art. 83 ust. 1 RODO, tak aby były one skuteczne, proporcjonalne

i odstraszające. Organ decydując czy nałożyć karę pieniężną oraz w jakiej powinna być ona wysokości bierze pod uwagę - w każdym indywidualnym przypadku - następujące kryteria:

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą, oraz rozmiaru poniesionej przez nie szkody;
- umyślny lub nieumyślny charakter naruszenia;
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą;
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32 RODO;
- wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego;
- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków;
- kategorie danych osobowych, których dotyczyło naruszenie;
- sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie;
- jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 RODO - przestrzeganie tych środków;
- stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 RODO lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 RODO; oraz
- wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

Grupa Robocza art. 29 w swoich wytycznych w sprawie stosowania i ustalania administracyjnych kar pieniężnych do celów rozporządzenia nr 2016/679 (WP 253), podkreśliła indywidualny charakter kary i branie pod uwagę przez organ nadzorczy w każdym przypadku z osobna kryteriów z art. 83 ust. 2 lit. a-k RODO: „(…) w świetle motywu 148 RODO organ nadzorczy jest odpowiedzialny za wybór najodpowiedniejszego środka (najodpowiedniejszych środków).”

Data wytworzenia informacji: 07.01.2019 r.

Czy pracodawca powinien zawierać umowy powierzenia z takimi podmiotami, jak ZUS czy bank?

Wykonując funkcję inspektora ochrony danych często spotykam się z wątpliwościami pracodawców dotyczącymi konieczności zawierania przez nich jako administratorów umów powierzenia przetwarzania danych osobowych z takim podmiotami, jak GUS, ZUS, urząd skarbowy czy bank. Czy takie umowy powinny być zawierane?

W przypadkach odnoszących się do przekazywania przez administratora, jako pracodawcy danych osobowych takim podmiotom, jak GUS, ZUS, czy urząd skarbowy mamy do czynienia z udostępnieniem danych na podstawie przepisów prawa, nie zaś z powierzeniem przetwarzania. Na administratorze, jako pracodawcy ciąży bowiem obowiązek przekazywania szeregu danych osobowych pracowników w związku z realizacją ustawowych zadań. Do obowiązków tych należą m.in.:

1. wobec ZUS – obowiązki wynikające z art. 49 ust. 2 i 4 ustawy z dnia 13 października 1998 r. o systemie ubezpieczeń społecznych na podstawie wzoru określonego w rozporządzeniu Ministra Rodziny, Pracy i Polityki Społecznej z dnia 20 grudnia 2018 r. w sprawie określenia wzorów zgłoszeń do ubezpieczeń społecznych i ubezpieczenia zdrowotnego, imiennych raportów miesięcznych i imiennych raportów miesięcznych korygujących, zgłoszeń płatnika składek, deklaracji rozliczeniowych i deklaracji rozliczeniowych korygujących, zgłoszeń danych o pracy w szczególnych warunkach lub o szczególnym charakterze, raportów informacyjnych, oświadczeń o zamiarze przekazania raportów informacyjnych oraz innych dokumentów,
2. wobec Urzędu Skarbowego - obowiązki w zakresie odprowadzania podatku dochodowego od osób fizycznych na podstawie ustawy z 26 lipca 1991 r. o podatku dochodowym od osób fizycznych,
3. wobec GUS - obowiązek wynikający z art. 237 § 3 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy na podstawie rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 7 stycznia 2009 r. w sprawie statystycznej karty wypadku przy pracy.

Odnosząc się do kwestii umów zawieranych przez pracodawcę z bankiem, to w tym przypadku również nie możemy mówić o powierzeniu przetwarzania danych. Pracodawca zawiera z bankiem umowę o świadczenie usług bankowych i to na jej podstawie udostępnia dane swoich pracowników w celu dokonania przelewów wynagrodzeń. Bank realizuje zadania wynikające z przepisów ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe i w momencie otrzymania od pracodawcy danych pracowników w celu świadczenia usług bankowych, staje się administratorem tych danych.

Data wytworzenia informacji: 12.04.2019 r.

Co należy zrobić, jeśli zawiadomienie o naruszeniu nie zostało odebrane przez adresata?

Co powinienem jako inspektor ochrony danych doradzić administratorowi, jeśli listowne zawiadomienie o naruszeniu ochrony danych osobowych skierowane do osoby, której dane dotyczą nie zostanie przez nią odebrane?

Co do zasady osoby, których dane dotyczą, należy zawiadomić o naruszeniu bezpośrednio, chyba że takie działanie wymagałoby niewspółmiernie dużego wysiłku. Nieodebranie przez osobę, której dane dotyczą informacji o naruszeniu, przesłanego za pomocą poczty tradycyjnej, powinno wskazywać administratorowi na konieczność podejmowania dalszych działań w celu skutecznego poinformowania tej osoby o naruszeniu.

Zgodnie z przepisami RODO (art. 12 ust. 1 RODO), przekazanie podmiotom informacji związanych z przetwarzaniem ich danych powinno nastąpić na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. W uzasadnionych przypadkach, informacji można udzielić ustnie, o ile potwierdzi się tożsamość osoby, której dane dotyczą. W sytuacji, gdy bezpośrednie kanały komunikacji zawiodą warto rozważyć wydanie publicznego komunikatu lub zastosowanie podobnego środka komunikacyjnego, za pomocą którego osoba, której dane dotyczą, zostanie skutecznie poinformowana.

Przykładami metod zawiadamiania o naruszeniu ochrony danych są np.: wiadomości e-mail, SMS, wiadomości bezpośrednie, rzucające się w oczy banery lub powiadomienia na stronach internetowych, komunikacja pocztowa oraz rzucające się w oczy reklamy w mediach drukowanych. Powyższe oznacza, że administrator wykorzysta szerszy zakres metod komunikacji, a nie tylko jeden kanał kontaktowy.

W przypadku kiedy administrator nie jest w stanie zawiadomić danej osoby fizycznej o naruszeniu, ponieważ przechowywane dane są niewystarczające do skontaktowania się z tą osobą, to zgodnie z wytycznymi GR Art. 29 w takim szczególnym przypadku administrator powinien ją poinformować tak szybko, jak jest to rozsądnie wykonalne (np. jeżeli osoba fizyczna skorzysta z przewidzianego w art. 15 RODO prawa do uzyskania dostępu do swoich danych osobowych i dostarczy administratorowi dodatkowe informacje wymagane do skontaktowania się z nią).

Data wytworzenia informacji: 12.04.2019 r.

Jak identyfikować podopiecznych Domu Pomocy Społecznej w związku z podawaniem leków?

Jako IOD wykonujący swoją funkcję w Domu Pomocy Społecznej zastanawiam się, czy dopuszczalne jest wywieszanie imiennych tabliczek przed pokojami podopiecznych.

Niewątpliwie zdrowie i życie ludzkie jest najwyższą wartością. Dlatego, w przypadku zderzenia tych wartości z zapewnieniem prywatności osób fizycznych i bezpieczeństwa ich danych osobowych rodzą się wątpliwości jak pogodzić te dwie ważne kwestie. Jedną z takich sytuacji jest konieczność właściwej identyfikacji przebywającego w Domu Pomocy Społecznej pensjonariusza celem podania przepisanych mu leków. W tego typu placówkach przebywają najczęściej osoby w podeszłym wieku, cierpiące na różne schorzenia, a co za tym idzie przyjmują odpowiednio zaordynowane przez lekarza leki. Zdarzają się sytuacje utraty i zaników pamięci podopiecznych, a wówczas personel nie będzie miał pewności co do tożsamości pacjenta, któremu należy podać właściwe leki. Bez wątpienia ryzyko podania niewłaściwego produktu leczniczego może mieć poważne konsekwencje dla zdrowia, a nawet życia danej osoby. Wobec tego, czy można uznać za prawidłową praktykę wywieszanie przy pokojach pensjonariuszy tabliczki z ich imionami i nazwiskami? Takie rozwiązanie prowadzi do udostępnienia danych osobowych pensjonariuszy osobom postronnym (np. odwiedzającym innych podopiecznych), a także budzi wątpliwości, czy będzie ono właściwie służyło zadeklarowanemu celowi. W trosce o zdrowie i życie pensjonariuszy oraz w celu wyeliminowania ryzyka związanego z możliwością błędnego podania leków, przykładowym rozwiązaniem powyższego problemu może być między innymi imienne oznaczenie konkretnej osoby, nie zaś pokoju, w którym została ona zakwaterowana. Pensjonariuszy można wyposażyć na przykład w imienne opaski, które pozwalałyby personelowi medycznemu na jednoznaczną identyfikację i właściwe podanie leków swoim podopiecznym. Jest to rozwiązanie, które nie dość, że pomoże osiągnąć cel, ale także pozwoli pozostać w zgodzie z przepisami o ochronie danych osobowych.

Data wytworzenia informacji: 31.07.2019 r.

Czy żłobek jest administratorem danych stażysty skierowanego na staż przez Powiatowy Urząd Pracy

Jako IOD często mierzę się z koniecznością dokonania oceny, komu przysługuje status administratora. Przykładem takiej sytuacji jest udostępnianie danych osobowych stażystów na podstawie umów zawieranych z Powiatowymi Urzędami Pracy. Wątpliwości dotyczą określenia, czy np. żłobek jest administratorem danych osobowych stażysty skierowanego przez PUP na staż, czy też jest - wobec tych danych – jedynie podmiotem przetwarzającym?

Żłobek jest administratorem danych osobowych stażysty w zakresie danych przetwarzanych w ramach umowy zawartej z Powiatowym Urzędem Pracy. Dodatkowo żłobek może przetwarzać dane osobowe stażysty wykraczające poza zakres tych, które były udostępnione na podstawie umowy z PUP, a są niezbędne do prawidłowego odbycia stażu. Przykładem może być pozyskiwanie danych stażysty w celu realizacji obowiązku związanego ze sprawdzeniem stażysty na podstawie przepisów ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym. W tym zakresie żłobek również jest administratorem.

Data wytworzenia informacji: 31.07.2019 r.

Jak długo powinny być udostępniane w BIP oświadczenia majątkowe, np. radnego, wójta?

W pracy IOD napotykam wątpliwości, jak długo mogą być udostępniane w Biuletynie Informacji Publicznej oświadczenia majątkowe, np. radnego. Czy jest jakiś konkretny przepis, który to reguluje, czy administrator powinien sam ocenić - zgodnie z ogólnymi zasadami ochrony danych osobowych?

Ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2019 r. poz. 506) w art. 24h ust. 6 wprost wskazuje na 6 letni termin przechowywania oświadczeń majątkowych osób zobowiązanych do ich składania np. wójta, radnego. Zatem po upływie wskazanego terminu przechowywania oświadczeń majątkowych, przetwarzanie danych w nich zawartych należy uznać za niedopuszczalne. Termin ten dotyczy zarówno oświadczeń złożonych przez osoby, które złożyły oświadczenie majątkowe i przestały pełnić swoją funkcję, jak i osoby, które nadal sprawują funkcję publiczną, a których oświadczenie, z uwagi na konieczność złożenia kolejnego, aktualnego oświadczenia o stanie majątkowym stało się nieaktualne. Również przetwarzanie (w tym przechowywanie i udostępnianie) danych zawartych w tych oświadczeniach w Biuletynie Informacji Publicznej nie powinno być dokonywane przez czas dłuższy, niż wymaga tego ustawa o samorządzie gminnym. W przeciwnym razie może to prowadzić do naruszenia art. 5 ust. 1 lit. b, c i e RODO, gdyż spowoduje, że informacje będą przetwarzane bez podstawy prawnej (powyżej terminu zakreślonego przez ustawodawcę) oraz przechowywane będą w postaci umożliwiającej identyfikację osoby, której dotyczą, dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

Data wytworzenia informacji: 31.07.2019 r.

Czy prywatny numer telefonu sołtysa stanowi informację publiczną?

W jednostce samorządu terytorialnego, w której pełnię funkcję inspektora ochrony danych, pojawiło się zagadnienie budzące moją wątpliwość. Urząd Gminy w celu kontaktu z sołtysami z terenu gminy, zbiera ich prywatne numery telefonów. Sołtysi nie posiadają służbowych telefonów ani służbowych kont poczty elektronicznej. Wobec tego czy prywatny numer telefonu sołtysa stanowi informację publiczną i może być udostępniany w trybie ustawy o dostępnie do informacji publicznej?

Zgodnie z art. 36 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2019 r. poz. 506), sołtys jest organem wykonawczym w sołectwie. Na mocy ust. 3 powołanego przepisu korzysta on z ochrony prawnej przysługującej funkcjonariuszom publicznym. Pojęcie funkcjonariusza publicznego zostało zdefiniowane w art. 115 § 13 pkt 4 ustawy z dnia 6 czerwca 1997 r. – Kodeks Karny (Dz. U. z 2018 r. poz. 1600 z późn. zm.) i stanowi, że funkcjonariuszem publicznym jest osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wykonywania decyzji administracyjnych. Przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2018 r. poz. 1330 z późn. zm.) precyzują natomiast wyrażone w art. 61 Konstytucji RP ogólne zasady korzystania z prawa do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne poprzez określenie zasad i trybu udostępniania, informacji publicznej oraz wskazanie właściwych w tym zakresie organów. Pojęcie informacji publicznej określone zostało w art. 1 ust. 1 oraz art. 6 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. W świetle ww. przepisów informacją publiczną jest każda informacja o sprawach publicznych. Zgodnie z treścią art. 6 ust. 1 pkt 2 lit. d ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, udostępnieniu podlega m.in. informacja o organach władzy publicznej, w tym o organach i osobach sprawujących w nich funkcje i ich kompetencjach. W myśl art. 2 ust. 1 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, na zasadach i w trybie określonym w jej przepisach, każdemu przysługuje prawo dostępu do informacji publicznej. Prawo do informacji publicznej podlega ograniczeniu jedynie w zakresie i na zasadach określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych, jak również ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania tych funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

W związku z powyższym dane osobowe sołtysa, o ile ściśle wiążą się z pełnioną przez sołtysa rolą publiczną i nie wkraczają w jego prywatność, podlegają ograniczonej ochronie prawnej. Nie budzi zatem wątpliwości ujawnianie przez urząd gminy takich danych sołtysa jak jego imię i nazwisko, adres, pod którym urzęduje, czy też służbowy numer telefonu i służbowy adres poczty elektronicznej. Inaczej sytuacja wygląda w przypadku prywatnego numeru telefonu sołtysa. Bowiem jak wyżej zaznaczono każda osoba, również sprawująca funkcję publiczną, posiada prawo do prywatności, w tym do nierozpowszechniania swojego prywatnego numeru telefonu. Wskazać należy, iż w polskim systemie prawnym nie ma generalnego obowiązku posiadania telefonu, taki obowiązek nie został również nałożony na sołtysa na mocy ustawy z dnia 8 marca 1990 r. o samorządzie gminnym. Konkludując – prywatnego numeru telefonu nie można uznać za informację publiczną podlegającą udostępnieniu.

Data wytworzenia informacji: 31.07.2019 r.

Kiedy administrator może pobrać opłatę za udzielenie informacji osobie, której dane dotyczą?

W swojej praktyce inspektora ochrony danych napotykam na wątpliwości dotyczące pobierania opłaty od osób realizujących swoje uprawnienia z RODO. Czy administrator na podstawie art. 12 ust. 5 RODO może pobrać opłatę uwzględniającą administracyjne koszty udzielenia informacji w przypadku, kiedy żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne? Czy opłata ta może być pobrana za czynności stricte administracyjne, tj. koszty pracy w postaci analizy żądania, przygotowania korespondencji?

Co do zasady za informacje podawane na podstawie art. 13 i 14 RODO oraz komunikację i działania podejmowane na mocy art. 15-22 i 34 RODO administrator nie może pobierać opłat. Wyjątek od tej zasady stanowią dwa przypadki, tj. kiedy żądania osoby, której dane dotyczą są ewidentnie nieuzasadnione lub nadmierne (art. 12 ust. 5 RODO). Z sytuacjami takimi mamy do czynienia w szczególności ze względu na ustawiczny charakter żądania (np. osoba, której dane dotyczą wielokrotnie, w krótkich odstępach czasu zwraca się do administratora o przekazanie informacji na podstawie przepisów rozdziału III RODO).

Jeżeli administrator uzna, że przedstawione żądania są nieuzasadnione lub nadmierne, w szczególności z uwagi na ich ustawiczny charakter, wówczas może on podjąć działania i pobrać rozsądną opłatę albo odmówić podjęcia działań w związku z żądaniem.

W przypadku decyzji administratora o nałożeniu opłaty trzeba pamiętać, że opłata ta musi być „rozsądna” tj. stanowić odzwierciedlenie istotnie poniesionych przez administratora kosztów. Wysokość opłaty powinna uwzględniać administracyjne koszty podejmowanych działań (udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań).

W odniesieniu do pytania „czy przedmiotowa opłata może być pobierana za czynności stricte administracyjne, tj. koszty pracy w postaci analizy żądania, przygotowania korespondencji" informujemy, że jak najbardziej możliwe jest objęcie tych czynności opłatą. Jak wskazuje w komentarzu Joanna Łuczak „w większości przypadków to właśnie ten element, a nie wartość zużytych materiałów, będzie stanowił najistotniejszy składnik opłaty."(Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz). Skorzystanie przez administratora z przysługującego mu prawa do pobrania opłaty nie ogranicza się jedynie do kwestii wydania kolejnej kopii danych i może dotyczyć również np. nieuzasadnionego żądania sprostowania, ograniczenia, czy usunięcia danych. W przypadku, gdy administrator już wcześniej dokonał ww. działań, a podmiot dalej występuje z takim samym żądaniem może wówczas pobrać opłatę, która uwzględni koszty udzielenia odpowiedzi na nieuzasadniony wniosek pomiotu danych.

Należy mieć na uwadze, że pobierane przez administratora opłaty nie mogą służyć ograniczeniu praw osób, których dane dotyczą, a jedynie mają zapobiegać nadużywaniu przez nie praw.

Data wytworzenia informacji: 06.09.2019 r.

Czy w przypadku dożywiania dzieci szkoła musi zawrzeć umowę powierzenia danych z OPS?

Gminny ośrodek pomocy społecznej na podstawie ustawy z dnia 12 marca 2004 r. o pomocy społecznej oraz uchwały nr 140 z dnia 15 października 2018 r. w sprawie ustanowienia wieloletniego rządowego programu „Posiłek w szkole i w domu" na lata 2019-2023 realizuje zadanie jakim jest dożywanie dzieci w szkołach. W związku z ww. zadaniem pomiędzy GOPS, a szkołą dochodzi do wymiany danych osobowych uczniów, którzy potrzebują takiej formy wsparcia. Moje wątpliwości jako inspektora ochrony danych dotyczą tego, czy w ww. przypadku będzie dochodziło do powierzenia danych osobowych uczniów między tymi podmiotami oraz konieczności zawarcia umowy, czy raczej będzie tu miało miejsce udostępnienie danych osobowych?

W ww. przypadku mamy do czynienia z udostępnieniem danych osobowych na podstawie przepisów prawa.

Kwestie realizacji zadania, jakim jest dożywianie dzieci w szkołach reguluje ustawa z dnia 12 marca 2004 r. o pomocy społecznej (Dz. U. z 2018 r., poz. 1508) oraz uchwała nr 140 z dnia 15 października 2018 r. w sprawie ustanowienia wieloletniego rządowego programu „Posiłek w szkole i w domu" na lata 2019-2023.

Zgodnie z art. 17 ust. 1 pkt 14 ustawy o pomocy społecznej do zadań własnych gminy o charakterze obowiązkowym należy m.in. dożywianie dzieci. Natomiast program „Posiłek w szkole i w domu" na lata 2019-2023 jest programem wspierania finansowego gmin w zakresie realizacji powyższego zadania. Koordynatorem programu na szczeblu gminy jest wójt, burmistrz, prezydent miasta, zaś sam program w gminie realizują samorządowe jednostki organizacyjne pomocy społecznej, przy udziale właściwych jednostek organizacyjnych gminy.

Na podstawie powyższego programu gmina realizuje pomoc w dożywianiu dzieci poprzez ośrodki pomocy społecznej, przy udziale właściwych jednostek organizacyjnych gminy tj. szkół oraz przedszkoli (pkt IV.1.1 programu). Stosownie, zaś do pkt III.1.2 ww. programu w szczególnie uzasadnionych przypadkach, gdy uczeń albo dziecko nie spełnia wymagań, o których mowa w programie, a wyraża chęć zjedzenia posiłku dyrektor szkoły lub przedszkola informuje ośrodek pomocy społecznej, właściwy ze względu na miejsce zamieszkania ucznia lub dziecka, o potrzebie udzielenia pomocy w formie posiłku.

Zgodnie z wyżej wskazanymi przepisami, aby możliwe było zrealizowanie celu, jakim jest dożywianie dzieci niezbędne jest przetwarzanie określonych danych osobowych przez ośrodek pomocy społecznej oraz szkołę.

Wobec powyższego ww. sytuacji nie zachodzi konieczność zawarcia między tymi podmiotami umowy powierzenia przetwarzania danych. Mamy tu bowiem do czynienia z udostępnieniem danych na podstawie przepisów prawa. Każdy z tych podmiotów jest odrębnym administratorem względem przetwarzanych przez siebie danych i przetwarza te dane w oparciu o obowiązujące przepisy prawa.

Data wytworzenia informacji: 06.09.2019 r.

Czy administrator musi kontrolować podmiot przetwarzający?

W związku z nadchodzącą kontrolą podmiotu przetwarzającego przez administratora, u którego sprawuję funkcję IOD, pojawiły się spory związane z interpretacją przepisu art. 28 ust. 3 lit. h RODO. Dlatego proszę o wskazówki, jak podmiot przetwarzający ma zrealizować i wykazywać spełnienie obowiązków wynikających z RODO przed administratorem. W szczególności, czy administrator realizując prawo kontroli podmiotu przetwarzającego wynikającego z umowy powierzenia danych może żądać od podmiotu przetwarzającego wglądu do wewnętrznej dokumentacji bezpieczeństwa.

Zgodnie z wyrażoną w art. 5 ust. 2 RODO zasadą rozliczalności, administrator jest odpowiedzialny za przestrzeganie przepisów prawa i musi być w stanie wykazać ich przestrzeganie. Co ważne, zasada ta ma zastosowanie zarówno do przetwarzania realizowanego samodzielnie przez administratora, jak i przetwarzania w jego imieniu przez podmiot przetwarzający. Obowiązkiem

administratora jest zadbanie o to, by korzystać z usług tylko takiego podmiotu przetwarzającego, który zapewnia wystarczające gwarancje – w szczególności jeśli chodzi o wiedzę fachową, wiarygodność i zasoby - wdrożenia środków technicznych i organizacyjnych, które odpowiadają wymogom RODO, w tym wymogom bezpieczeństwa przetwarzania i chronią prawa osób, których dotyczą (art. 28 ust. 1 RODO i motyw 81 RODO). Administrator musi więc szczególnie starannie zweryfikować, czy podmiot, któremu zamierza on powierzyć przetwarzanie danych osobowych, dysponuje koniecznymi w tym celu środkami i daje odpowiednie gwarancje przestrzegania obowiązujących przepisów prawa.

W związku z tym administrator powinien mieć możliwość sprawdzenia komu powierza dane osobowe oraz w jaki sposób będą one przetwarzane. Prawo dostępu do takich informacji oraz przeprowadzania audytów przysługuje administratorowi również w trakcie realizacji umowy powierzenia. W tym celu w art. 28 ust. 3 lit. h RODO na podmiot przetwarzający zostały nałożone obowiązki udostępniania administratorowi wszelkich informacji potwierdzających spełnienie wymogów RODO, a także umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczyniania się do nich.

Administrator jest bowiem zobowiązany do stałej kontroli, czy podmiot przetwarzający przetwarza dane zgodnie z prawem. Kontrole te mogą być przeprowadzane również doraźnie np. w przypadku wystąpienia naruszenia ochrony powierzonych danych osobowych. Zatem jakiekolwiek inne postanowienia umowy powierzenia, które w istocie ograniczały ww. prawa administratora należałoby uznać za niezgodne z RODO. Podobnie należy ocenić utrudnianie lub ograniczanie administratorowi możliwości przeprowadzania kontroli u podmiotu przetwarzającego lub ograniczanie jej zakresu.

Data wytworzenia informacji: 07.10.2019 r.

Czy komendant straży miejskiej musi posiadać odrębną politykę ochrony danych?

Mam pytanie dotyczące obowiązków dotyczących wewnętrznej polityki i innej dokumentacji wymaganej przez przepisy o ochronie danych osobowych. Czy komendant straży miejskiej funkcjonujący w strukturach urzędu gminy musi opracować taką odrębną wewnętrzną politykę?

Art. 24 RODO nakłada na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających zgodność przetwarzania z wymogami tego rozporządzenia. Zgodnie z ust. 2 tego artykułu – jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania – powyższe środki powinny obejmować wdrożenie przez administratora odpowiednich polityk ochrony danych. W przepisach rozporządzenia nie przewidziano przy tym

szczegółowych wymogów dotyczących zarówno zakresu merytorycznego, jak i formy dokumentacji ochrony danych. Biorąc pod uwagę jednak wynikającą z RODO zasadę rozliczalności, to od decyzji administratora zależy, w jaki sposób skonstruuje funkcjonujący u siebie system ochrony danych osobowych. Istotne jest aby przetwarzanie odbywało się zgodnie z RODO i aby administrator mógł to wykazać.

Wydaje się, że w przypadku podmiotów publicznych charakter, zakres, kontekst i cele prowadzonego przez nie przetwarzania wymagać będą zawsze wdrożenia odpowiednich polityk ochrony danych osobowych (trudno sobie wyobrazić aby podmiot publiczny mógł funkcjonować prawidłowo bez takich procedur). Warto zwrócić uwagę, że art. 24 ust. 2 RODO mówi o **politykach** ochrony danych osobowych, tak więc może to być więcej niż jeden dokument. Istotnym jest, aby swoim zakresem przedmiotowym i podmiotowym polityki te dotyczyły całości procesów przetwarzania prowadzonych u danego administratora i realnie wpływały na prawidłowość, bezpieczeństwo oraz przejrzystość przetwarzania.

W przypadku straży gminnej sytuacja jest o tyle specyficzna, że straż gminna jest jednostką organizacyjną gminy i może funkcjonować w strukturze urzędu gminy. Jednocześnie, ustawa z dnia 29 sierpnia 1997 r. o strażach gminnych (Dz. U. z 2018 r. poz. 928, z późn. zm.) w art. 10a ust. 2 wskazuje komendanta straży gminnej jako administratora danych osobowych przetwarzanych w celu, o którym mowa w art. 1 pkt 1 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 r. poz. 125).

Tym samym w części wykonywanych przez siebie zadań, straż gminna podlega pod inne niż RODO regulacje dot. ochrony danych osobowych. To powinna odzwierciedlać funkcjonująca w straży gminnej dokumentacja ochrony danych osobowych. Podkreślić również należy, że art. 31 ust. 4 ustawy z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości nakłada na komendanta straży gminnej jako administratora danych obowiązek uwzględniania w polityce danych osobowych sposobu dokumentowania niezbędnych środków technicznych i organizacyjnych zapewniających prawidłowość przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Tym samym, przetwarzanie tej kategorii danych ze względu na jej specyfikę oraz regulacje prawne, którym podlega będzie różnić się od danych osobowych przetwarzanych na podstawie RODO.

Nie istnieje *expressis verbis* obowiązek regulowania na poziomie urzędu gminy, w odrębnej polityce, zasad przetwarzania danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości przez straż gminną. Jednakże dokumentacja taka w wielu przypadkach (m.in. z uwagi na odrębnego administratora, jakim jest komendant straży gminnej) musi uwzględniać również wymogi określone przepisami ustawy z dnia 14 grudnia 2018 r.

Trzeba też pamiętać, że każdy z administratorów funkcjonujący w ramach jednej jednostki organizacyjnej ma również, m. in. obowiązek prowadzenia rejestru czynności przetwarzania i rejestru naruszeń ochrony danych. Wyżej wskazane rejestry mogą stanowić załącznik do wspólnego dokumentu polityki ochrony danych, przy czym zadbać trzeba o dookreślenie, którego administratora one dotyczą. Podobnie jest z załącznikami takimi jak , np. zarządzanie uprawnieniami dostępu, czy też procedura nadawania upoważnień. W odniesieniu do nich również warto wyraźnie wskazać, co oznacza używane w nich pojęcie administrator.

Podsumowując: administratorzy – wójt, burmistrz (prezydent miasta) oraz komendant straży – biorąc pod uwagę strukturę i realizowane przez nich zadania, jak również analizując dotychczasową zawartość dokumentu polityki, powinni dokonać oceny co do dalszego sposobu prowadzenia takiej dokumentacji. Każdy z administratorów – niezależnie od tego, czy będzie to wspólny dokument, czy odrębne polityki - musi być w stanie wykazać, że wywiązał się ze wszystkich ciążących na nim obowiązków wynikających z przepisów o ochronie danych osobowych. Im bardziej szczegółowo przedstawione są poszczególne procesy przetwarzania danych i związane z nimi procedury bezpieczeństwa, tym taki dokument będzie bardziej wartościowy i przydatny w procesie przetwarzania danych u danego administratora.

W sytuacji gdy nie będzie możliwości objęcia jednym dokumentem procesów i procedur funkcjonujących u różnych administratorów, stworzenie odrębnego dokumentu może ułatwić przestrzeganie tym administratorom przestrzeganie zasad ochrony danych i obowiązków określonych w różnych przepisach o ochronie danych osobowych.

Data wytworzenia informacji: 07.10.2019 r.

Czy biegli rewidenci mają status administratora w związku ze świadczeniem swoich usług?

Czy, a jeżeli tak, to z jakich powodów należy przyjąć, że biegły rewident (firma audytorska) ma status odrębnego administratora w związku ze świadczeniem usług na podstawie ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym?

Ocena roli firm audytorskich oraz biegłych rewidentów w prowadzonych przez nie operacjach przetwarzania danych powinna opierać się na przepisach prawa, w tym ustawy z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym (Dz. U. z 2019 r. poz. 1421, z późn. zm.), rozporządzeniu Parlamentu Europejskiego i Rady (UE) 537/2014 z dnia 16 kwietnia 2014 r. w sprawie szczegółowych wymogów dotyczących ustawowych badań sprawozdań finansowych jednostek interesu publicznego, uchylającym decyzję Komisji 2005/909/WE (Dz. Urz. UE L 158 z 27.05.2014, str. 77) oraz rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych

i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. Urz. UE L 119 z 04.05.2016, str1, z późn. zm.).

Kluczowe dla określenia, czy podmiot w danych operacjach przetwarzania występuje w roli administratora czy podmiotu przetwarzającego jest ustalenie czy realizuje własne cele w sposób przez siebie określony, czy też przetwarza dane na zlecenie administratora realizując „jego cel". Firmy audytorskie oraz biegli rewidenci wykonując swoje zadania nie są związane poleceniami klienta oraz muszą działać zgodnie z obowiązującymi je przepisami. Ustawa z dnia 11 maja 2017 r. o biegłych rewidentach, firmach audytorskich oraz nadzorze publicznym wskazuje, że istotą tego zawodu jest niezależność i obiektywizm w przeprowadzaniu badania. Biegły rewident jest obowiązany w szczególności: postępować zgodnie ze złożonym ślubowaniem; przestrzegać krajowych standardów wykonywania zawodu, wymogów niezależności oraz zasad etyki zawodowej. Dodatkowo art. 2b tej ustawy wskazuje wprost na sposoby zabezpieczenia danych przetwarzanych w ramach działalności firm audytorskich oraz biegłych rewidentów. Tym samym, charakter relacji pomiędzy firmami audytorskimi oraz biegłymi rewidentami a ich klientami wskazuje na to, że występują one w roli samodzielnych administratorów.

Data wytworzenia informacji: 07.11.2019 r.

Czy rzecznik praw konsumentów jest administratorem danych osobowych?

Czy rzecznik praw konsumentów jest administratorem przetwarzanych przez siebie danych osobowych czy takim administratorem jest starosta? Moja wątpliwość wynika z faktu, że ustawa o samorządzie powiatowym w art. 4 ust. 1 pkt 18 wskazuje, że powiat wykonuje określone ustawami zadania publiczne o charakterze ponadgminnym w zakresie ochrony praw konsumenta, z kolei art. 42 ustawy o ochronie konkurencji i konsumentów szczegółowo określa jakie zadania ma realizować w zakresie ochrony praw konsumenta rzecznik.

Administratorem w rozumieniu art. 4 pkt 7 RODO jest osoba fizyczna, prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W przypadku podmiotów z sektora publicznego cele i środki przetwarzania przez te podmioty danych osobowych będą co do zasady wynikały z przepisów prawa, które określają zadania i kompetencje tych podmiotów.

Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych.

Z art. 40 ust. 4 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369 z późn. zm.), zwanej dalej u.o.k.i.k, wynika, że rzecznika konsumentów wyodrębnia się organizacyjnie w strukturze starostwa powiatowego (urzędu miasta), a w powiatach powyżej 100 tys. mieszkańców i w miastach na prawach powiatu rzecznik konsumentów może wykonywać swoje zadania przy pomocy wyodrębnionego biura.

Powyższa ustawa wskazuje na liczne zadania rzecznika praw konsumenta, dla przykładu można wymienić: zapewnienie bezpłatnego poradnictwa konsumenckiego i informacji prawnej w zakresie ochrony interesów konsumentów; występowanie do przedsiębiorców w sprawach ochrony praw i interesów konsumentów; współdziałanie z właściwymi miejscowo delegaturami Urzędu, organami Inspekcji Handlowej oraz organizacjami konsumenckimi (art. 42. ust. 1 u.o.k.i.k).

Powiatowy (miejski) rzecznik konsumentów może również wytaczać powództwa na rzecz konsumentów oraz wstępować, za ich zgodą, do toczącego się postępowania w sprawach o ochronę interesów konsumentów oraz być oskarżycielem publicznym w rozumieniu przepisów ustawy z dnia 24 sierpnia 2001 r. - Kodeks postępowania w sprawach o wykroczenia (Dz. U. z 2018 r. poz. 475, ze zm.) w sprawach o wykroczenia na szkodę konsumentów (art. 42 ust. 2 u.o.k.i.k i art. 42 ust. 3 u.o.k.i.k.)

Powyższe przepisy określające zadania rzecznika - dla których realizacji konieczne jest przetwarzanie danych osobowych - pozwalają przyjąć, że rzecznik jest administratorem przetwarzanych w tych celach danych, niezależnie od tego, czy jest umiejscowiony w strukturze powiatu, czy nie.

Data wytworzenia informacji: 07.11.2019 r.

Czy administrator powinien udzielać upoważnień do przetwarzania danych?

Czy na gruncie RODO sytuacja się zmieniła i administrator nie powinien udzielać upoważnień do przetwarzania danych osobowych?

Art. 29 RODO wskazuje, że podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Zgodnie natomiast z art. 32 RODO administrator i podmiot przetwarzający uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, wdrażają odpowiednie środki techniczne

i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający charakterowi prowadzonego przetwarzania i związanego z nim ryzyka. Ust. 4 tego artykułu stanowi, że administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

Z przytoczonych norm wynika, że dane osobowe mogą być przetwarzane wyłącznie na polecenie administratora przez osoby działające z upoważnienia administratora lub podmiotu przetwarzającego. Wprawdzie terminu „*upoważnienie*" w języku polskim ma ugruntowane znaczenie – zgodnie ze Słownikiem Języka Polskiego PWN i oznacza: „pełnomocnictwo upoważniające do wykonania czynności urzędowych". Niemniej – w celu przybliżenia intencji prawodawcy unijnego – należy raczej odwołać się do anglojęzycznej wersji przepisów RODO. Tam użyte jest sformułowanie: „any person acting under the authority of the controller or of the procesor". Zwrot „acting under the authority" można przetłumaczyć jako „*działająca z upoważnienia*", jednak właściwsze wydaje się przyjęcie znaczenia: „*działająca pod władztwem lub z mocy"* administratora.

Dlatego przyjąć należy, że chodzi tu o zapewnienie, aby administrator miał kontrolę (władztwo) nad tym kto, w jakim zakresie ma dostęp do danych osobowych oraz na jakich zasadach i w jaki sposób je przetwarza. Przyjmowane przez administratora i podmiot przetwarzający środki (działania) powinny służyć m.in. zapobieganiu nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych oraz zapewnieniu, że osoby uprawnione do korzystania z systemu zautomatyzowanego przetwarzania będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem. Dzięki tym środkom osoby, które zostały dopuszczone do przetwarzania danych zostają poinformowane, jaki jest zakres ich uprawnień co do przetwarzania danych osobowych.

Dlatego środki takie powinny dotyczyć nie tylko osób na stałe zatrudnionych u administratora danych, ale także osób, którym administrator zlecił określone prace i które z tego powodu mają mieć dostęp do danych osobowych, np. praktykanci, stażyści. Wyjątkiem jest sytuacja, w której określone zadania na rzecz i zlecenie administratora danych wykonuje osoba, która jest podmiotem przetwarzającym lub pracownikiem takiego podmiotu.

Wydawanie upoważnień może być jednym z takich środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania. Taki cel miały również upoważnienia do przetwarzania danych osobowych wydawane przed 25 maja 2018 r. na gruncie podstawie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Wielu administratorów - po wejściu do stosowania RODO - nadal korzysta z takiego rozwiązania

i nadaje upoważnienia do przetwarzania danych osobowych. Na podstawie wydanych przez administratora danych upoważnień, stosuje się następnie mechanizmy kontroli dostępu do danych w systemie informatycznym służącym do przetwarzania danych osobowych (nadaje określone uprawnienia).

Obecnie w polskim porządku prawnym obowiązek nadawania upoważnień do przetwarzania danych osobowych wynika też z wielu przepisów sektorowych wprowadzonych ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. poz. 730). Powyższy obowiązek został wprowadzony np. w:

- art. 22(1b) par. 3 ustawy z 26 czerwca 1974 r. – Kodeks pracy (j.t. Dz.U. z 2020 r. poz. 1320, ost. zm. Dz.U. z 2021 r. poz. 1162),
- art. 5a ust. 4 ustawy z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne (t.j. Dz. U. z 2019 r. poz. 725 z późn. zm.),
- art. 2 ust. 7 ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska (t.j. Dz. U. z 2019 r. poz. 1355 z późn. zm.),
- art. 2b ust. 6 ustawy z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych (t.j. Dz. U. z 2019 r. poz. 1172 z późn. zm.),
- art. 8a ust. 3 ustawy z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (t.j. Dz. U. z 2018 r. poz. 1945 z późn. zm.).

W powyższych przypadkach do przetwarzania danych osobowych dopuszczone mogą być wyłącznie osoby posiadające pisemne upoważnienie wydane przez administratora.

Data wytworzenia informacji: 29.11.2019 r.

Czy administrator powinien nadawać upoważnienia np. sędziom?

Czy administrator powinien nadawać upoważnienia do przetwarzania danych osobowych określonym grupom zawodowym, których uprawnienia do przetwarzania danych wynikają z odrębnych przepisów np. sędziom? Zadania poszczególnych grup zawodowych uregulowane są w przepisach prawa, z których wynikają obowiązki oraz uprawnienia osób wykonujących swoje obowiązki. W sądzie, czyli instytucji, w której sprawuję funkcję inspektora ochrony danych taką grupą zawodową, która spełnia powyższe kryteria będą sędziowie. Stąd moje wątpliwości, czy administrator powinien nadawać sędziom upoważnienia pomimo tego, że ich

uprawnienia do przetwarzania wynikają z ustawy? Czy takie upoważnienia powinny być wydawane również innym osobom, którym zleca się wydawanie opinii czy wykonanie innych czynności (np. ławnikom)?

W przypadku nadawania upoważnień do przetwarzania danych osobowych osobom , których uprawnienia do przetwarzania danych osobowych wynikają z odrębnych przepisów, należy mieć na względzie cel, w jakim takie upoważnienia się nadaje. Wydawanie upoważnień może być bowiem jednym ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania zgodnie z art. 29 i art. 32 ust. 4 RODO i dlatego należy go odróżnić od uprawnienia do dostępu do danych osobowych przyznanego określonym funkcjom czy zawodom przez przepisy prawa w związku z wykonywanymi przez nich obowiązkami lub zadaniami.

Jeśli administrator decyduje się na zastosowanie środka organizacyjnego, jakim jest nadawanie upoważnień, wówczas również wobec np. audytorów wewnętrznych, sędziów czy ławników może być podjęty taki środek, niezależnie od tego, że uprawnienie tych osób do dostępu do wszelkich danych osobowych niezbędnych dla potrzeb prowadzonych postępowań lub czynności gwarantują im właściwe ustawy.

Wskazany w art. 29 oraz art. 32 ust. 4 RODO wyjątek od związania poleceniem administratora (wynikający z przepisów prawa Unii lub prawa państwa członkowskiego) dotyczy przypadków zobowiązania do przetwarzania płynącego z przepisów unijnych lub krajowych, nie zaś upoważnienia z nich wynikającego, np. udzielenia określonej informacji na żądanie sądu w ramach prowadzonego postępowania sądowego czy organom nadzoru w ramach postępowań kontrolnych.

Należy dodać, że administrator nie musi stosować w tym zakresie jednakowej metody wobec wszystkich grup pracowników, musi jednak być w stanie wykazać, że każda osoba, która przetwarza dane osobowe, działa na jego polecenie.

Data wytworzenia informacji: 29.11.2019 r.

Czy IOD może nadawać upoważnienia?

Czy administrator danych osobowych może udzielić IOD upoważnienia do nadawania upoważnień do przetwarzania danych osobowych?

Jeżeli administrator, w wykonaniu obowiązków określonych w art. 29 i art. 32 ust. 1 i 4 RODO, decyduje się na skorzystanie ze środka, jakim jest nadawanie upoważnień do przetwarzania danych osobowych, to może upoważnić inną osobę do nadawania upoważnień do przetwarzania danych w jego imieniu, ale osobą tą nie powinien być inspektor ochrony danych.

3 ZADANIA IOD

Przede wszystkim obowiązki określone w art. 29 i art. 32 ust. 1 i 4 RODO są obowiązkami administratora. Jest on zobowiązany do zapewnienia, aby dostęp do danych miały tylko osoby przez niego określone, działające na zasadach i w sposób wskazany przez administratora. Dlatego wydawanie upoważnień osobiście przez osobę kierującą lub zarządzającą podmiotem będącym administratorem może istotnie przyczynić się do prawidłowego zapewnienia takiej kontroli. Takie osoby powinny bowiem najlepiej znać organizację pracy w swojej jednostce i dzięki temu w sposób najwłaściwszy określić, komu oraz w jakim zakresie powinno być nadane stosowne upoważnienie do przetwarzania danych.

Zatem dla zapewnienia właściwego systemu ochrony danych w jednostce najkorzystniejszym rozwiązaniem byłoby nadawanie upoważnienia do przetwarzania danych przez samego administratora (podmiot przetwarzający) lub - w zależności od wielkości podmiotu i jego struktury - przez np. kierownika działu kadr lub kierowników innych komórek organizacyjnych. Osoby te bowiem mogą najbardziej precyzyjnie określać, komu oraz w jakim zakresie upoważnienie powinno zostać nadane, i na bieżąco je aktualizować.

Natomiast rola inspektora ochrony danych koncentruje się na monitorowaniu przestrzegania przepisów o ochronie danych osobowych i wewnętrznych polityk oraz prawidłowego wykonywania wynikających z nich obowiązków, a także doradzaniu i podnoszeniu świadomości w zakresie tych obowiązków. Dlatego IOD nie powinien być osobą, która sama realizuje obowiązki określone w art. 29 i art. 32 ust. 1 i 4 RODO. Powodowałoby to konflikt interesów, którego występowania zakazuje w odniesieniu do inspektorów art. 38 ust. 6. RODO.

Rola IOD może natomiast polegać na doradzaniu czy konsultowaniu rozwiązań, jakie administrator (lub podmiot przetwarzający) zamierza przyjąć w zakresie realizacji obowiązków z art. 29 i 32 ust. 1 i 4 RODO, w tym np. procedur nadawania upoważnień czy treści upoważnień.

Rolą IOD jest zatem wspieranie 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, organ nadzorczy udzielił upomnienia (sygn. sprawy ZWAD.405.31.331.2019).

W wydanej w tej sprawie decyzji wskazano, w szczególności że: „(…) 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) RODO, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów (…). 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 RODO, ale godzi w same fundamenty instytucji IOD, opartej w pierwszym rzędzie na niezależności jego funkcjonowania."

I choć praktyka administratora w powyższym zakresie została zmieniona, to jednak ze względu na to, że trwała ponad półtora roku, organ nadzorczy 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 RODO sprawia, iż wagę tego naruszenia uznać należy za znaczną".

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.

Data wytworzenia informacji: 29.11.2019 r.

Czy elektroniczna postać upoważnienia spełnia wymogi „pisemnego upoważnienia"?

Czy elektroniczną postać upoważnienia do przetwarzania danych osobowych (np. kreowanego i podpisywanego w dedykowanym temu procesowi systemie teleinformatycznym) można interpretować jako formę pisemną, a tym samym spełniającą dyspozycje przepisów prawa, odnoszących się do konieczności wydawania „pisemnych upoważnień do przetwarzania danych osobowych", wynikających z ustawy z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania RODO?

Nadawanie upoważnień w postaci elektronicznej należy uznać za wykonanie obowiązku nadania upoważnień w formie pisemnej. W świetle zasady rozliczalności jakakolwiek postać, w tym elektroniczna, która pozwala na udokumentowanie spełnienia obowiązków celem wykazania przestrzegania przepisów, a w tym przypadku wykonania obowiązku wynikającego z art. 29 RODO należy uznać za prawidłową.

Za przyjęciem takiego stanowiska przemawia również podejście co do formy pisemnej wskazanej w art. 30 ust. 3 RODO. Zgodnie z tym przepisem, rejestr czynności przetwarzania i rejestr kategorii czynności przetwarzania, mają formę pisemną, w tym formę elektroniczną. Jak wskazujemy w poradniku dotyczącym tego obowiązku (Wskazówki i wyjaśnienia dotyczące obowiązku rejestrowania czynności i kategorii czynności przetwarzania określonego w art. 30 ust. 1 i 2 RODO -

str. 13) rejestry powinny być prowadzone w formie pisemnej (art. 30 ust. 3), a zatem mogą być prowadzone zarówno w postaci papierowej, jak i elektronicznej.

Data wytworzenia informacji: 29.11.2019 r.

Jak należy wywiązać się z obowiązku informacyjnego przy zastosowaniu fotopułapek?

Gmina w ramach walki z dzikimi wysypiskami śmieci planuje zakup kilku tzw. foto-pułapek z czujnikami ruchu, które uaktywnią się w momencie zarejestrowania ruchu i nagrają np. osoby które nielegalnie pozbywają się odpadów wysypując je np. na polu, na nieużytkach gminnych czy innych ustronnych miejscach. Nagrania takie będą przeglądane przez upoważnione osoby - pracowników urzędu. Jeżeli zostanie zarejestrowany fakt nielegalnego pozbywania się odpadów nagranie zostanie wykorzystane jako dowód np. w postępowaniu mandatowym (stanowi to bowiem wykroczenie), pozostałe nagrania będą kasowane np. co 7 dni.

Jako inspektor najwięcej wątpliwości mam co do sposobu wypełnienia obowiązku informacyjnego. Rozważamy m.in. opublikowanie informacji o umieszczaniu na obszarze gminy mobilnych foto-pułapek wraz ze stosowną klauzulą informacyjną na stronie BIP oraz własnej stronie internetowej gminy, upublicznienie w/w informacji poprzez media lokalne (internet, radio, prasa). Dodatkowo osoby nagrane, wobec których wszczęto by postępowanie np. mandatowe, otrzymywałyby klauzulę informacyjną wraz z wezwaniem/informacją o wszczęciu postępowania. Informacje o foto-pułapkach nie byłyby natomiast z umieszczane bezpośrednio na obszarach, na których takie mobilne foto-pułapki byłyby instalowane, ponieważ w takim przypadku byłyby one nieskuteczne dla osiągnięcia celu ich stosowania, tzn. zniechęcenia mieszkańców do nielegalnego pozbywania się odpadów poprzez doprowadzenie do przekonania o nieuchronności kary u osób, które w sposób nielegalny pozbywają się odpadów. W przypadku konieczności umieszczania informacji wraz z foto-pułapkami, nielegalne wysypiska powstawałyby dalej - w miejscach w których aktualnie foto-pułapki nie byłyby zamontowane.

Przepisy RODO określają ogólne zasady przetwarzania i ochrony danych osobowych, zaś skonkretyzowanie tychże zasad ma miejsce w szczególnych wobec tej regulacji przepisach prawa. Kwestie stosowania monitoringu wizyjnego przez jednostki samorządu terytorialnego są regulowane następującymi przepisami: art. 9a ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, art. 4b ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym, art. 60a ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa. Każdy z ww. artykułów zawiera identycznie brzmiący ustęp, zgodnie z którym nieruchomości i obiekty budowlane objęte monitoringiem

oznacza się w sposób widoczny i czytelny informacją o monitoringu, w szczególności za pomocą odpowiednich znaków.

W związku z powyższym trzeba uznać, iż stosowanie przez jednostki samorządu terytorialnego gminy i powiatu monitoringu wizyjnego w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej, a w przypadku jednostek samorządu województwa w celu ochrony mienia, wymaga zawsze spełnienia obowiązku informacyjnego poprzez oznaczenie nieruchomości i obiektów budowlanych w sposób widoczny i czytelny informacjami o monitoringu, w szczególności za pomocą odpowiednich znaków. Zwolnienie z tego obowiązku może nastąpić jedynie na mocy osobnych postanowień rangi ustawowej, ograniczających konieczność wypełniania obowiązku informacyjnego w przypadku przetwarzania danych osobowych za pomocą monitoringu wizyjnego w określonym celu.

Zgodnie natomiast z art. 3 ust.1 ustawy z dnia 13 września 1996r. o utrzymaniu czystości i porządku w gminach, utrzymanie czystości i porządku w gminach należy do obowiązkowych zadań własnych gminy. Na terenie gminy, jak wskazuje art. 1 ustawy z dnia 29 sierpnia 1997 r. o strażach gminnych, działają straże gminne, które tworzone są do ochrony porządku publicznego. Ochrona porządku w miejscach publicznych zgodnie z art. 11 ust. 1 pkt 1 ww. ustawy należy do podstawowych zadań straży gminnej. Z kolei zgodnie z art. 10 ustawy o strażach gminnych straż wykonuje zadania w zakresie ochrony porządku publicznego, wynikające z ustaw i aktów prawa miejscowego.

Podkreślić należy, że pozostawienie odpadów w niedozwolonych miejscach jest ścigane i podlega karze grzywny. Stosownie bowiem do art. 154 ustawy z dnia 20 maja 1971r. Kodeks wykroczeń, kto wyrzuca na nienależący do niego grunt polny kamienie, śmieci, padlinę lub inne nieczystości (…) podlega karze grzywny do 1000 złotych.

Ponadto na podstawie art. 11 ust. 2 ustawy o strażach gminnych, w związku z realizowanymi zadaniami, straży przysługuje prawo do obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych w przypadku, gdy czynności te są niezbędne do wykonywania zadań oraz w celu m.in. utrwalania dowodów popełnienia przestępstwa lub wykroczenia czy przeciwdziałania przypadkom naruszania spokoju i porządku w miejscach publicznych.

Co więcej straż w celu realizacji ustawowych zadań może przetwarzać dane osobowe, z wyłączeniem danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, bez wiedzy i zgody osoby, której dane te dotyczą, uzyskane w wyniku wykonywania czynności

podejmowanych w postępowaniu w sprawach o wykroczenia(art. 10a ust. 1 ustawy o strażach gminnych).

Zgodnie z powyższym prawo do stosowania monitoringu posiadają straże gminne, które w ramach swoich uprawnień, wynikających z przepisów prawa, nie są zobowiązane do spełnienia obowiązku informacyjnego (przysługuje im bowiem uprawnienie do obserwowania i rejestrowania bez wiedzy i zgody osoby, której dane te dotyczą). Natomiast gmina - zgodnie z wyżej przytoczonymi zasadami - musiałaby spełnić obowiązek informacyjny w miejscu umieszczenia fotopułapki.

Data wytworzenia informacji: 02.03.2020 r.

Czy szkoła może udostępnić dane na temat liczby uczniów i innych mieszkających pod danym adresem?

Ostatnio my, inspektorzy ochrony danych w szkołach i placówkach oświatowych, zastanawiamy się, czy zasadne są kierowane do tych podmiotów żądania udostępnienia organowi prowadzącemu informacji dotyczących liczby uczniów oraz ich rodziców lub opiekunów prawnych zamieszkałych pod danym adresem, ze wskazaniem nazwy ulicy, numeru budynku i mieszkania, w celu weryfikacji liczby osób zamieszkujących na danej nieruchomości, wytwarzających odpady komunalne.

W przedstawionej sprawie należy kierować się przepisami ustawy o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2019 r. poz. 2010 z późn. zm). Przepisy te określają, jakie informacje i z jakich źródeł mogą być pozyskiwane w związku z realizacją zadań gminy w zakresie utrzymania czystości i porządku, w tym zapewnienia odbierania odpadów komunalnych od właścicieli nieruchomości i zagospodarowania tych odpadów. Wszelkie działania gminy powinny zatem korespondować z tymi przepisami.

Zgodnie z art. 6c ust. 1 ustawy o utrzymaniu czystości i porządku w gminach, gminy zobowiązane są do zorganizowania odbierania odpadów komunalnych od właścicieli nieruchomości, w których zamieszkują mieszkańcy. Przepis art. 6m ust. 1 tej ustawy obliguje właścicieli nieruchomości do złożenia do wójta, burmistrza lub prezydenta miasta deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi w określonym terminie.

Jednocześnie rada gminy może w drodze uchwały (jako aktu prawa miejscowego w rozumieniu art. 87 ust. 1 ustawy z dnia 2 kwietnia 1997 r. – Konstytucja Rzeczypospolitej Polskiej) nakładać na mieszkańców – właścicieli nieruchomości – pewne obowiązki w zakresie konieczności przedkładania informacji służących do ustalenia wysokości opłat za gospodarowanie odpadami komunalnymi, z uwzględnieniem art. 6m ust. 1a i 1b ustawy o utrzymaniu czystości i porządku

w gminach. Zatem art. 6m ust. 1a ustawy o utrzymaniu czystości i porządku w gminach wskazuje, że deklaracja zawiera dane niezbędne do określenia wysokości opłaty za gospodarowanie odpadami komunalnymi oraz wysokość opłaty za gospodarowanie odpadami komunalnymi. Stosownie zaś do art. 6m ust. 1b ustawy o utrzymaniu czystości i porządku w gminach rada gminy określając wzór deklaracji może wymagać podania następujących danych:

1. imię i nazwisko lub nazwę właściciela nieruchomości oraz adres miejsca zamieszkania lub siedziby,
2. adres nieruchomości,
3. dane stanowiące podstawę zwolnienia z opłaty za gospodarowanie odpadami komunalnymi,
4. numer telefonu właściciela nieruchomości,
5. adres poczty elektronicznej właściciela nieruchomości,
6. inne informacje niezbędne do wystawienia tytułu wykonawczego,
7. informacje dotyczące posiadania kompostownika przydomowego i kompostowania w nim bioodpadów stanowiących odpady komunalne.

Z powyższego nie wynika możliwość pozyskiwania przez gminy danych osobowych osób zamieszkujących daną nieruchomość. Przepisy te nie dają podstawy pozyskiwania danych w zakresie szerszym niż wyżej określony w przepisie czy też pozyskiwania danych osobowych z innych źródeł.

Warto wspomnieć, iż nawet przyjmowane przez rady gminy w uchwale rozwiązania nie mogą nakładać praw i obowiązków nie wynikających z ustawy, zarówno dla organów gminy jak i mieszkańców gminy – właścicieli nieruchomości. Ukształtowanie przedmiotowych obowiązków w zakresie przetwarzania danych osobowych w sposób dowolny, wbrew pierwotnym uprawnieniom ustawowym, będzie oznaczać naruszenie zasad wynikających z rozporządzenia 2016/679 (legalizmu, proporcjonalności i celowości).

Na marginesie należy nadmienić, że w ostatnim czasie Prezes UODO wystąpił do Ministra Spraw Wewnętrznych i Administracji, wskazując na konieczność respektowania w treści uchwał organów jednostek samorządu terytorialnego, określających wzory deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi, przepisów o ochronie danych osobowych.

Data wytworzenia informacji: 05.03.2020 r.

Czy w przypadku kierowania studenta na praktyki zawodowe konieczne jest powierzenie?

Zwracam się z pytaniem dotyczącym konieczności zawarcia umowy powierzenia przetwarzania danych osobowych w sytuacji, gdy uczelnia wysyła studentów na praktyki zawodowe. W takich przypadkach zawierana jest umowa dotycząca praktyk pomiędzy uczelnią a zakładem pracy. Czy w związku z tym powinna być również zawarta umowa powierzenia przetwarzania danych osobowych lub powinny zostać zastosowane zapisy dotyczące powierzenia w umowie głównej?

Odpowiadając sobie na tego rodzaju pytania należy mieć na uwadze, w jaki sposób przepisy o ochronie danych osobowych określają rolę administratora i podmiotu przetwarzającego. Zgodnie z art. 4 pkt 7 RODO administratorem danych osobowych jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który **samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych**. Podmiotem przetwarzającym jest zaś osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który **przetwarza dane osobowe w imieniu administratora** – art. 4 pkt 8 RODO.

Zatem w myśl przepisów RODO konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator danych osobowych zleca innemu podmiotowi (podmiotowi przetwarzającemu) działanie w swoim imieniu i w celach, które określa administrator. Istotne jest podkreślenie, że podmiot przetwarzający przetwarza dane w imieniu administratora, a nie w imieniu własnym i dla realizacji swoich celów.

Organizację praktyk studenckich reguluje ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce. Zgodnie z art. 67 ust. 5 tej ustawy studia są prowadzone na podstawie programu studiów, który może przewidywać odbycie przez studenta praktyk zawodowych (art. 67 ust. 5). Ponadto z przepisów tych wynika, że realizacja praktyk stanowi jeden z obowiązków studenta (art. 107 ust. 2 pkt 2). Zatem skierowanie studenta przez uczelnię do odbycia praktyk wynika z programu studiów, a praktyki te mają na celu uzyskanie przez studenta efektów uczenia się kształtujących umiejętności praktyczne, o których mowa w art. 64 ust. 2 pkt 1 powyższej ustawy.

Z drugiej strony - w przypadku zawarcia przez uczelnię umowy (porozumienia) w sprawie realizacji praktyki studenckiej, podmiot przyjmujący studenta na praktykę realizuje w zakresie zawartej umowy swoje własne zadania, wynikające z postanowień tej umowy oraz z przepisów szczególnych (np. zawartych w Kodeksie pracy przepisów dotyczących bhp), a także z regulacji wewnętrznych (np. ewidencja wejść i wyjść, ewidencja czasu odbywania praktyki, nadawanie upoważnień do przetwarzania danych osobowych, o ile oczywiście w ramach praktyk student będzie miał do takich danych dostęp). Tym samym podmiot, w którym student odbywa praktykę staje się administratorem jego danych osobowych w zakresie danych udostępnionych mu przez uczelnię oraz danych gromadzonych przez ten podmiot w celu realizacji umowy o praktykę. Każda ze stron tej umowy przetwarza dane studenta dla realizacji swoich celów oraz obowiązków i w tym zakresie jest administratorem tych danych.

Warto nadmienić, że w przypadku uczelni medycznych - oprócz wyżej podanych wskazówek, należy mieć na uwadze regulacje zawarte w ustawie o działalności leczniczej, zwłaszcza w dziale II, rozdziale 4 tej ustawy zatytułowanym: „Regulacje szczególne dotyczące działalności leczniczej obejmującej realizację zadań dydaktycznych i badawczych w powiązaniu z udzielaniem świadczeń zdrowotnych i promocją zdrowia".

Data wytworzenia informacji: 05.03.2020 r.

Czy w przypadku kierowania ucznia na praktyki zawodowe konieczne jest powierzenie?

Szkoła, w której pełnię funkcję inspektora, zobowiązana jest do organizacji praktycznej nauki zawodu swoich uczniów. Moja wątpliwość dotyczy tego, czy w takim przypadku mamy do czynienia z powierzeniem przetwarzania, czy z udostępnieniem danych uczniów. Czy szkoła musi zawierać umowy powierzenia z podmiotami, z którymi zawarła umowę dotyczącą praktycznej nauki zawodu?

Zgodnie z przepisami RODO konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator danych osobowych zleca przetwarzanie danych innemu podmiotowi (podmiotowi przetwarzającemu). Wówczas podmiot przetwarzający przetwarza dane w imieniu administratora, a nie w imieniu własnym (tj. nie staje się administratorem danych). Podmiot przetwarzający nie decyduje bowiem o celach i sposobach przetwarzania, gdyż przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO).

Kwestie związane z praktyczną nauką zawodu uregulowane zostały w ustawie Prawo oświatowe oraz w rozporządzeniach wykonawczych. Zgodnie z przepisami rozporządzenia Ministra Edukacji Narodowej z dnia 22 lutego 2019 r. w sprawie praktycznej nauki zawodu, uczniowie i słuchacze (dalej: uczniowie) publicznych szkół ponadgimnazjalnych prowadzących kształcenie zawodowe uczestniczą w zajęciach praktycznych bądź praktykach zawodowych. Mogą być one organizowane na podstawie umowy zawartej przez szkołę z pracodawcą w przypadku ucznia lub na podstawie umowy zawartej z pracodawcą przez młodocianego pracownika.

W przypadku organizacji praktycznej nauki zawodu przez szkołę przekazuje ona na mocy umowy dane osobowe uczniów podmiotowi, z którym zawarła umowę o realizacje takiej nauki. Podmiot ten z chwilą otrzymania danych ucznia staje się ich administratorem. Zwrócić bowiem należy uwagę, że zarówno szkoła, jak i pracodawca mają określone w ww. rozporządzeniu role i zadania związane z organizacją praktycznej nauki zawodu. Pracodawca zapewnia możliwość faktycznego odbywania praktyk, zapoznając praktykanta m.in. z organizacją pracy, regulaminem oraz

dyscypliną pracy. Może też upoważnić go do przetwarzania danych osobowych, jeżeli będzie to niezbędne w związku z odbywaniem praktyki.

Oznacza to, że zarówno szkoła, jak i podmiot przyjmujący uczniów na praktyczną naukę zawodu występują w roli odrębnych administratorów. Wobec powyższego – skoro nie występuje sytuacja określona w art. 28 RODO (tj. przetwarzanie danych w imieniu administratora) – nie ma obowiązku zawierania umowy powierzenia przetwarzania danych osobowych. W tej sytuacji mamy do czynienia z udostępnieniem danych osobowych niebędącym powierzeniem – podmiot, który otrzymuje dane osobowe, przetwarza je w celach, które samodzielnie kształtuje – nie w celach własnych udostępniającego.

Data wytworzenia informacji: 24.03.2020 r.

Jaka jest podstawa prawna przetwarzania danych osób upoważnionych do odbioru dziecka?

Czy jest jakieś stanowisko UODO w sprawie upoważnień do odbioru dziecka z przedszkola lub świetlicy? Czy należy tu przyjąć przesłankę z art. 6 ust. 1 lit. c RODO w związku z przepisami Prawa oświatowego czy też może przesłankę z art. 6 ust. 1 lit. e? Co z placówkami niepublicznymi – jaka przesłanka powinna być przyjmowana w ich przypadku?

Rozstrzygając wątpliwości, jaka przesłanka jest podstawą przetwarzania danych zawartych w upoważnieniu do odbioru dziecka z przedszkola lub szkoły, administrator powinien w pierwszej kolejności dokonać analizy przepisów ustawy Prawo oświatowe, które wskazują na zakres zadań i obowiązków przedszkola (szkoły) w zakresie zapewnienia odpowiedniego bezpieczeństwa dziecka.

Przepisy ustawy Prawo oświatowe wskazują, że statut przedszkola powinien zawierać m.in. szczegółowe zasady przyprowadzania i odbierania dzieci z przedszkola przez rodziców lub upoważnioną przez nich osobę zapewniającą dziecku pełne bezpieczeństwo (art. 102 ust. 1 pkt 6). A zatem można zasadnie przyjąć, że w przypadku przedszkola zastosowanie może mieć przesłanka wskazana w art. 6 ust. 1 lit. e RODO łącznie z przepisem krajowym, jakim jest art. 102 ust. 1 pkt 6 Prawa oświatowego. Natomiast w przypadku przedszkoli niepublicznych art. 6 ust. 1 lit. e RODO i art. 102 ust. 1 pkt 6 w zw. z art. 172 ust. 3 Prawa oświatowego.

W przypadku szkół publicznych należy mieć na uwadze brzmienie art. 68 ust. 1 pkt 6 ustawy Prawo oświatowe, zgodnie z którym dyrektor szkoły wykonuje zadania związane z zapewnieniem bezpieczeństwa uczniom i nauczycielom w czasie zajęć organizowanych przez szkołę lub placówkę. Można zatem przyjąć, że w przypadku szkoły publicznej zastosowanie może mieć

przesłanka wskazana w art. 6 ust. 1 lit. e RODO łącznie z przepisem krajowym, tj. art. 68 ust. 1 pkt 6 ustawy Prawo oświatowe.

W przypadku szkół niepublicznych - zgodnie z brzmieniem art. 172 ust. 2 pkt 3 Prawa oświatowego - statut szkoły lub placówki niepublicznej powinien określać organy szkoły lub placówki oraz zakres ich zadań. Wobec powyższego w przypadku szkoły niepublicznej podstawą będzie art. 6 ust. 1 lit. e RODO w związku z art. 172 ust. 2 pkt 3 ustawy Prawo oświatowe.

Data wytworzenia informacji: 24.03.2020 r.

Czy przekazanie dokumentacji do fumigacji powoduje konieczność zawarcia umowy powierzenia?

Czy w przypadku przekazania do odkażania (fumigacji) pudeł zawierających dokumenty (pudła są zamknięte, zapieczętowane i nie są na żadnym etapie odkażania otwierane przez pracowników zleceniobiorcy) należy zawrzeć umowę powierzenia przetwarzania danych? Dokumenty zawarte w pudłach mogą, ale nie muszą zawierać danych osobowych. W mojej ocenie odkażanie dokumentów jest czynnością techniczną, nie jest to czynność dokonywana na danych, a na pudłach zawierających bliżej nieokreślone dokumenty i w związku z tym ww. umowa nie jest potrzebna. Sytuację tę można porównać do przekazywania przesyłek poczcie w celu ich dostarczenia - wtedy przecież również nie ma potrzeby zawierania umowy powierzenia. Czy moja ocena jest prawidłowa?

Powierzenie przetwarzania danych osobowych będzie uzasadnione w sytuacji, jeśli administrator danych - w celu skorzystania z usługi fumigacji - przekazuje dokumenty zawierające dane osobowe, niezależnie od tego, czy dokumenty te są zapakowane w kartony. Powierzenie przetwarzania danych jest bowiem wówczas uzasadnieniem prawnym dla przekazania danych innemu, zewnętrznemu podmiotowi, a jednocześnie instrumentem służącym zapewnieniu przez administratora kontroli nad przetwarzanymi danymi osobowymi i ich bezpieczeństwem. Z drugiej strony podmiot przetwarzający zobowiązany zostaje do odpowiedniego zabezpieczenia danych, które otrzymuje od administratora (zabezpieczenia danych przed ujawnieniem, zniszczeniem, utratą danych osobowych czy nieautoryzowaną modyfikacją).

Inaczej jest natomiast w przypadku przetwarzania danych osobowych przez operatorów pocztowych. Poczta Polska i inni operatorzy pocztowi w związku z wykonywaniem usług pocztowych są administratorami danych osobowych nadawców i adresatów przesyłek, a jednocześnie odpowiadają za bezpieczeństwo przesyłek (i zawartych w nich danych osobowych) w ramach należytego wykonywania usług pocztowych oraz przestrzegania zasad i obowiązków określonych w Prawie pocztowym. Zgodnie z przepisami Prawa pocztowego operatorzy pocztowi zobowiązani są do ochrony tajemnicy pocztowej, która obejmuje informacje przekazywane

w przesyłkach pocztowych. Mają obowiązek zachowania należytej staranności w zakresie uzasadnionym względami technicznymi lub ekonomicznymi przy zabezpieczaniu urządzeń i obiektów wykorzystywanych przy świadczeniu usług pocztowych oraz zbiorów danych przed ujawnieniem tajemnicy pocztowej (art. 41 ust. 6 tej ustawy).

Data wytworzenia informacji: 24.03.2020 r.

Jakie informacje o pracownikach można udostępnić jako informację publiczną

Do urzędu miasta, w którym pełnię funkcję IOD, wpłynął, złożony w trybie ustawy o dostępie do informacji publicznej, wniosek o udzielenie informacji w zakresie imion i nazwisk pracowników urzędu pełniących funkcję publiczną, ich stanowisk służbowych oraz wynagrodzenia. Moje wątpliwości dotyczą tego, czy, a jeżeli tak, to jakie dane i w odniesieniu do jakich pracowników powinniśmy udostępnić. Czy w trybie dostępu do informacji publicznej urząd miasta jest obowiązany do przekazania informacji o wszystkich pracownikach urzędu, czy tylko o tych, którzy w związku z pełnieniem określonych funkcji bądź zajmowaniem określonych stanowisk są pracownikami podejmującymi decyzje? Czy podać informacje o wysokości otrzymywanego przez nie wynagrodzenia? Czy udostępniając takie dane, urząd miasta nie naruszy prywatności tych osób?

Na wstępie należy wskazać, że o udostępnieniu informacji lub o odmowie ich udostępnienia na podstawie wniosku o dostęp do informacji publicznej w określonym stanie faktycznym i prawnym rozstrzyga podmiot, do którego o te informacje się zwrócono. W razie odmowy udostępnienia informacji, wnioskodawca możne się zwrócić ze skargą do sądu administracyjnego (art. 21 ustawy o dostępie do informacji publicznej).

Relacje między prawem do ochrony danych osobowych a prawem dostępu do informacji publicznej określone zostały w art. 86 RODO. Zgodnie z tym przepisem, dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy ww. rozporządzenia. Również w motywie 154 RODO podkreślono konieczność pogodzenia tego prawa i ponownego wykorzystywania informacji sektora publicznego. Motyw ten wskazuje, że przepisy prawa krajowego powinny godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych,

i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie niniejszego rozporządzenia.

Przepis art. 86 oraz motyw 154 RODO w zakresie ważenia dwóch praw - prawa do ochrony danych osobowych i prawa do dostępu do informacji publicznej - odsyłają zatem do przepisów krajowych. Oznacza to, że przedstawione wyżej zagadnienie należy analizować w kontekście art. 5 ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, dalej zwanej „ustawą". Brzmienie ustępu 2 tego przepisu wskazuje, iż prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy jednak informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa.

Wobec powyższego podmiot, w którego dyspozycji znajdują się wnioskowane informacje, powinien każdorazowo ocenić, czy określone informacje mieszczą się w zakresie pojęcia informacji publicznej i czy ich udostępnienie na gruncie przepisów powołanej wyżej ustawy jest prawnie dopuszczalne. Oceniając dopuszczalność udostępnienia określonych informacji, należy ustalić, czy nie mamy do czynienia z przywołanymi wyżej ograniczeniami, w szczególności, czy ich udostępnienie nie spowoduje naruszenia prywatności osób fizycznych

Dlatego w pierwszej kolejności należy przeanalizować możliwość udostępnienia informacji publicznej po jej odpowiedniej anonimizacji. Anonimizacja jest bowiem uznawana w większości przypadków za wystarczający sposób ochrony tożsamości, a przez to prywatności osoby (wyrok WSA w Olsztynie z 22 grudnia 2015 r., sygn. II SA/Ol 1179/15). Jak wskazuje motyw 26 RODO, zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Jeśli natomiast ze względu na specyfikę innych danych zawartych w udostępnianej informacji mogłoby, nawet po anonimizacji danych osobowych, dojść do ustalenia imienia i nazwiska osoby fizycznej i przez to naruszenia jej prywatności, to będzie to przesłanka do wydania na podstawie art. 16 ust. 1 ustawy o dostępie do informacji publicznej decyzji o odmowie udostępnienia informacji publicznej.

Podkreślić należy, że wskazane w art. 5 ust. 2 ustawy ograniczenie nie dotyczy jednak informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Niestety, ustawa o dostępie do informacji publicznej nie zdefiniowała pojęcia „osoby pełniącej funkcję publiczną". Stąd problemy w określeniu zakresu tego wyłączenia.

Tu z pomocą przychodzi orzecznictwo sądowe dotyczące spraw o udostępnienie informacji publicznej z uwzględnieniem różnych kategorii pracowników.

Przykładem może być wyrok Wojewódzkiego Sądu Administracyjnego z 2019 r. (sygn. II SA/Gd 133/19), w którym WSA wskazał, że „za osobę pełniącą funkcję publiczną należy zatem uznać każdego, kto wykonując zadania w organach władzy publicznej lub też w strukturach osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej, jeżeli tylko jego zadania posiadają związek z dysponowaniem majątkiem państwowym lub samorządowym albo zarządzaniem sprawami związanymi z wykonywaniem swoich funkcji przez szeroko rozumiane Państwo. Nie ma przy tym znaczenia, na jakiej podstawie prawnej taka osoba wykonuje funkcję publiczną.” Dlatego w ocenie sądu „żądanie (…) w części, w jakiej odnosi się do nagród i premii pracowników Spółki nie pełniących funkcji publicznych nie znajduje podstaw w obowiązujących przepisach. Z całą pewnością udostępnieniu w trybie powoływanej ustawy podlegają natomiast informacje co do wysokości nagród i premii wypłaconych pracownikom pełniącym w Spółce rolę piastuna organu.”

Z kolei w ocenie WSA w Poznaniu zawartej w wyroku z 13 czerwca 2018 r. (sygn. II SAB/Po 26/18) „wskazanie, czy mamy do czynienia z funkcją publiczną, powinno zatem odnosić się do badania, czy określona osoba w ramach instytucji publicznej realizuje w pewnym zakresie nałożone na tę instytucję zadanie publiczne. Chodzi zatem nie tylko o funkcje kierownicze, ale również takie stanowiska i funkcje, których sprawowanie jest równoznaczne z podejmowaniem działań wpływających bezpośrednio na sytuację prawną innych podmiotów lub łączy się co najmniej z przygotowywaniem decyzji dotyczących innych podmiotów.”

Ponadto w powołanym wyroku sąd stwierdził także, że o tym, czy dani pracownicy należą do kręgu osób pełniących funkcję publiczną przesądza to, jakie funkcje i czynności wykonują w zakresie powierzonych im obowiązków, a także że wiedzę o tym ma organ bowiem on te obowiązki ustala i organizuje pracę urzędników.

Odnosząc się do kwestii udostępnienia, w trybie dostępu do informacji publicznej, innych informacji o osobach fizycznych, np. o wynagrodzeniach konkretnych pracowników urzędu, wskazać należy, iż również w takich sprawach wypowiadały się sądy. Niestety, w różny sposób oceniały zarówno zakres przedmiotowy oraz podmiotowy pojęcia »informacja publiczna«, jak i przesłanki odmowy udostępnienia informacji stanowiącej informację publiczną. Na przykład Sąd Najwyższy w uchwale z dnia 16 lipca 1993 r. (sygn. I PZP 28/93) stwierdził, że ujawnienie przez pracodawcę bez zgody pracownika wysokości jego wynagrodzenia za pracę może stanowić naruszenie dobra osobistego w rozumieniu art. 23 i 24 kodeksu cywilnego.

Od 2013 roku obserwowana jest jednak tendencja traktowania informacji dotyczących wynagrodzenia jako informacji publicznej i to podlegającej, z pewnymi ograniczeniami, udostępnieniu. Ważny jest tu wyrok Naczelnego Sądu Administracyjnego z 18 lutego 2015 r.

(sygn. I OSK 695/14), w którym NSA stwierdził, że informacja o wydatkach podmiotu publicznego na wynagrodzenia pracowników jest informacją publiczną. Nie oznacza to jednak zgody na publikowanie list nazwisk pracowników danej instytucji z ich wynagrodzeniem miesięcznym. „W tych ramach można żądać szczegółowych danych dotyczących wydatkowania środków publicznych na wynagrodzenia konkretnej grupy pracowników zatrudnionych na określonym stanowisku, a także pracownika, który jako jedyny zajmuje określone stanowisko w ramach struktury organizacyjnej podmiotu publicznego"- czytamy w wyroku NSA. Wynika z niego, że do publicznej wiadomości należy podać ogólne wydatki na wynagrodzenia i np. średnie wynagrodzenie na danym stanowisku. Udzielenie takich informacji „zazwyczaj nie musi się wiązać z koniecznością ingerencji w ich prawnie chronioną sferę prywatności. Dzieje się tak przede wszystkim wówczas, gdy w danym podmiocie na określonym stanowisku zatrudnionych jest kilka osób". Wówczas sfera prywatna pracownika jest chroniona. Tu dochodzimy do kluczowego fragmentu wyroku NSA: „Udostępnienie informacji publicznej polega bowiem na ujawnieniu wysokości wynagrodzenia wypłacanego na określonym stanowisku, bez wskazywania danych osobowych konkretnej osoby. Informacją publiczną nie jest bowiem to, jakie wynagrodzenie otrzymuje konkretna osoba, ale kwota wydawana na utrzymanie danego etatu ze środków publicznych". Podobną wykładnię można znaleźć w innym wyroku NSA z 18 lutego 2017 r. (sygn. I OSK 796/14).

Zdarzają się jednak i orzeczenia z odmienną wykładnią, choć wydały je sądy niższej instancji. Dla przykładu Wojewódzki Sąd Administracyjny w Gdańsku (sygn. II SA/Gd 557/19) uznał, że nauczyciele są osobami pełniącymi funkcje publiczne i dlatego nie ma podstaw do ograniczenia udostępnienia informacji publicznej w związku z ochroną ich prywatności, w tym informacji o ich wynagrodzeniu. W ocenie sądu „nie ulega też wątpliwości, że takiemu udostępnieniu podlegają informacje o przedmiocie nauczania, stażu pracy i wymiarze godzin pracy danego nauczyciela, albowiem zestawienie tych danych z informacją o wynagrodzeniu pozwala na dokonanie społecznej kontroli prawidłowości wydatkowania środków publicznych na zadania związane z edukacją."

Także Trybunał Konstytucyjny (wyrok TK z 20 marca 2006 r., sygn. K17/05) rozważał problematykę związaną z konfliktem między prawem do informacji publicznej a ochroną prawa do prywatności w odniesieniu do osób pełniących funkcje publiczne i jak wskazał, w każdym konkretnym przypadku należy ważyć obie chronione prawem wartości. Nie jest bowiem możliwe precyzyjne i jednoznaczne określenie sytuacji istnienia związku między życiem prywatnym a ograniczeniem prawa do prywatności z uwagi na obowiązek udzielenia informacji publicznej. Istnienie takiego związku oznacza, że informacja powinna się wiązać z funkcjonowaniem instytucji, w szczególności mogłaby mieć znaczenie dla ukształtowania się poglądu o sposobie jej funkcjonowania.

W wyroku tym TK wskazał również, że „w każdym wypadku musi być wyraźne powiązanie określonych faktów z życia prywatnego z funkcjonowaniem osoby, której dotyczą, w instytucji publicznej. Związek ten natomiast może wręcz być niekiedy niedostrzegalny dla przeciętnego odbiorcy, jednak z uwagi na pewne okoliczności dotyczące sfery prywatnej oraz te, które odnoszą się do realizowanej działalności osoby publicznej, ujawnienie takich pozornie niezwiązanych z tą działalnością informacji może mieć istotne znaczenie dla dobra publicznego (np. ze względu na istnienie lub zagrożenie powstania określonych ujemnych skutków w sferze publicznej). Tylko wtedy więc, jeśli ujawnione zdarzenia oddziaływają na sferę publicznego funkcjonowania podmiotu usprawiedliwiona będzie ingerencja w sferę życia prywatnego."

W powyższym wyroku Trybunał odniósł się także do pojęcia „osoby pełniącej funkcję publiczną". Zdaniem Trybunału nie jest też możliwe precyzyjne i jednoznaczne określenie, czy i w jakich okolicznościach osoba funkcjonująca w ramach instytucji publicznej będzie mogła być uznana za sprawującą funkcję publiczną. Trybunał stwierdził także, że „podejmując próbę wskazania ogólnych cech, jakie będą przesądzały o tym, że określony podmiot sprawuje funkcję publiczną, można bez większego ryzyka błędu uznać, iż chodzi o takie stanowiska i funkcje, których sprawowanie jest równoznaczne z podejmowaniem działań wpływających bezpośrednio na sytuację prawną innych osób lub łączy się co najmniej z przygotowywaniem decyzji dotyczących innych podmiotów. W opinii Trybunału spod zakresu funkcji publicznej wykluczone są zatem takie stanowiska, choćby pełnione w ramach organów władzy publicznej, które mają charakter usługowy lub techniczny".

Na przykładzie powyższych wyroków zauważyć można, że orzecznictwo dotyczące tematyki prawa do informacji publicznej nie jest jednolite i zdarza się, że sądy prezentują w nich odmienne poglądy. Stanowić ono może jednak dla dysponentów informacji publicznej (będących jednocześnie administratorami danych osobowych) źródło cennych wskazówek, jak interpretować poszczególne przepisy i pojęcia, którymi posługuje się w tych przepisach ustawodawca. Zastrzec przy tym należy, że cały czas pojawiają nowe orzeczenia. W każdej sprawie konieczne jest uwzględnianie szczegółów konkretnego wniosku o dostęp do informacji publicznej oraz innych konkretnych okoliczności mających wpływ na rozstrzygnięcie o sposobie załatwienia wniosku.

Wobec powyższego, rozpatrując wniosek o dostęp do informacji publicznej, należy zachować ostrożność i starannie ocenić, w określonym stanie faktycznym i prawnym, w jakim zakresie jest to wniosek o udostępnienie informacji publicznej i jakie informacje powinny być przekazane. Ta ostrożność wpisuje się w cały system prawa, w szczególności w prawo pracy chroniące prawa pracownicze i informacje z nimi związane, a także prawo ochrony danych osobowych, w tym RODO. Należy bowiem pamiętać, że udostępnianie danych osobowych zawartych w dokumentach urzędowych podlega przepisom RODO. Oznacza to, że w przypadku, gdy ujawnieniu w ramach krajowych systemów dostępu do informacji publicznej podlegają dane osobowe, to RODO

znajduje zastosowanie. W praktyce podmioty udostępniające te dane muszą pamiętać o przestrzeganiu m.in. zasady minimalizacji danych, która stanowi, że dane osobowe powinny być adekwatne i ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Oznacza, to że dane mogą być udostępnione tylko w takim zakresie, który jest niezbędny dla zrealizowania wniosku o dostęp do informacji publicznej, mając przy tym na uwadze także to, iż udostępnione informacje mogą zostać później np. opublikowane w prasie czy Internecie. Ponadto podmioty udostępniające dane osobowe powinny pamiętać także o tym, że osobie, której dane zostały udostępnione w trybie ustawy o dostępie do informacji publicznej, przysługuje skarga do organu nadzorczego.

Data wytworzenia informacji: 07.04.2020 r.

Czy należy odbierać zgodę na przetwarzanie od osób będących na kwarantannie?

Czy w związku z wymaganiami Głównego Inspektora Sanitarnego rzeczywiście należy odbierać zgody od osób na przekazywanie ich danych osobowych ośrodkom pomocy społecznej oraz innym podmiotom uczestniczącym w udzielaniu pomocy? Chodzi o zapewnienie pomocy osobom w podeszłym wieku, samotnym, niepełnosprawnym, na które nakładana jest decyzja o kwarantannie w momencie wydawania decyzji o objęciu kwarantanną. Jak wyjaśnia GIS, pozyskanie zgody umożliwi Państwowym Powiatowym Inspektorom Sanitarnym, w razie potrzeby, przekazanie danych osobowych osoby kwarantannowej ośrodkowi pomocy społecznej w celu udzielenia jej pomocy – posiłki, leki i wsparcie w realizacji innych potrzeb.

Odnosząc się do przedstawionych wątpliwości wskazać należy, że na stronie internetowej UODO 12 marca 2020 r. zostało zamieszczone „Oświadczenie Prezesa Urzędu Ochrony Danych Osobowych w sprawie koronawirusa" – **tekst w ramce poniżej**, zaś 19 marca 2020 r. oświadczenie Europejskiej Rady Ochrony Danych (EROD) w sprawie przetwarzania danych w kontekście pandemii COVID-19.

Informacja ze strony archiwalnej UODO

Oświadczenie Prezesa UODO w sprawie koronawirusa

W związku z wieloma pytaniami dotyczącymi przetwarzania danych dotyczących zdrowia na skutek działań zapobiegających rozprzestrzenianiu się wirusa COVID-19, Prezes UODO informuje, że kwestie z tym związane regulowane są w przepisach szczególnych, w tym przede wszystkim w tzw. specustawie. Przepisy o ochronie danych osobowych nie mogą być stawiane jako przeszkoda w realizacji działań w związku z walką z koronawirusem – twierdzi Prezes UODO.

Wskazane przepisy nie stoją w sprzeczności z zasadami przetwarzania danych i nie naruszają RODO.

Dają one narzędzia do podejmowania przez pracodawców określonych działań, które wynikają zarówno z zaleceń Głównego Inspektora Sanitarnego, jak i Prezesa Rady Ministrów.

Artykuł 17 specustawy dotyczącej przeciwdziałania COVID-19 wskazuje, że Główny Inspektor Sanitarny lub działający z jego upoważnienia państwowy wojewódzki inspektor sanitarny może wydawać pracodawcom m. in. decyzje nakładające obowiązek podjęcia określonych czynności zapobiegawczych lub kontrolnych i współdziałania z innymi organami administracji publicznej oraz organami Państwowej Inspekcji Sanitarnej. W zakresie podejmowanych przez pracodawców działań należy przede wszystkim śledzić na bieżąco komunikaty Państwowej Inspekcji Sanitarnej.

Prezes Rady Ministrów na wniosek wojewody, po poinformowaniu ministra właściwego do spraw gospodarki, ma prawo do wydawania poleceń przedsiębiorcom w związku z przeciwdziałaniem COVID-19. Polecenia te, wydawane w formie decyzji administracyjnej, podlegają natychmiastowemu wykonaniu z chwilą ich doręczenia lub ogłoszenia oraz nie wymagają uzasadnienia.

Przepisy te korespondują z RODO, które również przewidują sytuacje związane z ochroną zdrowia i zapobieganiem rozprzestrzeniania się chorób zakaźnych (art. 9 ust. 2 lit i art. 6 ust. 1 lit d).

Zgodnie z motywem 46 RODO przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest to niezbędne do ochrony interesu, które ma istotne znaczenie dla życia osoby której dane dotyczą np. gdy przetwarzanie jest potrzebne do celów humanitarnych w tym monitorowania epidemii i ich rozprzestrzeniania się.

Prezes UODO mając na uwadze powagę sytuacji przypomina, że wszelkie problemy związane ze zwalczaniem i zapobieganiem rozprzestrzeniania się koronawirusa powinny być w świetle powyższych unormowań w pierwszej kolejności zgłaszane do GIS.

Dlatego też organ nadzorczy zwraca się do wszystkich zainteresowanych szczegółami realizacji działań związanych z walką z koronawirusem, aby zwracali się do Głównego Inspektora Sanitarnego, jako organu właściwego w tej sprawie.

Jeśli chodzi o zasady ogólne i oświadczenie Prezesa UODO, to wskazał on w nim m.in., że przepisy o ochronie danych osobowych nie mogą być stawiane jako przeszkoda w realizacji działań w związku z walką z koronawirusem. Natomiast Europejska Rada Ochrony Danych Osobowych w powołanym wyżej oświadczeniu, wskazała że RODO jest obszernym aktem prawnym, który zawiera przepisy mające zastosowanie również do przetwarzania danych osobowych w kontekście takim, jak ten dotyczący COVID-19. RODO pozwala właściwym organom ds. zdrowia publicznego i pracodawcom na przetwarzanie danych osobowych w kontekście epidemii, zgodnie z prawem krajowym i na określonych w nim warunkach. Na przykład, gdy przetwarzanie danych jest konieczne ze względu na istotny interes publiczny w dziedzinie zdrowia publicznego. **W tych okolicznościach nie ma potrzeby polegania na zgodzie osób fizycznych.** Odnosząc się zaś do przetwarzania danych osobowych, w tym szczególnych kategorii danych przez właściwe organy publiczne (np. organy ds. zdrowia publicznego), Rada wskazała, że art. 6 i art. 9 RODO umożliwiają

przetwarzanie danych osobowych, w szczególności gdy wchodzą one w zakres mandatu prawnego organu publicznego przewidzianego w ustawodawstwie krajowym oraz warunków wskazanych w RODO.

Biorąc powyższe pod uwagę, pozyskiwanie zgody od osób, których dane dotyczą, w przedstawionej sytuacji, może budzić uzasadnione wątpliwości. Właściwymi podstawami powinny być raczej przesłanki określone w art. 6 ust. 1 lit. c lub lit. e RODO, w połączeniu z właściwymi przepisami szczególnymi określającymi zadania konkretnych organów i instytucji, np. ustawie z dnia 5 grudnia 2008 r. o zapobieganiu i zwalczania zakażeń i chorób zakaźnych u ludzi, ustawie z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, ustawie z dnia 12 marca 2004 r. o pomocy społecznej czy ustawach określających zadania poszczególnych podmiotów, w tym przede wszystkim w tzw. specustawie o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (z uwzględnieniem jej ostatnich zmian), która określa uprawnienia właściwych organów (tj. Główny Inspektor Sanitarny, Prezes Rady Ministrów) do wydawania zaleceń i decyzji co do działań, jakie należy podejmować. Konieczne jest zatem śledzenie na bieżąco wydawanych przepisów prawa.

W kontekście zadanego pytania warto zwłaszcza zwrócić uwagę na § 2 ust. 7 rozporządzenia Rady Ministrów z dnia 31 marca 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii (wejście w życie 31 marca 2020 r). Zgodnie z tym przepisem, organy Państwowej Inspekcji Sanitarnej udostępniają dane, o których mowa w ust. 3 i 4, dotyczące osób poddanych obowiązkowej kwarantannie lub izolacji w warunkach domowych właściwym ze względu na miejsce zamieszkania lub pobytu tych osób, ośrodkom pomocy społecznej, na ich wniosek.

Natomiast dopiero w sytuacji, gdy przesłanki z art. 6 ust. 1 lit. c lub lit. e nie mogłyby być zastosowane lub okazałyby się niewystarczające, a konieczne jest prowadzenie pilnych i niezbędnych działań mających na celu ratowanie zdrowia i zapobieganie rozprzestrzenianiu się epidemii, można rozważyć powołanie się na przesłankę określoną w art. 6 ust. 1 lit. d RODO, którą wskazuje również Prezes UODO w ww. oświadczeniu. Na możliwość jej zastosowania wskazuje również motyw 46 RODO, zgodnie z którym przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest to niezbędne do ochrony interesu, które ma istotne znaczenie dla życia osoby, której dane dotyczą, np. gdy przetwarzanie jest potrzebne do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się.

Data wytworzenia informacji: 07.04.2020 r.

Czy szczególny obowiązek upubliczniania decyzji administracyjnej zwalnia z anonimizacji danych?

Czy w przypadku obowiązkowej publikacji decyzji administracyjnych należy dokonywać anonimizacji danych osobowych? Na mocy obowiązujących przepisów dyrektor oddziału wojewódzkiego NFZ w sprawie odwołania w procesie kontraktowania świadczeń opieki zdrowotnej wydaje decyzję administracyjną. Jest ona zamieszczana - w terminie 2 dni od dnia jej wydania - na tablicy ogłoszeń oraz na stronie internetowej właściwego oddziału wojewódzkiego Funduszu (art. 154 ust. 3 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych). Zdarzają się sytuacje, kiedy w uzasadnieniu decyzji wskazywane są imiona i nazwiska osób uczestniczących w postępowaniu lub osób, których dotyczyły zarzuty (np. dotyczące niewystarczających uprawnień personelu medycznego). Czy tego typu dane powinny zostać zanonimizowane przed ich upublicznieniem?

Jak wskazuje art. 86 i motyw 154 RODO, dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy niniejszego rozporządzenia.

Zgodnie z przepisami ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w niniejszej ustawie (art. 1 ust. 1). Przepisy ustawy nie naruszają przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi, pod warunkiem że nie ograniczają obowiązków przekazywania informacji publicznej do centralnego repozytorium informacji publicznej, o którym mowa w art. 9b ust. 1, zwanym dalej "centralnym repozytorium"(art. 1 ust. 2).

Do kwestii stosowania przepisów ustawy o dostępie do informacji publicznej, w przypadku gdy zastosowanie mogą mieć przepisy innych ustaw odniósł się Naczelny Sąd Administracyjny w wyroku z 9 października 2009 r. I OSK 322/09: "(...) ustawa o dostępie do informacji publicznej reguluje ogólne zasady postępowania w tych sprawach a jej przepisów nie stosuje się wyłącznie wtedy gdy są one nie do pogodzenia z przepisami ustaw szczególnych, które w sposób odmienny regulują zasady i tryb dostępu do informacji publicznych."

Zgodnie z art. 154 ust. 3 ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, po rozpatrzeniu odwołania dyrektor oddziału wojewódzkiego Narodowego Funduszu Zdrowia wydaje decyzję administracyjną uwzględniającą lub oddalającą odwołanie. **Decyzja jest**

zamieszczana w terminie 2 dni od dnia jej wydania, na tablicy ogłoszeń oraz na stronie internetowej właściwego oddziału wojewódzkiego Funduszu

Wobec powyższego można przyjąć, że przepisy ustawy o dostępie do informacji publicznej i przepisy ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych pozostają w stosunku do siebie w relacji przepisu ogólnego do szczególnego.

Odnosząc się do kwestii danych osobowych w publikowanych decyzjach administracyjnych należy wskazać, że dostęp do informacji publicznej nie ma charakter nieograniczonego. Ograniczenie w tym zakresie przewidziano w art. 5 ust. 2 ustawy o dostępie do informacji publicznej. Zgodnie z tym przepisem prawo do informacji publicznej podlega ograniczeniu ze względu na **prywatność osoby fizycznej lub tajemnicę przedsiębiorcy.** Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Prywatność osoby, jako dobro chronione prawem powinno mieć pierwszeństwo przed innym dobrem prawem chronionym – dostępnością do informacji publicznej.

Należy także pamiętać, że udostępnianie danych osobowych zawartych w dokumentach urzędowych podlega przepisom RODO. Oznacza to, że w przypadku, gdy ujawnieniu w ramach krajowych systemów dostępu do informacji publicznej podlegają dane osobowe, to RODO znajduje zastosowanie. W praktyce podmioty udostępniające te dane muszą pamiętać o przestrzeganiu m.in. zasady minimalizacji danych (art. 5 ust. lit. c RODO), która stanowi, że dane osobowe powinny być **adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane**. Oznacza, to że dane mogą być udostępnione tylko w takim zakresie, który jest niezbędny dla zrealizowania celu, jakim w przedstawionym powyżej przypadku jest podanie do publicznej wiadomości informacji, iż organ podjął określonej treści decyzję.

Wobec powyższego jeżeli w treści decyzji znajdują się dane osób fizycznych np. imiona i nazwiska osób, których dotyczyły zarzuty (jak choćby niewystarczające uprawnienia personelu medycznego), to zamieszczając na tablicy ogłoszeń lub na stronie internetowej decyzję administracyjną, należy zachować ostrożność i starannie ocenić, w określonym stanie faktycznym i prawnym, jakie informacje powinny być przekazane, a jakie zanonimizowane przed upublicznieniem decyzji.

Data wytworzenia informacji: 18.05.2020 r.

W jaki sposób identyfikować osoby, które zwracają się do IOD jako punktu kontaktowego?

W związku z pełnieniem funkcji IOD zastanawiam się, jakie działania należy podjąć podczas realizacji zadania wynikającego z art. 38 ust. 4 RODO, aby zapewnić poufność informacji i zapobiec ewentualnemu przypadkowemu ujawnieniu danych osobowych osobie nieuprawnionej, np. podszywającej się pod konkretną osobę z imienia i nazwiska podczas rozmowy telefonicznej lub prowadzonej korespondencji. Pytanie to dotyczy zarówno bieżącego udzielania informacji telefonicznych i pocztą elektroniczną, a także działań podejmowanych w związku z realizacją praw tych osób na gruncie art. 15-22 RODO w związku z ich żądaniami kierowanymi na mój adres poczty elektronicznej.

Jednym z zadań inspektora ochrony danych (IOD) jest pełnienie roli punktu kontaktowego, czyli pośrednika między administratorem lub podmiotem przetwarzającym a osobami, których dane dotyczą. Rola ta jest mocno powiązana z obowiązkami administratora oraz podmiotu przetwarzającego i ma przyczyniać się do skuteczniejszego ich wykonywania. Zadania IOD w RODO zostały sformułowane w sposób ogólny, bez wskazania trybu oraz terminów ich realizacji. Taki sposób ujęcia obowiązków inspektora jest wyrazem nowego podejścia do ochrony danych osobowych opartego na analizie ryzyka i zasadzie rozliczalności, zapisanej w art. 5 ust. 2 RODO.

Prawodawca w art. 38 ust. 4 RODO uprawnił osoby, których dane dotyczą, do kontaktowania się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Przykładem takiej sprawy może być sytuacja, gdy dochodzi do naruszenia ochrony danych, które może powodować wysokie ryzyko naruszenia praw i wolności. W takiej sytuacji, znaczenie praw osób oraz roli inspektora uwydatnia się w sposób szczególny. Jak należy wnioskować z art. 34 ust. 2 RODO, w przypadkach takich naruszeń, osoby, których to naruszenie dotyczy, powinny mieć możliwość zwrócenia się do IOD lub innego punktu kontaktowego w celu uzyskania dodatkowych informacji, wykraczających poza zakres przekazany im w zawiadomieniu o naruszeniu.

W przypadku wystąpienia naruszenia, które może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator, zgodnie z art. 34 ust. 2 RODO, zawiadamia o naruszeniu osoby, których naruszenie dotyczy, przekazując im następujące informacje:

1. charakter naruszenia ochrony danych osobowych,
2. **imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;**
3. opis możliwych konsekwencji naruszenia ochrony danych osobowych;

4. opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu - w tym w stosownych przypadkach - środków w celu zminimalizowania jego ewentualnych negatywnych skutków.

Każdy z administratorów, aby móc sprawnie realizować swoje obowiązki związane z zasadą przejrzystości oraz realizacją praw osób, których dane dotyczą, w tym w sytuacji wystąpienia naruszenia ochrony danych osobowych, powinien, zgodnie z art. 12 oraz art. 24 ust. 2 RODO, dysponować odpowiednimi procedurami w zakresie obsługi takich praw i wniosków. Zgodnie z art. 12 ust. 1 RODO, administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (...) udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz **prowadzić z nią wszelką komunikację na mocy** art. 15 - 22 i **34 w sprawie przetwarzania.** W motywie 59 preambuły wskazuje się, że „administrator powinien przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną. Administrator powinien być zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki – najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny”.

W takich procedurach powinny być odzwierciedlone rozwiązania w zakresie weryfikacji tożsamości osoby uprawnionej do uzyskania informacji oraz bezpiecznego kanału udostępniania informacji o przetwarzanych danych. Art. 12 ust. 1 RODO wskazuje, że informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach - elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą. Osoba, której dane dotyczą, może wprawdzie zwrócić się o informacje za pośrednictwem takich środków komunikacji, jak np. telefon czy poczta elektroniczna, jednak w tym przypadku podmiot realizujący wniosek powinien zwrócić szczególną uwagę na obowiązek podjęcia stosowanych działań w celu uniemożliwienia udostępnienia informacji osobom do tego nieuprawnionym (istotne jest ustalenie tożsamości wnioskodawcy). Przy realizacji uprawnienia na odległość możliwość weryfikacji osoby uprawnionej może odbyć się np. poprzez uprawdopodobnienie tożsamości przez konieczność podania szczegółowych danych, które tę osobę jednoznacznie identyfikują i pozwalają zweryfikować jej tożsamość (nie wystarczy spytać o imię i nazwisko oraz adres, gdyż te informacje mogą być powszechnie dostępne, ale trzeba dokonać weryfikacji na podstawie znacznie bardziej szczegółowych danych, co do których prawdopodobieństwo, że będą one znane przez osoby postronne, jest znikome). Taką argumentację potwierdza treść art. 12 ust. 6 RODO, zgodnie z którym, **jeżeli administrator ma**

uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą. Ważne jest, aby podmiot realizujący uprawnienie miał pewność, że przekazuje informacje osobie uprawnionej do ich uzyskania. (P. Fajgielski w: Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), komentarz do art. 15, [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz. Wolters Kluwer Polska, 2018).

W przypadku wątpliwości co do tożsamości osoby usiłującej pozyskać informacje, powinno się odmówić ich udzielenia, ewentualnie podać informacje ogólne. Wobec tego w takiej sytuacji można w szczególności:

- udzielając informacji osobom, których dane dotyczą, ograniczyć się do przekazywania ogólnych informacji opublikowanych przez administratora na jego stronie internetowej i wysłanych przez niego w formie zawiadomień na indywidualne adresy poczty elektronicznej, lub
- odnosząc się do konkretnej osoby, udzielać informacji o jej kategoriach danych osobowych, których dotyczy naruszenie, ale bez podawania tych konkretnych danych.

Data wytworzenia informacji: 18.05.200 r.

Na jakiej podstawie gmina może udostępniać obraz z kamer Policji?

Na jakiej podstawie dopuszczalne jest udostępnianie przez gminę na rzecz Policji obrazu z kamer monitoringu w czasie rzeczywistym?

Na wstępie należy odpowiedzieć na pytanie, czy przeglądanie (podgląd) w czasie rzeczywistym obrazu rejestrowanego przez kamery monitoringu powinno być uznawane za przetwarzanie danych osobowych. W analizie tego zagadnienia istotne jest powołanie się na definicję zawartą w art. 4 ust. 2 RODO, zgodnie z którą przetwarzaniem jest operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, **przeglądanie**, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

Biorąc pod uwagę treść powołanej definicji przyjąć należy, że monitoring wizyjny w czasie rzeczywistym stanowi przetwarzanie danych osobowych. Potwierdzenie takiego stanowiska znaleźć można w Wytycznych 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń

wideo (dostępnych w języku angielskim), w których EROD, odnosząc się do prawa dostępu do danych wskazuje, że osoba, której dane dotyczą, ma prawo do uzyskania od administratora potwierdzenia, czy przetwarzane są jej dane osobowe. W przypadku nadzoru wideo oznacza to, że jeżeli żadne dane nie są przechowywane lub przekazywane w jakikolwiek sposób, wówczas po zakończeniu monitorowania w czasie rzeczywistym administrator może jedynie udzielić informacji, że dane osobowe nie są już przetwarzane (oprócz ogólnych obowiązków w zakresie informowania na mocy art. 13). Jeżeli jednak dane są nadal przetwarzane w momencie składania wniosku (tj. jeżeli dane są przechowywane lub stale przetwarzane w jakikolwiek inny sposób), osoba, której dane dotyczą, powinna uzyskać dostęp i informacje zgodnie z art. 15.

Odnosząc się natomiast do zagadnienia podstawy prawnej do udostępniania przez gminę na rzecz Policji obrazu z kamer monitoringu w czasie rzeczywistym wskazać należy, że zgodnie z powołanymi wyżej Wytycznymi EROD w sprawie monitoringu wizyjnego, „ujawnianie nagrań wideo organom ścigania jest również niezależnym procesem, który wymaga osobnego uzasadnienia dla administratora. Zgodnie z art. 6 ust. 1 lit. c przetwarzanie jest legalne, jeżeli jest konieczne do wypełnienia obowiązku prawnego, któremu podlega administrator. Chociaż obowiązujące prawo policyjne jest sprawą pozostającą pod wyłączną kontrolą państw członkowskich, to najprawdopodobniej istnieją ogólne zasady regulujące przekazywanie dowodów do organów ścigania w każdym państwie członkowskim. Przetwarzanie przez kontrolera przekazującego dane reguluje RODO. Jeżeli ustawodawstwo krajowe wymaga od administratora współpracy z organami ścigania (np. dochodzenie), podstawą prawną przekazania danych jest obowiązek prawny na mocy art. 6 ust. 1 lit. c.”

Uprawnienie jednostek samorządu gminnego do stosowania monitoringu wynika z art. 9a oraz art. 50 ust. 2 ustawy o samorządzie gminnym. Zgodnie ze wskazanym art. 9a, gmina w celu zapewnienia porządku publicznego i bezpieczeństwa obywateli oraz ochrony przeciwpożarowej i przeciwpowodziowej może stosować środki techniczne umożliwiające rejestrację obrazu (monitoring) w obszarze przestrzeni publicznej, za zgodą zarządzającego tym obszarem lub podmiotu posiadającego tytuł prawny do tego obszaru lub na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy lub jednostek organizacyjnych gminy, a także na terenie wokół takich nieruchomości i obiektów budowlanych, jeżeli jest to konieczne do zapewnienia porządku publicznego i bezpieczeństwa obywateli lub ochrony przeciwpożarowej i przeciwpowodziowej. Zgodnie zaś z treścią art. 50 ust. 2 ustawy o samorządzie gminnym, osoby uczestniczące w zarządzaniu mieniem komunalnym uprawnione są do tego, aby w celu ochrony tego mienia w szczególności stosować monitoring na terenie nieruchomości i w obiektach budowlanych stanowiących mienie gminy i na terenie wokół takich nieruchomości i obiektów budowlanych.

W przypadku Policji kwestii monitoringu miejsc publicznych dotyczy w szczególności art. 15 ust. 1 pkt 5a ustawy o Policji, zgodnie z którym Policjanci, wykonując czynności, o których mowa w art. 14 tej ustawy, mają prawo obserwowania i rejestrowania przy użyciu środków technicznych obrazu zdarzeń w miejscach publicznych, a w przypadku czynności operacyjno-rozpoznawczych i administracyjno-porządkowych podejmowanych na podstawie ustawy - także i dźwięku towarzyszącego tym zdarzeniom.

Policja w celu udostępnienia jej przez gminę danych uzyskanych w ramach bieżącego podglądu z kamer, powinna zwrócić się do gminy o udostępnienie danych w trybie określonym w art. 20 ustawy o Policji.

Zgodnie z ust. 1d tego przepisu, Policja w zakresie swojej właściwości przetwarza informacje, w tym dane osobowe, uzyskane ze zbiorów danych prowadzonych przez inne służby, instytucje państwowe oraz organy władzy publicznej. Przetwarzanie informacji, w tym danych osobowych, przez Policję może mieć charakter niejawny, odbywać się bez zgody i wiedzy, osoby której dane dotyczą, oraz z wykorzystaniem środków technicznych. Służby, instytucje państwowe oraz organy władzy publicznej są obowiązane do nieodpłatnego udostępnienia Policji informacji, w tym danych osobowych. W szczególności Policja jest uprawniona do uzyskiwania informacji, w tym danych osobowych:

1. gromadzonych w administrowanych przez nich zbiorach danych lub rejestrach;
2. uzyskanych przez te służby lub organy w wyniku wykonywania czynności operacyjno-rozpoznawczych, w tym prowadzonej kontroli operacyjnej.

Jednak aby móc pozyskiwać ww. dane w drodze teletransmisji, Policja powinna spełnić wymagania określone w ust. 1e ww. przepisu. Zgodnie z nim, podmioty, o których mowa w ust. 1d, mogą wyrazić pisemną zgodę na udostępnianie danych zgromadzonych w zbiorach danych jednostkom organizacyjnym Policji w drodze teletransmisji, bez konieczności składania wniosku pisemnie w postaci papierowej lub elektronicznej, jeżeli jednostki te spełniają łącznie następujące warunki :

1. posiadają urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał;
2. posiadają zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania;
3. jest to uzasadnione specyfiką lub zakresem wykonywanych zadań albo prowadzonej działalności.

W przypadku udostępnienia przez gminę danych uzyskanych w ramach bieżącego podglądu z kamer na rzecz podmiotu, jakim jest Policja, mamy do czynienia z odrębnym administratorem.

Nie będzie tu miała zastosowania instytucja współadministrowania. W przypadku podmiotów publicznych, o celach i środkach przetwarzania danych stanowią najczęściej przepisy prawa. Podmioty te są zobowiązane do przetwarzania danych osobowych dla realizacji określonych prawem celów, zazwyczaj także przy użyciu wskazanych środków. Zatem ze współadministrowaniem w sektorze publicznym możemy mieć do czynienia wówczas, gdy przepisy prawa przewidują wspólne realizowanie zadań/celów. Natomiast analiza wskazanych powyższej przepisów ustawy o samorządzie gminnym oraz ustawy o Policji wskazuje, iż gmina i Policja, monitorując/obserwując miejsca publiczne, realizują zbliżone, jednak nie tożsame cele.

Data wytworzenia informacji: 18.05.2020 r.

Który podmiot należy uznać za administratora danych przetwarzanych poza systemem EKSMON?

Czy powiatowy zespół ds. orzekania o niepełnosprawności jest administratorem danych osobowych przetwarzanych poza systemem EKSMON? Z przepisów prawa wynika, że powiatowe zespoły są administratorami danych przetwarzanych w prowadzonych przez siebie bazach danych Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności (EKSMON). Czy powiatowy zespół jest także administratorem danych przetwarzanych poza tym systemem, czy jest nim może starosta? Czy można tutaj mówić o współadministrowaniu? Przepisy dotyczące funkcjonowania powiatowych zespołów ds. orzekania o niepełnosprawności wskazują, że to zespół wykonuje określone tam zadania i obowiązki. Starosta jest tylko właściwy w materii ich powołania/odwołania. Jak zatem powinna wyglądać kwestia dokumentacji dotyczącej ochrony danych w powiatowym zespole? Czy z uwagi na zapewnienie mu przez starostę wszelkich środków techniczno-organizacyjnych może stosować się do zasad określonych przez starostę, jeśli faktycznie byłby odrębnym od starosty administratorem?

Zgodnie z definicją określoną w art. 4 pkt 7 RODO, „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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.

Jeśli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni wówczas współadministratorami (art. 26 ust. 1 RODO). W takim przypadku współadministratorzy w drodze wspólnych uzgodnień określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO.

3 ZADANIA IOD

W przypadku podmiotów realizujących zadania określone w przepisach prawa, cele, a często i sposoby przetwarzania, określone są w tych 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 wyznaczonych im ustawowo zadań. Do uznania danego podmiotu za administratora potrzebna jest zatem zawsze analiza konkretnych przepisów regulujących działalność danego podmiotu.

Zadania oraz zasady funkcjonowania powiatowego zespołu do spraw orzekania o niepełnosprawności (dalej jako „powiatowy zespół") określone zostały w szczególności w ustawie o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych oraz w rozporządzeniu Ministra Gospodarki, Pracy i Polityki Społecznej sprawie orzekania o niepełnosprawności i stopniu niepełnosprawności.

Do zadań zespołu, zgodnie z powołanymi wyżej przepisami, należy przede wszystkim merytoryczne rozpatrywanie wniosków w celu wydania orzeczenia o niepełnosprawności, stopniu niepełnosprawności lub wskazaniach do ulg i uprawnień osób posiadających orzeczenia o inwalidztwie lub niezdolności do pracy (§ 2 ww. rozporządzenia). Zgodnie z art. 6 ust. 5 powyższej ustawy zespoły orzekające o niepełnosprawności przetwarzają dane osobowe, w tym dane o stanie zdrowia, wyłącznie dla celów realizacji zadań oraz w zakresie niezbędnym do ich wykonania. Ponadto zgodnie z art. 6 ust. 6 tej ustawy, zabezpieczenia przetwarzania danych osobowych przez zespoły orzekające o niepełnosprawności polegają co najmniej na dopuszczeniu do przetwarzania danych osobowych wyłącznie osób posiadających pisemne upoważnienie wydane przez administratora oraz pisemnym zobowiązaniu osób upoważnionych do przetwarzania danych osobowych do zachowania ich poufności.

Powyższe przepisy prawa przesądzają o statusie powiatowego zespołu jako administratora w rozumieniu art. 4 pkt 7 RODO, niezależnie od tego, czy jest umiejscowiony w strukturze powiatu, czy nie. Za przyjęciem takiego stanowiska wskazuje również treść art. 6d ust. 2 ww. ustawy, zgodnie z którym powiatowe zespoły są administratorami danych w prowadzonych przez siebie bazach danych Elektronicznego Krajowego Systemu Monitoringu Orzekania o Niepełnosprawności, w którym przetwarza się dane w celu usprawnienia i podniesienia jakości orzekania o niepełnosprawności oraz realizacji zadań przez zespoły orzekające o niepełnosprawności.

Analiza przepisów ww. ustawy o rehabilitacji oraz rozporządzenia wskazuje także na zadania starosty związane z funkcjonowaniem powiatowych zespołów, w szczególności starosta w ramach zadań z zakresu administracji rządowej powołuje powiatowy zespół, po uzyskaniu zgody wojewody oraz przedkłada wojewodzie informacje o realizacji zadań (art. 6a ust. 1 ustawy),

a także powołuje i odwołuje przewodniczącego oraz członków powiatowego zespołu (§ 18 ust. 2 i 3 ww. rozporządzenia).

Powołane wyżej regulacje nie precyzują jednak kwestii organizacyjnych, w szczególności w jaki sposób mają działać powiatowe zespoły (czy jako odrębne podmioty, czy w strukturach starostwa), a także w jaki sposób ma być realizowana obsługa administracyjna, finansowa czy kadrowa powiatowych zespołów. Jedynie w § 18 ust. 5 ww. rozporządzenia wskazano, że przewodniczący powiatowego zespołu reprezentuje zespół na zewnątrz i organizuje jego obsługę administracyjno-biurową.

Powiatowy zespół, nawet jeśli umiejscowiony jest w strukturach starostwa, jest administratorem przetwarzanych przez siebie danych. Jednakże w takiej sytuacji również starosta przetwarza dane osobowe wnioskodawców powiatowego zespołu np. w związku z obsługą składanej przez nich korespondencji adresowanej do powiatowego zespołu albo też w związku z archiwizacją akt postępowań i w tym zakresie jest ich administratorem. Ponadto zgodnie z art. 34 oraz art. 35 ust. 2 i 3 ustawy o samorządzie powiatowym, starosta jest kierownikiem starostwa powiatowego i organizuje jego pracę, a także zwierzchnikiem służbowym pracowników starostwa i kierowników jednostek organizacyjnych powiatu.

Wobec powyższego w sytuacji, gdy starosta zapewnia obsługę działalności powiatowego zespołu, podmioty te będą wspólnie ustalać cele i sposoby przetwarzania danych osobowych, w ramach tych zadań. Pomiędzy tymi administratorami można zatem przyjąć relację współadministrowania uregulowaną w art. 26 RODO. Wówczas powiatowy zespół oraz starosta jako współadministratorzy powinni w drodze wspólnych uzgodnień w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. W myśl natomiast art. 26 ust. 2 RODO, uzgodnienia, o których mowa w ust. 1, muszą należycie odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść takich uzgodnień jest udostępniana podmiotom, których dane dotyczą.

Jakie wspólne uzgodnienia muszą uwzględniać faktyczne obowiązki powiatowego zespołu i starosty, związane z przetwarzaniem danych osobowych osób występujących do powiatowego zespołu, a wynikające m.in. z przepisów ustawy o rehabilitacji oraz wewnętrznych regulacji. Zarówno powiatowy zespół, jak i starosta mają swoje autonomiczne uprawnienia, z którymi związane jest przetwarzanie danych ww. osób w innych celach. Przykładowo, jedynie powiatowy

zespół uprawniony jest do przetwarzania danych osobowych w celu orzekania o niepełnosprawności. Starosta, w ramach współadministrowania, może być uprawniony np. do zapewnienia ochrony pomieszczeń czy przetwarzania tych danych w celach archiwizacyjnych. Należy wskazać, że co do zasady odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych w zakresie realizacji takich autonomicznych uprawnień kształtują przepisy prawa. Powiatowy zespół i starosta, w ramach wspólnych uzgodnień, powinni więc określić inne kwestie, nieuregulowane wprost w przepisach prawa, w tym m.in. kwestię odpowiedniego zabezpieczenia danych osobowych wnioskodawców czy też realizacji określonych obowiązków informacyjnych.

Warto nadmienić, że analogiczne podejście zostało zaprezentowane przez Prezesa UODO wobec relacji pomiędzy wojewodą a wojewódzką komisją do spraw orzekania o zdarzeniach medycznych - Newsletter UODO dla Inspektorów Ochrony Danych – Wydanie 2 (maj 2019) – **tekst w ramce poniżej.**

Informacja z Newslettera UODO

Wojewodę oraz wojewódzką komisję do spraw orzekania o zdarzeniach medycznych można uznać za współadministratorów (art. 26 RODO)

UODO - odnosząc się do przedstawionego mu zagadnienia odpowiedzialności za przetwarzanie danych w związku z obsługą wniosków o ustalenie zdarzenia medycznego wskazał, że wojewódzkie komisje do spraw orzekania o zdarzeniach medycznych oraz wojewodowie przetwarzają dane osobowe osób, które są stronami postępowań prowadzonych przez wojewódzkie komisje. Każdy z tych podmiotów uczestniczy w procesie przetwarzania przedmiotowych danych osobowych w innym zakresie. Do zadań Komisji należy przede wszystkim merytoryczne rozpatrywanie wniosków określonych osób fizycznych o ustalenie zdarzenia medycznego. Z drugiej strony przepisy ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta wskazują, że wojewoda uczestniczy w procesie przetwarzania danych osobowych wnioskodawców, w tym przede wszystkim w związku z obowiązkiem zapewnienia obsługi administracyjnobiurowej komisji wojewódzkiej. Wojewoda zapewnia wojewódzkiej komisji lokal do prowadzenia działalności w obrębie urzędu, odpowiednią obsługę kadrową, która jest upoważniona do wglądu do akt prowadzonych przez wojewódzkie komisje postępowań oraz do archiwizacji tych akt. Komisja i wojewoda, realizując swoje uprawnienia przysługujące im na podstawie odrębnych przepisów mogą zatem – stosownie do art. 26 RODO – określić w sposób przejrzysty zakresy swojej odpowiedzialności dotyczącej wypełnienia obowiązków wynikających z przepisów RODO. W ramach wspólnych uzgodnień powinni określić kwestie, nieuregulowane wprost w przepisach prawa, w tym m.in. kwestię odpowiedniego zabezpieczenia danych osobowych wnioskodawców czy też realizacji określonych obowiązków informacyjnych.

Niezależnie od poczynionych uzgodnień pomiędzy wojewódzką komisją a wojewodą, osoba, której dane dotyczą może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego ze współadministratorów, a więc zarówno w stosunku do komisji, jak i wojewody.

Odnosząc się natomiast do pytania o dokumentację dotyczącą ochrony danych wskazać należy, że istnienie w strukturach starostwa podmiotu, który jest odrębnym administratorem, nie musi oznaczać konieczności stworzenia procedur i polityk ochrony danych dotyczących przetwarzania w tym obszarze w odrębnym dokumencie. Jedna dokumentacja może bowiem regulować kwestie ochrony danych dotyczące administratorów istniejących w ramach tej samej jednostki. Przy czym kwestię tę, w kontekście prowadzonego przetwarzania należy starannie przemyśleć, a więcej informacji na ten temat znaleźć można w odpowiedzi na pytanie CZY KOMENDANT STRAŻY MIEJSKIEJ MUSI POSIADAĆ ODRĘBNĄ POLITYKĘ OCHRONY DANYCH?.

Data wytworzenia informacji: 18.05.2020 r.

Czy z laboratorium należy zawrzeć umowę powierzenia?

Samodzielny Publiczny Zespół Zakładów Zdrowotnych (SPZZOZ) zawarł umowę na wykonywanie badań przez laboratorium. Badania obejmują próbki pobrane i dostarczone przez szpital i przychodnie SPZZOZ od osób przebywających na oddziałach szpitalnych oraz od osób kierowanych na badanie przez poradnie/przychodnie wchodzące w skład SPZZOZ (objęte ww. umową). Czy do takiej umowy głównej powinno się zawrzeć umowę powierzenia przetwarzania danych osobowych?

Żeby określić status danego podmiotu w procesie przetwarzania należy przede wszystkim kierować się definicjami administratora i podmiotu przetwarzającego zawartymi w RODO.

Zgodnie z art. 4 pkt 7 RODO, „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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. Natomiast podmiot przetwarzający, zgodnie z art. 4 pkt 8 RODO, oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

Zatem w myśl przepisów RODO, konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator zleca wykonywanie swoich zadań innemu podmiotowi (podmiotowi przetwarzającemu). Istotne jest podkreślenie, że podmiot przetwarzający przetwarza dane w imieniu administratora, a nie w imieniu własnym (tj. nie staje się administratorem tych danych). Podmiot przetwarzający nie decyduje bowiem o celach i sposobach przetwarzania, gdyż przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO).

Inną kwestią jest udostępnienie danych osobowych innemu administratorowi. Do takiego udostępnienia danych dochodzi, jeśli dane te przekazywane są innemu podmiotowi w celu realizacji przez ten podmiot jego własnych zadań, wynikających np. z przepisów prawa. Staje się on wtedy odrębnym administratorem.

Regulacje dotyczące diagnostyki laboratoryjnej znaleźć można w szczególności w ustawie o działalności leczniczej, ustawie o prawach pacjenta i Rzeczniku Praw Pacjenta, ustawie o diagnostyce laboratoryjnej oraz w rozporządzeniu Ministra Zdrowia z dnia 23 marca 2006 r. w sprawie standardów jakości dla medycznych laboratoriów diagnostycznych i mikrobiologicznych.

Zgodnie z art. 11 ustawy o działalności leczniczej badania diagnostyczne zostały zaliczone do szczególnego rodzaju działalności leczniczej, jakim jest ambulatoryjne świadczenie zdrowotne. Bliższa charakterystyka tej działalności zawarta jest w ustawie o diagnostyce laboratoryjnej. Zgodnie z art. 1a tejże ustawy, medyczne laboratorium diagnostyczne wykonuje badania in vitro materiału biologicznego. Laboratorium diagnostyczne zazwyczaj jest zakładem leczniczym podmiotu leczniczego w rozumieniu przepisów ustawy o działalności leczniczej, ale może być także jednostką organizacyjną zakładu leczniczego podmiotu leczniczego, instytutu badawczego albo uczelni medycznej (art. 17 ustawy o diagnostyce laboratoryjnej).

W celu wykonywania badań diagnostycznych podmioty świadczące takie usługi przetwarzają dane osobowe osób, od których pochodzi materiał do tych badań. Dane te pozyskiwane są bezpośrednio od osób, których dotyczą lub też z innych źródeł, np. od szpitali, które zlecają tym podmiotom wykonywanie badań próbek pobranych od swoich pacjentów.

Przetwarzając powyższe dane osobowe, laboratorium diagnostyczne realizuje swoje własne zadania, związane chociażby z:

- obowiązkiem prowadzenia, przechowywania i udostępniania dokumentacji medycznej pacjenta (art. 24 w zw. z art. 23 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta),
- uprawnieniem diagnosty laboratoryjnego do zgłaszania Prezesowi Urzędu Rejestracji Produktów Leczniczych, Wyrobów Medycznych i Produktów Biobójczych lub podmiotowi odpowiedzialnemu za wprowadzenie produktu leczniczego do obrotu działania niepożądanego produktu leczniczego (art. 27a ustawy o diagnostyce laboratoryjnej),
- obowiązkiem diagnosty laboratoryjnego zgłaszania wyniku określonych badań właściwemu państwowemu inspektorowi sanitarnemu (art. 29 ust. 1 ustawy o zapobieganiu i zwalczania zakażeń i chorób zakaźnych u ludzi).

Ponadto zgodnie z art. 26 ust. 3 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną m.in. podmiotom udzielającym świadczeń zdrowotnych, jeżeli dokumentacja ta jest niezbędna do

zapewnienia ciągłości świadczeń zdrowotnych. Z takim udostępnieniem, a więc w celu zapewnienia ciągłości leczenia, mamy do czynienia w sytuacji, w której dane osobowe pacjentów są przekazywane przez placówkę medyczną do zewnętrznego laboratorium diagnostycznego.

Powyższe pozwala zasadnie przyjąć, że w przypadku gdy np. szpital zleca przeprowadzenie badań podmiotowi świadczącemu usługi z zakresu diagnostyki laboratoryjnej, podmiot ten przetwarza pozyskane w tym celu dane osobowe dla realizacji własnych zadań. W takiej sytuacji mamy zatem do czynienia z udostępnieniem danych osobowych na rzecz odrębnego administratora.

Powyższe oznacza, że nie istnieje tutaj relacja administrator – podmiot przetwarzający. Tym samym nie ma podstaw do zawarcia umowy powierzenia przetwarzania danych osobowych.

Data wytworzenia informacji: 03.06.2020 r.

Czy wojewoda może utworzyć bazę wyników badań w kierunku wirusa SARS-CoV-2?

Do urzędu wojewódzkiego wielokrotnie kierowane były prośby dotyczące usprawnienia sposobu przekazywania kompleksowych informacji nt. wyników badań laboratoryjnych wykonywanych w kierunku SARS-CoV-2., Czy w związku z tym wojewoda może (powołując się na art. 14 ust. 2 pkt 1 i art. 20a ustawy o zarządzaniu kryzysowym) pozyskiwać od laboratoriów prowadzących badania w kierunku SARS-CoV-2 na terenie województwa dobowe dane dotyczące: imienia i nazwiska, numeru PESEL, wyniku badania, daty pobrania materiału, wieku, adresu, telefonu? Czy po scaleniu wszystkich danych, tak stworzoną bazę danych może następnie udostępniać uprawnionym podmiotom na ich uzasadniony wniosek (np. podmioty lecznicze: szpitale, wojewódzka stacja ratownictwa medycznego)?

Co do zasady wszelkie działania podejmowane przez podmioty publiczne powinny mieć oparcie w obowiązujących przepisach prawa regulujących ich działalność. Wobec tego podstawa prawna do przetwarzania (w tym udostępniania) danych osobowych przez takie podmioty również powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami.

Przetwarzanie tzw. danych zwykłych może się odbywać jedynie po spełnieniu jednego z warunków określonych w art. 6 RODO, a w przypadku szczególnej kategorii danych osobowych po spełnieniu przesłanek określonych w art. 9 RODO, w połączeniu z właściwymi przepisami szczególnymi określającymi zadania konkretnych organów i instytucji. Zatem co do zasady, aby podmiot publiczny legalnie przetwarzał (w tym pozyskiwał i udostępniał) dane osobowe, musi istnieć przepis prawa, pozwalający na takie przetwarzanie. Podkreślić przy tym należy, że dane dotyczące zdrowia zaliczane są do szczególnych kategorii danych , przetwarzanie których może stanowić poważną ingerencję w sferę prywatności (a nawet intymności) osób, których dane

dotyczą, lub pociągać za sobą znacznie większe zagrożenia niż przetwarzanie tzw. danych zwykłych. Dlatego administrator, pozyskując takie dane, powinien zachować szczególną staranność oraz przetwarzać jedynie takie dane, które istotnie są konieczne do realizacji celu przetwarzania.

Rozważane przedsięwzięcie dotyczy utworzenia przez wojewodę bazy zawierającej dane osobowe osób poddanych badaniu w kierunku SARS-CoV-2 oraz wyników tych badań (imienia i nazwiska, numeru PESEL, wyniku badania, daty pobrania materiału, wieku, adresu, telefonu). Informacje te wojewoda pozyskiwałby od laboratoriów prowadzących badania w kierunku SARS-CoV-2 na terenie województwa, a następnie udostępniał np. podmiotom leczniczym, szpitalom, stacjom ratownictwa medycznego. Administrator rozważa możliwość przyjęcia za podstawę prawną do prowadzenia takiej bazy przepisów prawa zawartych w art. 14 ust. 2 pkt 1 i art. 20a ustawy o zarządzaniu kryzysowym. Zgodnie z art. 14 ust. 2 pkt 1 powyższej ustawy, do zadań wojewody w sprawach zarządzania kryzysowego należy kierowanie monitorowaniem, planowaniem, reagowaniem i usuwaniem skutków zagrożeń na terenie województwa. Natomiast zgodnie z art. 20a tej ustawy, organy właściwe w sprawach zarządzania kryzysowego mają prawo żądania udzielenia informacji, gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w ustawie.

Celem utworzenia takiej bazy miało by być usprawnienie sposobu przekazywania kompleksowych informacji nt. wyników badań laboratoryjnych wykonywanych w kierunku SARS-CoV-2. Administrator nie doprecyzował jednak, dla realizacji którego z zadań spośród zadań wskazanych w art. 14 ust. 2 pkt 1, niezbędne jest przetwarzanie wskazanych powyżej danych osób poddanych badaniom, ani w jakim celu i na jakiej podstawie dane te udostępniane byłyby podmiotom leczniczym.

Niemniej analizując powyższe przepisy należy stwierdzić, iż słuszne są wątpliwości co do uznania ich za podstawę prawną do prowadzenia takiego przetwarzania. Trudno bowiem wywieść z nich uprawnienie do utworzenia przez wojewodę bazy/rejestru zawierającego powyższe dane osobowe. Jednocześnie przypomnieć należy, że z uwagi na określoną w art. 7 Konstytucji RP zasadę działania organów publicznych na podstawie i w granicach prawa, organ publiczny nie może domniemywać swoich kompetencji, jeśli nie wynikają one wprost z przepisu prawa. Jednocześnie pomocniczo można wskazać, że zagadnienie gromadzenia oraz udostępniania informacji o osobach, u których stwierdzono COVID-19 uregulowane zostało w szczególności w rozporządzeniu Rady Ministrów z dnia 16 maja 2020 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, wydanym na podstawie art. 46a i art. 46b pkt. 1-6 i 8-12 ustawy o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi oraz w rozporządzeniu Ministra Zdrowia z dnia 7 kwietnia 2020 r.

w sprawie Krajowego Rejestru Pacjentów z COVID-19 wydanym na podstawie art. 20 ust. 1 ustawy o systemie informacji w ochronie zdrowia.

Zgodnie z przepisami rozporządzenia w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii w systemie teleinformatycznym udostępnionym przez jednostkę podległą ministrowi właściwemu do spraw zdrowia właściwą w zakresie systemów informacyjnych ochrony zdrowia, mogą być również przetwarzane dane innych osób podlegających obowiązkowej kwarantannie w związku z epidemią, o której mowa w § 1, a także osób podlegających izolacji w warunkach domowych, osób, w stosunku do których podjęto decyzję o wykonaniu testu diagnostycznego w kierunku SARS-CoV-2, oraz osób zakażonych tym wirusem (§ 2 pkt 4). Ponadto zgodnie z § 2 pkt 5 tego rozporządzenia dane osób, w stosunku do których podjęto decyzję o wykonaniu testu diagnostycznego w kierunku SARS-CoV-2, w tym dane zawarte w zleceniach wykonania takich testów wystawionych przez podmioty inne niż organy Państwowej Inspekcji Sanitarnej oraz wyniki tych testów, mogą być również przetwarzane w systemie teleinformatycznym stanowiącym moduł Krajowego Rejestru Pacjentów z COVID-19 prowadzonego przez Narodowy Instytut Kardiologii Stefana Kardynała Wyszyńskiego - Państwowy Instytut Badawczy w Warszawie. W kolejnych przepisach tego rozporządzenia został określony sposób udostępniania danych z powyższego systemu teleinformatycznego oraz Krajowego Rejestru Pacjentów z COVID-19.

W przedstawionej sytuacji wskazane byłoby zatem w pierwszej kolejności dokonanie analizy, czy ww. podmioty lecznicze nie są uprawnione są pozyskiwania powyższych danych z istniejących już ewidencji, w szczególności z powyższych systemów i rejestrów. Warto też zwrócić uwagę, że zadania związane z przeciwdziałaniem COVID-19 w obecnej sytuacji muszą być realizowane przez poszczególne podmioty we współpracy z Państwową Inspekcją Sanitarną. W związku z powyższym w oświadczeniu w sprawie koronawirusa z dnia 12 marca 2020 r., Prezes UODO wskazywał, że wszelkie problemy związane ze zwalczaniem i zapobieganiem rozprzestrzeniania się koronawirusa powinny być w świetle powyższych unormowań w pierwszej kolejności zgłaszane i wyjaśniane z GIS jako organem właściwym w tych sprawach.

Data wytworzenia informacji: 03.06.2020 r.

Co z obowiązkiem informacyjnym wobec członków zarządu osób prawnych?

Czy należy dopełniać obowiązek informacyjny na mocy art. 13 i 14 RODO w sytuacji, gdy w treści dokumentacji dotyczącej postępowań administracyjnych pojawiają się dane osób upoważnionych do reprezentacji spółek np. członków zarządu (organów spółek) bądź osób uprawnionych do składania oświadczeń w imieniu określonego podmiotu?

Zgodnie z art. 1 ust. 2 RODO regulacja ta chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych. Motyw 14 RODO wyjaśnia natomiast, że ochrona zapewniana przez RODO dotyczy „osób fizycznych, niezależnie od ich obywatelstwa lub miejsca zamieszkania, w związku z przetwarzaniem ich danych osobowych". Zgodnie z definicją zawartą w art. 4 pkt 1 RODO "dane osobowe" oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

W zdaniu drugim motywu 14 RODO wyjaśniono, że RODO nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. W związku z powyższym RODO chroni dane osobowe możliwych do zidentyfikowania osób fizycznych i wyklucza spod tej ochrony dane dotyczące osób prawnych. Zdarzają się sytuacje, w których dane o charakterze osobowym będą związane z danymi dotyczącymi osób prawnych. Przykładem tego mogą być dane osobowe osób pełniących funkcję organów osoby prawnej. W takich sytuacjach spełnienie przesłanki identyfikowalności przesądzić powinno o objęciu zakresem ochronnym RODO danych osobowych również w takich konfiguracjach.

W przypadku osób fizycznych pełniących funkcję członków organów osoby prawnej możliwość ich identyfikacji wynika w szczególności z faktu, iż dane takich osób ujawniane są w KRS. Oznacza to, że należy odmiennie odnosić się do informacji o osobach prawnych i osobach fizycznych reprezentujących osoby prawne.

Wobec powyższego należy przyjąć, że dane osób fizycznych pełniących funkcje członków organów osoby prawnej będą stanowiły dane osobowe, a nie będą zaś mieściły się w zakresie pojęcia danych osoby prawnej (w rozumieniu przywołanego wyżej motywu 14 RODO).

Podobnie sytuacja wygląda w odniesieniu do danych pełnomocników i pracowników osób prawnych. Komisja Europejska odpowiadając w 21 lutego 2018 r. na pisemne pytanie członka Parlamentu Europejskiego Richarda Sulika, wskazała, że motyw 14 RODO wyjaśnia, że rozporządzenie nie ma zastosowania do przetwarzania danych osobowych, które dotyczą osób prawnych, w tym nazwy i formy osoby prawnej oraz danych kontaktowych osoby prawnej. Adres e-mail osoby prawnej, taki jak ikeacontact@ikea.com, nie wchodzi w zakres rozporządzenia. Jednak dane osobowe pracowników osoby prawnej, w tym ich profesjonalne adresy e-mail, byłyby objęte zakresem rozporządzenia (np. Johnsmith@ikea.sk) (odp. KE dostępna pod linkiem: https://www.europarl.europa.eu/doceo/document/E-8-2017-007174-ASW_EN.html?redirect).

W wyroku z 9 marca 2017 r. w sprawie C-398/15 Trybunał Sprawiedliwości UE orzekł, że z orzecznictwa Trybunału wynika, że okoliczność, iż informacje wpisują się ramy działalności zawodowej, nie oznacza, że nie można ich scharakteryzować jako dane osobowe. Definicja danych osobowych odnosi się zatem do osób fizycznych bez względu na rolę, jaką odgrywają (czy są konsumentami, przedsiębiorcami czy pracownikami itd.).

Wobec powyższego uznać należy, że dane członków zarządu reprezentujących osobę prawną, dane pełnomocników osób prawnych, a także dane pracowników, którzy są osobami kontaktowymi osoby prawnej, będących możliwymi do zidentyfikowania osobami fizycznymi, będą danymi osobowymi podlegającymi ochronie RODO.

Wobec tego administrator jest zobligowany do wypełnienia w stosunku do takich osób obowiązku informacyjnego określonego w art. 13 lub 14 RODO, o ile nie zachodzi jedna z przesłanek zwalniających go z tego obowiązku.

Data wytworzenia informacji: 30.06.2020 r.

Czy lekarzom należy nadawać upoważnienia?

Czy lekarzom należy nadawać upoważnienia do przetwarzania danych osobowych? Czy takie same zasady w zakresie nadawania upoważnień będą obowiązywać lekarzy współpracującym z przychodnią na podstawie umowy cywilno-prawnej? Czy w związku z brzmieniem art. 24 ust. 2 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta, który stanowi, że do przetwarzania danych zawartych w dokumentacji medycznej w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu, są uprawnione osoby wykonujące zawód medyczny, konieczne jest dodatkowo nadawanie upoważnień przez administratora, czy wystarczy, że uprawnienie dla lekarza — w tym lekarza wykonującego swoją pracę na podstawie umowy cywilno-prawnej — do przetwarzania danych osobowych, znajdujących się w dokumentacji medycznej pacjenta, wynika z przywołanego powyżej przepisu.

Przepisy RODO (art. 29 oraz art. 32 ust. 4) zobowiązują administratora, aby miał kontrolę (władztwo) nad tym kto, w jakim zakresie ma dostęp do danych osobowych oraz na jakich zasadach i w jaki sposób je przetwarza. Innymi słowy dane osobowe mogą być przetwarzane wyłącznie na polecenie administratora przez osoby działające z upoważnienia administratora lub podmiotu przetwarzającego. Przyjmowane przez administratora i podmiot przetwarzający środki (działania) powinny służyć m.in. zapobieganiu nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych oraz zapewnieniu, że osoby uprawnione do korzystania z systemu

zautomatyzowanego przetwarzania będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem. Dzięki tym środkom osoby, które zostały dopuszczone do przetwarzania danych zostają poinformowane, jaki jest zakres ich uprawnień co do przetwarzania danych osobowych.

Wydawanie upoważnień może być jednym z takich środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania.

Dzięki takiemu rozwiązaniu administrator zapewnia kontrolę nad tym kto, z jakich powodów i w jaki sposób ma dostęp do przetwarzanych danych osobowych oraz jakich czynności na danych może dokonywać.

W powyższym pytaniu pojawiła się opinia, że nie ma potrzeby nadawania upoważnień do danych osobowych pacjenta osobom wykonującym zawód medyczny (np. lekarz, pielęgniarka, stomatolog), bowiem do przetwarzania tych danych osoby te uprawnia art. 24 ust. 2 pkt 1 ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta. Zgodnie z tym przepisem do przetwarzania danych zawartych w dokumentacji medycznej w celu ochrony zdrowia, udzielania oraz zarządzania udzielaniem świadczeń zdrowotnych, utrzymania systemu teleinformatycznego, w którym przetwarzana jest dokumentacja medyczna, i zapewnienia bezpieczeństwa tego systemu, są uprawnione osoby wykonujące zawód medyczny.

Odnosząc się do tego zagadnienia wskazać należy, że w przypadku nadawania upoważnień do przetwarzania danych osobowych osobom, których uprawnienia do przetwarzania danych osobowych wynikają z odrębnych przepisów, należy mieć na względzie cel, w jakim takie upoważnienia się nadaje. Jak wyżej wskazano wydawanie upoważnień może być bowiem jednym ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania zgodnie z art. 29 i art. 32 ust. 4 RODO i dlatego należy go odróżnić od uprawnienia do dostępu do danych osobowych przyznanego określonym funkcjom czy zawodom przez przepisy prawa w związku z wykonywanymi przez nich obowiązkami lub zadaniami.

Zatem jeśli administrator decyduje się na zastosowanie środka organizacyjnego, jakim jest nadawanie upoważnień, wówczas również wobec np. lekarzy może być podjęty taki środek, niezależnie od tego, że uprawnienie tych osób do dostępu do danych osobowych pacjenta gwarantują im właściwe ustawy.

Wskazany w art. 29 oraz art. 32 ust. 4 RODO wyjątek od związania poleceniem administratora (wynikający z przepisów prawa Unii lub prawa państwa członkowskiego) dotyczy przypadków zobowiązania do przetwarzania płynącego z przepisów unijnych lub krajowych, nie zaś upoważnienia z nich wynikającego, np. udzielenia określonej informacji na żądanie sądu

w ramach prowadzonego postępowania sądowego czy organom nadzoru w ramach postępowań kontrolnych.

Podsumowując należy stwierdzić, że w przypadku lekarzy (tak jak w przypadku sędziów i innych grup zawodowych, których uprawnienia do przetwarzania danych wynikają z odrębnych przepisów) mogą być nadawane upoważnienia do przetwarzania danych osobowych, jeśli administrator decyduje się właśnie w ten sposób realizować swoje obowiązki z art. 29 i 32 ust. 4 RODO.

W związku z powyższym należy przyjąć, że w odniesieniu do osób wykonujących zawody medyczne administrator nie musi nadawać upoważnienia tylko wtedy, gdy jest w stanie wykazać, że w inny skuteczny sposób zapewnia, że dane osobowe są przetwarzane wyłącznie na polecenie administratora przez osoby działające z upoważnienia administratora (zgodnie z art. 29 i art. 32 ust. 4 RODO). Niezależnie jaki środek organizacyjny obierze administrator musi być bowiem w stanie wykazać, że realizuje wskazane powyżej obowiązki z art. 29 i 32 ust. 4 RODO.

Odnosząc się zaś do drugiej kwestii, tj. czy wyżej wskazane zasady odnoszą się również do lekarzy współpracujących z administratorem, np. szpitalem na podstawie umowy cywilno-prawnej wskazać należy, że w kontekście tego pytania istotne jest, że zakres zadań osób wykonujących zawody medyczne, prowadzących działalność gospodarczą i pozostającej z podmiotem leczniczym w stosunku współpracy, jest najczęściej tożsamy z zakresem zadań pracowników zatrudnionych przez placówkę na innej podstawie (np. na podstawie umowy o pracę). W szczególności osoby wykonujące zawód w tej formie nie prowadzą własnej dokumentacji medycznej, lecz prowadzą ją w imieniu administratora. Umowa z podmiotem leczniczym zwykle zobowiązuje je do przestrzegania regulaminów podmiotu leczniczego i jego wewnętrznych procedur.

Jednym z warunków kwalifikowania danej relacji jako relacji administrator - podmiot przetwarzający jest to posiadanie przez podmiot przetwarzający statusu odrębnego (zewnętrznego) podmiotu od administratora. Dlatego pracownicy i inne osoby, które działają pod bezpośrednim zwierzchnictwem administratora (na przykład tymczasowo zatrudnieni pracownicy) nie są podmiotami przetwarzającymi, ponieważ przetwarzają dane będąc częścią organizacji administratora. Zgodnie z art. 29 RODO są one również związane instrukcjami administratora.

W przypadku, gdy działalność jest wykonywana przez lekarza w siedzibie podmiotu leczniczego i jest to swego rodzaju quasi zatrudnienie, to lekarz taki nie ma statusu podmiotu odrębnego od administratora danych. Jako że działalność ta może być wykonywana wyłącznie w zakładzie leczniczym na podstawie umowy z podmiotem leczniczym, stanowi ona substytut zatrudnienia. Inny słowy w przypadku lekarza zatrudnionego na kontrakcie tj. umowie cywilnej mamy do czynienia niejako z sytuacją pracodawca – pracownik i nie należy takiego lekarza traktować ani jako osobnego administratora ani jako podmiotu przetwarzającego.

Również w piśmiennictwie wskazuje się[1], że „na podmiocie leczniczym może ciążyć prawny obowiązek prowadzenia i przechowywania dokumentacji medycznej, nie zawsze jednak będzie on administratorem danych. Za administratora nie należy uważać osoby wykonującej zawód medyczny, prowadzącej działalność gospodarczą i pozostającej z podmiotem leczniczym w stosunku współpracy. Lekarze oraz pielęgniarki prowadzący indywidualną praktykę lekarską, wykonują zawód medyczny i mają prawny obowiązek prowadzenia dokumentacji medycznej, ale robią to w imieniu i na rzecz podmiotu leczniczego, który kieruje ruchem pacjentów i nierzadko zapewnia też odpowiednie zasoby techniczne i organizacyjne do udzielania świadczeń zdrowotnych. W takim przypadku nie mamy do czynienia ani z administratorem, ani z podmiotem przetwarzającym dane (procesorem). Osoby te powinny zostać potraktowane jako personel administratora i upoważnione do przetwarzania danych (ponieważ na tych osobach ciąży ustawowy obowiązek zachowania danych w tajemnicy, nie ma konieczności składania oświadczeń o zachowaniu poufności).”

A zatem - wprawdzie w każdym konkretnym stanie faktycznym należy starannie analizować podstawy, cele i poszczególne obowiązki podmiotów w danym procesie przetwarzania danych, ale są zasadne podstawy do uznania, że osoba wykonująca zawód medyczny, prowadząca jednoosobową działalność gospodarczą, pozostająca w stosunku prawnym z placówką medyczną, w zakresie w jakim wykonuje swoje zadania w ramach działalności leczniczej prowadzonej przez tą placówkę, nie jest ani innym administratorem ani podmiotem przetwarzającym. Co daje podstawy, aby stosować w stosunku do takiej osoby zasady przedstawione w pierwszej części odpowiedzi.

Zastrzec jednak należy, że w określonych sytuacjach możliwa będzie inna ocena statusu osoby wykonującej zawód medyczny. Zdarzyć się bowiem może, że np. osoba taka realizuje cele danego szpitala, ale również własne cele prowadząc za zgodą szpitala i na jego terenie indywidualną praktykę jako osobny podmiot wykonujący działalność leczniczą w rozumieniu art. 2 ust. 1 pkt 5, art. 4 i 5 ustawy o działalności leczniczej. Podmiotem wykonującym działalność leczniczą mogą być m.in. lekarz, pielęgniarka lub fizjoterapeuta wykonujący zawód w ramach działalności leczniczej jako praktykę zawodową. W każdej sytuacji koniecznie zatem brać trzeba pod uwagę konkretne okoliczności mające wpływ na ocenę charakteru działalności i celów realizowanych przez osobę wykonującą zawód medyczny, a tym samym jej statusu w świetle przepisów o ochronie danych osobowych.

Więcej informacji na temat upoważnień do przetwarzania danych w świetle przepisów RODO, można znaleźć na naszej stronie internetowej w zakładce Inspektor Ochrony Danych w pytaniach:

CZY ADMINISTRATOR POWINIEN UDZIELAĆ UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH?

[1] Korulczyk Katarzyna, Umowy powierzenia danych medycznych, Opublikowano: LEX/el. 2018

CZY ADMINISTRATOR POWINIEN NADAWAĆ UPOWAŻNIENIA NP. SĘDZIOM?

CZY IOD MOŻE NADAWAĆ UPOWAŻNIENIA?

CZY ELEKTRONICZNA POSTAĆ UPOWAŻNIENIA SPEŁNIA WYMOGI „PISEMNEGO UPOWAŻNIENIA”?

Data wytworzenia informacji: 30.06.2020 r.

Jaka jest podstawa przetwarzania danych członków rodziny pracownika korzystającego z ZFŚS?

Pracownicy, składając wniosek o uzyskanie świadczenia z ZFŚS i przedstawiając dane o swojej sytuacji życiowej, rodzinnej i materialnej, podają również dane członków swojej rodziny. Zastanawiam się, jaka jest podstawa prawna przetwarzania danych tych osób (dane małżonka, dzieci pracownika)? Czy właściwą przesłanką jest zgoda?

Zgodnie z przepisami ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, zarówno przyznawanie świadczeń, jak i ich wysokość uzależnione są od spełnienia przez osobę ubiegającą się o dane świadczenie określonych kryteriów socjalnych. Artykuł 8 ust. 1 wspomnianej ustawy zobowiązuje pracodawcę do tego, by uzależnił udzielenie ulgi lub świadczenia od sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu. A zatem podstawami uprawniającymi pracodawców do przetwarzania danych na potrzeby przyznania ulgowej usługi i świadczenia oraz dopłaty z zakładowego funduszu świadczeń socjalnych oraz ustalenia ich wysokości są art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. b RODO w połączeniu z właściwym, wyżej wskazanym przepisem ustawy o zakładowym funduszu świadczeń socjalnych.

Pracodawca nie powinien zatem pozyskiwać zgody na przetwarzanie danych osobowych od członków rodziny pracownika, bowiem żeby przyznać pracownikowi świadczenie z zakładowego funduszu świadczeń socjalnych, pracodawca musi poznać i ocenić sytuację życiową i materialną pracownika oraz członków jego rodziny, z którymi prowadzi on wspólne gospodarstwo domowe. W celu realizacji tych potrzeb musi więc przetwarzać dane osobowe tych osób, ale tylko te dane, które są niezbędne dla realizacji celu, w jakim je pozyskał.

Więcej informacji w zakresie przetwarzania danych osobowych w związku z prowadzeniem ZFŚS przez pracodawcę znajduje się w komunikacie UODO dostępnym pod linkiem: https://uodo.gov.pl/pl/138/1360 – **tekst w ramce poniżej**

Data wytworzenia informacji: 28.07.2020 r.

Informacja ze strony archiwalnej UODO

Jeśli pracodawca prowadzi ZFŚS, dotyczy go także RODO

Żeby przyznać pracownikowi świadczenie z zakładowego funduszu świadczeń socjalnych, pracodawca musi poznać i ocenić sytuację życiową i materialną pracownika oraz członków jego rodziny, z którymi prowadzi wspólne gospodarstwo domowe. W celu realizacji tych potrzeb musi więc przetwarzać dane osobowe tych osób, ale tylko te dane, które są niezbędne dla realizacji celu, w jakim je pozyskał. Pracodawca jest zobowiązany również do dokonywania przeglądu tych danych co najmniej raz w roku.

Warto zwrócić uwagę, że obowiązujące od 4 maja 2019 r. zmiany w ustawie o zakładowym funduszu świadczeń socjalnych (dalej: ustawa ZFŚS) nie wpływają na zmianę stanowiska Urzędu Ochrony Danych Osobowych dotyczącego zasad przetwarzania danych na potrzeby korzystania z usług i świadczeń finansowanych z zakładowego funduszu świadczeń socjalnych.

Pracodawca prowadzący ZFŚS ma prawo przetwarzać dane pracowników…

Zgodnie z przepisami tej ustawy, zarówno przyznawanie świadczeń, jak i ich wysokość uzależnione są od spełnienia przez osobę ubiegającą się o dane świadczenie określonych kryteriów socjalnych. Artykuł 8 ust. 1 wspomnianej ustawy zobowiązuje pracodawcę do tego, by uzależnił udzielenie ulgi lub świadczenia od sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu.

Oznacza to, że pracodawca musi poznać i ocenić sytuację życiową, a także materialną wszystkich członków rodziny pracownika, z którymi prowadzi on wspólne gospodarstwo domowe. Dlatego też w celu realizacji tych potrzeb musi przetwarzać dane osobowe pracownika i członków jego rodziny. Przetwarzanie tych danych nie może jednak prowadzić do gromadzenia ich w zakresie szerszym, niż jest to konieczne dla realizacji celu, w jakim dane te są pozyskiwane. Dodany w 2019 roku art. 8 ust. 1a ustawy określa, że pracownik przekazuje te dane pracodawcy w formie oświadczenia. Natomiast potwierdzenie danych w nim zawartych może odbywać się m.in. na podstawie oświadczeń i zaświadczeń o sytuacji życiowej.

… ale tylko w takim zakresie, jaki jest niezbędny do realizacji celów

W opinii UODO, jeżeli na potrzeby udokumentowania spełnienia określonych kryteriów przydatny byłby dostęp do różnych dokumentów, np. PIT-u małżonka, to powołana regulacja umożliwia pracodawcy jedynie wgląd do nich, ale nie daje prawa do przechowywania ich kopii czy innego utrwalania. Powodowałoby to gromadzenie danych w szerszym zakresie niż jest to niezbędne do celu przetwarzania. PIT współmałżonka to dokument zawierający również takie dane, jak np. nazwa zakładu pracy czy numer PESEL, które nie są niezbędne do potwierdzenia danych przedstawionych w oświadczeniu pracownika.

Tymczasem administratorzy, przetwarzając dane osobowe, nie powinni też zapominać o zasadach określonych w ogólnym rozporządzeniu o ochronie danych (RODO). Jedną z nich jest zasada minimalizacji danych, zgodnie z którą dane muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Przyjęło się, że adekwatność danych w stosunku do celu ich przetwarzania powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swymi danymi a interesem administratora (w tym przypadku pracodawcy).

Przepisy ustawy o ZFŚS nigdzie nie wskazują, by członkowie rodzin pracowników musieli podpisywać dodatkowe oświadczenia. Z regulacji tych wynika, że oświadczenie na temat sytuacji rodzinnej, życiowej i materialnej przedstawia pracownik.

Powyższe wyjaśnienia mają zastosowanie również w odniesieniu do przetwarzania danych o stanie zdrowia.

ZFŚS a RODO

Podstawami uprawniającymi pracodawców do przetwarzania danych na potrzeby przyznania ulgowej usługi i świadczenia oraz dopłaty z zakładowego funduszu świadczeń socjalnych i ustalenia ich wysokości są art. 6 ust. 1 lit. c oraz art. 9 ust. 2 lit. b RODO.

Pierwszy z powołanych przepisów legalizuje przetwarzanie danych osobowych, gdy jest ono niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Drugi natomiast ma zastosowanie w przypadku przetwarzania szczególnych kategorii danych (np. dotyczących zdrowia). Umożliwia on przetwarzanie takich danych, gdy jest to 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.

Pracodawca musi co najmniej raz w roku sprawdzić, jakie dane przetwarza

Przepisy ustawy o ZFŚS zakładają, że pracodawca w ramach Funduszu przetwarza dane osobowe przez okres niezbędny do przyznania ulgowej usługi i świadczenia czy też dopłaty z tego źródła oraz ustalenia ich wysokości, a także przez okres niezbędny do dochodzenia praw lub roszczeń (np. zobowiązania podatkowe ulegają przedawnieniu po pięciu latach).

Od 4 maja 2019 r. nowe przepisy nakładają również obowiązek dokonywania przez pracodawcę przeglądu danych osobowych zawartych w dokumentacji wytworzonej w ramach prowadzenia Funduszu – nie rzadziej niż raz w roku kalendarzowym, w celu ustalenia niezbędności ich dalszego przechowywania. Pracodawca jest zobowiązany również mocą powyższych przepisów do usuwania danych osobowych, których dalsze przechowywanie jest zbędne.

Prezes UODO wskazuje, że RODO wymaga nieprzerwanego, ciągłego, prawidłowego przetwarzania danych, w każdym procesie wykonywania operacji na danych. Nie wystarczy więc dokonać jednorazowego przeglądu danych w istniejących zasobach. Przepisy te nakazują pracodawcy usuwać dane osobowe, których dalsze przechowywanie jest zbędne, jest ściśle związane z zasadą ograniczenia celu (art. 5 ust. 1 lit. b RODO), tj. przyznawanie świadczeń socjalno-bytowych w ramach działania Funduszu.

W praktyce oznacza to, że zarówno w podmiotach publicznych, jak i niepublicznych, pracodawcy prowadzący ZFŚS muszą dokonywać corocznych przeglądów, aby zweryfikować, czy przetwarzają jedynie dane niezbędne do realizacji celów świadczeń socjalnych swoich pracowników. Co ważne, przegląd dotyczy całości dokumentacji.

Pracodawca nie może zapomnieć o archiwizacji, jeśli dotyczy go ten wymóg

W przypadku pracodawcy będącego podmiotem publicznym, który zgodnie z ustawą o narodowym zasobie archiwalnym i archiwach ma obowiązek archiwizowania wytworzonej dokumentacji, istotne

znaczenie przy realizacji obowiązków wynikających z ustawy o ZFŚS będą miały przepisy dotyczące archiwizacji. Oznacza to, że jeżeli dokumentacji z działania Funduszu zostanie przypisana kategoria archiwizacyjna z jednolitego rzeczowego wykazu akt, to dokumenty niezbędne do realizacji celów, dla których prowadzony jest Fundusz będą musiały być przechowywane przez określony w tej kategorii czas. Wówczas nie można ich zniszczyć aż do czasu, kiedy będą one podlegały brakowaniu. Zatem podmioty publiczne będą realizowały zarówno cele związane z ochroną danych osobowych w ramach działania Funduszu, jak i cele archiwizacyjne.

Odnosząc się natomiast do pracodawców działających jako podmioty prywatne, będą oni realizować jedynie obowiązki wynikające z ustawy o ZFŚS. Zgodnie z zasadą celowości pracodawcy mający status podmiotu prywatnego są zobowiązani dokonywać minimum raz w roku przeglądu danych osobowych oraz usuwać te dane, które dla celów związanych z prowadzeniem Funduszu są zbędne.

Czy z dokumentacji pracowniczej należy usuwać dane nadmiarowe?

Czy zasada minimalizacji danych oznacza, że z dokumentacji pracowniczej należy usuwać dane nadmiarowe, które zostały pozyskane jeszcze przed rozpoczęciem stosowania RODO? Czyli, czy konieczne jest zanonimizowanie danych pracowników (w tym także znajdujących się w archiwum zakładowym) pozyskanych wcześniej na podstawie obowiązujących przepisów, skoro teraz już nie ma podstawy prawnej do ich gromadzenia?

Prowadzenie dokumentacji pracowniczej to kwestia, którą regulują przepisy prawa pracy. To, w jaki sposób i jak długo należy przetwarzać dane osobowe pracowników oraz przechowywać dokumenty wchodzące w skład zasobu kadrowego, określają przepisy sektorowe. To z ich uwzględnieniem należy stosować zasady, o których mowa w ogólnym rozporządzeniu o ochronie danych. Dane osobowe wchodzące w skład dokumentacji pracowniczej nie muszą być usuwane z akt osobowych pracownika, jeżeli zostały zebrane zgodnie z przepisami obowiązującymi w chwili ich pozyskania.

Od 1 stycznia 2019 r. obowiązują nowe przepisy dotyczące dokumentacji pracowniczej, tj. rozporządzenie Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej. Mają one zastosowanie do dokumentacji pracowników, których stosunek pracy został nawiązany począwszy od 1 stycznia 2019 r. (§ 19). Natomiast do dokumentacji w sprawach związanych ze stosunkiem pracy oraz akt osobowych pracowników, pozostających w dniu wejścia w życie ww. rozporządzenia w stosunku pracy, zgromadzonych przed tym dniem, odnośnie do zakresu przetwarzanych danych stosuje się przepisy obowiązujące przed dniem wejścia w życie niniejszego rozporządzenia, tj. przepisy obowiązujące w dniu pozyskania danych (§ 20 ust. 1). Warto dodać, że od 1 stycznia 2019 r. obowiązują również przepisy ustawy z 10 stycznia 2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu

przechowywania akt pracowniczych oraz ich elektronizacją, które przewidują skrócenie (w zależności od tego, kiedy pracownik został zatrudniony) dotychczas obowiązujących terminów przechowywania dokumentacji pracowniczej.

Odnosząc się do realizacji zasady minimalizacji danych (art. 5 ust. 1 lit. c RODO) oraz usuwania danych nadmiarowych znajdujących się w teczkach osobowych pracowników, wskazać należy, że w przypadku podmiotu publicznego, który – zgodnie z ustawą z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach dalej: ustawa o narodowym zasobie archiwalnym i archiwach), ma obowiązek archiwizowania wytworzonej dokumentacji – istotne znaczenie odnośnie do dokumentacji pracowniczej będą miały przepisy dotyczące archiwizacji. Oznacza to, że jeżeli dokumentacji pracowniczej zostanie przypisana kategoria archiwizacyjna z jednolitego rzeczowego wykazu akt, to dokumenty te będą musiały być przechowywane przez określony w tej kategorii czas. Art. 5 tej ustawy i przywołane przepisy wykonawcze przewidują, jaka dokumentacja, wytwarzana w organach państwowych i samorządowych, przekazywana jest po określonym czasie do właściwych archiwów państwowych, a jaka może ulec – po spełnieniu określonych w ustawie warunków – brakowaniu (dokumentacja niearchiwalna).

Zatem usuwanie danych z takiej dokumentacji będzie się odbywało dopiero w chwili jej brakowania, ponieważ podmioty te mają obowiązki wynikające z przepisów o narodowym zasobie archiwalnym i archiwach.

Podkreślenia wymaga, że art. 3 ustawy o narodowym zasobie archiwalnym i archiwach wskazuje, że materiały archiwalne stanowiące narodowy zasób archiwalny przechowuje się wieczyście. Dokumenty te podlegają ochronie przed uszkodzeniem z uwagi na ich wartość historyczną, co wiąże się z zapewnieniem im odpowiednich warunków gwarantujących ochronę przed utratą, uszkodzeniem lub zniszczeniem (zgodnie z art. 12 i 13 ustawy o narodowym zasobie archiwalnym i archiwach). Należy jednak zaznaczyć, że do narodowego zasobu archiwalnego nie zalicza się wszystkich dokumentów wytworzonych przez administrację publiczną, a jedynie taką dokumentację, która jest źródłem informacji o wartości historycznej.

Data wytworzenia informacji: 07.04.2020 r.

Czy z sołtysem należy zawierać umowę powierzenia?

Czy sołtys, który realizuje zadania publiczne, takie jak doręczanie korespondencji, decyzji podatkowych, czy realizuje zadania inkasenta, a w związku z tym posiada dostęp do danych osobowych, które znajdują się w dyspozycji wójta (administratora danych) będzie musiał mieć umowę powierzenia? Czy wystarczająca jest forma udzielenia mu przez wójta upoważnienia do przetwarzania danych osobowych?

Przy ocenie, czy w danej sytuacji administrator powinien udzielić upoważnienia do przetwarzania danych, czy zawrzeć umowę powierzenia przetwarzania, decydujące znaczenie ma charakter relacji łączącej te podmioty.

Zgodnie z art. 29 RODO, podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Przepis ten adresowany jest do podmiotów przetwarzających, a także do osób działających z upoważnienia administratora lub podmiotu przetwarzającego, mających dostęp do danych osobowych (pracowników, osób zatrudnionych na podstawie umów cywilnoprawnych, stażystów, praktykantów, wolontariuszy). Osoby te charakteryzuje pewna zależność od administratora. Właśnie takim osobom administrator może nadać imienne upoważnienie do przetwarzania danych, jeśli przyjął taki sposób wykazywania, że osoby te działają z jego upoważnienia.

Analizując natomiast zagadnienie powierzenia przetwarzania danych wskazać należy, że współpraca pomiędzy administratorem i podmiotem przetwarzającym nie zawiera w sobie podległości wobec administratora. Sytuacja taka występuje zazwyczaj w przypadku podejmowania współpracy z podmiotami prowadzącymi działalność gospodarczą w formie zarówno jednoosobowej działalności gospodarczej, jak i spółki. Przykładami takiej współpracy, w związku z którą powinna zostać zawarta umowa dotycząca powierzenia przetwarzania danych osobowych, jest współpraca z biurem księgowym czy firmą informatyczną.

Sołtys jest organem wykonawczym sołectwa, które jest jednostką pomocniczą gminy tworzoną przez radę gminy w drodze uchwały. Zgodnie z art. 35 ustawy o samorządzie gminnym, rada gminy w odrębnym statucie określa organizację i zakres działania jednostki pomocniczej. Statut powinien zawierać zaś m.in.: organizację oraz zadania jednostki pomocniczej, zakres zadań przekazywanych jednostce przez gminę i sposób ich realizacji, zakres i formy kontroli oraz nadzoru organów gminy nad działalnością organów jednostki pomocniczej.

Zgodnie z art. 6 ust. 12 i art. 19 ust. 2 ustawy podatkach i opłatach lokalnych, rada gminy może zarządzić pobór opłat i podatków lokalnych w drodze inkasa. W takiej uchwale, rada gminy może również określić inkasentów i wysokość wynagrodzenia za inkaso, a także może wprowadzić obowiązek prowadzenia przez inkasentów ewidencji osób, zobowiązanych do uiszczania opłaty miejscowej oraz określić szczegółowy zakres danych zawartych w tej ewidencji.

Zgodnie z art. 9 ustawy Ordynacja podatkowa, inkasentem jest osoba fizyczna, osoba prawna lub jednostka organizacyjna niemająca osobowości prawnej, obowiązana do pobrania od podatnika podatku i wpłacenia go we właściwym terminie organowi podatkowemu.

Zgodnie zaś z art. 144 § 4 ustawy Ordynacja podatkowa, w przypadku gdy organem podatkowym jest wójt, burmistrz (prezydent miasta), pisma może doręczać sołtys, za pokwitowaniem.

W przedstawionej w pytaniu sytuacji na inkasenta wyznaczony został sołtys. Pełni on też funkcję doręczyciela.

Sołtys, działając jako inkasent, przetwarza dane osobowe osób zobowiązanych do uiszczania opłat i podatków, zawarte w nakazach płatniczych, czy też otrzymanym wykazie mieszkańców miejscowości, kwitariuszu oraz prowadzonej przez siebie ewidencji. Zaś doręczając pisma, przetwarza dane ich adresatów.

Jak wyżej wskazano środki organizacyjne, którymi mogą być również upoważnienia, powinny dotyczyć nie tylko osób na stałe zatrudnionych u administratora danych, ale także osób, którym administrator zlecił określone prace i które z tego powodu mają mieć dostęp do danych osobowych.

Sołtys, jako osoba stojąca na czele sołectwa, będącego jednostką pomocniczą, nie jest co do zasady pracownikiem samorządowym. Przepisy prawa nie przewidują też zakazu zatrudniania sołtysa przez jego macierzystą gminę (tj. urząd gminny) na innym stanowisku na podstawie umowy o pracę lub na podstawie innych umów cywilno-prawnych.

Wobec powyższego można przyjąć, że w przypadku zlecenia sołtysowi zadań inkasenta lub doręczyciela właściwe będzie uznanie, iż wykonuje on te zadania w ramach quasi zatrudnienia, a co za tym idzie udzielenie mu upoważnienia do przetwarzania danych (o ile administrator przyjął je jako środek organizacyjny służący zapewnieniu kontroli nad dostępem do danych osobowych).

Podsumowując można przyjąć, że z jednej strony sołtys występuje jako wykonawca uchwał rady gminy, z drugiej reprezentuje sołectwo przed organami gminy.

Wobec powyższego w przypadkach gdy sołtys będzie działał w celu wykonywania zadań wskazanych w ustawach (np. ustawy Ordynacja podatkowa), uchwałach rady gminy, zarządzeniach wójta zgodnie z statutem sołectwa będzie on reprezentował gminę przed mieszkańcami i może działać na podstawie upoważnienia od wójta np. jako inkasent lub doręczyciel. Gdy sołtys będzie realizował inne zadania wynikające ze statutu sołectwa związane z reprezentacją mieszkańców sołectwa przed gminą, wówczas dojść może do sytuacji, w której sołtys lub sołectwo – ze względu na okoliczności danego przypadku – będzie mogło zostać uznane za administratora.

Data wytworzenia informacji: 28.07.2020 r.

Kto jest administratorem w przypadku PKZP działającej przy pracodawcy?

Który podmiot należy uznać za administratora danych przetwarzanych w ramach działalności Pracowniczej Kasy Zapomogowo – Pożyczkowej działającej przy pracodawcy? Czy między PKZP a pracodawcą, jeśli PKZP uzna się za administratora danych, powinna być zawarta umowa powierzania przetwarzania danych osobowych ? Czy w statucie PKZP można zawrzeć informację, że do przetwarzania danych osobowych stosuje się zasady opisane w Polityce Ochrony Danych obowiązującej u pracodawcy?

Przesądzenie, jaki jest status Pracowniczej Kasy Zapomogowo-Pożyczkowej (PKZP) działającej u danego pracodawcy i który z podmiotów (PKZP czy zakład pracy) jest, w świetle przepisów o ochronie danych osobowych, administratorem danych osobowych przetwarzanych w związku z działaniem PKZP, wymaga przede wszystkim dokonania analizy konkretnych przepisów mających zastosowanie w określonej sytuacji. O tym, czy dany podmiot jest administratorem, decyduje przede wszystkim rodzaj i charakter nadanych mu przez prawo kompetencji oraz wyznaczone przepisami prawa zadania. Definicja administratora wskazuje, że jest nim osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych (art. 4 pkt 7 RODO).

W odniesieniu do pracodawcy to w ramach stosunku pracy powstają określone prawa i obowiązki pomiędzy pracodawcą a pracownikiem, których realizacja wiąże się z koniecznością przetwarzania danych pracownika (na podstawie odpowiednich przepisów Kodeksu pracy bądź też innych przepisów prawa).

Natomiast art. 39 ustawy z dnia z dnia 23 maja 1991 r. o związkach zawodowych przewiduje możliwość tworzenia u pracodawców PKZP. Członkami tych kas mogą być pracownicy, emeryci, renciści. Szczegółowe zasady organizowania i działania tych kas określa rozporządzenie Rady Ministrów z dnia 19 grudnia 1992 r. w sprawie pracowniczych kas zapomogowo-pożyczkowych oraz spółdzielczych kas oszczędnościowo-kredytowych w zakładach pracy (dalej: rozporządzenie w sprawie PKZP). Kasy te zostały powołane do udzielania jej członkom pomocy materialnej w formie pożyczek oraz zapomóg na zasadach określonych w statucie.

Zarówno pracodawca (zakład pracy), jak i PKZP, w zakresie przetwarzanych przez siebie danych osobowych, samodzielnie ustalają własne cele i sposoby ich przetwarzania, dlatego też zasadnie można uznać, że powinni być traktowani jako oddzielni administratorzy.

Natomiast w § 4 rozporządzenia w sprawie PKZP przewidziano pomoc ze strony pracodawcy (zakładu pracy) przy realizacji zadań PKZP (m.in. prowadzenia księgowości, obsługi kasowej i prawnej, dokonywania na rzecz PKZP potrąceń w listach płac, listach wypłat zasiłków chorobowych i zasiłków wychowawczych, wpisowego, wkładów miesięcznych i rat pożyczek,

przyjmowania wpłat wnoszonych przez emerytów i rencistów oraz osoby przebywające na urlopach wychowawczych, odprowadzania wpłat na rachunek bankowy PKZP oraz informowania przynajmniej raz w roku członków kas o stanie ich wkładów i zadłużeń), a szczegółowe warunki świadczonej pomocy ma określać umowa zawierana pomiędzy pracodawcą a PKZP. W ramach tak prawnie ukształtowanych relacji, można zasadnie uznać, że podmioty te współdziałają ze sobą, a zatem wspólnie ustalają cele i sposoby przetwarzania danych osobowych wykorzystywanych w tym celu, przetwarzają je więc jako współadministratorzy.

Dlatego nie ma podstaw, aby w opisanym przypadku zawierać umowy powierzenia przetwarzania danych. Podmiot przetwarzający ma bowiem zupełnie inny status – przetwarza dane osobowe w imieniu administratora i w tym zakresie podlega jego kontroli.

Dlatego też wzajemne relacje pomiędzy tymi podmiotami w kwestiach nieuregulowanych przepisami rozporządzenia w sprawie PKZP powinny być określone, np. w porozumieniu lub umowie pomiędzy uprawnionymi podmiotami. W drodze wspólnych uzgodnień podmioty te powinny w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. W myśl natomiast art. 26 ust. 2 RODO uzgodnienia, o których mowa w ust. 1, muszą należycie odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

Takie wspólne uzgodnienia muszą uwzględniać faktyczne obowiązki pracodawcy i PKZP związane z przetwarzaniem danych osobowych członków PKZP, wynikające m.in. z przepisów rozporządzenia w sprawie PKZP. Zarówno pracodawca, jak i PKZP mają swoje autonomiczne uprawnienia, z którymi związane jest przetwarzanie danych osobowych członków w innych celach. Przykładowo, jedynie PKZP reprezentowana przez zarząd uprawniona jest do podejmowania decyzji co do przyjmowania członków PKZP i skreślania ich z listy, przyznawania pożyczek i ustalania okresów ich spłaty, podejmowania decyzji w sprawie odroczenia spłaty pożyczek czy przyznawania zapomóg.

Pracodawca, w ramach współadministrowania, może być uprawniony, np. do zapewnienia ochrony pomieszczeń, prowadzenia księgowości, obsługi kasowej i prawnej, dokonywania na rzecz PKZP potrąceń w listach płac, listach wypłat zasiłków chorobowych i zasiłków wychowawczych, wpisowego, wkładów miesięcznych i rat pożyczek. Należy wskazać, że co do zasady odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych w zakresie

realizacji takich autonomicznych uprawnień kształtują przepisy prawa. Pracodawca i PKZP, w ramach wspólnych uzgodnień, powinni więc określić inne kwestie, nieuregulowane wprost w przepisach prawa, w tym m.in. kwestię nadawania upoważnień pracownikom wyznaczonym przez pracodawcę do prowadzenia księgowości, obsługi kasowej i prawnej PKZP, kwestię odpowiedniego zabezpieczenia danych osobowych członków PKZP czy też realizacji określonych obowiązków informacyjnych.

Dokonanie wspólnych ustaleń pomiędzy współadministratorami, o których mowa w art. 26 RODO, umożliwia doprecyzowanie sposobu obsługi technicznej PKZP przez pracodawcę przy zachowaniu autonomicznych kompetencji PKZP w zakresie jej odrębnych zadań jako administratora.

W nawiązaniu do zagadnienia dotyczącego możliwości zawarcia w statucie PKZP informacji, że do przetwarzania danych osobowych stosuje się zasady opisane w Polityce Ochrony Danych obowiązującej u pracodawcy należy wskazać, że 24 RODO nakłada na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających zgodność przetwarzania z wymogami tego rozporządzenia. Zgodnie z ust. 2 tego artykułu – jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania – powyższe środki powinny obejmować wdrożenie przez administratora odpowiednich polityk ochrony danych. Biorąc jednak pod uwagę wynikającą z RODO zasadę rozliczalności, to od decyzji administratora zależy, w jaki sposób skonstruuje funkcjonujący u siebie system ochrony danych osobowych. Istotne jest, aby przetwarzanie odbywało się zgodnie z RODO i aby administrator mógł to wykazać. Na naszej stronie internetowej w zakładce Inspektor Ochrony Danych można znaleźć wskazówki prowadzenia wspólnej polityki ochrony danych w przypadku funkcjonowania 2 administratorów danych w ramach jednej jednostki organizacyjnej (CZY KOMENDANT STRAŻY MIEJSKIEJ MUSI POSIADAĆ ODRĘBNĄ POLITYKĘ OCHRONY DANYCH?).

Data wytworzenia informacji: 28.07.2020 r.

Czy do pism w postępowaniu administracyjnym należy dołączać „rozdzielniki”?

Proszę o informację, jakie w tej chwili jest stanowisko UODO w sprawie rozdzielnika do decyzji administracyjnej. Czy w decyzji skierowanej do osoby fizycznej - strony postępowania umieszczamy wg rozdzielnika (do wiadomości) dane osobowe, tj. imię, nazwisko, adres innej osoby fizycznej będącej kolejną stroną w tym samym postępowaniu? Śledzę Waszą stronę na bieżąco, ale być może coś umknęło mej uwadze. Czy informację umieszczoną w drugim linku mam interpretować w ten sposób, że jednak strony postępowania umieszczamy pod decyzją?

https://archiwum.giodo.gov.pl/318/id_art/1838/j/pl – **tekst w ramce poniżej.**

Informacja ze strony archiwalnej GIODO

Czy rozsyłanie "rozdzielników" do uczestników postępowań administracyjnych nie narusza przepisów ustawy o ochronie danych osobowych?

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych osiągnięcie efektu zapewnienia stronom postępowania administracyjnego realizacji przysługujących im uprawnień (prawa do informacji na temat toczącego się postępowania) jest możliwe w inny sposób, np. poprzez wysyłanie pism (zawiadomień, postanowień, decyzji) bez załączania rozdzielnika otrzymujących je osób, który to wykaz jest ważny przede wszystkim dla organu prowadzącego postępowanie.

Uzasadnienie

Wprawdzie przepisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Kpa) przewidują dopuszczalność zapoznania się przez stronę w toku postępowania administracyjnego z danymi innych uczestników tego postępowania oraz nakładają na organy administracji publicznej obowiązek należytego i wyczerpującego informowania stron o okolicznościach faktycznych i prawnych, które mogą mieć wpływ na ustalenie ich praw i obowiązków będących przedmiotem postępowania administracyjnego, jednakże żaden z przepisów Kpa nie nakazuje umieszczania w korespondencji kierowanej do poszczególnych uczestników toczącego się postępowania, rozdzielnika zawierającego dane osobowe jego wszystkich uczestników.

Jedna ze spraw przedstawionych Generalnemu Inspektorowi dotyczyła udostępnienia osobom trzecim danych osoby, która kierując skargę do właściwego wojewody, zainicjowała postępowanie w sprawie dotyczącej legalności budowy, wszczęte przez Powiatowego Inspektora Nadzoru Budowlanego. Wysyłane do Skarżącej w trakcie tego postępowania zawiadomienia o oględzinach zawierały wykaz obejmujący dane osobowe (tj. imię i nazwisko) wszystkich ich adresatów.

Generalny Inspektor wskazał, że przepisy Kodeksu postępowania administracyjnego oraz Prawa budowlanego przewidują dopuszczalność przeprowadzenia, w toku postępowania administracyjnego, dowodu z oględzin, jak też określają też sposób przeprowadzenia tego rodzaju dowodu. Natomiast kwestię treści zawiadomienia o oględzinach regulują, ograniczając się do sformułowania wymogu, aby zawierało ono wskazanie miejsca i terminu oględzin. Przepisy nie nakazują natomiast umieszczania w korespondencji kierowanej do poszczególnych uczestników toczącego się postępowania wykazu zawierającego dane osobowe wszystkich pozostałych uczestników tegoż postępowania. Stosowanie takiej praktyki nie znajduje więc wyraźnego oparcia w przepisach obowiązującego prawa.

Powiatowy Inspektorat Nadzoru Budowlanego, do którego Generalny Inspektor Ochrony Danych Osobowych wystąpił w tej sprawie przychylił się do twierdzenia, że stosowanie sugerowanej przez Generalnego Inspektora praktyki leży zarówno w interesie urzędu jak i obywateli.

W związku z powyższym bezspornym pozostaje, że strony w toczącym się postępowaniu administracyjnym są uprawnione do zapoznawania się z informacjami zawartymi w materiale zgromadzonym w tym postępowaniu, w tym z danymi osobowymi identyfikującymi pozostałe strony. Jednakże oznaczenie wszystkich stron postępowania albo innych osób biorących udział w postępowaniu

powinno mieć miejsce w samej treści rozstrzygnięcia administracyjnego, nie zaś za pomocą rozdzielnika stanowiącego zbiorczą listę szczegółowych danych osobowych stron postępowania.

https://uodo.gov.pl/pl/138/561 - z tego linka odzyskanie treści nie jest możliwe

W obecnym stanie prawnym co do zasady aktualność zachowuje stanowisko prezentowane przez Generalnego Inspektora Ochrony Danych Osobowych jeszcze przed wejściem w życie RODO. Zgodnie z tym stanowiskiem, dołączanie do pism w postępowaniu administracyjnym „rozdzielników" zawierających dane wszystkich uczestników postępowania (w tym także osób niebędących stronami postępowania) jest błędną praktyką. Może bowiem prowadzić do ujawnienia danych osobowych w sposób naruszający przepisy procedury administracyjnej (stanowisko to zawarte jest w materiale „Czy rozsyłanie „rozdzielników" do uczestników postępowań administracyjnych nie narusza przepisów ustawy o ochronie danych osobowych?" dostępnym na archiwalnej stronie GIODO pod adresem https://archiwum.giodo.gov.pl/pl/400/1838) – **tekst w ramce poniżej.**

Informacja ze strony archiwalnej UODO

Czy rozsyłanie "rozdzielników" do uczestników postępowań administracyjnych nie narusza przepisów ustawy o ochronie danych osobowych?

Zdaniem Generalnego Inspektora Ochrony Danych Osobowych osiągnięcie efektu zapewnienia stronom postępowania administracyjnego realizacji przysługujących im uprawnień (prawa do informacji na temat toczącego się postępowania) jest możliwe w inny sposób, np. poprzez wysyłanie pism (zawiadomień, postanowień, decyzji) bez załączania rozdzielnika otrzymujących je osób, który to wykaz jest ważny przede wszystkim dla organu prowadzącego postępowanie.

Uzasadnienie

Wprawdzie przepisy ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Kpa) przewidują dopuszczalność zapoznania się przez stronę w toku postępowania administracyjnego z danymi innych uczestników tego postępowania oraz nakładają na organy administracji publicznej obowiązek należytego i wyczerpującego informowania stron o okolicznościach faktycznych i prawnych, które mogą mieć wpływ na ustalenie ich praw i obowiązków będących przedmiotem postępowania administracyjnego, jednakże żaden z przepisów Kpa nie nakazuje umieszczania w korespondencji kierowanej do poszczególnych uczestników toczącego się postępowania, rozdzielnika zawierającego dane osobowe jego wszystkich uczestników.

Jedna ze spraw przedstawionych Generalnemu Inspektorowi dotyczyła udostępnienia osobom trzecim danych osoby, która kierując skargę do właściwego wojewody, zainicjowała postępowanie w sprawie dotyczącej legalności budowy, wszczęte przez Powiatowego Inspektora Nadzoru Budowlanego. Wysyłane do Skarżącej w trakcie tego postępowania zawiadomienia o oględzinach zawierały wykaz obejmujący dane osobowe (tj. imię i nazwisko) wszystkich ich adresatów.

Generalny Inspektor wskazał, że przepisy Kodeksu postępowania administracyjnego oraz Prawa budowlanego przewidują dopuszczalność przeprowadzenia, w toku postępowania administracyjnego, dowodu z oględzin, jak też określają też sposób przeprowadzenia tego rodzaju dowodu. Natomiast kwestię treści zawiadomienia o oględzinach regulują, ograniczając się do sformułowania wymogu, aby zawierało ono wskazanie miejsca i terminu oględzin. Przepisy nie nakazują natomiast umieszczania w korespondencji kierowanej do poszczególnych uczestników toczącego się postępowania wykazu zawierającego dane osobowe wszystkich pozostałych uczestników tegoż postępowania. Stosowanie takiej praktyki nie znajduje więc wyraźnego oparcia w przepisach obowiązującego prawa.

Powiatowy Inspektorat Nadzoru Budowlanego, do którego Generalny Inspektor Ochrony Danych Osobowych wystąpił w tej sprawie przychylił się do twierdzenia, że stosowanie sugerowanej przez Generalnego Inspektora praktyki leży zarówno w interesie urzędu jak i obywateli.

W związku z powyższym bezspornym pozostaje, że strony w toczącym się postępowaniu administracyjnym są uprawnione do zapoznawania się z informacjami zawartymi w materiale zgromadzonym w tym postępowaniu, w tym z danymi osobowymi identyfikującymi pozostałe strony. Jednakże oznaczenie wszystkich stron postępowania albo innych osób biorących udział w postępowaniu powinno mieć miejsce w samej treści rozstrzygnięcia administracyjnego, nie zaś za pomocą rozdzielnika stanowiącego zbiorczą listę szczegółowych danych osobowych stron postępowania.

GIODO wskazywał w nim, iż osiągnięcie efektu zapewnienia stronom postępowania administracyjnego realizacji przysługujących im uprawnień (prawa do informacji na temat toczącego się postępowania) jest możliwe poprzez wysyłanie pism (zawiadomień, postanowień, decyzji) bez załączania rozdzielnika otrzymujących je osób, który to wykaz jest ważny głównie dla organu prowadzącego postępowanie. GIODO podkreślił w swym stanowisku, iż wprawdzie przepisy KPA przewidują dopuszczalność zapoznania się przez stronę w toku postępowania administracyjnego z danymi innych uczestników tego postępowania oraz nakładają na organy administracji publicznej obowiązek należytego i wyczerpującego informowania stron o okolicznościach faktycznych i prawnych, które mogą mieć wpływ na ustalenie ich praw i obowiązków będących przedmiotem postępowania administracyjnego, jednak żaden z przepisów KPA nie nakazuje umieszczania w korespondencji kierowanej do poszczególnych uczestników toczącego się postępowania rozdzielnika zawierającego dane osobowe jego wszystkich uczestników. W związku z tym bezsporne pozostaje, że strony w toczącym się postępowaniu administracyjnym są uprawnione do zapoznawania się z informacjami zawartymi w materiale zgromadzonym w tym postępowaniu, w tym z danymi osobowymi identyfikującymi pozostałe strony. Jednak oznaczenie wszystkich stron postępowania albo innych osób biorących udział w postępowaniu powinno mieć miejsce w samej treści rozstrzygnięcia administracyjnego, nie zaś za pomocą odrębnych wykazów zawierających szczegółowe dane osobowe.

Zaznaczyć także należy, że oznaczenie stron postępowania musi spełniać wymogi zasady minimalizacji danych, o której mowa w art. 5 ust. 1 lit. c RODO – m.in. co do zasady nie powinno zawierać numeru PESEL.

Data wytworzenia informacji: 10.08.2020 r.

Jaka jest podstawa do przetwarzania przez poradnie psychologiczne szczególnych kategorii danych?

Czy poradnie psychologiczno-pedagogiczne, przetwarzając dane o stanie zdrowia na potrzeby realizowanej pomocy psychologiczno-pedagogicznej (w tym przeprowadzania diagnozy i sporządzania opinii oraz orzeczeń), mogą stosować którąkolwiek inną przesłankę, niż określona w art. 9 ust. 2 lit. a RODO?

Europejska Rada Ochrony Danych w wytycznych z 4 maja 2020 r. dotyczących zgody wskazała, że administratorzy, chcąc przetwarzać szczególne kategorie danych osobowych, w pierwszej kolejności powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b)–j) RODO. Jeżeli żaden z nich nie będzie miał zastosowania, wówczas jedyną możliwą przesłanką uprawniającą do przetwarzania takich danych jest uzyskanie wyraźniej zgody, spełniającej przewidziane w RODO warunki (wytyczne dostępne są na stronie Europejskiej Rady Ochrony Danych pod linkiem: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl). Wobec powyższego zanim administrator podejmie decyzję, aby opierać przetwarzanie szczególnych kategorii danych na zgodzie, powinien wcześniej dokonać analizy innych przesłanek.

Przepisy regulujące działalność poradni psychologiczno-pedagogicznych znaleźć można przede wszystkim w ustawie Prawo oświatowe oraz w rozporządzeniach wykonawczych.

Zgodnie z art. 2 pkt 6 ustawy Prawo oświatowe, poradnie psychologiczno-pedagogiczne, w tym poradnie specjalistyczne, udzielające dzieciom, młodzieży, rodzicom i nauczycielom pomocy psychologiczno-pedagogicznej, a także pomocy uczniom w wyborze kierunku kształcenia i zawodu, wchodzą w skład systemu oświaty.

Ustawa Prawo oświatowe nie zawiera kompleksowego uregulowania zasad działania poradni psychologiczno-pedagogicznych. W ustawie tej znaleźć można natomiast przepisy, z których wynika, iż w określonych sytuacjach niezbędne jest przedstawienie opinii lub orzeczenia wydanego przez taką poradnię, np. zgodnie z art. 36 ust. 1 i 2, na wniosek rodziców naukę w szkole podstawowej może także rozpocząć dziecko, które w danym roku kalendarzowym kończy 6 lat, jeżeli dziecko posiada opinię o możliwości rozpoczęcia nauki w szkole podstawowej, wydaną przez publiczną poradnię psychologiczno-pedagogiczną albo niepubliczną poradnię

psychologiczno-pedagogiczną. Zgodnie zaś z art. 115 ust. 1, na wniosek lub za zgodą rodziców albo pełnoletniego ucznia dyrektor szkoły, po zasięgnięciu opinii rady pedagogicznej i publicznej poradni psychologiczno-pedagogicznej, w tym poradni specjalistycznej, może zezwolić uczniowi na indywidualny program lub tok nauki oraz wyznaczyć nauczyciela – opiekuna.

W innych przepisach ustawy wskazywane są zaś uprawnienia poradni publicznych i niepublicznych do wydawania określonych opinii oraz orzeczeń. Zgodnie np. z art. 127 ust. 10, opinie o potrzebie wczesnego wspomagania rozwoju dziecka oraz orzeczenia o potrzebie kształcenia specjalnego albo indywidualnego obowiązkowego rocznego przygotowania przedszkolnego i indywidualnego nauczania, a także o potrzebie zajęć rewalidacyjno-wychowawczych wydają zespoły orzekające działające w publicznych poradniach psychologiczno-pedagogicznych, w tym w poradniach specjalistycznych. Przepis ten określa również, jakie informacje powinno zawierać orzeczenie o potrzebie kształcenia specjalnego.

Zgodnie natomiast z ustępem 11 powyższego przepisu, opinie w sprawie dostosowania wymagań edukacyjnych wynikających z programu nauczania do indywidualnych potrzeb ucznia, u którego stwierdzono specyficzne trudności w uczeniu się, uniemożliwiające sprostanie tym wymaganiom, wydają również niepubliczne poradnie psychologiczno-pedagogiczne, w tym niepubliczne specjalistyczne poradnie psychologiczno-pedagogiczne.

Szczegółowe zasady działania poradni publicznych oraz wydawania przez nie orzeczeń i opinii zawarte są w rozporządzeniach wykonawczych, w szczególności w rozporządzeniu Ministra Edukacji Narodowej z dnia 1 lutego 2013 r. w sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, w tym publicznych poradni specjalistycznych oraz w rozporządzeniu Ministra Edukacji Narodowej z dnia 7 września 2017 r. w sprawie orzeczeń i opinii wydawanych przez zespoły orzekające działające w publicznych poradniach psychologiczno-pedagogicznych.

Zgodnie z § 1 rozporządzenia w sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, poradnie psychologiczno-pedagogiczne diagnozują dzieci i młodzież oraz udzielają dzieciom i młodzieży oraz rodzicom bezpośredniej pomocy psychologiczno-pedagogicznej. Ponadto realizują zadania profilaktyczne i wspierające wychowawczą i edukacyjną funkcję przedszkola, szkoły i placówki, w tym wspierają nauczycieli w rozwiązywaniu problemów dydaktycznych i wychowawczych. Poradnie psychologiczno-pedagogiczne również organizują i prowadzą wspomaganie przedszkoli, szkół i placówek w zakresie realizacji zadań dydaktycznych, wychowawczych i opiekuńczych.

Efektem diagnozowania dzieci i uczniów są m.in. wydawane przez poradnie opinie oraz orzeczenia. Zgodnie § 5 rozporządzenia w sprawie orzeczeń i opinii wydawanych przez zespoły orzekające działające w publicznych poradniach psychologiczno-pedagogicznych, poradnia wydaje opinię i orzeczenie na pisemny wniosek rodzica dziecka albo pełnoletniego ucznia. Złożenie

takiego wniosku nie jest obowiązkowe, tak samo jak korzystanie z pomocy, którą oferuje poradnia. Jest to dobrowolna decyzja rodziców dziecka albo pełnoletniego ucznia. W § 6 tego rozporządzenia wskazano informacje, jakie powinien zawierać wniosek o wydanie opinii lub orzeczenia. Zgodnie z ust. 4 tego przepisu, jeżeli do wydania orzeczenia lub opinii jest niezbędna informacja o stanie zdrowia dziecka lub ucznia, wnioskodawca dołącza do wniosku wydane przez lekarza zaświadczenie o stanie zdrowia dziecka lub ucznia.

W celu udzielania przez poradnie pomocy psychologiczno-pedagogicznej, o której mowa w ustawie Prawo oświatowe, niezbędne jest przetwarzanie danych osobowych, w tym szczególnych kategorii tych danych (np. informacji o stanie zdrowia).

W przypadku przetwarzania przez poradnię szczególnych kategorii danych w celu udzielenia pomocy psychologiczno-pedagogicznej przesłankę legalizującą stanowić będzie art. 9 ust. 2 lit. g RODO, tj. przetwarzanie to jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. W przypadku tej przesłanki niezbędne jest wskazywanie dodatkowo przepisów prawa konkretyzujących zadania poradni.

Z inną sytuacją mamy do czynienia wówczas, gdy rodzice podejmują decyzję o tym, że złożą orzeczenie lub opinię w jednostce systemu oświaty, do której uczęszcza ich dziecko. Zgodnie bowiem z § 6 ust. 2 rozporządzenia w sprawie szczegółowych zasad działania publicznych poradni psychologiczno-pedagogicznych, w tym publicznych poradni specjalistycznych w przypadku, gdy opinia dotyczy dziecka uczęszczającego do przedszkola, szkoły lub placówki albo pełnoletniego ucznia uczęszczającego do szkoły lub placówki, na pisemny wniosek odpowiednio rodziców albo pełnoletniego ucznia, poradnia przekazuje kopię opinii do przedszkola, szkoły lub placówki, do której dziecko albo pełnoletni uczeń uczęszcza. Oznacza to, że dane dotyczące dziecka są przekazywane między ww. administratorami jedynie na podstawie zgody rodziców albo pełnoletniego ucznia.

Uwagę zwrócić także należy na treść § 6 ust. 2 pkt 1 powołanego wyżej rozporządzenia w sprawie orzeczeń i opinii wydawanych przez zespoły orzekające działające w publicznych poradniach psychologiczno-pedagogicznych, w którym wskazano, że wniosek o wydanie orzeczenia lub opinii zawiera także **oświadczenie wnioskodawcy o wyrażeniu zgody na przetwarzanie danych osobowych, o której mowa w** art. 23 ust. 1 pkt 1 **ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2016 r. poz. 922), w celu wydania orzeczenia lub opinii.**

Odnosząc się do treści tego przepisu zauważyć należy, że jeszcze Generalny Inspektor Ochrony Danych Osobowych na etapie opiniowania projektu ww. rozporządzenia zgłaszał uwagi co do treści tego przepisu. GIODO wskazał wówczas, że „co do zasady, jeśli przetwarzanie danych

osobowych nie ma podstaw w przepisach prawa, wtedy zgoda osoby, której dane są przetwarzane, jest wymagana. Projektodawca powinien natomiast stworzyć takie regulacje w przepisach ustawy, aby wymóg udostępniania określonych danych osobowych miał podstawę w przepisach prawa (zasada praworządności, legalizmu). Jeżeli przetwarzanie danych osobowych ma swoje uzasadnienie w obowiązujących przepisach prawa, określających podstawę prawną, cel i zakres przetwarzanych danych - odbieranie zgody na takie przetwarzanie nie jest prawidłowe. Jeżeli zaś określone w projekcie rozporządzenia informacje, do których przedłożenia są zobligowane osoby ubiegające się o wydanie orzeczenia lub opinii nie wynikają z ustawy lub jeśli tylko niektóre z nich wynikają z jej przepisów, to rozwiązanie polegające na przetwarzaniu tych danych na podstawie zgody jest niedopuszczalne. To przepisy powszechnie obowiązującego prawa powinny w sposób wyczerpujący wyznaczyć zasady przetwarzania danych osobowych. Przepisy nie powinny być uzupełniane czy zastępowane mocą oświadczeń woli osób, których dane dotyczą, tym bardziej że zgoda na przetwarzanie danych osobowych może być odwołana w każdym czasie." Uwagi te nie zostały jednak przez projektodawcę uwzględnione (treść powołanego wyżej pisma zamieszczona jest na stronie archiwalnej GIODO pod linkiem: https://archiwum.giodo.gov.pl/pl/1520275/10092 – **tekst w ramce poniżej**).

Informacja ze strony archiwalnej GIODO

DOLiS-023-302/17 – Uwagi GIODO z 7 lipca 2017 r. do projektu rozporządzenia Ministra Edukacji Narodowej w sprawie wydawania orzeczeń i opinii przez zespoły orzekające działające w publicznych poradniach psychologiczno-pedagogicznych

Wobec powyższego należy przyjąć, że podstawą do przetwarzania szczególnych kategorii danych osobowych w celu wydania orzeczenia lub opinii nie powinna być zgoda, lecz wskazana wyżej przesłanka z **art. 9 ust. 2 lit. g RODO** w związku z odpowiednimi przepisami ustawy Prawo oświatowe.

Data wytworzenia informacji: 10.08.2020 r.

Czy związek zawodowy może mieć dostęp do danych z wniosków o przyznanie świadczeń z ZFŚS?

Uprzejmie proszę o wskazanie, czy art. 27 ust. 2 ustawy z dnia 23 maja 1991 r. o związkach zawodowych stanowi podstawę prawną do udostępnienia przedstawicielom związków zawodowych danych osobowych zawartych we wnioskach o przyznanie świadczeń z Zakładowego Funduszu Świadczeń Socjalnych.

W szkole nie funkcjonuje komisja socjalna, w związku z czym wnioski składane są bezpośrednio do dyrektora szkoły. Przedmiotowe wnioski zawierają dane osobowe osób uprawnionych

(w tym pracowników i byłych pracowników) i ich rodzin. Przyznawanie świadczeń jest dokonywane w uzgodnieniu z organizacją związkową. Jednak mając na uwadze, iż w procesie przyznawania świadczeń z ZFŚS dochodzi do przetwarzania danych również tych osób, które nie są członkami związku zawodowego, zachodzi wątpliwość, czy na gruncie przywołanego powyżej przepisu, dopuszczalne jest udostępnienie danych osobowych organizacji związkowej.

Jeżeli przepisy prawa – w tym ustawy o związkach zawodowych – nie wskazują wprost na kompetencje związków zawodowych w określonej materii, to takiego uprawnienia nie można domniemywać. Ponadto związek zawodowy nie może żądać udostępnienia danych, gdy jest w stanie zrealizować swoje uprawnienia w inny sposób.

Zgodnie z art. 28 ust. 1 pkt 1-4 ustawy o związkach zawodowych, pracodawca jest obowiązany udzielić na wniosek zakładowej organizacji związkowej informacji niezbędnych do prowadzenia działalności związkowej, w szczególności informacji dotyczących: warunków pracy i zasad wynagradzania; działalności i sytuacji ekonomicznej pracodawcy związanych z zatrudnieniem oraz przewidywanych w tym zakresie zmian; stanu, struktury i przewidywanych zmian zatrudnienia oraz działań mających na celu utrzymanie poziomu zatrudnienia; działań, które mogą powodować istotne zmiany w organizacji pracy lub podstawach zatrudnienia.

Warto wskazać na wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie (II SA/Wa 1217/15), w uzasadnieniu którego wskazano, że: „przepisy art. 10, art. 251 ust. 2, art. 28 i art. 30 ustawy o związkach zawodowych (...) uprawniają ten Związek (jak i każdy związek zawodowy) do posiadania informacji o wykonywaniu przez członków obowiązku, jakim jest uiszczanie składek związkowych. Prawa tego nie można ograniczyć (...) jedynie do informacji zbiorczej o wpływie łącznej kwoty w danym miesiącu z tytułu składek członkowskich. Bowiem prawo Związku to nie tylko prawo do wiedzy o ogólnym bilansie wpływu składek na konto Związku w danym miesiącu,(...), ale także prawo do informacji, którzy konkretnie członkowie obowiązek uregulowania składki wykonali. (...) praktyka (...) przedstawienia imiennego zestawiania wpłat w odnotowanym przy nazwisku członka wysokością wpłaty w niczym nie narusza tajemnicy uzyskiwanych przez tego członka wynagrodzenia, albowiem wysokość składki członkowskiej nie jest pochodną od wysokości wynagrodzenia, ale jest stała (10 złotych od członka – pracownika i 1 zł od członka – emeryta).”

Ponadto istotne wskazówki znajdują się w Uchwale Sądu Najwyższego 7 sędziów z dnia 16 lipca 1993 r. I PZP 28/93. W orzeczeniu tym wskazano, że zawarte w art. 8, 23 ust. 1 i art. 26 pkt 3 ustawy z dnia 23 maja 1991 r. o związkach zawodowych uprawnienie do kontrolowania przez związki zawodowe przestrzegania prawa pracy oznacza także uprawnienie do kontrolowania wysokości wynagrodzeń pracowników; nie oznacza natomiast uprawnienia do żądania od pracodawcy udzielenia informacji o wysokości wynagrodzenia pracownika bez jego zgody. Ponadto podkreślono, że ujawnienie przez pracodawcę bez zgody pracownika wysokości jego

wynagrodzenia za pracę może stanowić naruszenie dobra osobistego w rozumieniu art. 23 i 24 Kodeksu cywilnego.

Zgodnie z art. 27 ust. 1 ustawy o związkach zawodowych, ustalanie zasad wykorzystania zakładowego funduszu świadczeń socjalnych, w tym podział środków z tego funduszu na poszczególne cele i rodzaje działalności, ustala pracodawca w regulaminie uzgodnionym z zakładową organizacją związkową. Również przyznawanie świadczeń z funduszu, o którym mowa w ust. 1, jest dokonywane w uzgodnieniu z zakładową organizacją związkową (art. 27 ust. 2).

Ponadto art. 27 ust. 2 ustawy o związkach zawodowych nie stanowi podstawy prawnej do udostępnienia przez pracodawcę przedstawicielom związków zawodowych danych osobowych zawartych we wnioskach o przyznanie świadczeń z Zakładowego Funduszu Świadczeń Socjalnych.

Art. 8 ust. 2 ustawy o zakładowym funduszu świadczeń socjalnych stanowi, że zasady i warunki korzystania z usług i świadczeń finansowanych z ZFŚS, z uwzględnieniem ust. 1-1b, oraz zasady przeznaczania środków Funduszu na poszczególne cele i rodzaje działalności socjalnej określa pracodawca w regulaminie ustalanym zgodnie z art. 27 ust. 1 albo art. 30 ust. 6 ustawy z dnia 23 maja 1991 r. o związkach zawodowych. Z przepisem tym koresponduje art. 27 ust. 1 ustawy z dnia 23 maja 1991 r. o związkach zawodowych, zgodnie z którym ustalanie zasad wykorzystania zakładowego funduszu świadczeń socjalnych, w tym podział środków z tego funduszu na poszczególne cele i rodzaje działalności, ustala pracodawca w regulaminie uzgodnionym z zakładową organizacją związkową. Choć więc w art. 27 ust. 2 ustawy o związkach zawodowych mowa jest o uzgadnianiu z zakładową organizacją związkową przyznawania świadczeń z zakładowego funduszu świadczeń socjalnych, to uzgodnienia te obejmują konkretne mechanizmy i kryteria dystrybucji świadczeń socjalnych wśród pracowników. Nie wydaje się zatem uzasadniona taka wykładnia art. 27 ust. 2 ustawy o związkach zawodowych, zgodnie z którą należy uzgadniać z zakładową organizacją związkową każdą indywidualną kwestię dotyczącą świadczeń socjalnych przyznawanych konkretnemu pracownikowi [Daniel Książek [w:] Krzysztof Wojciech Baran (red.), Daniel Książek, Mariusz Lekston, Jan Piątkowski, Iwona Sierocka, Artur Tomanek *Zbiorowe prawo zatrudnienia. Komentarz*, komentarz do art. 27 ustawy o związkach zawodowych].

W przypadku, kiedy u pracodawcy funkcjonuje komisja socjalna, to „w celu prawidłowej realizacji zadań nałożonych na komisję, powinna ona mieć w swoim składzie pracodawcę lub jego przedstawiciela, przedstawiciela pracowników i przedstawiciela związków zawodowych." (Barbara Tomaszewska *Ustawa o zakładowym funduszu świadczeń socjalnych. Komentarz*, komentarz do art. 8). Jeżeli w komisji socjalnej rozpatrującej wnioski pracowników o przyznanie świadczeń z zakładowego funduszu świadczeń socjalnych zasiada przedstawiciel związków zawodowych, to przedstawiciel ten będzie miał dostęp do danych osobowych zawartych w poszczególnych

wnioskach, jest jednak zobowiązany do zachowania tajemnicy (art. 8 ust. 1b zdanie drugie ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych).

Informacje dotyczące relacji pracodawcy ze związkami zawodowymi można znaleźć również w materiale UODO: „Ochrona danych osobowych w miejscu pracy. Poradnik dla pracodawców", w rozdziale 4.2.1 Przetwarzanie danych osobowych pracowników w ramach relacji pracodawcy z organizacją związkową — dostępnym pod linkiem https://uodo.gov.pl/pl/220/545).

Data wytworzenia informacji: 08.10.2020 r.

Kto jest administratorem danych osobowych przetwarzanych w urzędzie wojewódzkim?

Zwracam się z prośbą o opinię na temat prawidłowości zakwalifikowania wojewody jako administratora danych osobowych przetwarzanych w związku z realizacją wszystkich zadań przypisanych wojewodzie oraz związanych z funkcjonowaniem urzędu, realizowanych przez pracowników urzędu (oczywiście poza zadaniami przypisanymi ustawowo innym podmiotom, np. Komisji ds. orzekania o zdarzeniach medycznych). Czy sam wojewoda, czy może jednak wojewoda i dyrektor generalny urzędu są administratorami danych osobowych w urzędzie wojewódzkim?

Na wstępie - dla porządku - należy wskazać, że administratorem – w rozumieniu przepisów RODO (art. 4 pkt 7) – 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 efekcie, pojęcie administratora ma bardzo szeroki zakres znaczeniowy, gdyż może nim być w zasadzie każdy podmiot, o ile ustala cele i sposoby przetwarzania danych osobowych.

W przypadku podmiotów szeroko rozumianego sektora publicznego podmiot będący administratorem może być wprost wskazany w konkretnym przepisie prawa, jednak najczęściej ma miejsce sytuacja, w której wskazanie podmiotu pełniącego tę rolę wymaga analizy przepisów stanowiących podstawę przetwarzania danych osobowych. O tym, czy dany organ jest administratorem, decyduje przede wszystkim rodzaj i charakter nadanych mu przez prawo kompetencji z obszaru spraw publicznych oraz wyznaczone ustawowo zadania.

W zależności więc od danych, które są przetwarzane, oraz podstawy prawnej przetwarzania i kompetencji poszczególnych podmiotów (organów) do przetwarzania, administratorem może być urząd, organ albo np. jednostka samorządu terytorialnego.

Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych. Ocena będzie zależała od tego, o jakie dane osobowe oraz o jakie zadania chodzi w określonym przypadku.

W odniesieniu do urzędu wojewódzkiego pomocniczo można wskazać, że co do zasady w przypadku przetwarzania danych pracowników lub kandydatów do pracy administratorem jest jednostka organizacyjna będąca pracodawcą w rozumieniu prawa pracy (w przypadku pracowników urzędu wojewódzkiego pracodawcą jest ten urząd), natomiast - wobec danych interesantów (w tej samej jednostce organizacyjnej) za administratora może być uznany właściwy do realizacji określonych zadań (podejmowania decyzji, uchwał) - organ jednoosobowy lub kolegialny. W tym przypadku organem takim będzie zazwyczaj wojewoda, nie zaś dyrektor generalny. Dyrektor generalny urzędu co do zasady dokonuje jedynie pewnych czynności w imieniu kierownika jednostki, a nie w swoim własnym. Regulamin organizacyjny, plany działalności i inne wewnętrzne dokumenty warunkujące cel przetwarzania danych zatwierdza kierownik jednostki, a nie dyrektor generalny. Ponadto dyrektor również sam nie decyduje o sposobach przetwarzania, gdyż np. kwestie finansowe, muszą być zatwierdzone przez kierownika jednostki, co w znaczący sposób determinuje możliwość samodzielnego decydowania w tym zakresie.

Data wytworzenia informacji: 25.08.2020 r.

Jaki jest status WIOŚ w związku z wizyjnym systemem kontroli składowisk odpadów?

Czy Wojewódzki Inspektor Ochrony Środowiska jest współadministratorem czy odrębnym administratorem danych pozyskiwanych z wizyjnego systemu kontroli składowisk odpadów? Czy w przypadku udostępnienia przez podmiot prowadzący magazynowanie odpadów lub zarządzający składowiskiem odpadów obrazu z wizyjnego systemu kontroli w czasie rzeczywistym na rzecz wojewódzkiego inspektora ochrony środowiska dochodzi do współadministrowania danymi osobowymi?

Aby określić status danego podmiotu w procesie przetwarzania należy przede wszystkim kierować się definicją administratora zawartą w RODO. Na podstawie 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.

Jeśli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania są oni wówczas współadministratorami (art. 26 ust. 1 RODO). W takim przypadku współadministratorzy

w drodze wspólnych uzgodnień określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO. Zwrócić należy uwagę, że w przypadku podmiotu publicznego współadministrowanie musi znajdować oparcie w przepisach prawa, z których to przepisów wynikać ma istnienie między współadministratorami wspólnoty celów i sposobów przetwarzania.

Inną kwestią jest udostępnienie danych osobowych na rzecz odrębnego administratora. Do udostępnienia danych osobowych dochodzi jeśli dane te przekazywane są innemu podmiotowi w celu realizacji przez podmiot jego własnych zadań, wynikających np. z przepisów prawa. Staje się on wtedy odrębnym administratorem odpowiedzialnym za legalność i bezpieczeństwo posiadanych danych, zobligowanym do podjęcia odpowiednich środków organizacyjnych i technicznych w taki sposób, aby zagwarantować maksymalną ochronę praw i wolności każdej osobie fizycznej.

Zgodnie z art. 25 ust. 6a ustawy o odpadach **prowadzący magazynowanie odpadów**, z wyjątkiem wstępnego magazynowania odpadów przez ich wytwórcę, o którym mowa w art. 3 ust. 1 pkt 5 lit. a, **lub zarządzający składowiskiem odpadów jest obowiązany do prowadzenia wizyjnego systemu kontroli** miejsca magazynowania lub składowania odpadów, zgodnie z ust. 6b-6f. 6h i 6i oraz przepisami wydanymi na podstawie ust. 8a.

Wizyjny system kontroli miejsca magazynowania lub składowania odpadów prowadzi się przy użyciu urządzeń technicznych zapewniających przez całą dobę zapis obrazu i identyfikację osób przebywających w tym miejscu (art. 25 ust. 6d).

Zgodnie z art. 25 ust. 6f ustawy o odpadach w przypadku magazynowania lub składowania wymienionych w tym przepisie odpadów palnych **prowadzący magazynowanie odpadów lub zarządzający składowiskiem odpadów zapewnia wojewódzkiemu inspektorowi ochrony środowiska właściwemu ze względu na lokalizację miejsca magazynowania lub składowania odpadów dostępność obrazu z wizyjnego systemu kontroli tego miejsca w czasie rzeczywistym przez system teleinformatyczny.**

Zgodnie zaś z art. 25 ust. 6h ww. ustawy **prowadzący magazynowanie odpadów lub zarządzający składowiskiem odpadów zapewnia dostępność obrazu w czasie rzeczywistym wojewódzkiemu inspektorowi ochrony środowiska, o którym mowa w ust. 6f, przez przekazanie informacji umożliwiających logowanie do wizyjnego systemu kontroli** miejsca magazynowania lub składowania odpadów w sposób zapewniający zachowanie tych informacji w poufności.

Stosownie do art. 25 ust. 6g ww. ustawy wojewódzki inspektor ochrony środowiska wykorzystuje dostęp do rejestrowanego obrazu w czasie rzeczywistym w przypadku:

1. prowadzonej kontroli, o której mowa w art. 9 ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska;

2. powzięcia uzasadnionego podejrzenia popełnienia przestępstwa przeciwko środowisku określonego w art. 182, art. 183 lub art. 186 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny albo wykroczenia określonego w art. 154 § 2 ustawy z dnia 20 maja 1971 r. - Kodeks wykroczeń, albo wykroczeń, o których mowa w art. 10b ust. 1 pkt 1-15 ustawy z dnia 20 lipca 1991 r. o Inspekcji Ochrony Środowiska.

Dostępność obrazu w czasie rzeczywistym zapewnia się przez udostępnienie WIOŚ loginu i hasła dostępu do systemu kontroli, za pośrednictwem systemu teleinformatycznego, za pomocą odpowiedniego telekomunikacyjnego urządzenia końcowego w rozumieniu art. 2 pkt 43 ustawy Prawo telekomunikacyjne. W § 3 rozporządzenia Ministra Środowiska w sprawie wizyjnego systemu kontroli miejsca magazynowania lub składowania odpadów zawarto informacje o wymaganiach technicznych dla urządzeń wykorzystywanych do prowadzenia wizyjnego systemu kontroli oraz wytyczne dotyczące tego systemu.

Ustawa o odpadach wprost nie wymienia wojewódzkiego inspektora ochrony środowiska jako administratora. W takiej sytuacji należy wziąć pod uwagę, iż pojęcie administratora ma bardzo szeroki zakres znaczeniowy, gdyż może nim być w zasadzie każdy podmiot, o ile ustala cele i sposoby przetwarzania danych osobowych oraz fakt, iż 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 zakresu zadań publicznych, jakie przepisy te mu przypisują.

Analiza powyższych przepisów pozwala zasadnie przyjąć, że w przypadku udostępnienia przez podmiot prowadzący magazynowanie odpadów lub zarządzający składowiskiem odpadów obrazu z wizyjnego systemu kontroli w czasie rzeczywistym na rzecz wojewódzkiego inspektora ochrony środowiska, inspektor przetwarza pozyskane w ten sposób dane osobowe dla realizacji własnych zadań. W takiej sytuacji mamy zatem do czynienia z udostępnieniem danych osobowych na rzecz odrębnego administratora.

Data wytworzenia informacji: 25.08.2020 r.

Czy w celu wytworzenia legitymacji należy skorzystać z powierzenia przetwarzania?

Przepisy dotyczące sektora oświaty przesądzają, że to dyrektor szkoły wystawia nauczycielowi legitymację służbową. Procedura wyrabiania legitymacji bywa różna, ale zawsze zaangażowana jest przy tym firma zewnętrzna. Niekiedy to sam nauczyciel przekazuje do niej swoje dane potrzebne do wyrobienia legitymacji i rozliczenia kosztów, a czasami robi to dyrektor.
W związku z tym, że wyrobienie legitymacji służbowej nauczyciela to usługa, bardzo często nie ma pisemnej umowy, jest jedynie faktura, która stanowi podstawę rozliczenia. Bardzo często

jest też tak, że faktura jest wystawiana bezpośrednio na nauczyciela. Powstaje jednak pytanie, czy w świetle RODO przekazanie danych do firmy należy formalizować w postaci umowy przetwarzania, a jeżeli tak, to w którym przypadku?

Zgodnie z art. 11a ust. 1 ustawy Karta Nauczyciela, dyrektor szkoły, na wniosek nauczyciela, wystawia nauczycielowi legitymację służbową. Ponadto zgodnie z treścią § 2 ust. 1 rozporządzenia Ministra Edukacji Narodowej z dnia 29 września 2006 r. w sprawie wzoru oraz trybu wystawiania legitymacji służbowej nauczyciela, legitymację wydaje dyrektor szkoły w terminie 30 dni od dnia złożenia przez nauczyciela wniosku o jej wystawienie. Szkoła udostępnia podmiotowi zewnętrznemu w celu wykonania legitymacji dane osobowe w zakresie: imię i nazwisko, kolorowe zdjęcie posiadacza legitymacji oraz podpis posiadacza.

Biorąc pod uwagę treść przytoczonych przepisów, w przedstawionej sytuacji zasadne jest zawarcie umowy powierzenia przetwarzania danych osobowych przez szkołę z podmiotem zewnętrznym, który wytwarza legitymacje służbowe dla nauczycieli.

Data wytworzenia informacji: 28.08.2020 r.

Czy mediator jest administratorem danych?

Kto jest administratorem danych przetwarzanych w związku z mediacją w postępowaniu administracyjnym? Czy Urząd Gminy działając na podstawie Kpa powinien zawrzeć z mediatorem umowę powierzenia, czy jednak dochodzi do udostępnienia danych osobowych i mamy dwóch ADO?

Ustalając kwestię podmiotu, któremu w procesie przetwarzania danych osobowych będzie przysługiwał status administratora, należy w każdym przypadku kierować się definicją tego pojęcia. Zgodnie z art. 4 pkt 7 RODO „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę 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.

Zupełnie inny status cechuje podmiot przetwarzający. Zgodnie z art. 28 ust. 1 RODO z powierzeniem przetwarzania danych osobowych mamy do czynienia, gdy przetwarzanie jest dokonywane przez zewnętrzny podmiot w imieniu administratora. Podmiot przetwarzający nie działa we własnych celach, bo cele przetwarzania oraz polecenia co do przetwarzania są formułowane przez administratora.

Zatem w myśl przepisów RODO konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator zleca wykonywanie swoich zadań innemu podmiotowi (podmiotowi przetwarzającemu). Istotne jest podkreślenie, że podmiot przetwarzający przetwarza dane w imieniu administratora, a nie w imieniu własnym (tj. nie staje się administratorem tych danych). Podmiot przetwarzający nie decyduje bowiem o celach i sposobach przetwarzania, gdyż przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO).

W przypadku podmiotów realizujących zadania określone przepisami prawa, rozstrzygając, który z nich w danej sytuacji jest administratorem w odniesieniu do konkretnych danych osobowych, zazwyczaj należy dokonać analizy przepisów prawa określających te zadania. Tak jest również w przypadku mediacji w postępowaniu administracyjnym.

Kwestie związane z przeprowadzaniem mediacji w postępowaniu administracyjnym uregulowano w art. 96a-96n Kodeksu postępowania administracyjnego (Kpa). Stanowią one, że mediacja może być przeprowadzona w toku postępowania administracyjnego, jeżeli pozwala na to charakter sprawy (art. 96a § 1 Kpa). Określają też zakres zadań (kompetencji) zarówno organu administracji publicznej, jak i mediatora.

Z art. 96h Kpa wynika, że organ administracji publicznej przekazuje niezwłocznie mediatorowi dane kontaktowe uczestników mediacji, po uzyskaniu zgody uczestników mediacji na jej przeprowadzenie. W przepisie zabrakło wskazania, że wraz z danymi kontaktowymi organ przekazuje mediatorowi odpis postanowienia o skierowaniu sprawy do mediacji. Taka praktyka – jak wskazuje się w literaturze przedmiotu[2]- jest jednak zasadna. **Nie ulega zatem wątpliwości, że mediator staje się administratorem danych osobowych udostępnionych wraz z postanowieniem o skierowaniu sprawy do mediacji**, w związku z przypisanym mu w ustawie zadaniem polegającym na przeprowadzeniu mediacji mającej na celu wyjaśnienie i rozważenie okoliczności faktycznych i prawnych sprawy oraz dokonanie ustaleń dotyczących jej załatwienia w granicach obowiązującego prawa.

Pozyskiwanie przez mediatora danych osobowych może następować także w toku przeprowadzanego przez niego „spotkania" mediacyjnego (art. 96n § 2 Kpa) i innych czynności związanych z mediacją (np. zgodnie z art. 96i Kpa, mediator zapoznaje się z aktami sprawy wraz ze sporządzaniem z nich notatek, kopii lub odpisów, chyba że uczestnik mediacji nie wyraził zgody na zapoznanie się z aktami). Jego zadaniem jest również wspieranie uczestników mediacji w formułowaniu przez nich propozycji ugodowych (art. 96k Kpa).

[2] Wilbrandt-Gotowicz Martyna. Art. 96(h). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019.)

Mediator jest nie tylko osobą, której działanie ma doprowadzić do merytorycznego zakończenia sporu, ale także wykonuje związane z mediacją obowiązki o charakterze administracyjnym lub technicznym[3]. Między innymi mediator przeprowadza mediację w ustalonym przez niego terminie i miejscu (art. 96k kpa). W przepisach Kpa dotyczących mediacji pozostawiono mediatorom swobodę co do sposobu organizacji przebiegu mediacji. Nie przesądza się bowiem ani o formie mediacji (czy ma ona przyjmować formę spotkania lub spotkań mediatora z uczestnikami mediacji albo innych sposobów dokonywania ustaleń, np. w drodze komunikacji elektronicznej, wideokonferencji itp.), ani o jej technikach. Wskazanie czasu i miejsca mediacji powinno jednak znaleźć się w protokole z przebiegu mediacji, o którym mowa w art. 96m Kpa[4]. Na tym tle dopuszczalne jest prowadzenie mediacji zarówno w trybie gabinetowym, w drodze indywidualnych negocjacji ze stroną i przedstawicielem organu lub z tymi podmiotami łącznie, jak i zorganizowanie posiedzenia w sposób zbliżony do rozprawy administracyjnej[5]. Mediator sporządza także protokół z przebiegu mediacji o treści określonej w art. 96m § 2 Kpa i niezwłocznie przedkłada go organowi administracji publicznej w celu włączenia go do akt sprawy, a odpisy doręcza uczestnikom mediacji.

Powyższe wskazuje na to, że mediator jest odrębnym administratorem przetwarzanych danych osobowych, bo jak wskazują przytoczone przepisy – samodzielnie określa cele i sposoby przetwarzania danych. Jako administrator zobowiązany jest on zatem do spełnienia obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO, w stosunku do stron postępowania. Przetwarzanie danych osobowych w toku postępowania mediacyjnego zobowiązuje również mediatora do przestrzegania zasad wskazanych w art. 5 RODO jak: zgodność z prawem, rzetelność i przejrzystość, ograniczenie celu przetwarzania, minimalizacja danych; prawidłowość, ograniczenie przechowywania oraz integralność i poufność.

Administratorem danych osobowych stron postępowania mediacyjnego jest również organ administracji publicznej.

Należy podkreślić, że zgodnie zasadą wyrażoną w art. 13 § 2 Kpa, organ administracji publicznej podejmuje wszystkie uzasadnione na danym etapie postępowania czynności umożliwiające przeprowadzenie mediacji lub zawarcie ugody, a zwłaszcza udziela wyjaśnień o możliwościach i korzyściach polubownego załatwienia sprawy. Mediacja może być podjęta zarówno z urzędu przez organ administracji publicznej bądź też na wniosek strony postępowania. W pierwszym przypadku będzie wyrazem pozytywnej oceny przez organ przesłanki materialnej (charakter

[3] Ziemianin Karolina. RODO W POSTĘPOWANIU MEDIACYJNYM. W: Ochrona danych osobowych w postępowaniach sądowych i przed organami administracji publicznej. Wolters Kluwer Polska, 2019

[4] Wilbrandt-Gotowicz Martyna. Art. 96(k). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019.

[5] J. Wegner-Kowalska, Mediacja (art. 13, art. 96a–96g [w:] Reforma prawa o postępowaniu administracyjnym. Raport zespołu eksperckiego z prac w latach 2012–2016, red. Z. Kmieciak, Warszawa 2017, s. 81).

sprawy pozwala na przeprowadzenie mediacji) i formalnej (sprawa w toku) mediacji. Ponadto powinna ona być następstwem oszacowania przez organ, że mediacja ma szanse zakończenia się akceptowanymi przez jej uczestników ustaleniami, a w wyniku mediacji możliwe jest realizowanie w szerszym zakresie standardów postępowania wynikających z zasad ogólnych (m.in. zasady prawdy obiektywnej, zasady przekonywania, zasady czynnego udziału w postępowaniu) niż w tradycyjnym modelu postępowania[6]. A zatem w przypadku wydania postanowienia o skierowaniu sprawy do mediacji organ administracji będzie administratorem danych osobowych stron postępowania mediacyjnego. Jemu również przekazywany jest protokół z przebiegu mediacji sporządzony przez mediatora, wraz z ustaleniami mediacyjnymi, celem załączenia go do akt postępowania administracyjnego (art. 96m Kpa). Załatwienie sprawy przez organ administracji polega przede wszystkim na wydaniu decyzji administracyjnej, która powinna uwzględniać w swym rozstrzygnięciu w całości ustalenia mediacyjne. Jeżeli jednak część z ustaleń mediacyjnych nie mieści się w granicach obowiązującego prawa, organ powinien rozstrzygnąć sprawę z uwzględnieniem jedynie tych ustaleń, które nie naruszają prawa. Zobowiązany jest on bowiem w każdym przypadku respektować zasadę legalności. W sytuacji gdy ustalenia mediacyjne odpowiadają prawu, organ zobligowany jest do rozstrzygnięcia sprawy w sposób zgodny w całości z tymi ustaleniami.[7] Organ administracji jako odrębny administrator zatwierdza też ugodę zawartą przed mediatorem (o ile oczywiście zakres sprawy objętej danym postępowaniem dopuszcza taki sposób załatwienia sprawy).

A zatem w postępowaniu mediacyjnym zarówno organ administracji publicznej, jak i mediator to odrębni administratorzy przetwarzanych przez siebie danych. Każdy we własnym zakresie realizuje konkretne zadania wynikające z powołanych wyżej przepisów prawa. Żeby możliwe było przeprowadzenie mediacji, której celem jest wyjaśnienie i rozważenie okoliczności faktycznych i prawnych sprawy oraz dokonanie ustaleń dotyczących jej załatwienia w granicach obowiązującego prawa, niezbędne jest przetwarzanie określonych danych osobowych przez mediatora. W tym przypadku mamy jednak do czynienia z udostępnieniem danych osobowych niebędącym powierzeniem – podmiot, który otrzymuje dane osobowe, przetwarza je w celach, które samodzielnie kształtuje – nie w celach własnych udostępniającego, gdyż jak wynika to z art. 96k Kpa, mediator – prowadząc mediację – dąży do polubownego rozwiązania sporu, a także wspiera uczestników mediacji w formułowaniu propozycji ugodowych. To do niego właśnie należy przyjęcie rozwiązania zmierzającego do porozumienia między stronami (uczestnikami mediacji).

[6] Wilbrandt-Gotowicz Martyna. Art. 96(b). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019

[7] Wilbrandt-Gotowicz Martyna. Art. 96(n). W: Komentarz aktualizowany do Kodeksu postępowania administracyjnego. System Informacji Prawnej LEX, 2019

Wobec powyższego w tej sytuacji **nie zachodzi konieczność zawarcia między tymi podmiotami umowy powierzenia przetwarzania danych.** Mamy tu bowiem do czynienia z udostępnieniem danych na podstawie przepisów prawa.

Inaczej przedstawia się relacja pomiędzy mediatorem a organem administracji prowadzącym postępowanie w sytuacji, gdy jest on uczestnikiem mediacji, a uzgodnienia mediacyjne przyjmą formę posiedzenia mediacyjnego w siedzibie tego organu administracji. Zapewnienie obsługi technicznej posiedzenia mediacyjnego należeć będzie do organu administracji prowadzącego postępowanie. W takich uwarunkowaniach dochodzi do sytuacji, kiedy organ administracji jak i mediator wspólnie będą ustalać cele i sposoby przetwarzania danych osobowych, w ramach ustawowo przypisanych im zadań. **Pomiędzy tymi administratorami zachodzić będzie relacja współadministrowania uregulowana w art. 26 RODO.**

Mediator oraz organ administracji prowadzący postępowanie jako współadministratorzy powinni w drodze wspólnych uzgodnień w przejrzysty sposób określić odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14 RODO, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą. W myśl natomiast art. 26 ust. 2 RODO, uzgodnienia, o których mowa w ust. 1, muszą należycie odzwierciedlać odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą.

Takie wspólne uzgodnienia muszą uwzględniać faktyczne obowiązki mediatora i organu administracji prowadzącego postępowanie, związane z przetwarzaniem danych osobowych uczestników mediacji. Zarówno mediator. jak i organ administracji prowadzący postępowanie mają swoje autonomiczne uprawnienia, z którymi związane jest przetwarzanie danych osobowych uczestników mediacji w innych celach.

Przykładowo, jedynie do mediatora jako podmiotu aktywnego w procesie mediacji należy podejmowanie czynności polegających na wspieraniu uczestników mediacji w formułowaniu przez nich propozycji ugodowych. Organ administracji prowadzący postępowanie, w ramach współadministrowania, może być uprawniony np. do zapewnienia ochrony pomieszczeń. Należy wskazać, że co do zasady odpowiedzialność za przestrzeganie przepisów o ochronie danych osobowych w zakresie realizacji takich autonomicznych uprawnień kształtują przepisy prawa. Mediator i organ administracji prowadzący postępowanie, w ramach wspólnych uzgodnień, powinni więc określić inne zagadnienia, nieuregulowane wprost w przepisach prawa, w tym m.in.

kwestię odpowiedniego zabezpieczenia danych osobowych czy też realizacji określonych obowiązków informacyjnych.

Dokonanie wspólnych ustaleń pomiędzy współadministratorami, o których mowa w art. 26 RODO, umożliwia doprecyzowanie sposobu obsługi technicznej mediatorów przez organ administracji prowadzący postępowanie przy zachowaniu autonomicznych kompetencji mediatora w zakresie jego odrębnych zadań jako administratora.

Data wytworzenia informacji: 30.06.2020 r.

Kto jest administratorem danych przetwarzanych w celu wydania karty seniora?

Urzędy gmin lub miast na prawach powiatów mają wiele wątpliwości dotyczących wskazania administratora w procesie wydawania kart seniora lub kart młodzieży. Jest to spowodowane tym, że urzędy wspomagają się w bieżącej pracy jednostkami budżetowymi, np. miejskimi ośrodkami pomocy rodzinie. Wielu inspektorów ochrony danych ma problem z określeniem roli administratora, podmiotu przetwarzającego lub współadministratora. Zwracam się zatem do Państwa z prośbą o interpretację przepisów w tym zakresie i wskazanie, kto pełni rolę administratora w przypadku realizacji zadań z zakresu wydawania lokalnych kart, np. karty seniora czy karty młodzieży.

Zgodnie z definicją zawartą w art. 4 pkt 7 RODO, administratorem jest osoba fizyczna, prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

W przypadku szeroko rozumianego sektora publicznego podmiot będący administratorem może być wprost wskazany w konkretnym przepisie prawa, jednak najczęściej ma miejsce sytuacja, w której wskazanie podmiotu pełniącego tę rolę wymaga analizy przepisów stanowiących podstawę przetwarzania danych osobowych. O tym, czy dany podmiot publiczny jest administratorem, decydują wówczas przede wszystkim rodzaj i charakter nadanych mu przez prawo kompetencji z obszaru spraw publicznych oraz wyznaczone ustawowo zadania.

Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych. Ocena będzie zależała od tego, o jakie dane osobowe oraz o jakie zadania chodzi w określonym przypadku.

Zgodnie z art. 17 ust. 2 pkt 4 ustawy o pomocy społecznej, do zadań własnych gminy należy m.in. podejmowanie innych zadań z zakresu pomocy społecznej wynikających z rozeznanych potrzeb gminy, w tym tworzenie i realizacja programów osłonowych.

Na podstawie ww. przepisu w gminach realizowane są programy lokalne polegające np. na wydawaniu określonym grupom mieszkańców lokalnych kart (kart seniora, kart młodzieży itp.) uprawniających do korzystania bezpłatnie lub na preferencyjnych warunkach np. z komunikacji miejskiej, obiektów sportowych czy kulturalnych.

W przedstawionym stanie faktycznym na podstawie ww. przepisu rada miasta podjęła uchwałę w sprawie przyjęcia Programu Karta Młodzieży.

W powyższej uchwale określono zadania prezydenta miasta, który odpowiada za określenie warunków wydania i korzystania z Karty Młodzieży oraz za określenie wzoru karty i wniosku o jej wydanie. W celu zrealizowania tego zadania prezydent miasta wydał Zarządzenie w sprawie realizacji tego programu, określając warunki wydawania i korzystania z karty. W zarządzeniu tym wskazał m.in., że wniosek o wydanie karty należy złożyć do Miejskiego Ośrodka Pomocy Rodzinie (MOPR) oraz że wykonanie zarządzenia powierza się Miejskiemu Ośrodkowi Pomocy Rodzinie.

Zgodnie z przekazanymi informacjami MOPR realizować będzie zadania powierzone przez prezydenta miasta w zakresie: zbierania danych zawartych na wnioskach, przechowywania wniosków, wydawania kart, wydawania duplikatów kart, niszczenia kart.

Jednocześnie wskazać należy, że zgodnie z art. 110 ust. 1 ustawy o pomocy społecznej, zadania pomocy społecznej w gminach wykonują jednostki organizacyjne - ośrodki pomocy społecznej lub centra usług społecznych, o których mowa w ustawie o realizowaniu usług społecznych przez centrum usług społecznych.

Jeszcze przed wejściem w życie RODO, Generalny Inspektor Ochrony Danych Osobowych stanął na stanowisku, a następnie wielokrotnie podkreślał, iż „uprawnienia gmin, jako administratorów danych podlegają dekoncentracji, w ślad za merytoryczną kompetencją, z którą związane jest przetwarzanie danych osobowych". Wskazywał m.in., że jednostki pomocnicze, jakimi są dzielnice działają na podstawie prawa miejscowego, ich organy wykonują funkcje administracji we własnym imieniu […]. To właśnie dzielnica jest administratorem danych przetwarzanych w związku z wykonywaniem przez nią ustawowych zadań. Analogiczne podejście prezentowane było w stosunku do ośrodka pomocy społecznej w sytuacji, gdy organ właściwy (tj. wójt, burmistrz lub prezydent miasta) skorzystał z uprawnienia do upoważnienia kierownika ośrodka pomocy społecznej do realizacji w całości określonych zadań.

Zatem, co do zasady, jeżeli w danej jednostce organizacyjnej przekazuje się całość zadania na podmiot upoważniony, wówczas to ten podmiot realizuje to zadanie we własnym imieniu i staje się odrębnym administratorem.

W analizowanym przypadku gmina realizuje opisane zadanie własne poprzez działania podległej jej jednostki - Miejskiego Ośrodka Pomocy Rodzinie.

Wobec powyższego jeżeli gmina przekazuje do realizacji zadanie z zakresu pomocy społecznej (np. realizację programu, o którym mowa w art. 17 ust. 2 pkt 4 ustawy o pomocy społecznej) ośrodkowi pomocy społecznej, a więc podmiotowi ustanowionemu do wykonywania takich zadań (art. 100 ust. 1 ustawy o pomocy społecznej), wówczas uzasadnione jest twierdzenie, że ośrodek ten będzie realizował swoje zadanie wynikające z tych przepisów oraz doprecyzowane w aktach prawa miejscowego i w tym zakresie będzie decydował o celach i sposobach przetwarzania danych osobowych.

Data wytworzenia informacji: 23.09.2020 r.

Obowiązek informacyjny w związku z Rejestrem Danych Kontaktowych

Czy urząd, pozyskując dane osobowe z Rejestru Danych Kontaktowych, powinien spełnić obowiązek informacyjny z art. 14 RODO w stosunku do osób, które wyrażą zgodę na przetwarzanie ich danych w tym rejestrze czy też można skorzystać ze zwolnienia z obowiązku informacyjnego, o którym mowa w art. 14 ust. 5 RODO?

Obowiązek informacyjny, tj. obowiązek przekazania przez administratora osobie, której dane dotyczą, określonych informacji, uregulowany został w art. 13 i art. 14 RODO. Obowiązek ten jest ściśle związany z jednym z uprawnień składających się na prawo do ochrony danych osobowych – uprawnieniem osoby, której dane dotyczą, do „bycia poinformowanym" o fakcie i okolicznościach przetwarzania danych. Zauważyć jednak należy, że obowiązek informacyjny nie ma charakteru bezwzględnego i podlega ograniczeniu.

Artykuł 14 RODO nakłada na administratora obowiązek poinformowania osoby, której dane dotyczą, w przypadku, gdy jej dane są pozyskiwane z innych źródeł niż bezpośrednio od tej osoby. Zgodnie z art. 14 ust. 5 lit. c RODO, administrator jest zwolniony z tego obowiązku informacyjnego w sytuacji, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem (przepisami prawa UE lub prawa państwa członkowskiego, któremu podlega administrator), przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą. Wskazane zwolnienie obejmuje przypadki, w których przepisy zawierają wyraźne regulacje dotyczące przetwarzania (pozyskiwania lub ujawniania) danych. Ma ono szczególne znaczenie dla podmiotów publicznych (zwłaszcza administracji publicznej), które – zgodnie z zasadą legalizmu – opierają swoje działania na przepisach prawa. Należy jednak zwrócić uwagę, że obejmuje ono jedynie gromadzenie danych z innych źródeł, natomiast nie przewidziano go w odniesieniu do gromadzenia przez administrację publiczną danych od osób, których one dotyczą. Warunkiem

zastosowania tego zwolnienia jest również spełnienie wymogu, aby przepisy regulujące przetwarzanie danych przewidywały odpowiednie środki chroniące prawa osób, których dane poddawane są przetwarzaniu.

Wątpliwości dotyczą tego, czy urząd powinien spełnić obowiązek informacyjny z art. 14 RODO, w stosunku do osób, które wyrażą zgodę na przetwarzanie ich danych w Rejestrze Danych Kontaktowych (RDK). W sytuacji podmiotu wykonującego zadania publiczne analiza ewentualnego zwolnienia z obowiązku informacyjnego powinna być w pierwszej kolejności poprzedzona oceną, czy zastosowanie znajdzie art. 14 ust. 5 RODO, a dopiero w dalszej kolejności należy wziąć pod uwagę treść art. 4 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, mając na uwadze spełnienie określonych w tym przepisie warunków.

Wskazać należy, że zgodnie z art. 14 ust. 5 lit. c RODO, organ publiczny, pozyskując dane osobowe nie od osoby, której one dotyczą, nie jest obowiązany spełniać obowiązku informacyjnego określonego w art. 14 ust. 1 i 2 RODO, gdy podstawą przetwarzania danych osobowych jest obowiązek ciążący na administratorze wynikający z przepisów prawa.

Z ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne wynika, że dostęp do danych z RDK, przysługuje wskazanym w ustawie uprawnionym podmiotom i ma na celu ułatwienie kontaktu z osobami fizycznymi, w związku z usługami i zadaniami publicznymi realizowanymi na rzecz tych osób. Jak wynika z uzasadnienia ustawy, RDK „stanowić ma elektroniczny odpowiednik popularnych niegdyś często używanych książek telefonicznych, ale z uwagi na fakt prowadzenia go w formie elektronicznej o wiele bezpieczniejszy i chroniony z punktu widzenia ochrony danych osobowych” (https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=3789). Udostępnienie danych, odmowa udostępnienia danych oraz cofnięcie dostępu do danych zgromadzonych w RDK następuje w drodze decyzji administracyjnej ministra właściwego do spraw informatyzacji, po uprzednim złożeniu przez uprawniony podmiot jednorazowego uproszczonego wniosku i spełnieniu łącznie określonych w ustawie warunków (art. 20m ustawy o informatyzacji). Organowi gminy zapewniono dostęp do danych zgromadzonych w RDK bez konieczności składania uproszczonego wniosku.

Tak jak to zostało podkreślone wyżej, możliwość skorzystania przez podmiot publiczny z wyłączenia określonego w art. 14 ust. 5 lit. c RODO może nastąpić w sytuacji, gdy podstawą przetwarzania danych osobowych jest obowiązek ciążący na administratorze wynikający z przepisów prawa, czyli wówczas, gdy konkretny **przepis prawa obliguje podmiot** do pozyskania lub ujawniania określonych danych osobowych nie od osoby, której dane dotyczą.

Należy wskazać, że z przepisów ustawy o informatyzacji wynika, że RDK ma na celu ułatwienie kontaktu z osobami fizycznymi podmiotom realizującym określone usługi i zadania na ich rzecz. Zatem ustawa ta przewiduje jedynie uprawnienie określonych podmiotów do pozyskania danych

zgromadzonych w RDK, w związku z realizacją podejmowanych przez nich zadań czy usług w interesie osób fizycznych, nie kreuje jednak takiego obowiązku po stronie tych podmiotów.

Jeżeli chodzi o przesłankę wyłączenia określonego w art. 14 ust. 5 lit. a RODO, należy mieć na uwadze, że osoba, której dane dotyczą, musi dysponować już określonymi informacjami. Ustawa o informatyzacji wskazuje określony krąg podmiotów uprawnionych do pozyskania danych w określonym celu, w tym wprowadziła możliwość udostępnienia danych z RDK innym nieokreślonym w ustawie podmiotom, na podstawie porozumienia zawartego z ministrem właściwym do spraw informatyzacji (art. 20m ust. 1 pkt 2 ustawy o informatyzacji). Jednak to decyzja administracyjna ministra właściwego do spraw informatyzacji będzie kreować „listę" uprawnionych podmiotów mających dostęp do RDK. Należy też wskazać, że minister właściwy do spraw informatyzacji może wydać też decyzję w przedmiocie cofnięcia dostępu do danych w RDK na skutek okoliczności zwartych w ustawie. Informacje skierowane do osób fizycznych, które udostępniają swoje dane osobowe w RDK w klauzuli informacyjnej (dostępna na stronie internetowej Ministerstwa: Skorzystaj z Rejestru Danych Kontaktowych (RDK), są powieleniem przepisów ustawy i nie dają odpowiedzi co do rzeczywistej listy podmiotów posiadających dostęp do RDK.

Wobec tego, jeżeli nie zaistnieją okoliczności uzasadniające skorzystanie z wyłączeń, o których mowa w art. 14 ust. 5 RODO lub art. 4 ustawy o ochronie danych osobowych, administrator pozyskujący dane osobowe nie od osoby, której one dotyczą, musi taki obowiązek wypełnić. Należy bowiem podkreślić, że każdy administrator w zakresie przetwarzania danych powinien kierować się zasadami wynikającymi z art. 5 RODO. Zgodnie z zasadą przejrzystości, o której mowa w art. 5 ust. 1 lit. a RODO, dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Zasada przejrzystości wymaga, aby wszelkie informacje i komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Ma ona również istotne znaczenie w aspekcie zapewnienia osobom, których dane dotyczą, możliwości korzystania ze wszystkich praw wynikających z RODO.

Przekazanie informacji dotyczących administratora będzie miało istotne znaczenie także z punktu widzenia uprawnień podmiotu danych wynikających z art. 20k ust. 2 pkt 2 ustawy o informatyzacji. W przepisie tym wskazano bowiem, że dane do RDK mogą być także przekazywane, aktualizowane lub usuwane za pośrednictwem uprawnionego podmiotu, posiadającego dostęp do RDK, na wniosek złożony osobiście w siedzibie tego podmiotu przez osobę, której dane dotyczą.

Wiele wskazówek oraz przykładów dotyczących sposobów spełniania obowiązku informacyjnego znaleźć można w szczególności w Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP260 rev.01 dostępnych pod linkiem: Wytyczne grupy roboczej, a także

w prezentacjach ze szkoleń oraz webinariach dot. obowiązku informacyjnego dostępnych na stronie internetowej UODO, np. https://uodo.gov.pl/pl/189/727, https://uodo.gov.pl/pl/213/930

Data wytworzenia informacji: 23.09.2020 r.

Czy przesłanką przetwarzania przez organy publiczne może być art. 6 ust. 1 lit. f RODO?

Z uwagi na sprzeczne opinie, z którymi można się spotkać na szkoleniach oraz w literaturze przedmiotu, zwracam się z prośbą o udzielenie informacji w zakresie możliwości stosowania art. 6 ust. 1 lit. f RODO przez podmioty publiczne.

Przepis art. 6 ust. 1 lit. f RODO stanowi, iż przetwarzanie jest zgodne z prawem w przypadku gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Wyżej wymieniona podstawa prawna przetwarzania danych osobowych ma zastosowanie w sytuacji gdy administrator nie posiada zgody osoby, której dane dotyczą, nie istnieje żaden przepis, który mógłby stanowić podstawę do przetwarzania danych osobowych oraz gdy administrator nie może powołać się na realizację umowy, a mimo to przetwarzanie danych należy uznać za legalne z uwagi na „prawnie uzasadniony interes" administratora lub strony trzeciej. Przesłanka ta ma charakter dodatkowy, uzupełniający pozostałe podstawy dopuszczalności przetwarzania.

W treści powołanego wyżej przepisu znajduje się zastrzeżenie, iż podstawa prawna wskazana w lit. f nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Analiza tej normy prowadzi do wniosku, że omawiana przesłanka może być stosowana również przez podmioty publiczne, jednakże nie w sytuacji, w której realizują one swoje zadania określone w przepisach jako ustawowe kompetencje.

Zastosowanie powyższej podstawy prawnej powinno mieć miejsce w sytuacji, gdy administrator nie może powołać się na żadną inną podstawę przetwarzania danych. Administrator będący podmiotem publicznym określając legalność przetwarzania danych powinien sprawdzić, czy nie istnieje żaden przepis prawa, który mógłby stanowić podstawę do przetwarzania danych (art. 6 ust. 1 lit. c), a w następnej kolejności dokonać analizy czy przetwarzanie danych jest niezbędne do wykonywania zadania realizowanego w interesie publicznym (art. 6 ust. 1 lit. e).

Podkreślenia wymaga, że oparcie przetwarzania danych osobowych na przepisie art. 6 ust. 1 lit. f wymaga kumulatywnego spełnienia dwóch przesłanek pozytywnych. Po pierwsze, musi występować prawnie uzasadniony interes, który jest realizowany przez administratora lub przez stronę trzecią. Po drugie, niezbędna jest weryfikacja, czy przetwarzanie danych osobowych jest niezbędne dla realizacji celu wynikającego z prawnie uzasadnionych interesów. Nie wystarczy zatem samo występowanie takich interesów, lecz dodatkowo ich realizacja musi wymagać przetwarzania danych osobowych.

Następnie należy ocenić, czy nie jest spełniona przesłanka o charakterze negatywnym w postaci występowania w danym stanie faktycznym interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec prawnie uzasadnionych interesów administratora lub strony trzeciej. Stosowanie tej negatywnej przesłanki polega w istocie na wyważeniu dwóch dóbr chronionych prawem, tj. prawnie uzasadnionego interesu administratora lub strony trzeciej z jednej strony i interesów, podstawowych praw oraz wolności podmiotu danych z drugiej. Z treści motywu 47 wynika, że aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu.

Wobec powyższego w przypadku, gdyby administrator chciał skorzystać z tej podstawy przetwarzania danych, powinien przeprowadzić tzw. test równowagi, tzn. dokonać oceny, czy interes administratora lub strony trzeciej, przemawiający za przetwarzaniem danych, jest prawnie uzasadniony, czy przetwarzanie jest niezbędne do realizacji celu wynikającego z tego interesu, a następnie rozważyć, czy interesy lub podstawowe prawa i wolności osoby, której dane dotyczą nie przeważają nad prawnie uzasadnionym interesem administratora lub strony trzeciej.

Przy interpretacji przepisów dotyczących prawnie uzasadnionego interesu oraz przy przeprowadzaniu testu równowagi, pomocne mogą być wskazówki zawarte w Opinii 6/2014 Grupy Roboczej Art. 29 w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy art. 7 dyrektywy 95/46/WE (dostępnej na archiwalnej stronie UODO pod linkiem: https://archiwum.giodo.gov.pl/pl/1520203/7813 **tekst w ramce poniżej**), które mimo zmiany stanu prawnego, w znacznej mierze zachowują swoją aktualność.

Informacja ze strony archiwalnej GIODO

Opinia 6/2014 w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46/WE (WP 217)

W dniu 9 kwietnia 2014 r. Grupa Robocza Art. 29 przyjęła opinię w sprawie pojęcia prawnie uzasadnionych interesów administratora danych na mocy artykułu 7 dyrektywy 95/46/WE.

Jednocześnie informuję, że zgodnie art. 13 ust.1 lit. d i art. 14 ust. 2 lit. d RODO, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f osobie, której dane dotyczą, należy przekazać informację na temat prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. W Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679 (dostępnych pod linkiem: Wytyczne grupy roboczej) Grupa Robocza Art. 29 wskazuje, że „w ramach najlepszej praktyki administrator może również przedstawić osobie, której dane dotyczą, informacje uzyskane w wyniku testu równowagi, który należy przeprowadzić, aby można było oprzeć się na art. 6 ust.1 lit. f jako podstawie prawnej przetwarzania, zanim jakiekolwiek dane osobowe osoby, której dane dotyczą, zostaną zebrane. Aby nie przytłoczyć odbiorcy informacjami, można je włączyć do warstwowego oświadczenia o ochronie prywatności / warstwowej informacji o polityce prywatności. W każdym przypadku stanowisko GR29 jest takie, że z informacji udzielonych osobie, której dane dotyczą, powinno jasno wynikać, iż informacje dotyczące testu równowagi mogą uzyskać na żądanie. Jest to istotne dla skutecznej przejrzystości w przypadku gdy osoby, których dane dotyczą, mają wątpliwości, czy test równowagi przeprowadzono rzetelnie lub chcą złożyć skargę do organu nadzorczego."

Data wytworzenia informacji: 24.09.2020 r.

Czy trzeba precyzyjnie określać okres przechowywania danych?

Czy administrator jest zobowiązany do precyzyjnego wskazania okresu przechowywania danych, nawet gdy przepisy prawa nie określają go jednoznacznie? Nie znaleźliśmy w przepisach wprost określonego okresu przechowywania danych osobowych (np. ile dni, miesięcy, lat należy przechowywać dane osobowe przetwarzane w określonym celu). Czy jesteśmy zobowiązani do jego wskazania, jeśli z przepisów nie wynika to wprost?

Zgodnie z art. 5 ust. 1 lit. e RODO, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("ograniczenie przechowywania").

Żeby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu (motyw 39 RODO). W tym celu administrator powinien dokonać analizy dotyczących jego działalności przepisów

prawa. W przypadku wielu podmiotów publicznych doprecyzowanie przepisów archiwizacyjnych (ustawy o narodowym zasobie archiwalnym i archiwach) stanowi instrukcja kancelaryjna.

W przypadku zaś podmiotów, w odniesieniu do których brak jest szczegółowych regulacji w tym zakresie, należy stosować ww. wskazane zasady ogólne wynikające z RODO. Konieczność samodzielnego określenia przez administratora okresu przechowywania danych osobowych może zachodzić bowiem nawet w sytuacji, w której cele przetwarzania danych określone są w przepisach prawa. W takich sytuacjach obowiązkiem administratora jest dokonanie oceny, czy cele zostały osiągnięte i czy dane są mu nadal potrzebne.

W piśmiennictwie zwraca się uwagę, że kwestie okresu przechowywania danych zależne są od celu przetwarzania i powinny być oceniane przez administratora mającego pełną wiedzę o danym procesie przetwarzania: „Ogólną zasadą jest zakaz przechowywania danych w nieskończoność. Należy zauważyć, że z tą zasadą koresponduje prawo do usunięcia danych (prawo do bycia zapomnianym). Jednocześnie o tym, jak długo dane mogą być przechowywane, decyduje cel ich przetwarzania. Podkreślenia wymaga, że zgodnie z art. 6 ust. 4 może dojść do zmiany celu, jak również okresy przechowywania mogą być szczegółowo określone w przepisach szczególnych. Z tego względu nie zawsze proste będzie określenie konkretnych okresów przechowywania danych, będzie ono bowiem wymagało analizy wszystkich celów i przepisów, które w tym zakresie mogą mieć zastosowanie.”[8]

Wskazanie okresu, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, określenie kryteriów ustalania tego okresu, jest jednym z elementów podawanych podczas dopełniania obowiązku informacyjnego spełnianego wobec osoby, której dane dotyczą, na mocy art. 13 ust. 2 lit. a i art. 14 ust. 2 lit. a RODO. W Wytycznych Grupy Roboczej Art. 29 w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP260 rev.01 w załączniku dotyczącym informacji, które należy przekazać osobie, której dane dotyczą, na podstawie art. 13 lub art. 14 wskazano (str. 46), że okres przechowywania (lub kryteria jego ustalania) może być podyktowany takimi czynnikami, jak wymogi ustawowe lub wytyczne branżowe, jednak informacja o nim powinna być sformułowana w taki sposób, aby osoba, której dane dotyczą, miała możliwość ocenienia – na podstawie własnej sytuacji – ile będzie trwał okres przechowania w przypadku określonych danych/celów. Ogólne stwierdzenie przez administratora, że dane osobowe będą przechowywane tak długo, jak jest to niezbędne do prawnie uzasadnionych celów przetwarzania, jest niewystarczające. W stosownych przypadkach należy ustalić różne okresy przechowywania dla różnych kategorii danych osobowych lub różnych celów przetwarzania, w tym okresy archiwizacji.

[8] P. Drobek [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 5.

Dodać należy, że precyzyjne określenie tego okresu jest też wymagane również w związku z obowiązkiem prowadzenia rejestru czynności przetwarzania (art. 30 ust. 1 lit. f RODO).

Data wytworzenia informacji: 15.10.2020 r.

Czy trzeba dopełniać obowiązku informacyjnego wobec rodziny pracownika korzystającego z ZFŚS?

Czy pracodawca powinien spełnić obowiązek informacyjny wobec członków rodziny pracownika korzystającego z zakładowego funduszu świadczeń socjalnych (ZFŚS) w przypadku, gdy będą przetwarzane dane dotyczące jego sytuacji życiowej, rodzinnej (w tym dane członków jego rodziny)? Czy może w tym przypadku będzie miało zastosowanie zwolnienie z tego obowiązku określone w art. 14 ust. 5 lit. c. RODO?

Artykuł 8 ust. 1 ustawy o zakładowym funduszu świadczeń socjalnych zobowiązuje pracodawcę do tego, by uzależnił udzielenie ulgi lub świadczenia od sytuacji życiowej, rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu. Oznacza to, że pracodawca musi poznać i ocenić sytuację życiową, a także materialną wszystkich członków rodziny pracownika, z którymi prowadzi on wspólne gospodarstwo domowe. Dlatego w celu realizacji tych potrzeb musi przetwarzać dane osobowe pracownika i członków jego rodziny. Udostępnienie pracodawcy danych osobowych osoby uprawnionej do korzystania z Funduszu, w celu przyznania ulgowej usługi i świadczenia oraz dopłaty z Funduszu i ustalenia ich wysokości, następuje w formie oświadczenia. Pracodawca może żądać udokumentowania danych osobowych w zakresie niezbędnym do ich potwierdzenia. Potwierdzenie może odbywać się w szczególności na podstawie oświadczeń i zaświadczeń o sytuacji życiowej (w tym zdrowotnej), rodzinnej i materialnej osoby uprawnionej do korzystania z Funduszu (art. 8 ust. 1a ww. ustawy).

Zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych (motyw 60). Dlatego art. 13 i 14 RODO nakładają na administratorów obowiązek informowania osób, których dane przetwarzają, o fakcie i okolicznościach przetwarzania danych. Jednocześnie jednak w ww. artykułach przewidziane zostały wyjątki od tego obowiązku.

Zgodnie z art. 14 ust. 5 lit. c. RODO, administrator jest zwolniony ze spełniania obowiązku informacyjnego w sytuacji, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem (przepisami prawa UE lub prawa państwa członkowskiego, któremu podlega administrator), przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane

dotyczą. Art. 8 ustawy o zakładowym funduszu świadczeń socjalnych określa zasady pozyskiwania danych członków rodziny pracownika w związku z korzystaniem przez niego z ZFŚS. Wobec tego w takim przypadku można zasadnie rozważać skorzystanie ze wskazanego w art. 14 ust. 5 lit. C RODO zwolnienia.

Data wytworzenia informacji: 15.10.2020 r.

Jaki jest status projektanta w związku z wykonywaniem prac projektowych?

Czy w sytuacji, gdy przedmiotem umowy jest kompleksowe wykonanie prac projektowych obejmujące w szczególności pozyskanie na rzecz zamawiającego prawa dysponowania terenem, niezbędnym do wybudowania inwestycji, w tym m.in. pozyskanie danych osobowych właścicieli nieruchomości z ewidencji gruntów i budynków lub bezpośrednio od właścicieli nieruchomości, wykonawca (projektant) jest procesorem czy też jest odrębnym od zamawiającego administratorem danych osobowych pozyskanych z ewidencji gruntów i budynków lub bezpośrednio od osób?

Artykuł 4 pkt 7 RODO wskazuje, że pojęcie „administrator" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.

W celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem, czy jednak istnieje konieczność zawarcia umowy powierzenia, należy przede wszystkim dokonać analizy okoliczności faktycznych z uwzględnieniem zadań określonych podmiotów wynikających m.in. z przepisów prawa oraz zawartej między zamawiającym (inwestorem) a projektantem (wykonawcą) umowy o wykonanie prac projektowych.

Rozpatrując status zarówno projektanta (wykonawcy), jak i zamawiającego (inwestora), należy przede wszystkim wziąć pod uwagę, czy dany podmiot samodzielnie decyduje o sposobach i celach przetwarzania, uwzględniając przy tym ustalony między nimi zakres obowiązków i odpowiedzialności oraz szczegóły wynikające z konkretnych postanowień umownych.

Artykuł 17 Prawa budowlanego stanowi, że projektant jest uczestnikiem procesu budowlanego, którego efektem ma być powstanie zaprojektowanej przez niego inwestycji. Ma on interes prawny w dostępie do danych osobowych zawartych w ewidencji gruntów i budynków, bowiem jednym z podstawowych obowiązków projektanta – wskazanych w art. 20 Prawa budowlanego jest m.in. uzyskanie wymaganych opinii, uzgodnień i sprawdzeń rozwiązań projektowych w zakresie wynikającym z odrębnych przepisów.

W wielu przypadkach, gdy następuje przekazanie realizacji zadania (zamówienia) innemu podmiotowi, który realizuje je (także w zakresie przetwarzania danych) w sposób niezależny, samodzielnie decydując o sposobach i celach przetwarzania, a zadania i obowiązki uczestników procesu budowlanego są wyraźnie rozdzielone i określone, istnieją podstawy do uznania ich za odrębnych administratorów. Powierzenie przetwarzania powinno mieć natomiast miejsce wówczas, gdy zewnętrzny podmiot przetwarza dane w imieniu administratora, w celu i w sposób przez niego określony. W niektórych przypadkach warto zwrócić uwagę na rozwiązanie określone w art. 26 RODO, tj. instytucję współadministrowania.

Wiele pomocnych wskazówek w zakresie rozstrzygania kwestii statusu podmiotów znaleźć można w wytycznych Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO. Dokument ten jest jeszcze w fazie konsultacji, jednak zapoznanie się z nim z pewnością ułatwi dokonywanie oceny co do poszczególnych ról w konkretnym procesie przetwarzania danych. Szczególnie pomocny może okazać się schemat zamieszczony w załączniku nr 1 (Annex 1, str. 46), zawierający pytania ułatwiające dokonywanie tej oceny.

Data wytworzenia informacji: 15.10.2020 r.

Czy z firmą szkoleniową trzeba zawrzeć umowę powierzenia?

W związku z koniecznością przeprowadzenia szkolenia BHP dla naszych pracowników planujemy skorzystać z usług firmy szkoleniowej. Zastanawiamy się jednak, jak prawidłowo określić rolę naszą i tej firmy w procesie przetwarzania danych osobowych. Czy pracodawca w każdym przypadku, gdy kieruje pracownika na szkolenie (BHP, podnoszące kwalifikacje), powinien zawrzeć z firmą szkoleniową umowę powierzenia, o której mowa w art. 28 ust. 3 RODO?

W celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem, czy jednak istnieje konieczność zawarcia umowy powierzenia, należy przede wszystkim dokonać analizy okoliczności faktycznych z uwzględnieniem zadań określonych podmiotów wynikających m.in. z przepisów prawa oraz zawartej pomiędzy nimi umowy. Trzeba brać pod uwagę, jak w szczegółach realizowane są obowiązki przeprowadzenia szkolenia w konkretnym przypadku i jak pracodawca i firma szkoleniowa uzgodniły swoje role oraz zadania w zakresie przetwarzania danych, a także na ile samodzielnie i w jakich celach podmioty te przetwarzają dane w celach związanych ze szkoleniem.

W wielu przypadkach, gdy następuje przekazanie realizacji zadania innemu podmiotowi, który realizuje je (także w zakresie przetwarzania danych) w sposób niezależny, samodzielnie decydując o sposobach i celach przetwarzania, a zadania i obowiązki tego podmiotu są dodatkowo dość

szczegółowo określone w przepisach prawa, istnieją podstawy do uznania ich za odrębnych administratorów. Powierzenie przetwarzania powinno mieć natomiast miejsce wówczas, jeśli zewnętrzny podmiot przetwarza dane w imieniu administratora, w celach i w sposób przez niego określony. W niektórych przypadkach warto zwrócić uwagę na rozwiązanie określone w art. 26 RODO, tj. instytucję współadministrowania.

Zgodnie z art. 94 pkt 4 ustawy Kodeks pracy, pracodawca jest obowiązany w szczególności zapewniać bezpieczne i higieniczne warunki pracy oraz prowadzić systematyczne szkolenie pracowników w zakresie bezpieczeństwa i higieny pracy. Natomiast zgodnie z brzmieniem § 4 ust. 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy, szkolenie może być organizowane i prowadzone przez pracodawców lub, na ich zlecenie, przez jednostki organizacyjne prowadzące działalność szkoleniową w dziedzinie bezpieczeństwa i higieny pracy. Pracodawca może zatem realizować obowiązek nałożony na niego w art. 94 pkt 4 Kodeksu pracy samodzielnie lub za pośrednictwem firmy zewnętrznej (korzystając z jej usług).

Firma zewnętrzna w procesie przetwarzania może występować w roli organizatora szkolenia, o którym mowa w § 4 pkt 1 rozporządzenia Ministra Gospodarki i Pracy z dnia 27 lipca 2004 r. w sprawie szkolenia w dziedzinie bezpieczeństwa i higieny pracy. W § 5 pkt. 1-6 tego rozporządzenia zostały określone obowiązki organizatora szkolenia. Należy do nich zapewnienie: programu poszczególnych rodzajów szkolenia opracowanego dla określonych grup stanowisk; programu szkolenia instruktorów w zakresie metod prowadzenia instruktażu - w przypadku prowadzenia takiego szkolenia; wykładowców i instruktorów posiadających zasób wiedzy, doświadczenie zawodowe i przygotowanie dydaktyczne zapewniające właściwą realizację programów szkolenia; odpowiednich warunków lokalowych do prowadzenia działalności szkoleniowej; wyposażenie dydaktyczne niezbędne do właściwej realizacji programów szkolenia; właściwy przebieg szkolenia oraz prowadzenia dokumentacji w postaci programów szkolenia, dzienników zajęć, protokołów przebiegu egzaminów i rejestru wydanych zaświadczeń.

Jednostka organizacyjna prowadząca działalność szkoleniową w dziedzinie bezpieczeństwa i higieny pracy, realizując nałożone na nią w ww. rozporządzeniu obowiązki, przetwarza dane pracownika w związku ze sporządzaniem protokołów z przebiegu egzaminów i rejestru wydanych zaświadczeń oraz w zakresie nawiązania współpracy (zawarcia stosownych umów) z wykładowcami i instruktorami posiadającymi zasób wiedzy, doświadczenie zawodowe i przygotowanie dydaktyczne zapewniające właściwą realizację programów szkolenia (§ 5 pkt. 3 i 6 ww. rozporządzenia Ministra Gospodarki i Pracy). W tym zakresie zasadnie można uznać, że przetwarza dane jako administrator w rozumieniu przepisów o ochronie danych osobowych.

Odnosząc się do zagadnienia, kto jest administratorem w przypadku „szkoleń podnoszących kwalifikacje pracowników”, wskazuję, że również w tym wypadku należy dokonać analizy, kto

podejmuje decyzje w zakresie kluczowych kwestii dla danego procesu przetwarzania. Na przykład, rola pracodawcy, który kieruje swoich pracowników na szkolenie, może ograniczać się tylko do rozdysponowania formularzy przygotowanych przez firmę, która oferuje szkolenie, a wszystkie kluczowe decyzje co do procesu przetwarzania danych należą do firmy szkoleniowej.

Warto nadmienić, że pomocą w dokonywaniu oceny ról poszczególnych podmiotów są Wytyczne Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO. Warto zwrócić uwagę na schemat zamieszczony w załączniku nr 1 (Annex 1, str. 46), zawierający pytania ułatwiające dokonywanie tej oceny.

Data wytworzenia informacji: 15.10.2020 r.

Czy izba wytrzeźwień musi wypełniać obowiązek informacyjny z art. 14 RODO?

Izba wytrzeźwień może przyjąć do wytrzeźwienia osoby doprowadzone przez właściwe służby, tj. policję oraz straż miejską. Funkcjonariusz doprowadzający ma obowiązek sporządzenia „protokołu doprowadzenia w celu wytrzeźwienia", który zawiera dane osobowe osoby doprowadzonej. Dodatkowo wiele innych danych izba pozyskuje już bezpośrednio od doprowadzonej osoby, np. bada zawartość alkoholu w wydychanym powietrzu w celu podjęcia decyzji zarówno o przyjęciu do izby, jak i zwolnieniu z izby po wytrzeźwieniu. W związku z tym, czy oprócz elementów przewidzianych przez art. 13 RODO, izba powinna poinformować o dodatkowych elementach przewidzianych w art. 14 RODO (kategorie odnośnych danych osobowych, źródło pochodzenia danych osobowych)? Czy zachodzi tutaj może wyłączenie przewidziane przez art. 14. ust. 5 lit. c RODO?

Jednym z przewidzianych w RODO obowiązków administratora jest obowiązek informacyjny, tj. obowiązek przekazania przez administratora osobie, której dane dotyczą, określonych informacji. W świetle przepisów RODO obowiązek informacyjny należy spełniać, chyba że zachodzi jedna z przesłanek, która z niego zwalnia. Kwestia ta została odmiennie uregulowana w zależności od tego, czy mamy do czynienia z pierwotnym (art. 13 RODO) czy z wtórnym pozyskiwaniem danych (art. 14 RODO).

Artykuł 14 RODO stanowi o obowiązku informacyjnym w przypadku, gdy dane są pozyskiwane z innych źródeł niż od osoby, której one dotyczą, a jednym z wyjątków zwalniających od dopełniania tego obowiązku jest przypadek, gdy pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem (przepisami prawa UE lub prawa państwa członkowskiego, któremu podlega administrator), przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą (art. 14 ust. 5 lit. c RODO). Wskazane zwolnienie obejmuje sytuacje, w których przepisy zawierają wyraźne regulacje dotyczące przetwarzania (pozyskiwania

lub ujawniania) danych. Ma ono szczególne znaczenie dla podmiotów publicznych (zwłaszcza administracji publicznej), które – zgodnie z zasadą legalizmu – opierają swoje działania na przepisach prawa. Zwrócić należy jednak uwagę, że obejmuje ono jedynie gromadzenie danych z innych źródeł, natomiast nie przewidziano go w odniesieniu do gromadzenia przez administrację publiczną danych od osób, których one dotyczą.

Inspektor ochrony danych wskazał w pytaniu, że dane osób przebywających w izbie wytrzeźwień pozyskiwane są przez izbę zarówno od osoby, której dotyczą, jak i z innych źródeł, tj. z protokołu przekazanego przez doprowadzającego tę osobę do izby.

Jeśli izba przetwarzałaby jedynie dane pozyskane z ww. innych źródeł, wówczas zasadnie można rozważać zastosowanie przesłanki zwolnienia wskazanej w art. 14 ust. 5 lit. c RODO. Jednak w tej sytuacji izba pozyskuje część danych również bezpośrednio od osoby. Z tego względu należy przyjąć, że rozwiązaniem gwarantującym zachowanie przejrzystości będzie - zaproponowane przez przesyłającego powyższe pytanie inspektora - rozwiązanie, aby w informacji kierowanej do osoby, której dane dotyczą, oprócz elementów przewidzianych przez art. 13 RODO, informować o dodatkowych źródłach pochodzenia danych osobowych.

Warto przy tym przypomnieć, że wiele wskazówek oraz przykładów w jaki sposób spełniać obowiązek informacyjny znaleźć można w szczególności w Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP260 rev.01 dostępnych pod linkiem: Wytyczne grupy roboczej, a także w prezentacjach ze szkoleń oraz webinariach dot. obowiązku informacyjnego dostępnych na stronie internetowej UODO (np.: https://uodo.gov.pl/pl/189/727, https://uodo.gov.pl/pl/213/930).

Data wytworzenia informacji: 12.11.2020 r.

Na jakiej podstawie OPS przetwarza dane wolontariuszy w akcji „Wspieraj Seniora”?

Czy prawidłowe jest przyjęcie przez ośrodek pomocy społecznej (OPS), że przetwarzanie danych osobowych wolontariuszy biorących udział w akcji „Wspieraj Seniora” następuje na podstawie zgody? Czy nie jest właściwszym zawarcie umowy z wolontariuszem zgłaszającym się do OPS i wtedy wybranie art. 6 ust. 1 lit. b RODO jako przesłanki legalizującej przetwarzanie?

Zgodnie z art. 42 ust. 1 pkt 2 i 3 ustawy o działalności pożytku publicznego i o wolontariacie wolontariusze mogą wykonywać świadczenia m.in. na rzecz organów administracji publicznej oraz jednostek organizacyjnych podległych organom administracji publicznej lub nadzorowanych przez te organy (z wyłączeniem prowadzonej przez te organy i jednostki działalności gospodarczej).

Wymienione w tym przepisie podmioty, na rzecz których wolontariusze mogą wykonywać świadczenia, zwane są w ww. ustawie "korzystającymi".

Zgodnie natomiast z art. 44 ust. 1 ustawy o działalności pożytku publicznego i o wolontariacie, podstawą podjęcia przez wolontariusza na rzecz korzystającego świadczeń jest porozumienie pomiędzy nim a korzystającym. Przepis ten stanowi, że świadczenia wolontariuszy są wykonywane w zakresie, w sposób i w czasie określonych w porozumieniu.

Wobec tego podstawą przetwarzania przez ośrodek pomocy społecznej danych osobowych wolontariusza w celu zawarcia i realizacji takiego porozumienia będzie art. 6 ust. 1 lit. b RODO (tj. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy).

Ponadto należy wskazać, że pomocne informacje dotyczące bezpiecznego korzystania ze świadczeń wolontariuszy znaleźć można w materiale pt. „Wolontariat musi szczególnie dbać o ochronę danych beneficjentów”- link: https://uodo.gov.pl/pl/138/1284 - **z tego linka odzyskanie treści nie jest możliwe**. Zaleca się w nim m.in. aby zrobić szkolenie dla wolontariuszy w celu zapoznania ich z polityką poufności oraz zasadami przetwarzania danych osobowych, a także, aby zwracać szczególną uwagę kogo upoważnia się do dostępu do danych i co się dzieje z danymi na każdym etapie ich przetwarzania.

Data wytworzenia informacji: 12.11.2020 r.

Czy kilku administratorów może mieć jedną dokumentację ochrony danych osobowych?

Czy administratorzy funkcjonujący w ramach tej samej jednostki mogą opracować wspólną dokumentację ochrony danych osobowych?

Istnienie w strukturach, np. urzędu gminy czy starostwa, więcej niż jednego podmiotu będącego odrębnym administratorem, nie musi oznaczać konieczności stworzenia procedur i polityk ochrony danych osobowych w odrębnych dokumentach dla każdego z administratorów. Jedna dokumentacja może bowiem regulować kwestie ochrony danych dotyczące administratorów istniejących w ramach tej samej jednostki. Przy czym kwestię tę, w kontekście prowadzonego przetwarzania, należy starannie przemyśleć oraz zapewnić to, by z dokumentacji jasno wynikało, jakich administratorów i danych, za które oni odpowiadają, dokumentacja ta dotyczy.

Artykuł 24 RODO nakłada na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, zapewniających zgodność przetwarzania z wymogami tego rozporządzenia. Zgodnie z ust. 2 tego artykułu – jeżeli jest to proporcjonalne w stosunku do

czynności przetwarzania – powyższe środki powinny obejmować wdrożenie przez administratora odpowiednich polityk ochrony danych. W przepisach rozporządzenia nie przewidziano szczegółowych wymogów dotyczących zarówno zakresu merytorycznego, jak i formy polityk ochrony danych. W świetle zasady rozliczalności do administratora należy decyzja, w jaki sposób skonstruuje funkcjonujący u siebie system ochrony danych osobowych, przy czym system ten powinien dotyczyć całości procesów przetwarzania prowadzonych u danego administratora i realnie wpływać na prawidłowość, bezpieczeństwo oraz przejrzystość przetwarzania.

W przypadku podmiotów publicznych charakter, zakres, kontekst i cele prowadzonego przez nie przetwarzania wskazują na obowiązek wdrożenia odpowiednich polityk ochrony danych osobowych. Warto również zwrócić uwagę, że art. 24 ust. 2 RODO mówi o **politykach** ochrony danych osobowych, tak więc może to być nie jeden dokument, a zespół kilku dokumentów (polityk tematycznych) obejmujących wszelkie informacje o stosowanych środkach i procedurach związanych z ochroną danych osobowych. W odniesieniu do poszczególnych elementów tej dokumentacji należy również przemyśleć, jakie kategorie osób zatrudnionych w jednostce organizacyjnej muszą się z nimi zapoznać i stosować w związku z wykonywanymi przez siebie zadaniami.

Zdarzyć się też mogą sytuacje, w których poszczególni administratorzy funkcjonujący w ramach jednej jednostki organizacyjnej podlegać będą jednocześnie również innym niż RODO regulacjom dotyczącym ochrony danych osobowych, np. ustawie z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Regulacje te mogą przewidywać specyficzne rozwiązania dotyczące prowadzenia dokumentacji ochrony danych, które również powinny być uwzględnione przez administratorów w prowadzonej dokumentacji. Więcej informacji na ten temat znaleźć można w odpowiedzi na pytanie „CZY KOMENDANT STRAŻY MIEJSKIEJ MUSI POSIADAĆ ODRĘBNĄ POLITYKĘ OCHRONY DANYCH?”.

Reasumując, administratorzy funkcjonujący w ramach tej samej jednostki, biorąc pod uwagę strukturę i realizowane przez nich zadania, powinni dokonać oceny co do odpowiedniego w ich przypadku sposobu prowadzenia dokumentacji ochrony danych osobowych. W sytuacji, gdy nie będzie możliwości objęcia jednym dokumentem procesów i procedur funkcjonujących u różnych administratorów, stworzenie odrębnego dokumentu może ułatwić tym administratorom przestrzeganie zasad ochrony danych i obowiązków określonych w różnych przepisach o ochronie danych osobowych. Każdy z administratorów – niezależnie od tego, czy będzie to wspólny dokument czy odrębne polityki - musi być bowiem w stanie wykazać, że wywiązał się ze wszystkich ciążących na nim obowiązków wynikających z przepisów o ochronie danych osobowych.

Data wytworzenia informacji: 26.11.2020 r.

Jaki jest status geodetów w postępowaniu rozgraniczeniowym?

Proszę o potwierdzenie stanowiska, które wypracowaliśmy wspólnie z IOD z różnych jednostek. Sprawa dotyczy geodetów, którzy niejednokrotnie współpracują z jednostkami samorządu terytorialnego lub występują do jednostek samorządu w imieniu inwestorów (osób fizycznych).

W naszej ocenie zakres uprawnień przysługujący geodecie przemawia za tym, aby traktować go w postępowaniu rozgraniczeniowym jako odrębnego administratora, a więc zawarcie umowy powierzenia nie jest konieczne, a wręcz stanowiłoby działanie nieprawidłowe. Geodeta zbiera dowody świadczące o stanie prawnym nieruchomości i dokonuje ich oceny mając na uwadze gradację tych dowodów wynikającą z przepisów art. 33, 34 i 35 ustawy Prawo geodezyjne i kartograficzne. Bada również, czy zachodzą przesłanki do zawarcia ugody granicznej i powinien odmówić spisania takiej ugody, gdyby jej treść była wyraźnie sprzeczna ze zgromadzonym w sprawie miarodajnym materiałem dowodowy. Czynności podejmowane przez geodetę w trakcie rozprawy granicznej, sytuują zdaniem niektórych przedstawicieli doktryny geodetę w pozycji mediatora-koncyliatora. Organ administracji prowadzący postępowanie rozgraniczeniowe nie dysponuje w stosunku do geodety środkami dyscyplinującymi przewidzianymi w kodeksie postępowania administracyjnego. Ponadto obowiązki geodety są znacznie szersze niż obowiązki biegłych w innych postępowaniach. Wprawdzie właściwy organ przed wydaniem decyzji administracyjnej, działając na podstawie art. 33 ust. 2 ww. ustawy dokonuje oceny prawidłowości wykonania czynności ustalenia przebiegu granic a w przypadku stwierdzenia wadliwości w tym zakresie zwraca dokumentację do poprawy i uzupełnienia, jednak mimo to geodeta sporządzając przedmiotową dokumentację samodzielnie dokonuje oceny treści w niej umieszczonych, a więc decyduje o celach i sposobie przetwarzania danych.

W przypadku wielu podmiotów to, w jakich celach i zakresie mają one przetwarzać dane – w związku z realizacją konkretnych zadań lub czynności - wynika z przepisów, które te zadania określają. W takiej sytuacji prawo w sposób pośredni określa, kto jest administratorem. Przepisy prawa mogą bowiem nakładać na podmioty publiczne lub prywatne obowiązek pozyskiwania określonych danych i wykorzystania ich w określonym celu. Jak wskazuje Europejska Rada Ochrony Danych podmioty te powinny być wówczas uznawane za administratorów danych w odniesieniu do przetwarzania, które jest niezbędne do wykonania określonego obowiązku (por. Wytyczne w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO).

Skoro zatem o tym, czy dany organ, jednostka organizacyjna albo innego rodzaju podmiot jest administratorem danych osobowych, może decydować rodzaj i charakter nadanych im przez prawo kompetencji oraz wyznaczone ustawowo zadania, to do uznania danego podmiotu za administratora danych potrzebna jest zatem analiza przepisów prawa określających te zadania.

3 ZADANIA IOD

Zasady rozgraniczania nieruchomości określone zostały w ustawie z 17 maja 1989 r. Prawo geodezyjne i kartograficzne, zwanej dalej „ustawą”, oraz w rozporządzeniu wykonawczym do tej ustawy wydanym przez Ministrów Spraw Wewnętrznych i Administracji oraz Rolnictwa i Gospodarki Żywnościowej z dnia 14 kwietnia 1999 r. w sprawie rozgraniczania nieruchomości, zwanym dalej „rozporządzeniem”. Zgodnie z art. 29 ww. ustawy rozgraniczenia nieruchomości dokonują wójtowie (burmistrzowie, prezydenci miast) oraz, w wypadkach określonych w ustawie, sądy.

Zgodnie zaś z art. 31 ust. 1 ustawy czynności ustalania przebiegu granic wykonuje geodeta upoważniony przez wójta (burmistrza, prezydenta miasta).

W razie sporu co do przebiegu linii granicznych, geodeta nakłania strony do zawarcia ugody. Ugoda zawarta przed geodetą posiada moc ugody sądowej (art. 31 ust. 4 ustawy).

Stosownie do art. 33 ust. 1 wójt (burmistrz, prezydent miasta) wydaje decyzję o rozgraniczeniu nieruchomości, jeżeli zainteresowani właściciele nieruchomości nie zawarli ugody, a ustalenie przebiegu granicy nastąpiło na podstawie zebranych dowodów lub zgodnego oświadczenia stron. Wydanie tej decyzji poprzedza m.in. dokonanie przez wójta, burmistrza (prezydenta miasta) oceny prawidłowości wykonania czynności ustalenia przebiegu granic nieruchomości przez upoważnionego geodetę oraz zgodności sporządzonych dokumentów z przepisami; w wypadku stwierdzenia wadliwego wykonania czynności upoważnionemu geodecie zwraca się dokumentację do poprawy i uzupełnienia (art. 33 ust. 2 ustawy).

Zgodnie z art. 34 ust. 1 i ust. 2 jeżeli w razie sporu co do przebiegu linii granicznych nie dojdzie do zawarcia ugody lub nie ma podstaw do wydania ww. decyzji upoważniony geodeta tymczasowo utrwala punkty graniczne według ostatniego stanu spokojnego posiadania, dokumentów i wskazań stron, oznacza je na szkicu granicznym, sporządza opinię i całość dokumentacji przekazuje właściwemu wójtowi (burmistrzowi, prezydentowi miasta), który umarza postępowanie administracyjne i przekazuje sprawę z urzędu do rozpatrzenia sądowi.

Wskazane powyżej rozporządzenie w sprawie rozgraniczania nieruchomości precyzuje w szczególności sposób i tryb wykonywania przez geodetę czynności ustalania przebiegu granic i sporządzania dokumentacji przy rozgraniczaniu nieruchomości. Zgodnie z postanowieniami tego aktu do zadań geodety w ramach postępowania rozgraniczającego należy w szczególności: dokonanie wywiadu terenowego, przeprowadzenie analizy informacji zawartych w dokumentach uzyskanych z państwowego zasobu geodezyjnego i kartograficznego oraz znajdujących się w księgach wieczystych, a także w dokumentacji uzyskanej od stron postępowania, ustalanie terminu rozpoczęcia czynności rozgraniczenia i doręcza stronom wezwania do stawienia się na gruncie, sporządzenie protokołu granicznego, nakłanianie stron do zawarcia ugody (§8 i § 11). Podczas negocjacji geodeta przedstawia stronom wszystkie dowody i argumenty za proponowanym przebiegiem granicy, a także informuje, że w razie braku ugody do rozpatrzenia

sprawy właściwy jest sąd (§ 13). Jeśli natomiast geodeta doprowadzi do zawarcia ugody wówczas zobowiązany jest do sporządzenia aktu ugody (§ 14).

Z powyższych przepisów wynika, że geodeta w tym postępowaniu występuje jako posiadający określoną wiedzę geodezyjną specjalista. Jest to szczególne rozwiązanie, bo wymienione czynności związane z ustaleniem granic wykonuje podmiot zewnętrzny - tzn. podmiot występujący poza strukturą prowadzącego postępowanie organu administracji.[9]

W treści powołanych wyżej przepisów ustawy oraz rozporządzenia został wskazany zakres zadań (kompetencji) zarówno wójta (burmistrza, prezydenta), jak i geodety w związku z przeprowadzeniem postępowania rozgraniczającego.

Jak wskazuje się w doktrynie geodeta samodzielnie gromadzi materiał dowodowy, ustala krąg podmiotów zainteresowanych wynikiem postępowania, wyznacza termin „rozprawy", wzywa na nią strony i „rozprawę" tę prowadzi, sporządzając z niej protokół graniczny.[10] Posiada kompetencje do zakończenia sprawy poprzez doprowadzenie stron do zawarcia cywilnoprawnej umowy o skutkach ugody sądowej. Do zadań geodety należy również dokonywanie pomiarów i sporządzanie dokumentacji technicznej.

Do zadań wójta (burmistrza, prezydenta miasta) należy natomiast w szczególności wszczęcie postępowania rozgraniczeniowego, wyznaczenie geodety, w określonych sytuacjach ocena prawidłowości wykonania czynności ustalenia przebiegu granic nieruchomości przez upoważnionego geodetę, wydawanie decyzji o rozgraniczeniu nieruchomości, jeżeli zainteresowani właściciele nieruchomości nie zawarli ugody, a także umarzanie postępowania administracyjnego i przekazywanie sprawy z urzędu do rozpatrzenia sądowi.

Wobec tego można zasadnie przyjąć, że w powyższym postępowaniu wójt (burmistrz, prezydent), jak i upoważniony przez wójta geodeta w zakresie przetwarzania danych niezbędnych do przeprowadzenia rozgraniczenia to odrębni administratorzy. Każdy z nich w swoim własnym zakresie realizuje konkretne zadania wynikające z powołanych wyżej przepisów prawa i przetwarza dane, które są niezbędne dla realizacji tych zadań. Tym samym zawarcie umowy powierzenia w przedstawionej sytuacji jest zbędne.

Data wytworzenia informacji: 29.12.2020 r.

[9] Durzyńska Magdalena i in., Prawo geodezyjne i kartograficzne. Komentarz, art. 31, Lex online

[10] Lang Jacek (red.), Maćkowiak Jarosław (red.), Myśliński Tomasz (red.), Stefańska Ewa (red.), Prawo geodezyjne i kartograficzne. Komentarz, wyd. II, art. 31, Lex online

Czy Policja może udostępnić poszkodowanemu dane sprawcy wypadku?

Jestem inspektorem ochrony danych w jednej z jednostek Policji. Mam wątpliwość, czy możemy osobom poszkodowanym udostępnić dane osobowe uczestników zdarzenia drogowego (np. wypadku), jeśli zwracają się oni z wnioskiem o udostępnienie takich danych, wskazując, że chcą dochodzić roszczeń na drodze cywilnoprawnej. Wniosek do sądu nie został jeszcze złożony. Zastanawiam się przy tym, czy przepisy prawa nie wskazują osobie poszkodowanej innej drogi uzyskiwania potrzebnych jej do dochodzenia roszczeń informacji.

Przepisem dającym uprawnienie do otrzymania przez osobę uczestniczącą w wypadku drogowym, na jej żądanie, danych osobowych kierującego pojazdem, danych właściciela lub posiadacza pojazdu oraz danych dotyczących zakładu ubezpieczeń, z którym zawarta jest umowa obowiązkowego ubezpieczenia odpowiedzialności cywilnej jest art. 44 ust. 1 pkt 4 ustawy Prawo o ruchu drogowym. Zgodnie z jego treścią kierujący pojazdem w razie uczestniczenia w wypadku drogowym jest obowiązany podać swoje dane personalne, dane personalne właściciela lub posiadacza pojazdu oraz dane dotyczące zakładu ubezpieczeń, z którym zawarta jest umowa obowiązkowego ubezpieczenia odpowiedzialności cywilnej, na żądanie osoby uczestniczącej w wypadku. Niespełnienie tego obowiązku przez kierującego pojazdem może wyczerpywać znamiona art. 97 Kodeksu wykroczeń.[11]

Warto również nadmienić, że zgodnie z art. 16 ust. 2 pkt 1 ustawy **o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych** w razie zaistnienia zdarzenia objętego ubezpieczeniem obowiązkowym osoba uczestnicząca w nim jest obowiązana m.in. do udzielenia pozostałym uczestnikom zdarzenia niezbędnych informacji koniecznych do identyfikacji zakładu ubezpieczeń, łącznie z podaniem danych dotyczących zawartej umowy ubezpieczenia.[12]

[11] Zgodnie z art. 97 Kodeksu wykroczeń uczestnik ruchu lub inna osoba znajdująca się na drodze publicznej, w strefie zamieszkania lub strefie ruchu, a także właściciel lub posiadacz pojazdu, który wykracza przeciwko innym przepisom ustawy z dnia 20 czerwca 1997 r. - Prawo o ruchu drogowym lub przepisom wydanym na jej podstawie, podlega karze grzywny do 3000 złotych albo karze nagany.

[12] Art. 17 ustawy o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych stanowi natomiast, że jeżeli osoba objęta ubezpieczeniem obowiązkowym odpowiedzialności cywilnej lub osoba występująca z roszczeniem, z winy umyślnej lub rażącego niedbalstwa, nie dopełniły obowiązków wymienionych w art. 16 tej ustawy, a miało to wpływ na ustalenie istnienia lub zakresu ich odpowiedzialności cywilnej bądź też na zwiększenie rozmiarów szkody, zakład ubezpieczeń może dochodzić od tych osób zwrotu części wypłaconego uprawnionemu odszkodowania lub ograniczyć wypłacane tym osobom odszkodowanie. Ciężar udowodnienia faktów, uzasadniających zwrot zakładowi ubezpieczeń części odszkodowania lub ograniczenia odszkodowania, spoczywa na zakładzie ubezpieczeń.

Na podstawie informacji uzyskanych na podstawie powyższych przepisów od kierującego pojazdem poszkodowany może zgłosić zdarzenie ubezpieczycielowi, który jest uprawniony uzyskać od Policji dodatkowe informacje na temat wypadku. Zgodnie z art. 42 ust. 1 ustawy o działalności ubezpieczeniowej i reasekuracyjnej m.in. Policja na wniosek zakładu ubezpieczeń, w zakresie zadań przez ten zakład ubezpieczeń wykonywanych i w celu ich wykonania, w związku z wypadkiem lub zdarzeniem losowym będącym podstawą ustalania odpowiedzialności, udzielają informacji o stanie sprawy oraz udostępniają zebrane materiały, jeżeli są one niezbędne do ustalenia okoliczności tych wypadków i zdarzeń losowych oraz wysokości odszkodowania lub świadczenia. Ust. 3 tego artykułu stanowi, że zakład ubezpieczeń, na żądanie ubezpieczonego lub uprawnionego z umowy ubezpieczenia, udostępnia posiadane przez siebie informacje związane z wypadkiem lub zdarzeniem losowym będącym podstawą ustalenia jego odpowiedzialności oraz ustalenia okoliczności wypadków i zdarzeń losowych, jak również wysokości odszkodowania lub świadczenia.

Zgodnie z art. 25 ustawy o działalności ubezpieczeniowej Policja na wniosek zakładu ubezpieczeń, w zakresie zadań przez ten zakład ubezpieczeń wykonywanych i w celu ich wykonania, w związku z wypadkiem lub zdarzeniem będącym podstawą ustalania odpowiedzialności, udziela informacji o stanie sprawy oraz udostępnia zebrane materiały, jeżeli są one niezbędne do ustalenia okoliczności tych wypadków i zdarzeń losowych oraz wysokości odszkodowania lub świadczenia.

Z przepisów Prawa o ruchu drogowym, a także ustawy **o ubezpieczeniach obowiązkowych, Ubezpieczeniowym Funduszu Gwarancyjnym i Polskim Biurze Ubezpieczycieli Komunikacyjnych** wynika zatem uprawnienie poszkodowanego do otrzymania danych osobowych sprawcy wypadku.

Co jednak w sytuacji, gdy uczestnik zdarzenia zwraca się o udzielenie informacji dotyczących zdarzenia drogowego do Policji? Wówczas udostępnianie danych następować będzie na podstawie właściwej procedury. W sytuacji wypadku w komunikacji[13] Policja, będąc w posiadaniu powyższych informacji z racji prowadzonego postępowania, jest uprawniona udzielić ich uczestnikowi wypadku komunikacyjnego[14] - https://archiwum.giodo.gov.pl/pl/344/1318 - **treść w ramce poniżej.**

[13] Przestępstwo wypadku komunikacyjnego zostało określone w art. 177 kodeksu karnego. To sytuacja, w której występuje zdarzenie drogowe w ruchu lądowym w postaci nieumyślnego naruszenia obowiązujących zasad bezpieczeństwa czego skutkiem jest zniszczenie mienia oraz śmierć jednego z uczestników lub obrażenia ciała powodujące naruszenie czynności narządu ciała lub rozstrój zdrowia trwające dłużej niż 7 dni.

[14] O takim uprawnieniu poszkodowanego w wypadku Urząd (wówczas Biuro Generalnego Inspektora Ochrony Danych Osobowych) informował na swojej stronie internetowej jeszcze przed wejściem w życie zreformowanych przepisów o ochronie danych osobowych (https://archiwum.giodo.gov.pl/pl/344/1318).

Informacja ze strony archiwalnej GIODO

Czy Policja może odmówić uczestnikom wypadków komunikacyjnych udostępnienia informacji o danych osobowych innych uczestników tych wypadków oraz informacji o ubezpieczycielach, z którymi sprawcy wypadków zawarli umowy ubezpieczenia?

Nie, gdyż z przepisów prawa wynika uprawnienie poszkodowanego do otrzymania danych osobowych sprawcy wypadku.

Uzasadnienie

Przepisem, kształtującym uprawnienie do otrzymywania przez osobę uczestniczącą w wypadku komunikacyjnym, na jej żądanie, danych osobowych kierującego pojazdem, danych właściciela lub posiadacza pojazdu oraz danych dotyczących zakładu ubezpieczeń, z którym zawarta jest umowa obowiązkowego ubezpieczenia odpowiedzialności cywilnej jest art. 44 ust. 1 pkt 4 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym. Zgodnie z jego treścią kierujący pojazdem w razie uczestniczenia w wypadku drogowym jest obowiązany podać swoje dane personalne, dane personalne właściciela lub posiadacza pojazdu oraz dane dotyczące zakładu ubezpieczeń, z którym zawarta jest umowa obowiązkowego ubezpieczenia odpowiedzialności cywilnej, na żądanie osoby uczestniczącej w wypadku.

Przepis ten jest podstawą do pozyskiwania przez wszystkich uczestników wypadków drogowych informacji o wymienionych w nim podmiotach i osobach. Wobec tego odmowę udostępnienia tych danych przez Policję należałoby traktować jako nadużycie ustawy o ochronie danych osobowych, wypływająca z jej niewłaściwej interpretacji.

Reasumując, skoro z przepisów Prawa o ruchu drogowym wynika uprawnienie poszkodowanego do otrzymania danych osobowych sprawcy wypadku, Policja, jako uprawniona do przetwarzania danych, tj. zbierania, utrwalania, przechowywania, udostępniania i usuwania danych ze zbioru na mocy przepisów ustawy z dnia 6 kwietnia 1990 r. o Policji, będąc w ich posiadaniu z racji prowadzonego postępowania, jest zobowiązana takiej informacji udzielić.

W tym przypadku zastosowanie znajduje art. 156 § 5 Kodeksu postępowania karnego (k.p.k.), który stanowi, że (jeżeli nie zachodzi potrzeba zabezpieczenia prawidłowego toku postępowania lub ochrony ważnego interesu państwa) w toku postępowania przygotowawczego stronom, obrońcom, pełnomocnikom i przedstawicielom ustawowym udostępnia się akta, umożliwia sporządzanie odpisów lub kopii oraz wydaje odpłatnie uwierzytelnione odpisy lub kopie; prawo to przysługuje stronom także po zakończeniu postępowania przygotowawczego.

Ta sama zasada dotyczyć będzie spraw o wykroczenie (kolizja drogowa), ponieważ art. 38 § 1 Kodeksu postępowania w sprawach o wykroczenia odsyła do odpowiedniego stosowania do czynności procesowych prowadzonych w postępowaniu w sprawach o wykroczenia przytoczonego wyżej art. 156 § 5 k.p.k.

Udostępnienie informacji (w tym danych osobowych) dotyczących ustaleń Policji w zakresie zdarzenia drogowego może nastąpić również na podstawie przepisów Kodeksu postępowania administracyjnego (k.p.a) dotyczących wydawania zaświadczeń. Art. 217 k.p.a stanowi, że zaświadczenie wydaje się m.in., jeżeli osoba ubiega się o zaświadczenie ze względu na swój interes prawny w urzędowym potwierdzeniu określonych faktów lub stanu prawnego. Przepis ten umożliwia wydanie przez Policję zaświadczenia zawierającego informacje o charakterze, miejscu i czasie zaistnienia zdarzenia, może też zawierać dane o wykonanych przez Policję czynnościach i stwierdzonych uszkodzeniach pojazdów biorących udział w zdarzeniu, a także dane osobowe określone w przytoczonym na wstępie art. 44 ust. 1 pkt 4 Prawa o ruchu drogowym. Wniosek o wydanie zaświadczenia spełnić musi wymogi podania wskazane w art. 63 kpa oraz zawierać odpowiednie uzasadnienie (dochodzenie roszczeń w postępowaniu sądowym), które jest konieczne by organ mógł stwierdzić, czy dopuszczalne jest udostępnienie danych osobowych.

Data wytworzenia informacji: 29.12.2020 r.

Czy IOD może w imieniu administratora zawierać umowy powierzenia?

Czy administrator może upoważnić inspektora ochrony danych do zawierania w jego imieniu wskazanych w art. 28 ust. 3 RODO umów powierzenia z podmiotami zewnętrznymi? Czy obowiązujące przepisy, w tym w szczególności przepisy RODO, wytyczne itp. umożliwiają wdrożenie ww. rozwiązań, czy też jasno wskazują na niemożność ich zastosowania?

Przepisy RODO wymagają przeprowadzenia w tym zakresie oceny pod kątem wypełnienia przez administratora obowiązku określonego w art. 38 ust. 6. Przepis ten wskazuje, że IOD może wykonywać inne (niż te które zostały mu przypisane w RODO) zadania i obowiązki. W dalszej części przepisu występuje jednak zastrzeżenie, iż administrator lub podmiot przetwarzający zobowiązani są zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów.

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 podejmowanie 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. Konflikt interesów może być również rezultatem nadmiaru obowiązków przydzielonych do wykonania IOD, jeśli IOD musi wybrać między obowiązkami, jakie będzie realizował, a którym nie podoła z powodu braku czasu koniecznego na ich wykonanie. Powyższe

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

Inspektor ochrony danych to funkcja, która ma szczególny status w świetle RODO. W związku z monitorowaniem przestrzegania przepisów o ochronie danych osobowych, inspektor musi mieć zagwarantowane odpowiednie warunki funkcjonowania, a więc takie, które pozwolą mu na efektywną, niezależną oraz prawidłową realizację swojej roli i obowiązków wynikających wprost z przepisów prawa.

Dlatego w opisanym przypadku konieczne jest zbadanie, na czym konkretnie miałyby polegać czynności, które inspektor miałby podjąć w związku z zawieraniem umów powierzenia przetwarzania. Trzeba ustalić, czy np. inspektor nie został obarczony zadaniem sporządzenia projektu umowy i w związku z tym, czy to do niego nie należało określenie, w jaki sposób ukształtowana będzie relacja między administratorem i podmiotem przetwarzającym oraz prawa i zobowiązania stron tej umowy. Taka sytuacja powodowałaby konflikt interesów, ponieważ IOD następnie w ramach swoich ustawowych obowiązków zobowiązany byłby ocenić prawidłowość i zgodność z przepisami podjętych w tym zakresie decyzji.

Inspektor nie powinien zatem podejmować 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. Zwraca na to uwagę Grupa Robocza art. 29 w Wytycznych dotyczących inspektorów ochrony danych wskazując, że inspektor nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych. Wymóg niepowodowania konfliktu interesów jest ściśle związany z wymogiem wykonywania zadań w sposób niezależny. Ze względu na indywidualny charakter każdej organizacji ten aspekt powinien być analizowany osobno dla każdego podmiotu.

Wiele informacji na temat kryteriów oceny, czy osoba pełniąca funkcję IOD może pełnić również inne funkcje i obowiązki można znaleźć w zakładce IOD/Wyznaczenie i status IOD na stronie internetowej UODO (Wyznaczenie i status IOD).

Data wytworzenia informacji: 29.12.2020 r.

Czy w przypadku PPE pracodawca powinien zawrzeć umowę powierzenia

Czy pracodawca powinien zawrzeć umowę powierzenia z instytucją finansową oferującą PPE (pracowniczy program emerytalny)?

Jak zwykle w takich sytuacjach, aby określić status danego podmiotu w procesie przetwarzania danych osobowych, należy przede wszystkim kierować się definicjami administratora i podmiotu przetwarzającego zawartymi w RODO. Ponadto jeśli dane są przetwarzane przez podmioty realizujące zadania określone przepisami prawa, należy sięgnąć do takich przepisów.

Zasady tworzenia i działania *pracowniczych programów emerytalnych,* warunki, które powinny spełniać podmioty realizujące programy, oraz warunki uczestnictwa w tych programach określone zostały w szczególności w ustawie z dnia 20 kwietnia 2004 r. o pracowniczych programach emerytalnych (ustawa o PPE).

Zgodnie z jej art. 10 ust. 1, program emerytalny tworzy się:

1. przez zawarcie umowy zakładowej albo umowy międzyzakładowej;
2. następnie przez zawarcie umowy z instytucją finansową, z zastrzeżeniem art. 17 ust. 3, albo utworzenie towarzystwa emerytalnego i funduszu emerytalnego albo nabycie przez pracodawcę akcji istniejącego towarzystwa emerytalnego;
3. następnie przez rejestrację programu przez organ nadzoru.

Zgodnie z art. 17 ust. 1 ustawy o PPE, pracodawca zawiera umowę z instytucją finansową, która określa warunki gromadzenia środków i zarządzania nimi. W przypadku programu w formie funduszu emerytalnego, warunki gromadzenia środków i zarządzania nimi określa statut funduszu.

Kwestie dotyczące deklaracji o przystąpieniu do programu uregulowane zostały w art. 18 powyższej ustawy. Zgodnie z ust. 1 tego przepisu, przystąpienie pracownika do programu na warunkach określonych w umowie zakładowej następuje na podstawie deklaracji o przystąpieniu do programu złożonej w postaci elektronicznej pozwalającej na utrwalenie jej treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono, po upływie miesiąca od dnia jej złożenia, chyba że pracodawca potwierdzi w postaci elektronicznej pozwalającej na utrwalenie treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono, przystąpienie do programu w terminie wcześniejszym.

Deklaracja zawiera oświadczenie pracownika, że otrzymał kopię umowy zakładowej i zapoznał się z jej treścią, akceptuje jej warunki, oraz może zawierać rozrządzenie na wypadek śmierci pracownika (art. 18 ust. 2).

Pracodawca przyjmuje deklarację i potwierdza uczestnikowi jej przyjęcie w postaci elektronicznej pozwalającej na utrwalenie treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono (art. 18 ust. 4). Jeżeli pracownikowi nie przysługuje prawo do uczestnictwa w programie, pracodawca zwraca deklarację wraz z uzasadnieniem odmowy jej przyjęcia w postaci elektronicznej pozwalającej na utrwalenie treści

na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono (art. 18 ust. 5).

Zgodnie z art. 20 ust. 1 ustawy o PPE, **w sprawach dotyczących programu uczestnik składa oświadczenie woli pracodawcy lub za jego pośrednictwem** w postaci elektronicznej pozwalającej na utrwalenie jego treści na trwałym nośniku informacji lub w innej postaci, jeżeli w umowie zakładowej tak określono.

Powyższe przepisy określają zadania każdego z podmiotów zaangażowanych w realizację programu, w tym zadania pracodawcy. W takiej sytuacji zawieranie umowy powierzenia nie jest konieczne, ponieważ pracodawca realizuje tutaj swoje - określone przez ustawodawcę zadania – i w tym zakresie jest odrębnym administratorem.

Oczywiście niezależnie od tego w każdej konkretnej sytuacji trzeba analizować, czy w określonych procesach przetwarzania (w konkretnej relacji między pracodawcą a instytucją finansową) realizowane są tylko takie zadania (operacje na danych). Jeśli dane osobowe przetwarzane są również w innych celach, np. marketingowych, wówczas należy dokonać dodatkowo analizy w tym zakresie. Należy w szczególności ustalić, jakie dane są w tym celu przetwarzane, przez które podmioty, a także którego z tych podmiotów cele są realizowane, a w związku z tym który podmiot decyduje o celach i sposobach przetwarzania tych danych.

Data wytworzenia informacji: 01.02.2021 r.

Czy IOD powinien sporządzić plan audytów?

Obowiązujące przed RODO przepisy dotyczące trybu i sposobu wykonywania zadań przez administratora bezpieczeństwa informacji (ABI) wskazywały, że tzw. sprawdzenia planowe ABI powinien przeprowadzać według planu sprawdzeń, który powinien obejmować okres nie krótszy niż kwartał i nie dłuższy niż rok. Czy w aktualnym stanie prawnym, w przypadku dużej organizacji zatrudniającej ponad 1200 osób (np. urząd wojewódzki) inspektor ochrony danych może zaplanować (podzielić) audyty na dwa lub trzy lata?

W aktualnym stanie prawnym nie ma przepisów, które wprost i jednakowo dla wszystkich wskazywałyby okres, na jaki należy opracować plan audytów. Niemniej, aby prawidłowo realizować zadanie z art. 39 ust. 1 lit. b RODO, warto planować swoje działania, tj. posiadać plan audytów.

Zgodnie z powołanym art. 39 ust. 1 lit. b RODO, inspektor odpowiada m.in. za monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych polityk ustanowionych w tym zakresie przez administratora lub podmiot przetwarzający. Realizacja tego zadania przez inspektora nie powinna mieć charakteru jednorazowego, lecz charakter ciągły

i długofalowy. Na tę aktywność składa się zbieranie informacji o prowadzonych procesach przetwarzania; analizowanie i ocena zgodności tego przetwarzania z wymogami oraz informowanie, doradzanie i rekomendowanie określonych działań administratorowi albo podmiotowi przetwarzającemu.

Zaplanowanie audytów - zwłaszcza, gdy IOD monitoruje przestrzeganie przepisów w dużej organizacji - pozwoli mu dobrze wywiązywać się z powyższego zadania. Taki plan powinien uwzględniać wiele czynników zależnych od specyfiki danego administratora i prowadzonych przez niego procesów (czynności) przetwarzania danych. Konieczne jest jego dostosowanie do przeprowadzonej w organizacji oceny ryzyka (do tego zobowiązuje IOD art. 39 ust. 2 RODO) i przypisanie wyższego priorytetu obszarom, które mają szczególne znaczenie dla systemu ochrony danych u konkretnego administratora. Pomocny w planowaniu audytów będzie rejestr czynności przetwarzania.

Plan ułatwia jak najlepsze i realne wykorzystanie zasobów, którymi IOD dysponuje. Tworzenie planu pomaga ustalić, czy zasoby te są wystarczające, a także, czy we wszystkich monitorowanych obszarach IOD ma zapewnione przez administratora współdziałanie ze strony osób przetwarzających dane osobowe i posiadających wiedzę na temat tego przetwarzania.

Sporządzając plan audytów, warto przemyśleć takie jego elementy, jak: częstotliwość przeprowadzania, metody, kryteria i zakres poszczególnych audytów (w zależności od obszaru poddawanego ocenie), tryb uruchamiania audytów, zasady i sposób jego dokumentowania (w tym czas przechowywania raportu z audytu), zasady i sposób raportowania jego wyników. Trzeba pamiętać, że - z uwagi na podejście oparte na ryzyku i nieprzewidziane zdarzenia, na które należy szybko reagować – plan audytów powinien przewidywać tryb doraźny.

Zarówno plan audytów, jak i wyniki z audytów są dla administratora (kierownictwa, kadry zarządzającej) ważnym elementem rozliczalności (art. 5 ust. 2 RODO), sprawowania kontroli, jak wykonywane są obowiązki z zakresu ochrony danych, czy funkcjonujące w podmiocie rozwiązania techniczne i organizacyjne są zgodne z przepisami oraz wewnętrznymi politykami, a także czy zostały skutecznie wdrożone. Mogą wskazywać, jakie obszary organizacji potrzebują pomocy i wiedzy fachowej, aby prawidłowo wykonywać powierzone zadania.

Data wytworzenia informacji: 01.02.2021 r.

Jak postępować, gdy dojdzie do zagubienia zwrotnego potwierdzenia odbioru?

W sprawozdaniu z działalności Prezesa UODO za 2019 r. (https://uodo.gov.pl **129-131) wskazano, że w przypadku zagubienia przesyłki pocztowej obowiązki określone w art. 33 i 34**

RODO spoczywają na nadawcy przesyłki, ponieważ to on „posiada wiedzę o tym, jakie dane przekazywane są w przesyłce, a tym samym może ocenić, jakim ryzykiem dla praw i wolności osoby fizycznej skutkuje utrata przesyłki". Co jednak w przypadku, gdy operator pocztowy, z którego usług korzystamy, zagubi jedynie zwrotne potwierdzenie odbioru? Kto w tym przypadku powinien ocenić konsekwencje takiego zdarzenia?

W przypadku, gdy dojdzie do zagubienia tylko zwrotnego potwierdzenia odbioru, podmiotem zobowiązanym do dokonania oceny w zakresie konsekwencji takiego zdarzenia jest operator pocztowy. Zwrotne potwierdzenie odbioru jest elementem dodatkowej usługi (przesyłki za zwrotnym potwierdzeniem odbioru) oraz zawiera takie dane, jak imię i nazwisko, adres adresata i nadawcy przesyłki, a także datę, imię i nazwisko odbiorcy.

Poczta Polska i inni operatorzy pocztowi w związku z wykonywaniem usług pocztowych są administratorami danych osobowych nadawców i adresatów przesyłek, a jednocześnie odpowiadają za bezpieczeństwo przesyłek (i zawartych w nich danych osobowych) w ramach należytego wykonywania usług pocztowych oraz przestrzegania zasad i obowiązków określonych w Prawie pocztowym (jak wskazujemy w odpowiedzi na pytanie CZY PRZEKAZANIE DOKUMENTACJI DO FUMIGACJI POWODUJE KONIECZNOŚĆ ZAWARCIA UMOWY POWIERZENIA?).

Warto przypomnieć, że operatorzy pocztowi mają obowiązek zachowania należytej staranności w zakresie uzasadnionym względami technicznymi lub ekonomicznymi przy zabezpieczaniu urządzeń i obiektów wykorzystywanych przy świadczeniu usług pocztowych oraz zbiorów danych przed ujawnieniem tajemnicy pocztowej (art. 41 ust. 6 ustawy Prawo pocztowe). Do zachowania tajemnicy pocztowej są obowiązani: operator pocztowy oraz osoby, które z racji wykonywanej działalności mają dostęp do tajemnicy pocztowej. Tajemnica pocztowa obejmuje informacje przekazywane w przesyłkach pocztowych, informacje dotyczące realizowania przekazów pocztowych, dane dotyczące podmiotów korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia usług pocztowych lub korzystania z tych usług (art. 41 ust. 1 ww. ustawy).

Data wytworzenia informacji: 01.02.2021 r.

Czy pracownik działu kadr urzędu gminy może przetwarzać dane kierowników jednostek organizacyjnych?

Czy pracownicy działu kadr urzędu gminy mogą przetwarzać dane osobowe (w tym dotyczące wynagrodzeń) przygotowując dokumenty w sprawach z zakresu prawa pracy w stosunku do kierowników gminnych jednostek organizacyjnych (z wyłączeniem dyrektorów samorządowych instytucji kultury)? Czy w związku z tym pomiędzy daną gminną jednostką organizacyjną

a wójtem (burmistrzem, prezydentem) powinna zostać podpisana umowa powierzenia lub porozumienie o współadministrowaniu?

Zgodnie z brzmieniem art. 3 kodeksu pracy (dalej: k.p.) pracodawcą – obok osoby fizycznej – może być każda jednostka organizacyjna zatrudniająca pracowników, nawet nieposiadająca osobowości prawnej.

Sąd Najwyższy w wyroku z dnia 20 października 1998 r., I PKN 390/98, stwierdził, że gminny ośrodek pomocy społecznej, jako jednostka organizacyjna zatrudniająca pracowników, jest pracodawcą w rozumieniu art. 3 Kodeksu pracy, również wobec kierownika ośrodka, choćby kompetencja do jego zatrudnienia i zwolnienia należała do zarządu gminy, a kompetencja do wydawania poleceń dotyczących pracy przysługiwała burmistrzowi (wójtowi). W uzasadnieniu orzeczenia wskazano, że ośrodek jest w miejskiej gminie wyodrębnioną jednostką organizacyjną, samodzielnie zatrudniającą swoich pracowników, a więc spełnia przesłanki określone w art. 3 k.p.

Ponadto Sąd Najwyższy w powyższym orzeczeniu wyjaśnił, że kwestię statusu jednostki organizacyjnej jako pracodawcy (art. 3 k.p.) należy odróżniać od sprawy organów lub osób upoważnionych do dokonywania za tego pracodawcę czynności z zakresu stosunku pracy (art. 3^1 k.p.). A zatem dla kierownika gminnej jednostki organizacyjnej stanowiącej jednostkę organizacyjną gminy pracodawcą jest ta gminna jednostka organizacyjna, natomiast uprawnionym do dokonywania za tę jednostkę czynności z zakresu prawa pracy wobec kierownika samorządowej jednostki organizacyjnej, jest wójt gminy (art. 7 pkt 1 ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych, dalej: u.p.s.).

Jak wskazuje M. Tomaszewska (***Komentarz do ustawy o pracownikach samorządowych [w:] Prawo urzędnicze. Komentarz***, red. K. W. Baran, Warszawa 2014, art. 7.) przez kategorię pojęciową "dokonywania czynności z zakresu prawa pracy" rozumie się następujące czynności prawne:

- oświadczenie woli (takie np. jak oświadczenie o zawarciu umowy o pracę, wypowiedzenie stosunku pracy, wypowiedzenie zmieniające),
- tzw. działania prawne niebędące oświadczeniami woli w ścisłym tego słowa znaczeniu, lecz mające doniosłość prawną, tzn. powodujące określony skutek w sferze zatrudnienia (np. udzielenie i odwołanie z urlopu, przeniesienie pracownika do innej pracy, zastosowanie wobec pracownika kary za nieprzestrzeganie ustalonego porządku, regulaminu pracy, przepisów bezpieczeństwa i higieny pracy oraz przepisów przeciwpożarowych),
- czy wreszcie oświadczenie wiedzy (np. wystawienie świadectwa pracy).

Ponadto jak wynika z art. 30 ust. 2 pkt 5 w zw. z art. 11a ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (dalej: u.s.g.) to do ustawowych zadań własnych wójta (burmistrza,

prezydenta miasta) należy, m.in. zatrudnianie i zwalnianie kierowników gminnych jednostek organizacyjnych.

Wójt (burmistrz, prezydent miasta) jako kierownik urzędu gminy, wykonuje również uprawnienia zwierzchnika służbowego nie tylko w stosunku do pracowników urzędu gminy, ale także w stosunku do kierowników gminnych jednostek organizacyjnych (art. 33 ust. 5 u.s.g. oraz art. 7 pkt 1 i 3 u.p.s.).

Z kolei, z art. 39 ust. 3 u.p.s. wynikają szczególne uprawnienia, jakie ustawodawca przyznał wójtom (burmistrzom, prezydentom miast), jak również starostom i marszałkom w zakresie wydawania przez nich zarządzeń określających maksymalne miesięczne wynagrodzenie kierowników jednostek budżetowych, gospodarstw pomocniczych tych jednostek oraz zakładów budżetowych jednostek samorządu terytorialnego. Wójt (burmistrz, prezydent miasta), starosta lub marszałek mogą określić w treści danego aktu, samodzielnie, obok wynagrodzenia zasadniczego (podstawowego) również dodatkowe jego składniki, o ile uznają za stosowne przyznanie tychże składników. Należy bowiem zauważyć, że zgodnie z art. 36 ust. 4 i ust. 5 u.p.s. pracownikowi samorządowemu może zostać przyznany dodatek funkcyjny oraz dodatek specjalny (ten ostatni z tytułu okresowego zwiększenia obowiązków służbowych lub powierzenia dodatkowych zadań), a zatem wskazane dodatki nie posiadają charakteru obligatoryjnego. Podobnie z literalnego brzmienia art. 36 ust. 6 ww. ustawy wynika, że również nagroda jest świadczeniem fakultatywnym - może zostać przyznana pracownikom samorządowym, dla których podstawę zatrudnienia stanowi powołanie lub umowa o pracę, za szczególne osiągnięcia w pracy zawodowej (odpowiedź sekretarza stanu w Ministerstwie Spraw Wewnętrznych i Administracji na zapytanie nr 4267 w sprawie interpretacji przepisów dotyczących wynagradzania kierowników samorządowych jednostek organizacyjnych; http://orka2.sejm.gov.pl).

Mając powyższe na uwadze należy wskazać, że **administratorem przetwarzanych danych osobowych kierownika danej jednostki organizacyjnej jest ta jednostka jako pracodawca, ale także wójt (burmistrz, prezydent miasta)**,niebędący pracodawcą, a jedynie dokonujący konkretnych, wskazanych w przepisach czynności z zakresu prawa pracy, ponieważ „Do zadań wójta należy w szczególności: (...) zatrudnianie i zwalnianie kierowników gminnych jednostek organizacyjnych". **Będą to zatem oddzielni administratorzy wykonujący zadania na podstawie odrębnych przepisów** i nie będzie tutaj zachodziła relacja współadministrowania, o której mowa w art. 26 RODO.

Jednocześnie należy wskazać, że zgodnie z art. 33 ust. 1 u.s.g. wójt wykonuje zadania przy pomocy urzędu gminy, jest też kierownikiem urzędu i zwierzchnikiem służbowym pracowników urzędu, w tym pracowników działu kadr.

Zgodnie z art. 29 RODO, podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych

przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego. Przepis ten adresowany jest do podmiotów przetwarzających, a także do osób działających z upoważnienia administratora lub podmiotu przetwarzającego, mających dostęp do danych osobowych (pracowników, w tym pracowników działu kadr, osób zatrudnionych na podstawie umów cywilnoprawnych, stażystów, praktykantów, wolontariuszy). Osoby te charakteryzuje pewna zależność od administratora. Właśnie takim osobom administrator może nadać imienne upoważnienie do przetwarzania danych, jeśli przyjął je jako środek organizacyjny służący zapewnieniu kontroli nad dostępem do danych osobowych (więcej informacji na temat upoważnień można znaleźć w zamieszczonej na stronie internetowej UODO zakładce Inspektor Ochrony Danych/Zadania IOD m.in. w odpowiedzi na pytanie CZY ADMINISTRATOR POWINIEN UDZIELAĆ UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH?). Wobec powyższego pracownik działu kadr urzędu gminy może przetwarzać dane osobowe kierowników gminnych jednostek organizacyjnych, w tym danych dotyczących ich wynagrodzenia, na polecenie administratora – wójta (burmistrza, prezydenta miasta).

Data wytworzenia informacji: 03.03.2021 r.

Jaki jest status komisji antymobbingowej?

Czy komisja antymobbingowa powołana przez pracodawcę w myśl przepisów prawa pracy jest odrębnym administratorem?

W celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem należy dokonać analizy konkretnych okoliczności i podstaw prawnych funkcjonowania określonego podmiotu.

W pierwszej kolejności należy określić, czy, a jeżeli tak, to w jakich celach komisja antymobbingowa działająca u pracodawcy przetwarza dane osobowe. W następnym kroku należy ocenić, kto określa cele i sposoby przetwarzania danych. Należy tu wziąć pod uwagę podstawy prawne i zasady działania takiego podmiotu wynikające zarówno z powszechnie obowiązujących przepisów prawa, jak i regulacji wewnętrznych pracodawcy (np. zarządzenia, regulaminy).

Jeśli chodzi o przepisy powszechnie obowiązujące, które dotyczą mobbingu to będą to przepisy ustawy Kodeks pracy. Zgodnie z art. 94^3 § 2 tej ustawy mobbing oznacza działania lub zachowania dotyczące pracownika lub skierowane przeciwko pracownikowi, polegające na uporczywym i długotrwałym nękaniu lub zastraszaniu pracownika, wywołujące u niego zaniżoną ocenę przydatności zawodowej, powodujące lub mające na celu poniżenie lub ośmieszenie pracownika, izolowanie go lub wyeliminowanie z zespołu współpracowników. **Przeciwdziałanie mobbingowi należy do obowiązków pracodawcy** (§ 1 ww. przepisu).

Jak wskazano w komentarzu do tego przepisu „co do sposobów realizacji tego obowiązku, to pracodawca może używać środków organizacyjnych i perswazyjnych, a gdy są one nieskuteczne, może stosować sankcje przewidziane w prawie pracy. Jak wynika z wyroku SN z 3.08.2011 r., I PK 35/11, OSNP 2012/19–20, poz. 238, pracodawca powinien (…) przeciwdziałać mobbingowi, w szczególności szkoląc pracowników – informując o niebezpieczeństwie i konsekwencjach mobbingu czy stosując procedury, które umożliwią wykrycie i zakończenie tego zjawiska. Dobór właściwych środków uzależniony pozostaje od konkretnego pracodawcy, jak na przykład rodzaju środowiska pracy, charakteru i ilości interakcji między pracownikami, grożących wystąpieniem tego negatywnego zjawiska, wpływem rodzaju wykonywanej pracy. JAKI JEST STATUS KOMISJI ANTYMOBBINGOWEJ?

Zauważyć należy, że żaden przepis ustawowy nie zobowiązuje pracodawcy do powoływania **komisji** antymobbingowej, nie określa jej zadań, ani sposobu rozpatrywania spraw, a jej powołanie stanowi zazwyczaj element polityki/procedury wewnętrznej pracodawcy. Procedury takie określać mogą sposób zgłaszania niepożądanych praktyk, rozpatrywania skarg, a także organy powołane przez pracodawcę do prowadzenia takich spraw, ich skład i sposób wyboru (np. komisja antymobbingowa, pełnomocnicy, rzecznicy zaufania, mediatorzy).

Pracodawcy mają zatem swobodę tworzenia i nazwania organu, który będzie prowadził takie postępowania. Zazwyczaj jest to kilkuosobowy zespół określany jako komisja antymobbingowa. Pracodawca może też zdecydować, czy powołuje komisję stałą czy będzie ona tworzona odrębnie do każdego postępowania wyjaśniającego, czy w składzie komisji będą tylko pracownicy firmy czy także zewnętrzni eksperci.

Dla jednoznacznej oceny, w jakiej roli występuje taka komisja w kontekście przepisów o ochronie danych osobowych, niezbędna jest znajomość konkretnych okoliczności faktycznych i prawnych. Jednak pomocniczo można wskazać, że do statusu komisji antymobbingowej odniósł się Sąd Apelacyjny w Krakowie w orzeczeniu z 27 stycznia 2016, III APa 20/15, w którym stwierdził, że komisje antymobbingowe powoływane każdorazowo przez pracodawcę do zbadania skarg pracowników, **realizują w istocie zadania samego pracodawcy i stanowią „ramię" tego pracodawcy** (zob. uchwała SN z 7 stycznie 1992r. I PZP 62/91) w realizacji jego zadań polegających na przeciwdziałaniu tym negatywnym zjawiskom w stosunkach pracy. Zatem to nie przepisy ustawy czy rozporządzeń wykonawczych, lecz sam pracodawca w uchwale zarządu spółki samodzielnie określił zasady, na jakich ma odbywać się przeciwdziałanie tym zjawiskom, określił skład, sposób wyboru członków komisji, wyznaczył jej kompetencję, zwolnił członków komisji z obowiązku świadczenia pracy w czasie jej posiedzeń, określił procedurę dochodzenia do końcowych wniosków, a także konsekwencje tych wniosków w zakresie poszczególnych stosunków pracy „pracowników obwinionych". Działalność tej komisji, cele dla których została powołana i procedura w którą została wyposażona stanowiły wyłączną domenę pracodawcy,

związaną z realizacją obowiązków tego pracodawcy wobec pracowników wynikających z przepisów kodeksowych (…). Podobnie do statusu komisji antymobbingowej odniósł się WSA w Gliwicach w wyroku z dnia 11 grudnia 2019 r., III SA/Gl 888/19 (wskazał, że Dyrektor Szpitala Wojewódzkiego w postępowaniu występuje jako pracodawca, a komisja antymobbingowa jest jego ciałem pomocniczym).

Powyższe przemawia za uznaniem, że komisja antymobbingowa samodzielnie nie ustala celów i sposobów przetwarzania danych osobowych, a tym samym nie spełnia kryteriów wymaganych dla kwalifikacji jej jako odrębnego administratora. Zgodnie z przytoczonymi powyżej orzeczeniami sądów, komisja taka stanowi organ pomocniczy pracodawcy, powoływany przez pracodawcę w celu realizacji jego zadań.

Data wytworzenia informacji: 03.03.2021 r.

Czy inspektorowi ochrony danych należy nadawać upoważnienie do przetwarzania danych?

Czy IOD powinien posiadać upoważnienie do przetwarzania danych osobowych nadane przez administratora? Dostępne opinie na ten temat są sprzeczne. Przeciwko nadawaniu upoważnień inspektorowi wysuwa się argument, że takie upoważnienie jest zbędne ze względu na prawo inspektora do właściwego i niezwłocznego włączania go we wszystkie sprawy dotyczące ochrony danych osobowych u administratora oraz z uwagi na jego zadania określone w art. 39 ust. 1 RODO.

Odpowiadając na takie pytanie przede wszystkim należy wziąć pod uwagę cel, w jakim takie upoważnienia się nadaje. Takie upoważnienia mogą być jednym ze środków organizacyjnych, którego celem jest zapewnienie przez administratora odpowiedniej kontroli nad procesem ich przetwarzania.

Przepisy RODO zobowiązują administratora, aby miał kontrolę (władztwo) nad tym kto, w jakim zakresie ma dostęp do danych osobowych oraz na jakich zasadach i w jaki sposób je przetwarza. Dane osobowe mogą być przetwarzane wyłącznie na polecenie administratora przez osoby działające z upoważnienia administratora lub podmiotu przetwarzającego (art. 29 oraz art. 32 ust. 4). Przyjmowane przez administratora i podmiot przetwarzający środki wobec osób, za których działania administrator i podmiot przetwarzający odpowiada, powinny służyć m.in. zapobieganiu nieuprawnionemu pozyskiwaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych. Dzięki tym środkom osoby, które zostały dopuszczone do przetwarzania danych zostają również poinformowane, jaki jest zakres ich uprawnień co do przetwarzania danych osobowych. Dlatego środek ten należy odróżnić od uprawnienia do dostępu do danych osobowych przyznanego określonym funkcjom

czy zawodom przez przepisy prawa w związku z wykonywanymi przez nich obowiązkami lub zadaniami.

Patrząc z tej perspektywy, jeżeli administrator decyduje się na skorzystanie ze środka, jakim jest nadawanie upoważnień do przetwarzania danych w wykonaniu obowiązków określonych w art. 29 i art. 32 ust. 1 i 4 RODO, to taki środek uzasadniony jest również wobec inspektora ochrony danych, niezależnie od tego, że uprawnienie tej osoby do dostępu do danych osobowych wynika z RODO.

Jednocześnie wskazuję, iż analogiczne podejście i więcej informacji na temat upoważnień do przetwarzania danych można znaleźć na naszej stronie internetowej w zakładce Inspektor Ochrony Danych/Zadania IOD, m.in. w odpowiedziach na pytania: CZY ADMINISTRATOR POWINIEN NADAWAĆ UPOWAŻNIENIA NP. SĘDZIOM?, CZY LEKARZOM NALEŻY NADAWAĆ UPOWAŻNIENIA?

Data wytworzenia informacji: 03.03.2021 r.

Czy GUS może zobowiązać gminy do przekazania mu innych danych niż te, które gmina może gromadzić?

Urząd gminy został zobowiązany do przekazania do GUS danych jednostkowych o właścicielach nieruchomości w rozumieniu ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach oraz ich współmałżonkach składających deklaracje i ich korekty o wysokości opłaty za gospodarowanie odpadami komunalnymi. Ustawa o utrzymaniu czystości wskazuje jedynie na uprawnienie gminy do pozyskiwania danych właściciela nieruchomości, nie odnosi się natomiast do jego stanu cywilnego. Czy zatem żądanie GUS o udostępnienie tego rodzaju danych nie jest nadmiarowe?

Zgodnie z art. 13 ust. 1 ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz. U. z 2020 r. poz. 443 ze zm.) organy administracji publicznej, Zakład Ubezpieczeń Społecznych, Narodowy Fundusz Zdrowia, Komisja Nadzoru Finansowego, a także inne państwowe lub samorządowe osoby prawne, organy rejestrowe oraz inne podmioty prowadzące rejestry urzędowe lub niepubliczne systemy informacyjne, przekazują lub udostępniają nieodpłatnie służbom statystyki publicznej zgromadzone dane w szczegółowym zakresie, postaci i terminach, określonych w programie badań statystycznych statystyki publicznej, w szczególności w postaci zbiorów danych z systemów teleinformatycznych, w tym wyników pomiarów, danych monitoringu środowiska, a w przypadku braku systemu teleinformatycznego – w innej utrwalonej postaci. W związku z powyższym przepisem **tylko dane już zgromadzone na podstawie obowiązujących przepisów prawa w zakresach i celach wynikających z tych przepisów ww. podmioty mają obowiązek przekazać na rzecz GUS**. Tym samym przepis ten nie uprawnia, ani nie

zobowiązuje wskazanych podmiotów do pozyskiwania innych danych na rzecz GUS a następnie ich dalszego przetwarzania (przechowywania).

Natomiast zgodnie z art. 6m ust. 1b ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach (t.j. Dz. U. z 2020 r., poz. 1439) rada gminy określając wzór deklaracji może wymagać podania następujących danych: imię i nazwisko lub nazwę właściciela nieruchomości oraz adres miejsca zamieszkania lub siedziby; adres nieruchomości; dane stanowiące podstawę zwolnienia z opłaty za gospodarowanie odpadami komunalnymi; numer telefonu właściciela nieruchomości; adres poczty elektronicznej właściciela nieruchomości; inne informacje niezbędne do wystawienia tytułu wykonawczego; informacje dotyczące posiadania kompostownika przydomowego i kompostowania w nim bioodpadów stanowiących odpady komunalne.

Do zakresu danych wymaganych w treści wzoru deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi odniósł się Wojewódzki Sąd Administracyjny w Poznaniu, w wyroku z 12 stycznia 2017 r. (I SA/Po 1459/16). Stwierdził, że „przepisy ustawy o utrzymaniu czystości i porządku w gminach nie upoważniają organu stanowiącego jednostki samorządu terytorialnego do żądania podawania przez właścicieli nieruchomości informacji obejmujących dane osób zamieszkujących daną nieruchomość. Zatem na potrzeby ustalenia wysokości opłaty za gospodarowanie odpadami komunalnymi, wystarczające jest ustalenie samej liczby osób zamieszkałych pod danym adresem, a nie ich danych osobowych. Wysokość opłat jest określana na podstawie wyłącznie liczby osób, a nie ich danych identyfikacyjnych. Jednocześnie art. 51 Konstytucji określa, że ujawnienie informacji dotyczących osoby może odbywać się tylko na podstawie ustawy i ogranicza pozyskiwanie informacji o obywatelach do przypadków niezbędnych i uznawanych w demokratycznym państwie. W rezultacie gromadzenie danych osobowych osób zamieszkujących na terenie nieruchomości, na której powstają odpady, nie jest niezbędne do ustalenia wysokości opłaty, która uzależniona jest tylko od liczby osób zamieszkujących nieruchomość”.

Podobnie orzekł Wojewódzki Sąd Administracyjny w Olsztynie w wyroku z dnia 7 października 2020 r. (I SA/Ol 404/20), w którym wskazał, że podawanie danych współmałżonka w deklaracji o wysokości opłaty za gospodarowanie odpadami komunalnymi składanej przez właściciela nieruchomości, stanowi wyjście poza granice upoważnienia wynikającego z ustawy o utrzymaniu czystości i porządku w gminach. Nie zawsze bowiem zaistnieje, nawet potencjalna możliwość skierowania egzekucji do małżonka składającego deklarację. Przyjęcie zaś w tym zakresie uniwersalnego założenia, ewentualności wykorzystania takich danych i gromadzenia ich niejako "na wyrost" uznane musi być za praktykę nie dającą się pogodzić za zasadą legalizmu działań organów administracji publicznej.

Z ww. przepisów wynika, że gmina ma prawo do przetwarzania danych jedynie właściciela nieruchomości (w tym numer telefonu właściciela nieruchomości oraz adres jego poczty

elektronicznej właściciela), który składa deklarację i ponosi odpowiedzialność za rzetelność zawartych w niej informacji. Tym samym gmina nie ma prawa przetwarzania danych o innych osobach zamieszkujących daną nieruchomość, w konsekwencji czego nie ma podstaw do przekazania GUS innych danych niż dane właściciela nieruchomości.

Jednocześnie warto przypomnieć, że w wystąpieniu skierowanym do Prezesa GUS z dnia 15 października 2019 r. (znak: ZSPU.070.9.2019), Prezes UODO zwracał już uwagę na to, iż działania odnoszące się do pozyskiwania danych osobowych w celu realizowania zadań przez GUS muszą być zgodne z zasadami ochrony danych osobowych. Przepisy z zakresu statystyki publicznej **są podstawą do udostępnienia jedynie tych danych osobowych, które administrator może posiadać zgodnie z prawem dla realizacji ściśle określonych celów, przy zachowaniu zasad, o których mowa w art. 5 RODO (np. zasady proporcjonalności, minimalizacji, ograniczenia czasowego).** W opinii Prezesa UODO zarówno przy tworzeniu przepisów prawa, jak i systemów informatycznych umożliwiających transfer danych, GUS powinien rozważyć jaki zakres danych osobowych jest niezbędny do skutecznej realizacji zadań programu badań statystycznych statystyki publicznej za określony rok (co zostało zasygnalizowane przez Prezesa UODO w ww. korespondencji). Jak bowiem wynika z art. 89 RODO przy przetwarzaniu danych do celów archiwalnych, badań naukowych lub historycznych albo do celów statystycznych szczególną uwagę należy przykładać do zasady minimalizacji danych (…). Oznacza to konieczność zachowania odpowiedniej proporcji między zakresem danych a celem ich przetwarzania, choć może być rozumiane także bardziej restrykcyjnie jako konieczność ograniczenia zakresu danych do niezbędnego minimum[15].

Data wytworzenia informacji: 03.03.2021 r.

Czy wobec osób z władz związku zawodowego trzeba spełniać obowiązek informacyjny?

Urząd Ochrony Danych Osobowych stoi na stanowisku, że osoby fizyczne pełniące funkcje członków organów osoby prawnej, których dane ujawnione są w KRS, należy odmiennie traktować niż dane o osobach prawnych. W konsekwencji dane członków zarządu reprezentujących osobę prawną, którzy są możliwymi do zidentyfikowania osobami fizycznymi, będą danymi osobowymi podlegającymi ochronie RODO. Czy zatem słuszne będzie przyjęcie analogicznego stanowiska w stosunku do osób wskazanych pracodawcy na podstawie art. 32

[15] P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, art. 89.

ustawy o związkach zawodowych, tj. członków zarządu i byłych członków zarządu związku zawodowego? Czy należy wypełnić wobec nich obowiązek informacyjny z art. 13 lub 14 RODO? Jaka jest prawidłowa podstawa prawna przetwarzania tego typu danych osobowych przez pracodawcę? Czy może mieć miejsce sytuacja, w której za podstawę uprawniającą pracodawcę do przetwarzania danych dotyczących przynależności do związków zawodowych można uznać przesłankę określoną w art. 9 ust. 2 lit. e RODO (np. gdy to związki zawodowe przekażą pracodawcy dane, o których mowa w art. 32 ustawy o związkach zawodowych)?

Dane osób fizycznych pełniących funkcje członków zarządu związku zawodowego są danymi osobowymi w rozumieniu przepisów o ochronie danych osobowych. Wobec tego administrator jest zobligowany do wypełnienia w stosunku do takich osób obowiązku informacyjnego określonego w art. 13 lub art. 14 RODO, chyba że zachodzi jedna z przesłanek zwalniających go z tego obowiązku. Jedną z takich sytuacji jest przypadek, w którym pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą (art. 14 ust. 5 lit c RODO).

Jeśli zaś chodzi o podstawę prawną uprawniającą pracodawcę do przetwarzania danych osobowych członków zarządu organizacji związkowej, w tym danych szczególnej kategorii, ujawniających przynależność do związków zawodowych, to będzie nią właściwa przesłanka z art. 9 RODO w połączeniu z przepisem szczególnym dotyczącym funkcjonowania związków zawodowych. Zasady współdziałania pracodawcy ze związkami zawodowymi określają przepisy ustawy z dnia 23 maja 1991 r. o związkach zawodowych

Zgodnie z art. 32 ust. 9^2 wskazanej ustawy, zarząd zakładowej organizacji związkowej lub komitet założycielski zakładowej organizacji związkowej wskazują pracodawcy na piśmie osoby, których stosunek prawny podlega ochronie, o której mowa w ust. 1, poprzez podanie imienia i nazwiska tych osób, a także czasu trwania ochrony. Zmiany we wskazaniu są dokonywane przez zarząd lub komitet założycielski zakładowej organizacji związkowej na piśmie w terminie 7 dni od dnia zaistnienia zmiany.

W tej sytuacji zasadne będzie przyjęcie jako podstawy prawnej do przetwarzania przez pracodawcę ww. danych przesłanki wskazanej w art. 9 ust. 2 lit. b RODO, zgodnie z którą przetwarzanie danych szczególnej kategorii, w tym przypadku danych ujawniających przynależność do związku zawodowego, 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.

W literaturze wskazuje się, że „według prawa polskiego przynależnością do związków zawodowych mogą legitymować się pracownicy (bez względu na podstawę stosunku pracy), członkowie rolniczych spółdzielni produkcyjnych, osoby wykonujące pracę na podstawie umowy agencyjnej (o ile nie są one pracodawcami), emeryci i renciści, bezrobotni w rozumieniu przepisów o zatrudnieniu, osoby skierowane do zakładów pracy w celu odbycia służby zastępczej, jak również funkcjonariusze Policji, Straży Granicznej i Służby Więziennej oraz strażacy Państwowej Straży Pożarnej (art. 2 ustawy o związkach zawodowych). Sam zaś związek zawodowy to dobrowolna i samorządna organizacja ludzi pracy, powołana do reprezentowania i obrony ich praw, interesów zawodowych i socjalnych (art. 1 ust. 1 ustawy o związkach zawodowych). Z uwagi na powyższy zakres podmiotowy omawiana kategoria danych może dotyczyć wyłącznie osób związanych ze sferą zatrudnienia."[16]

Wobec powyższego przetwarzanie przez pracodawcę danych ww. osób w celach określonych w powyższym przepisie ustawy o związkach zawodowych można uznać za „niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy". A zatem podstawę do przetwarzania przez pracodawcę danych osobowych ujawniających przynależność do związków zawodowych członków zarządu tego związku w celu realizacji zadań wynikających z ustawy o związkach zawodowych stanowić będzie art. 9 ust. 2 lit. b RODO wraz z właściwym przepisem ustawy o związkach zawodowych.

Co zaś do tego, czy w sytuacji, gdy to związki zawodowe przekażą pracodawcy dane, o których mowa w art. 32 ustawy o związkach zawodowych, można uznać, że przesłanką uprawniającą do ich przetwarzania jest art. 9 ust. 2 lit. e RODO (zgodnie z którym przetwarzanie szczególnych kategorii danych osobowych jest dopuszczalne, jeśli dane te zostały w sposób oczywisty upublicznione przez osobę, której dane dotyczą), to wskazać należy, że jeżeli uprawnienie do przetwarzania (w tym udostępniania lub pozyskiwania) danych osobowych wynika z przepisów prawa, nie ma potrzeby wskazywania innych podstaw prawnych.

Data wytworzenia informacji: 02.04.2021 r.

Czy komornikowi należy udostępnić dane w postaci nr rachunku bankowego pracownika?

Czy komornikowi sądowemu, na żądanie wniesione w trybie art. 761 § 1 1 kodeksu postepowania cywilnego należy udostępnić informację o numerze rachunku bankowego pracownika? Na stronie archiwalnej GIODO znajduje się odpowiedź na podobne pytanie

[16] M. Kuba [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, komentarz do art. 9, Lex online.

(https://archiwum.giodo.gov.pl/318/id_art/3277/j/pl – **tekst w ramce poniżej), ale w odpowiedzi wskazana jest inna podstawa z kpc. Czy stanowisko to jest aktualne w świetle obowiązujących przepisów?**

Informacja ze strony archiwalnej GIODO

Czy komornik jest uprawniony do tego, aby otrzymać numer rachunku bankowego dłużnika od jego pracodawcy?

Nie, gdyż nie uprawniają go do tego przepisy prawa.

Uzasadnienie

Podstawę prawną do przetwarzania przez komornika danych osobowych dłużnika na potrzeby prowadzonego postępowania egzekucyjnego stanowią przepisy ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego (kpc), ustawy z dnia 29 sierpnia 1997 r. o komornikach sądowych i egzekucji oraz rozporządzenia Ministra Sprawiedliwości z dnia 9 marca 1968 r. w sprawie czynności komorników.

W celu zajęcia wynagrodzenia za pracę, komornik – na podstawie art. 882 § 1 kpc – wzywa pracodawcę, aby w ciągu tygodnia: przedstawił za okres trzech miesięcy poprzedzających zajęcie, za każdy miesiąc oddzielnie, zestawienie periodycznego wynagrodzenia dłużnika za pracę oraz oddzielenie jego dochodu z wszelkich innych tytułów. Ponadto wzywa pracodawcę, aby podał, w jakiej kwocie i w jakich terminach zajęte wynagrodzenie będzie przekazywane wierzycielowi oraz w razie istnienia przeszkód do wypłacenia wynagrodzenia za pracę złożył oświadczenie o rodzaju tych przeszkód, a w szczególności podał, czy inne osoby roszczą sobie prawa, czy i w jakim sądzie toczy się sprawa o zajęte wynagrodzenie i czy oraz o jakie roszczenia została skierowana do zajętego wynagrodzenia egzekucja przez innych wierzycieli. Natomiast po stronie pracodawcy istnieje obowiązek niezwłocznego zawiadomienia komornika oraz wierzyciela o każdej zmianie ww. okoliczności (na podstawie art. 882 § 2 kpc).

Ponadto, stosownie do art. 881 § 3 kpc komornik wzywa pracodawcę, aby w granicach określonych w paragrafie drugim nie wypłacał dłużnikowi poza częścią wolną od zajęcia żadnego wynagrodzenia, lecz: przekazywał zajęte wynagrodzenie bezpośrednio wierzycielowi egzekwującemu, zawiadamiając komornika o pierwszej wypłacie (pkt 1), albo przekazywał zajęte wynagrodzenie komornikowi w wypadku, gdy do wynagrodzenia jest lub zostanie w dalszym toku postępowania egzekucyjnego skierowana jeszcze inna egzekucja, a wynagrodzenie w części wymagalnej nie wystarcza na pokrycie wszystkich egzekwowanych świadczeń wymagalnych (pkt 2).

W związku z powyższym stwierdzić należy, iż udostępnianie przez pracodawcę informacji w postaci numeru rachunku bankowego nie wynika z żadnych norm prawa kształtujących obowiązki komornika. W związku z powyższym racjonalny ustawodawca uznał pozyskiwanie przez komornika numeru rachunku bankowego dłużnika jest zbędne do prowadzenia egzekucji z wynagrodzenia o pracę.

Zgodnie z przepisami RODO, podmiot może przetwarzać (w tym udostępniać) dane osobowe zwykłe po spełnieniu jednej z przesłanek określonych w art. 6 RODO. Jedną z wymienionych w tym przepisie przesłanek jest sytuacja, że przetwarzanie jest niezbędne do wypełnienia

obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO). W takim przypadku - jak stanowi ust. 3 tego artykułu - podstawa przetwarzania musi być określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator.

W przypadku żądania przez komornika określonych danych w toku prowadzonego przez niego postępowania, należy sięgnąć do właściwych przepisów (tu: przepisów prawa krajowego) określających uprawnienia komornika. Podstawę prawną do pozyskiwania przez komornika danych osobowych dłużnika na potrzeby prowadzonego postępowania egzekucyjnego stanowią przepisy ustawy z dnia 17 listopada 1964 r. Kodeks postępowania cywilnego, w tym art. 761 § 1^1 Kodeksu postępowania cywilnego - powołany jako podstawa żądania komornika w zasygnalizowanej sytuacji.

Przepis ten ustanawia przykładowy, niezamknięty katalog osób i instytucji, do których organ egzekucyjny może zwracać się o udzielenie informacji. Wśród tych podmiotów wskazano „inne instytucje i osoby nieuczestniczące w postępowaniu", do których można zaliczyć pracodawców. Podmioty te, na żądanie organu egzekucyjnego zobowiązane są udostępnić informacje na temat stanu majątkowego dłużnika lub danych umożliwiających identyfikację składników jego majątku oraz danych adresowych w zakresie niezbędnym do zapewnienia prawidłowego toku postępowania. Do informacji takich może należeć numer rachunku bankowego dłużnika. Ocena, które informacje są niezbędne w konkretnym przypadku, należy bowiem do komornika. Warto nadmienić, że zgodnie z art. 222 pkt 8 ustawy o komornikach sądowych, komornik odpowiada dyscyplinarnie za zawinione działania lub zaniechania (przewinienia dyscyplinarne), takie jak m. in. pozyskiwanie informacji z naruszeniem art. 761 § 1 kpc.

Od wykonania takiego żądania można uchylić się w takim zakresie, w jakim według przepisów części pierwszej Kodeksu można odmówić przedstawienia dokumentu lub złożenia zeznań w charakterze świadka albo odpowiedzi na zadane pytanie. Informacji udziela się w oparciu o dane przekazane przez organ egzekucyjny, w terminie przez niego wyznaczonym, o ile przepisy szczególne nie przewidują innego terminu (art. 761 § 2 i § 2^1 kpc).

Natomiast art. 882 § 1 kpc. powołany w materiale zamieszczonym na stronie archiwalnej GIODO określa obowiązki pracodawcy **w związku z zajęciem wynagrodzenia za pracę** w ramach egzekucji prowadzonej przez komornika. Celem tego przepisu jest zatem uregulowanie czynności zajęcia wynagrodzenia za pracę. Na podstawie tego przepisu komornik wzywa pracodawcę, aby w ciągu tygodnia: przedstawił za okres trzech miesięcy poprzedzających zajęcie, za każdy miesiąc oddzielnie, zestawienie periodycznego wynagrodzenia dłużnika za pracę oraz oddzielenie jego dochodu z wszelkich innych tytułów. Ponadto wzywa pracodawcę, aby podał, w jakiej kwocie i w jakich terminach zajęte wynagrodzenie będzie przekazywane wierzycielowi oraz w razie istnienia przeszkód do wypłacenia wynagrodzenia za pracę złożył oświadczenie o rodzaju tych przeszkód, a w szczególności podał, czy inne osoby roszczą sobie prawa, czy i w jakim sądzie toczy

się sprawa o zajęte wynagrodzenie i czy oraz o jakie roszczenia została skierowana do zajętego wynagrodzenia egzekucja przez innych wierzycieli. Natomiast po stronie pracodawcy istnieje obowiązek niezwłocznego zawiadomienia komornika oraz wierzyciela o każdej zmianie ww. okoliczności (na podstawie art. 882 § 2 kpc).

Udostępnienie danych komornikowi w powyższych sytuacjach będzie następowało zatem w wykonaniu obowiązku nałożonego przepisem prawa na administratora na podstawie art. 6 ust. 1 lit c RODO w połączeniu z właściwym przepisem procedury cywilnej, w zależności od tego, jaki cel lub podstawę prawną powołał komornik. Przy realizacji tego obowiązku należy pamiętać o przestrzeganiu zasady integralności i poufności danych określonej w art. 5 ust. 1 lit. f RODO, czyli zapewnić odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

Data wytworzenia informacji: 02.04.2021 r.

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

Proszę o przedstawienie stanowiska odnośnie publikacji w Biuletynie Informacji Publicznej oraz na tablicy ogłoszeń danych osobowych w zakresie imienia i nazwiska zawartych w zawiadomieniu o czynnościach podjętych w celu ustalenia przebiegu granic działek ewidencyjnych na podstawie art. 38 ust. 4 rozporządzenia Ministra Rozwoju Regionalnego i Budownictwa z dnia 29 marca 2001 r. w sprawie ewidencji gruntów i budynków (Dz. U. z 2019 r. poz. 393 ze zm.). Czy starosta otrzymując od zewnętrznego podmiotu dane osobowe zawarte w zawiadomieniu może ingerować (anonimizacja danych nadmiarowych) w treść zawiadomienia, o którym mowa powyżej, czy też to zewnętrzny podmiot powinien przekazać zanonimizowany dokument. Czy w opisanej sytuacji starosta jest administratorem danych osobowych?

W przedstawionej sytuacji należy kierować się ściśle treścią powołanego przepisu, bo jednoznacznie rozstrzyga on przedstawione wątpliwości. § 38 ust. 4 rozporządzenia Ministra Rozwoju Regionalnego i Budownictwa z dnia 29 marca 2001 r. w sprawie ewidencji gruntów i budynków (t.j. Dz. U. z 2019 r. poz. 393) wskazuje, w jakich przypadkach i przez jaki okres czasu starosta jest zobowiązany do udostępnienia na stronach internetowych Biuletynu Informacji Publicznej oraz na tablicy ogłoszeń starostwa powiatowego informacji określonych w ust. 2 pkt 1-3 tego paragrafu w celu zawiadomienia właściwych osób o czynnościach podjętych w celu ustalenia przebiegu granic działek ewidencyjnych. Przepis jednoznacznie wskazuje, że

zamieszczenie informacji następuje na żądanie wykonawcy, ale niezależnie od tego, w jakim zakresie czy formie wykonawca przekazał te informacje staroście, udostępnieniu w BIP i na tablicy ogłoszeń powinny podlegać jedynie te informacje, które podane są w § 38 ust. 2 pkt 1-3, a nie obejmują one imienia i nazwiska. Informacje mogą być udostępnione jedynie przez ściśle wskazany w przepisie czas. Przepis nakłada ten obowiązek na starostę i w zakresie przetwarzania danych osobowych dla realizacji tego zadania będzie on administratorem w rozumieniu przepisów o ochronie danych osobowych.

Data wytworzenia informacji: 02.04.2021 r.

Która przesłanka jest podstawą przetwarzania danych przez pracodawcę stosującego monitoring?

Proszę o potwierdzenie, że po zmianach przepisów w 2019 r. nadal pozostaje aktualne, iż podstawą prawną przetwarzania danych osobowych pracownika przetwarzanych w związku ze stosowaniem monitoringu w zakładzie pracy powinien być prawnie uzasadniony interes pracodawcy (art. 6 ust. 1 lit. f RODO). Takie stanowisko zostało zaprezentowane jeszcze przed wejściem życie nowelizacji Kodeksu Pracy z dnia 4 maja 2019 r. podczas Szkolenia dla Inspektorów Ochrony Danych z sektora zatrudnienia, które odbyło się 4 października 2018 r. Powyższe zagadnienie budzi szereg wątpliwości pracodawców oraz inspektorów ochrony danych, które dodatkowo pogłębiają sprzeczne opinie wyrażane w prasie fachowej oraz innych publikacjach.

Kodeks pracy nie nakłada na pracodawcę obowiązku stosowania monitoringu, a jedynie daje mu taką możliwość. Skorzystanie z tej możliwości jest jednak obwarowane konkretnymi warunkami i może nastąpić jedynie w ściśle określonych w tym Kodeksie celach, a mianowicie:

- w przypadku monitoringu wizyjnego do zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub kontroli produkcji lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę (art. 22^2 k.p.),
- w przypadku monitoringu poczty elektronicznej i innych form monitoringu do zapewnienia organizacji pracy umożliwiającej pełne wykorzystanie czasu pracy oraz właściwego użytkowania udostępnionych pracownikowi narzędzi pracy (art. 22^3 § 1-4 k.p).

W uzasadnieniu projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 wskazano, że celem wprowadzenia przepisów regulujących monitoring pracowników jest zabezpieczenie interesów pracowników przed dowolnym wykorzystywaniem monitoringu przez pracodawców. Dlatego uregulowano kwestię monitoringu

w przepisach prawa oraz ograniczono możliwość wykorzystywania monitoringu do celów wskazanych w przepisach.

Za przesłankę przetwarzania danych osobowych pracowników w związku ze stosowaniem monitoringu w powyższych celach i na warunkach określonych w Kodeksie pracy należy uznać art. 6 ust. 1 lit. f RODO. Powołanie się na tę przesłankę wymaga przeprowadzenia uprzedniej starannej oceny, określanej jako test równowagi. Jej istotą jest ustalenie, czy interes administratora (lub strony trzeciej), przemawiający za przetwarzaniem danych, jest prawnie uzasadniony, czy przetwarzanie jest niezbędne do realizacji celu wynikającego z tego interesu, a następnie rozważenie, czy interesy lub podstawowe prawa i wolności osoby, której dane dotyczą nie przeważają nad prawnie uzasadnionym interesem administratora lub strony trzeciej (więcej na temat tego testu i materiałów przydatnych w jego przeprowadzeniu m.in. w odpowiedzi na pytanie CZY PRZESŁANKĄ PRZETWARZANIA PRZEZ ORGANY PUBLICZNE MOŻE BYĆ ART. 6 UST. 1 LIT. F RODO?).

Możliwość stosowania monitoringu przez pracodawcę zachodzi zatem wyłącznie, gdy cel przetwarzania nie może być osiągnięty za pomocą innych środków, które są mniej inwazyjne w stosunku do podstawowych praw i wolności osoby, której dane dotyczą. Pracodawca jako administrator powinien być w stanie wykazać zasadność jego stosowania, w tym proporcjonalność tego środka do celu, jakiemu ma on służyć. Powinien wiedzieć, jakie argumenty przeważają, by uznać, że monitoring jest lepszym środkiem niż inne dostępne służące temu samemu celowi oraz czy niepożądane negatywne skutki dla pracowników nie przeważają nad taką formą kontroli. Innymi słowy taka forma nadzoru może być stosowana po upewnieniu się, że inne środki prewencyjne czy ochrony są ewidentnie niewystarczające lub niemożliwe do zastosowania.

W zakresie zagadnienia związanego z monitoringiem pracowników warto mieć na uwadze również:

1. Opinię 2/2017 Grupy Roboczej art. 29 na temat przetwarzania danych w miejscu pracy (https://sip.lex.pl/orzeczenia-i-pisma-urzedowe/pisma-urzedowe/opinia-2-2017-grupy-roboczej-art-29-na-temat-184991577)
2. Wytyczne EROD 3/2019 w sprawie przetwarzania danych osobowych za pomocą urządzeń wideo (https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201903_video_devices_pl.pdf),
3. materiały zmieszczone na stronie internetowej Urzędu:

– Montujesz kamery w miejscu pracy. Sprawdź, o czym należy pamiętać, dostępne pod linkiem: https://uodo.gov.pl/pl/138/1634 **– tekst w ramce poniżej**

Informacja ze strony archiwalnej UODO

Montujesz kamery w miejscu pracy. Sprawdź, o czym należy pamiętać

Zasady stosowania monitoringu wizyjnego w miejscu pracy reguluje Kodeks pracy. Ale pamiętajmy, że w momencie nagrywania obrazu przez kamery, obejmującego wizerunek pracowników, dochodzi do przetwarzania danych osobowych. Zatem pracodawca w tym przypadku powinien również brać pod uwagę przepisy RODO. Jak zadbać o pracowników oraz mienie pracodawcy, jednocześnie robiąc to w zgodzie z ogólnym rozporządzaniem?

Europejska Rada Ochrony Danych przyjęła 10 lipca 2019 r. Wytyczne 3/2019 w sprawie przetwarzania danych osobowych przez urządzenia wideo, które mają na celu wyjaśnienie, w jaki sposób RODO ma zastosowanie do przetwarzania danych osobowych w przypadku korzystania z urządzeń wideo oraz zapewnienie spójnego stosowania ogólnego rozporządzenia o ochronie danych w tym zakresie. Wskazują one m.in., że dokonując wyboru rozwiązań technicznych administrator powinien brać pod uwagę technologie przyjazne prywatności, które zwiększają bezpieczeństwo. Przykładami takich technologii są systemy umożliwiające maskowanie lub mieszanie obszarów, które nie są istotne dla obszaru objętego nadzorem.

Pracodawca, decydując się na założenie monitoringu wizyjnego w zakładzie pracy, powinien określić konkretny cel, w którym będzie on wykorzystywany. Monitoring ma służyć zapewnieniu bezpieczeństwa pracowników lub ochrony mienia, lub kontroli produkcji, lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, a obszar nadzoru może obejmować teren zakładu pracy lub teren wokół zakładu pracy.

Nagrywasz? Informuj

Pracodawca korzystający z monitoringu powinien poinformować osoby, które potencjalnie mogą zostać nim objęte, o tym, że monitoring jest stosowany i jaki obszar jest nim objęty. Powinien spełnić także obowiązek informacyjny wynikający z art. 13 RODO, czyli m.in. podać swoją nazwę, adres, obszar oraz cel monitorowania, okres przetwarzania danych – co ma również istotne znaczenie dla dochodzenia roszczeń, czy też wskazać ewentualnych odbiorców danych.

Pracownicy natomiast muszą mieć świadomość, że w miejscu, w którym się znajdują, wprowadzono monitoring. Pracodawca, zgodnie z kodeksem pracy, oznacza pomieszczenia i teren monitorowany w sposób widoczny i czytelny, za pomocą odpowiednich znaków lub ogłoszeń dźwiękowych, nie później niż jeden dzień przed jego uruchomieniem.

Tablice informujące o zainstalowanym monitoringu powinny być widoczne, umieszczone w sposób trwały w niezbyt dużej odległości od nadzorowanych miejsc. Ich wymiary muszą być proporcjonalne do miejsca, gdzie zostały umieszczone. Stosowane mogą być dodatkowo piktogramy informujące o objęciu dozorem kamer. Z uwagi na to, że należy dopełnić obowiązku informacyjnego określonego w art. 13 RODO, nie jest jednak wystarczające oznaczenie obszaru objętego monitoringiem jedynie piktogramami. Nie oznacza to jednak konieczności umieszczania wszystkich informacji wskazanych w tym przepisie przy tabliczce informacyjnej. W takiej sytuacji możliwe jest zastosowanie warstwowych not informacyjnych. A więc na

tablicy wystarczające mogą być informacje o tym przez kogo, w jakim celu i na jakich podstawach prawnych jest prowadzony monitoring oraz dane kontaktowe IOD, jeżeli został powołany. Należy także poinformować jaki obszar obejmuje monitoring, jakie prawa ma osoba obserwowania oraz gdzie możemy zapoznać się z dodatkowymi informacjami na ten temat.

Jednocześnie, należy podkreślić, że pracodawca powinien zamieścić informacje o celach, zakresie oraz sposobie zastosowania monitoringu w układzie zbiorowym pracy lub w regulaminie pracy albo w obwieszczeniu, jeżeli pracodawca nie jest objęty układem zbiorowym pracy lub nie jest obowiązany do ustalenia regulaminu pracy.

Wizja, bez fonii

Monitoring to środek techniczny umożliwiający rejestrację obrazu. Co za tym idzie – monitoring wizyjny nie może nagrywać dźwięku. Stosowanie kamer rejestrujących również dźwięk może, w przypadkach nieuregulowanych przepisami prawa, zostać uznane za naruszenie prywatności oraz za nadmiarową formę przetwarzania danych, a co za tym idzie wiązać się z odpowiedzialnością nie tylko administracyjną i cywilną ale również i karną. Ponadto, w trakcie nagrania obrazu i dźwięku za pośrednictwem kamery będzie dochodzić do ujawnienia tajemnic prawnie chronionych.

Kodeks pracy zawiera zamknięty katalog miejsc, w których założenie monitoringu jest zabronione. Są to np. łazienki, szatnie czy pomieszczenia socjalne, chyba że stosowanie monitoringu w tych pomieszczeniach jest niezbędne do realizacji określonego celu i nie naruszy to godności oraz innych dóbr osobistych pracownika, w szczególności poprzez zastosowanie technik uniemożliwiających rozpoznanie przebywających w tych pomieszczeniach osób. Monitoring pomieszczeń sanitarnych wymaga uzyskania uprzedniej zgody zakładowej organizacji związkowej, a jeżeli u pracodawcy nie działa zakładowa organizacja związkowa – uprzedniej zgody przedstawicieli pracowników wybranych w trybie przyjętym u danego pracodawcy.

Monitorowany obszar powinien zostać ograniczony również do niezbędnego zasięgu, tak aby przetwarzać dane, które są niezbędne do realizacji celu, w jakim monitoring ten został zastosowany.

Warto podkreślić, że przywołana regulacja daje pracodawcy uprawnienie skorzystania z monitoringu wizyjnego, nie jest to zatem jego obowiązek. Wprowadzenie tej formy monitoringu powinno być poprzedzone wnikliwą analizą jej konieczności, tym samym uznania, że do zapewnienia bezpieczeństwa np. pracownikom, nie można zastosować mniej ingerujących w prywatność środków umożliwiających zapewnienie tego bezpieczeństwa.

Kodeks pracy przewiduje zamknięty katalog sytuacji wprowadzenia tej szczególnej formy przetwarzania danych osobowych. Nie można zatem wykraczać poza jego zakres i stosować to uprawnienie w celu oceny jakości wykonywanej pracy przez pracowników. Narusza to bowiem ich prywatność, a pracownicy mają do niej prawo nawet w miejscu wykonywania swojej pracy.

Pracodawca stosując narzędzia ingerujące w prywatność pracowników musi przestrzegać pewnych zasad i pamiętać, że życie prywatne może rozciągać się na działalność zawodową jednostki.

Udostępniaj nagranie pracownikowi, jeśli otrzymasz takie żądanie

Pracodawca, od którego pracownik domaga się udostępnienia dotyczących go nagrań z monitoringu wizyjnego powinien wziąć pod uwagę to żądanie. Podstawą takiego działania będzie art. 15 ust. 1 RODO. Administrator ma obowiązek udostępnić osobie informacji związanych z przetwarzaniem jej danych osobowych, jak cel przetwarzania, kategorię danych osobowych, odbiorców lub kategorii odbiorców, którym dane osobowe zostały lub zostaną ujawnione, planowanego okresu przechowywania danych osobowych oraz innych informacji wskazanych w przywołanym przepisie.

Należy pamiętać, że zgodnie z art. 15 ust. 1 RODO - Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące. Administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu (np. kopię nagrań monitoringu). Jeżeli osoba ta zwraca się o kopię drogą elektroniczną, i jeżeli nie zaznaczy inaczej, informacji udziela się w powszechnie stosowanej formie elektronicznej.

Data wytworzenia informacji: 29.04.2021 r.

Czy w jedn. organizacyjnych samorządu terytorialnego funkcjonuje kilku odrębnych administratorów?

W związku problemami praktycznymi oraz interpretacyjnymi w przedmiocie statusu administratora w samorządzie terytorialnym zwracam się z prośbą o udzielenie odpowiedzi na następujące pytanie: czy w strukturach jednostek samorządu terytorialnego należy wyróżnić kilku odrębnych administratorów, np. urząd gminy (jako pracodawcę), wójta (organ wykonawczy), radę gminy (organ stanowiący). Jakie niesie to za sobą konsekwencje, np. czy oznacza to konieczność opracowania oddzielnych dokumentacji ochrony danych osobowych dla każdego z tych administratorów czy też powinna to być dokumentacja uwzględniająca współpracę pomiędzy administratorami? Czy należy powołać inspektora ochrony danych dla każdego z tych administratorów?

Zgodnie z definicją zawartą w 4 pkt 7 RODO „administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Określając status administratora w odniesieniu do konkretnego przetwarzania należy uwzględniać element zarówno podmiotowy (tzn. administratorem może być osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot), jak i to, że w przypadku podmiotów sektora publicznego (o ile podmiot będący administratorem nie jest wskazany wprost w konkretnym przepisie) najczęściej ma miejsce sytuacja, w której rola ta wynika z zakresu zadań publicznych, jakie przepisy mu przypisują i dla których realizacji niezbędne jest przetwarzanie danych.

Wskazuje na to również Grupa Robocza Art. 29 w opinii 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający” (str. 11 opinii, https://ec.europa.eu/justice/article-

29/documentation/opinion-recommendation/files/2010/wp169_pl.pdf). Jednocześnie w dokumencie tym podkreśla się, że konkretne stosowanie pojęcia administratora danych staje się obecnie coraz bardziej złożone, ze względu na zróżnicowanie form prawnych oraz organizacyjnych różnych podmiotów, które faktycznie decydują o celach i sposobach przetwarzania.

Taki sposób identyfikowania administratora podpowiada również Europejska Rada Ochrony Danych w Wytycznych EROD 7/2020 w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO (https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_pl.pdf). Zgodnie z tymi Wytycznymi, istnieją przypadki, w których administrator lub kryteria jego wyznaczania są wprost określone w przepisie prawa, jednak bardziej powszechne są sytuacje, w których status ten wynika z tego, że ustawa nakłada na dany podmiot zadanie lub obowiązek gromadzenia i przetwarzania określonych danych. Wówczas administratorem jest zwykle organ wyznaczony na mocy prawa do realizacji tego zadania publicznego. W takim przypadku prawo, choć pośrednio, określa, kto jest administratorem. Innymi słowy prawo może nakładać na podmioty publiczne lub prywatne obowiązek przetwarzania określonych danych, a podmioty te uznawane są zazwyczaj uznawane za administratorów w odniesieniu do przetwarzania, które jest niezbędne do wykonania tego obowiązku (pkt 21-22 ww. Wytycznych).

Zgodnie z przyjętą w RODO definicją, pojęcie administratora ma bardzo szeroki zakres znaczeniowy, gdyż może nim być w zasadzie każdy podmiot, o ile ustala cele i sposoby przetwarzania danych osobowych. Wobec powyższego w zależności od danych osobowych, które są przetwarzane oraz podstawy prawnej przetwarzania i kompetencji poszczególnych podmiotów (organów) do przetwarzania, administratorem może być zarówno organ np. wójt lub burmistrz (prezydent), rada gminy, gminne jednostki organizacyjne (np. ośrodek pomocy społecznej lub szkoła), a także - w odniesieniu do danych pracowników i kandydatów do pracy - gminna jednostka organizacyjna jaką jest urząd gminy.

Rozstrzygając więc, który podmiot jest w danej sytuacji administratorem w odniesieniu do konkretnych danych osobowych, należy przede wszystkim dokonać analizy przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych. Ocena ta powinna być dokonywana w odniesieniu do konkretnego procesu przetwarzania.

Tytułem przykładu podać można, że art. 18 ust. 1 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2020 r. poz. 713 z późn. zm.) stanowi, że do właściwości rady gminy należą wszystkie sprawy pozostające w zakresie działania gminy, o ile ustawy nie stanowią inaczej. Natomiast art. 18 ust. 2 tej ustawy wskazuje na katalog zadań przypisanych do wyłącznej właściwości rady gminy. A zatem, w tych przypadkach, w których przepisy prawa wskazują, że

określone zadania należą do właściwości rady gminy i dla ich wykonania niezbędne jest przetwarzanie określonych danych, należy uznać radę gminy za administratora tych danych.

Takim sposobem identyfikowania administratora na podstawie norm, które określają zadania podmiotu będącego administratorem, Prezes UODO (wcześniej GIODO) posługiwał się w wielu dotychczasowych decyzjach, ale też we wskazówkach i poradnikach publikowanych na jego stronie internetowej (np. w decyzji w sprawie przetwarzania danych przez Burmistrza Aleksandrowa Kujawskiego https://uodo.gov.pl/decyzje/ZSPU.421.3.2019, w poradniku Ochrona danych osobowych w kampanii wyborczej – poradnik https://uodo.gov.pl/pl/138/497, poradniku Ochrona danych osobowych w szkołach i placówkach oświatowych https://uodo.gov.pl/pl/201/481)

Jako przykład posłużyć może również materiał „Realizacja autonomicznych uprawnień kontrolnych radnego" zamieszczonym Newsletterze dla Inspektorów Ochrony Danych (wrzesień 2020), str. 7 (https://uodo.gov.pl/p/archiwum-newslettera-dla-iod – **tekst w ramce poniżej**), gdzie UODO wskazał, że 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. Natomiast z inną sytuacją mamy do czynienia wówczas, gdy radny wykonuje swoje autonomiczne uprawnienia kontrolne, o których mowa w art. 24 ust. 2 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym. Wówczas radny będzie odrębnym administratorem, gdyż to on będzie ustalał cele i sposoby przetwarzania danych osobowych pozyskanych w związku z tego typu swoją aktywnością.

Informacja ze strony archiwalnej UODO – Newsletter wrzesień 2020, str. 7

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.

Funkcjonowanie kilku administratorów w gminie uzasadnia fakt, iż jednostki organizacyjne samorządu terytorialnego i ich organy realizują różne zadania, przypisane im na podstawie przepisów prawa. Przykładem takich złożonych sytuacji są np. wybory na ławników, gdzie do przetwarzania danych kandydatów na ławników i ławników zgodnie z przepisami prawa uprawnionych jest kilka podmiotów, a zatem wobec tych danych można wskazać kilku administratorów, m.in. radę gminy dokonującą wyboru oraz burmistrza jako organ zapewniający przeprowadzenie tych wyborów.

Podobne podejście Prezes UODO prezentuje również w odpowiedziach na pytania inspektorów zamieszczonych na stronie internetowej UODO w zakładce Inspektor Ochrony Danych/Zadania, a w szczególności:

- KTO JEST ADMINISTRATOREM DANYCH OSOBOWYCH PRZETWARZANYCH W URZĘDZIE WOJEWÓDZKIM?

- CZY RZECZNIK PRAW KONSUMENTÓW JEST ADMINISTRATOREM DANYCH OSOBOWYCH?
- KTO JEST ADMINISTRATOREM DANYCH PRZETWARZANYCH W CELU WYDANIA KARTY SENIORA?
- CZY PRACOWNIK DZIAŁU KADR URZĘDU GMINY MOŻE PRZETWARZAĆ DANE KIEROWNIKÓW JEDNOSTEK ORGANIZACYJNYCH?

Przykładem funkcjonowania więcej niż jednego administratora w jednej jednostce organizacyjnej jest przedstawiona w Newsletter UODO dla Inspektorów Ochrony Danych (Wydanie 2, maj 2019,– **tekst w ramce poniżej**), sytuacja związana z przetwarzaniem danych w związku z załatwianiem wniosków o ustalenie zdarzenia medycznego na podstawie ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta przez wojewódzką komisję do spraw orzekania o zdarzeniach medycznych oraz wojewodę. Każdy z tych podmiotów uczestniczy w procesie przetwarzania przedmiotowych danych osobowych w innym zakresie. Do zadań Komisji należy przede wszystkim merytoryczne rozpatrywanie wniosków określonych osób fizycznych o ustalenie zdarzenia medycznego. Z drugiej strony wojewoda uczestniczy w procesie przetwarzania danych osobowych wnioskodawców, w tym przede wszystkim w związku z obowiązkiem zapewnienia obsługi administracyjno-biurowej komisji wojewódzkiej (zapewnienie lokalu do prowadzenia działalności w obrębie urzędu, odpowiednią obsługę kadrową, która jest upoważniona do wglądu do akt prowadzonych przez wojewódzkie komisje postępowań oraz do archiwizacji tych akt).
W odniesieniu do tej sytuacji Prezes UODO wskazywał na współadministrowanie określone w art. 26 RODO. Przyjęcie w tej sytuacji współadministrowania może ułatwić obu administratorom wywiązanie się z obowiązków określonych w przepisach RODO.

Informacja ze strony archiwalnej UODO - Newsletter Wydanie 2, maj 2019

Wojewodę oraz wojewódzką komisję do spraw orzekania o zdarzeniach medycznych można uznać za współadministratorów (art. 26 RODO)

UODO - odnosząc się do przedstawionego mu zagadnienia odpowiedzialności za przetwarzanie danych w związku z obsługą wniosków o ustalenie zdarzenia medycznego wskazał, że wojewódzkie komisje do spraw orzekania o zdarzeniach medycznych oraz wojewodowie przetwarzają dane osobowe osób, które są stronami postępowań prowadzonych przez wojewódzkie komisje. Każdy z tych podmiotów uczestniczy w procesie przetwarzania przedmiotowych danych osobowych w innym zakresie. Do zadań Komisji należy przede wszystkim merytoryczne rozpatrywanie wniosków określonych osób fizycznych o ustalenie zdarzenia medycznego. Z drugiej strony przepisy ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta wskazują, że wojewoda uczestniczy w procesie przetwarzania danych osobowych wnioskodawców, w tym przede wszystkim w związku z obowiązkiem zapewnienia obsługi administracyjnobiurowej komisji wojewódzkiej. Wojewoda zapewnia wojewódzkiej komisji lokal do prowadzenia działalności w obrębie urzędu, odpowiednią obsługę kadrową, która jest upoważniona do wglądu do akt prowadzonych przez wojewódzkie komisje postępowań oraz do archiwizacji tych akt. Komisja i wojewoda, realizując swoje uprawnienia przysługujące im na podstawie odrębnych przepisów mogą zatem – stosownie do art. 26 RODO – określić w sposób przejrzysty zakresy swojej

odpowiedzialności dotyczącej wypełnienia obowiązków wynikających z przepisów RODO. W ramach wspólnych uzgodnień powinni określić kwestie, nieuregulowane wprost w przepisach prawa, w tym m.in. kwestię odpowiedniego zabezpieczenia danych osobowych wnioskodawców czy też realizacji określonych obowiązków informacyjnych.

Niezależnie od poczynionych uzgodnień pomiędzy wojewódzką komisją a wojewodą, osoba, której dane dotyczą może wykonywać przysługujące jej prawa wynikające z RODO wobec każdego ze współadministratorów, a więc zarówno w stosunku do komisji, jak i wojewody.

Jednocześnie należy zauważyć, że istnienie w strukturach gminy, powiatu, czy województwa więcej niż jednego podmiotu będącego odrębnym administratorem, nie musi oznaczać konieczności stworzenia procedur i polityk ochrony danych osobowych w odrębnych dokumentach dla każdego z administratorów. Jedna dokumentacja może bowiem regulować kwestie ochrony danych dotyczące administratorów istniejących w ramach tej samej jednostki. Szersze informacje na ten temat znaleźć można zej na ten temat UODO wypowiedział się w odpowiedzi na pytanie: CZY KILKU ADMINISTRATORÓW MOŻE MIEĆ JEDNĄ DOKUMENTACJĘ OCHRONY DANYCH OSOBOWYCH?

Jeżeli zaś chodzi o obowiązek wyznaczenia inspektora ochrony danych, np. przez radę gminy, to wskazać należy, że na podstawie art. 37 ust. 1 lit a RODO zobowiązane są do tego organy lub podmioty publiczne, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Natomiast zgodnie z brzmieniem art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych — który to przepis prawa krajowego określa kierunek interpretacji użytego w art. 37 ust. 1 lit. a RODO, pojęcia „organ lub podmiot publiczny” — podmiotami zobowiązanymi do wyznaczenia inspektora ochrony danych osobowych są m.in. podmioty i organy publiczne, które są jednostkami sektora finansów publicznych. Zgodnie z art. 9 pkt 1 ustawy o finansach publicznych sektor finansów publicznych tworzą m.in. organy władzy publicznej.

Gdy w ramach danej jednostki organizacyjnej np. urzędu gminy działa kilku administratorów zobowiązanych do wyznaczenia IOD, mogą oni wyznaczyć do pełnienia tej funkcji jedną, tę samą osobę. Zgodnie z brzmieniem art. 37 ust. 3 RODO jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć - z uwzględnieniem ich struktury organizacyjnej i wielkości - jednego inspektora ochrony danych. Skorzystanie z takiego rozwiązania wymaga dokonania analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora. Więcej informacji na ten temat znaleźć można w zamieszczonej na stronie internetowej UODO odpowiedzi na pytanie CZY KIEROWNIK URZĘDU STANU CYWILNEGO JEST ADMINISTRATOREM I CZY MUSI WYZNACZYĆ IOD?

Data wytworzenia informacji: 29.04.2021 r.

Jaka jest podstawa przetwarzania danych studentów, którym udziela się pomocy materialnej?

Jaka jest podstawa przetwarzania danych studentów w przypadku przyznawania im pomocy materialnej przez uczelnię? Uczelnia, w której pełnię funkcję IOD zamierza utworzyć Biuro ds. Obsługi Osób Niepełnosprawnych. Do zadań biura ma należeć wspieranie studentów w trudnych sytuacjach życiowych, w tym udzielenie pomocy materialnej bądź pomocy psychologicznej. Czy właściwą przesłanką przetwarzania danych osobowych będzie zgoda?

Zgodnie z przepisami RODO, podmiot może przetwarzać dane osobowe wyłącznie wtedy, gdy istnieje podstawa prawna przetwarzania danych. Przetwarzanie tzw. danych zwykłych może się odbywać jedynie po spełnieniu jednego z warunków określonych w art. 6 RODO, a w przypadku szczególnej kategorii danych osobowych i danych osobowych dotyczących wyroków skazujących i czynów zabronionych po spełnieniu przesłanek określonych w art. 9 i 10 RODO.

Jednym z praw studenta jest możliwość ubiegania się o przyznanie pomocy materialnej. W art. 86 ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2021 r. poz. 478 z późn. zm.) zostały wskazane formy tej pomocy tj. stypendium socjalne; stypendium dla osób niepełnosprawnych; zapomoga; stypendium rektora; stypendium finansowane przez jednostkę samorządu terytorialnego; stypendium za wyniki w nauce lub w sporcie finansowane przez osobę fizyczną lub osobę prawną niebędącą państwową ani samorządową osobą prawną.

Właściwą przesłanką przetwarzania danych zwykłych w przypadku prowadzenia postępowania w celu przyznania pomocy materialnej studentowi przez uczelnię jest art. 6 ust. 1 lit. c RODO, a w przypadku danych szczególnej kategorii jest art. 9 ust. 2 lit. g RODO w powiązaniu z art. 86 ustawy z dnia 20 lipca 2018 r. - Prawa o szkolnictwie wyższym i nauce.

Odnosząc się do drugiej części pytania dotyczącej odbierania zgody na przetwarzanie danych osobowych przez Biuro w związku ze świadczeniem pomocy psychologicznej studentom oraz pomagania w trudnych sytuacjach życiowych wskazać należy, że Europejska Rada Ochrony Danych w wytycznych z 4 maja 2020 r. dotyczących zgody wskazała, że administratorzy, chcąc przetwarzać szczególne kategorie danych osobowych, w pierwszej kolejności powinni zbadać konkretne wyjątki przewidziane w art. 9 ust. 2 lit. b–j RODO. Jeżeli żaden z nich nie będzie miał zastosowania, wówczas jedyną możliwą przesłanką uprawniającą do przetwarzania takich danych jest uzyskanie wyraźniej zgody, spełniającej przewidziane w RODO warunki (wytyczne dostępne są na stronie Europejskiej Rady Ochrony Danych pod linkiem: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_pl).

Wobec powyższego zanim administrator podejmie decyzję, aby opierać przetwarzanie szczególnych kategorii danych na zgodzie, powinien wcześniej dokonać analizy innych przesłanek.

Data wytworzenia informacji: 29.04.2021 r.

Jaka powinna być podstawa prawna przetwarzania danych osobowych osób wystawiających referencje?

W procesie rekrutacyjnym administrator może otrzymać od kandydata, z jego inicjatywy, dokument referencji, w którym oprócz opinii o kandydacie mogą pojawić się dane osobowe wystawcy referencji, tj. imię, nazwisko, stanowisko, miejsce pracy, ewentualnie adres e-mail i telefon. Administrator nie ma możliwości pozyskania zgody wystawcy referencji, czy zasadne jest założenie, że przetwarzanie opierane jest na przesłance wynikającej z art. 6 ust. 1 lit. f RODO - prawnie uzasadniony interes administratora polega na zapewnieniu możliwości przetwarzania informacji przedstawionych przez kandydata?

Tak jak słusznie wskazano w treści pytania podstawą przetwarzania danych osoby trzeciej udzielającej rekomendacji jest (przy spełnieniu warunków określonych w tym przepisie) art. 6 ust. 1 lit. f RODO. Prawnie uzasadniony interes pracodawcy związany będzie z możliwością wykorzystania informacji zawartych w treści referencji. Pomocne podpowiedzi związane ze złożeniem przez kandydata do pracy tzw. referencji można znaleźć w komunikacie na naszej stronie, pt. „ABC rekrutacji" (https://uodo.gov.pl/pl/138/1599 – **tekst w ramce poniżej**).

Informacja ze strony archiwalnej UODO

ABC rekrutacji

Przygotowując się do rekrutacji, pracodawca powinien gruntownie przeanalizować, jakie dane będzie mógł pozyskać od kandydata do pracy, aby na ich podstawie była możliwa ocena, czy dana osoba spełnia kryteria niezbędne do objęcia stanowiska, o które się ubiega.

Pracodawca musi pamiętać, że proces rekrutacyjny będzie wiązał się z pozyskiwaniem przez niego danych osobowych zawartych w dokumentach rekrutacyjnych. Warto podkreślić, że pracodawca nie może żądać od kandydata danych nadmiarowych, które są niepotrzebne do przeprowadzenia rekrutacji. Ponadto dane osobowe nie mogą być zbierane na zapas, tj. bez wykazania przez administratora zgodnego z prawem celu ich pozyskania i niezbędności do realizacji tego celu.

Jakie dane można pozyskać?

Zgodnie z art. 22^1§ 1kodeksu pracy, pracodawca żąda od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:

1) imię (imiona) i nazwisko;

2) datę urodzenia;

3) dane kontaktowe wskazane przez taką osobę;

4) wykształcenie;

5) kwalifikacje zawodowe;

6) przebieg dotychczasowego zatrudnienia.

Co więcej, pracodawca może żądać podania wykształcenia, kwalifikacji zawodowych oraz przebiegu dotychczasowego zatrudnienia, ale tylko wtedy gdy jest to niezbędne do wykonywania pracy określonego rodzaju lub na określonym stanowisku.

Katalog danych, które mogą być przetwarzane w procesie rekrutacji przez pracodawcę jest zamknięty, co oznacza, że pracodawca nie może przetwarzać danych, które wykraczają poza ten zakres.

Wyrażam zgodę na przetwarzanie danych…

W tym miejscu należy podkreślić, że do przetwarzania wyżej wymienionych danych nie jest potrzebna zgoda. Dotychczasowa praktyka zamieszczenia w liście motywacyjnym CV zgody na przetwarzanie danych w celach rekrutacyjnych nie jest właściwa. Zgoda, a w szczególności wyraźna zgoda na przetwarzanie wybranych danych, może być niezbędna jedynie w określonych sytuacjach. Na przykład, kandydat może zgodzić się na przetwarzanie jego danych na potrzeby przyszłych rekrutacji przez wskazany czas.

Referencje

Co się tyczy referencji należy też pamiętać, że złożenie przez kandydata do pracy tzw. referencji nie uprawnia pracodawcy do kontaktu z podmiotem je wystawiającym w celu pozyskania dodatkowych informacji o kandydacie. Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Potencjalny pracodawca nie może tym samym zwrócić się do poprzedniego pracodawcy o informację, jakie zadania realizował kandydat u tego podmiotu oraz jaką ma opinię o kandydacie do pracy. Podczas procesu rekrutacyjnego źródłem informacji, które dotyczą przebiegu pracy zawodowej, powinien być sam kandydat.

Jakich danych nie trzeba pozyskiwać?

Pracodawca nie może żądać od kandydata danych wykraczających poza zakres, który został wskazany w kodeksie pracy, w szczególności takich, które nie mają związku z celem, jakim jest zatrudnienie pracownika. Może się oczywiście zdarzyć, że osoba kandydująca na konkretne stanowisko będzie musiała spełnić pewne określone prawem wymogi, np. wymóg niekaralności i wówczas pracodawca będzie uprawniony do pozyskania informacji o nim w tym zakresie. Zdarza się, że osoby kandydujące do pracy przekazują z własnej inicjatywy więcej danych, niż jest to wskazane w kodeksie pracy. Przepisy kodeksu pracy nie nakładają obowiązku przekazywania pracodawcy przez kandydata do pracy swojego zdjęcia (niezależnie od formy jego udostępnienia). Niekiedy podajemy także informację ostanie cywilnym, numer PESEL, miejsce urodzenia czy nawet imiona rodziców.

W takiej sytuacji dane osobowe kandydata, o ile nie należą do szczególnej kategorii danych, są przetwarzane przez potencjalnego pracodawcę na podstawie zgody, która może polegać na oświadczeniu bądź zachowaniu, które wdanym kontekście jasno wskazuje, że osoba, której dane dotyczą godzi się na przetwarzanie jej danych osobowych, które sama przekazała. Zatem o ile kandydat sam z własnej woli

zechce udostępnić dodatkowe informacje na swój temat, np. zdjęcie, to wyrażona przez niego zgoda na ich wykorzystanie będzie elementem legalizującym przetwarzanie tych danych na potrzeby naboru przez pracodawcę.

Trzeba przypomnieć, że zgoda osoby, której dane dotyczą, oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.

Warto również dodać, że pracodawca nie może sugerować kandydatowi do pracy zakresu innych danych, które z własnej woli kandydat miałby przekazywać.

Innym przykładem danych, których pracodawca nie może żądać od osoby ubiegającej się o zatrudnienie jest informacja o toczących się i niezakończonych postępowaniach karnych oraz o ich przebiegu. Tego typu informacje nie mieszczą się w katalogu danych, które mogą być przez niego przetwarzane.

Toczące się postępowanie karne nie musi bowiem doprowadzić do prawomocnego skazania danej osoby. Informacji o takich postępowaniach nie zawiera również Krajowy Rejestr Karny, w którym wskazuje się dane, m.in. osób prawomocnie skazanych oraz przeciwko którym prawomocnie umorzono postępowanie karne.

Po dokonaniu wyboru

Jeżeli cel przetwarzania związany z rekrutacją, w związku z którą pozyskano dane, ustaje to dane nie powinny być dłużej przetwarzane. Jednocześnie administrator musi ocenić, czy nie wystąpią inne cele i podstawy prawne uzasadniające ich przetwarzanie (np. archiwizacja). Ponadto w przypadku gdy toczy się spór związany z niezatrudnieniem jest jeszcze kwestia przetwarzania w celu dochodzenia roszczeń.

Pracodawca administratorem

Jak stanowi art. 5RODO administrator powinien przetwarzać dane zgodnie z prawem, rzetelnie iw sposób przejrzysty dla osoby, której one dotyczą. Powinien też zbierać je w konkretnych, wyraźnych i prawnie uzasadnionych celach inie wykorzystywać ich w sposób niezgodny z tymi celami. Jednocześnie RODO zobowiązuje go, by pozyskując dane osobowe, w sposób jasny, przejrzysty i zrozumiały informował m.in. o pełnej nazwie i adresie swojej siedziby; ocelu i podstawie prawnej przetwarzania danych osobowych, a także o okresie, przez który zebrane dane będą przechowywane.

Pracodawca ma obowiązek poinformować kandydata do pracy o tych okolicznościach w chwili pozyskiwania tych danych w sposób jasny, czytelny i łatwo dostępny dla kandydata. Może to zrobić np. w treści ogłoszenia o pracę lub w informacji zwrotnej bezpośrednio po otrzymaniu od kandydata aplikacji do pracy.

Każda osoba, która ma wątpliwość, czy po zakończeniu rekrutacji usunięto jej dane osobowe, ma prawo – zgodnie z art. 15 RODO – zwrócić się do administratora z pytaniem, czy i jakie dotyczące jej dane przetwarza oraz w jakim celu to robi ina jakiej podstawie. Gdyby okazało się, że mimo zakończonej rekrutacji jej dane nadal są przetwarzane, to może zażądać od administratora ich usunięcia.

Data wytworzenia informacji: 18.05.2021 r.

Czy uczelnia może udostępnić dane studentów wyłącznie w oparciu o ustawę o Straży Granicznej?

Nasza uczelnia (będąca uczelnią niepubliczną) otrzymała od Straży Granicznej pismo, zawierające wniosek o udostępnienie danych studentów, w związku z prowadzoną sprawą. Jako podstawę prawną wniosku wskazano wyłącznie przepisy ustawy o Straży Granicznej. Czy istotnie w przypadku uczelni dopuszczalność udostępnienia danych osobowych studentów należy rozpatrywać wyłącznie w oparciu o przepisy tej ustawy?

Każdy wniosek o udostępnienie danych wymaga indywidualnej analizy. Rozpatrujący go administrator, który podejmuje ostateczną decyzję w tej sprawie, musi wziąć przy tym pod uwagę konkretne okoliczności faktyczne i prawne, w tym obowiązujące przepisy prawa, rodzaj danych osobowych, cel oraz uzasadnienie potrzeby posiadania danych przez podmiot, który występuje o ich udostępnienie. Analiza otrzymanego wniosku pod kątem wskazanej podstawy prawnej powinna za każdym razem obejmować sprawdzenie przez administratora wskazanego przepisu prawa i ocenę, czy faktycznie wynika z niego uprawnienie wnioskodawcy.

Warto wówczas mieć na uwadze określoną w art. 7 Konstytucji RP zasadę działania organów publicznych na podstawie i w granicach prawa, organ publiczny nie może domniemywać swoich kompetencji jeśli nie wynikają one wprost z przepisu prawa. Dlatego gdy o udostępnienie danych osobowych występuje podmiot realizujący zadania publiczne, powinien w pierwszej kolejności wyraźnie wskazać przepisy uprawniające go do pozyskania danych. W przypadku zaś stwierdzenia braku podstawy prawnej do udostępnienia danych osobowych, administrator nie powinien takich danych udostępnić.

Pytanie inspektora dotyczy wątpliwości w zakresie podstawy prawnej do udostępniania przez uczelnię niepubliczną na rzecz Straży Granicznej danych osobowych studentów.

W przypadku organów Straży Granicznej kwestie uprawnień do pozyskiwania danych osobowych należy rozpatrywać w szczególności w oparciu o przepisy ustawy o Straży Granicznej. Należy jednak zwrócić uwagę, że w przypadku udostępniania danych osobowych studentów, decydujące znaczenie mogą mieć przepisy ustawy Prawo o szkolnictwie wyższym i nauce oraz aktów wykonawczych do tej ustawy. Przepisy te określają bowiem m.in. podmioty uprawnione oraz warunki, na jakich mogą mieć one dostęp do danych osobowych studentów. W szczególności zgodnie z art. 344 ust. 3 pkt 4c tej ustawy, dostęp do danych zawartych w wykazie studentów (który stanowi bazę danych wchodzącą w skład Zintegrowanego Systemu Informacji o Szkolnictwie Wyższym i Nauce POL-on, nazywany "Systemem POL-on") przysługuje Komendantowi Głównemu Straży Granicznej oraz komendantom oddziałów Straży Granicznej i komendantom placówek Straży Granicznej - w celu realizacji ich zadań, w szczególności

określonych w art. 1 ust. 2 pkt 2a ustawy o Straży Granicznej - w zakresie danych, o których mowa w ust. 1 art. 344.

Natomiast tryb i sposób *udostępniania* danych z tego wykazu określa rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 6 marca 2019 r. w sprawie danych przetwarzanych w Zintegrowanym Systemie Informacji o Szkolnictwie Wyższym i Nauce POL-on. W szczególności zgodnie z § 17 ust. 4 tego rozporządzenia uprawnione podmioty (w tym organy Straży Granicznej), które chcą posiadać dostęp do danych zawartych w tym systemie, powinny złożyć do Ministra Edukacji i Nauki wniosek o założenie konta w systemie POL-on.

Podsumowując można wskazać, że jeżeli przesłany przez Straż Graniczną wniosek o udostępnienie danych osobowych budzi wątpliwości pod względem jego podstaw prawnych, dobrym rozwiązaniem jest zwrócenie się do wnioskodawcy o wyjaśnienie tych wątpliwości. Straż Graniczna bowiem ma prawo przetwarzać dane osobowe w związku z prowadzonymi czynnościami, jednak w każdym przypadku musi legitymować się podstawą prawą swoich działań. Jednocześnie warto mieć na uwadze, że administrator, do którego zwrócono się o udostępnienie danych, powinien dokonać oceny podstawy prawnej wskazanej przez wnioskodawcę, a także oceny, czy wnioskowane dane osobowe nie podlegają szczególnej regulacji w zakresie ich udostępniania. W przedstawionym przypadku należy dodatkowo dokonać analizy regulacji zawartych w ustawie Prawo o szkolnictwie wyższym i nauce. Zgromadzenie powyższych informacji pozwoli administratorowi na dokonanie szczegółowej analizy dopuszczalności takiego udostępnienia.

Data wytworzenia informacji: 28.06.2021 r.

Jak prawidłowo usuwać dane pozyskane dla przyznania Karty Dużej Rodziny?

Uprzejmie proszę o wskazówki, w jaki sposób należy usunąć dane osoby, która utraciła prawo do posiadania Karty Dużej Rodziny (dalej KDR) z wniosku oraz innych dokumentów potwierdzających prawo do przyznania Karty, gdy prawo utraciła tylko jedna osoba? Zgodnie z ustawą o Karcie Dużej Rodziny (art. 21 ust. 4 i 5) dane osobowe są usuwane z wniosku o przyznanie KDR oraz innych dokumentów potwierdzających prawo przyznania KDR. Usunięcie odbywa się niezwłocznie po okresach wskazanych w ustawie. Jeżeli prawo do KDR traci tylko jedna z osób ujętych we wniosku, to jak prawidłowo usunąć jej dane, pozostawiając dane pozostałych osób? Czy należy je wymazywać korektorem?

Zgodnie z zasadą ograniczenia przechowywania (retencji) sformułowaną w art. 5 ust. 1 lit. e RODO, dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w są one przetwarzane.

Administrator zobowiązany jest zatem ustalić, przez jaki okres może posiadać dane osobowe przetwarzane w określonym celu oraz jakie czynności musi podjąć po upływie tego okresu. W odniesieniu do niektórych danych kwestia ta wynika wprost z przepisów prawa.

Zgodnie z art. 21 ust. 4 ustawy o Karcie Dużej Rodziny, nazywanej dalej „ustawą o KDR", dane osobowe, o których mowa w ust. 1 tego artykułu, są przetwarzane przez okres 1 roku od dnia utraty prawa do korzystania z Karty Dużej Rodziny, z wyjątkiem informacji dotyczących osób, którym Karta nie została przyznana, które przetwarza się przez okres 1 roku od dnia, w którym decyzja odmawiająca prawa do Karty stała się ostateczna. Ponadto w myśl art. 21 ust. 5 ustawy o KDR, dane osobowe, o których mowa w ust. 1 tego artykułu, wraz z wnioskiem o przyznanie Karty i dokumentami potwierdzającymi prawo do przyznania Karty, usuwa się niezwłocznie po upływie okresów przetwarzania, o których mowa w ust. 4.

Odnosząc się do kwestii usuwania danych wówczas, gdy we wniosku o przyznanie karty zawarte byłyby - poza danymi osoby, która utraciła prawo do korzystania z karty - dane innych osób uprawnionych nadal do korzystania z karty, wskazuję, że usuwanie niektórych danych (w tym przypadku danych dotyczących osoby, która utraciła prawo do korzystania z karty) z takiego wniosku, wydaje się działaniem niewłaściwym i wpłynęłoby na integralność tego dokumentu. Organ nie powinien ingerować w treść dokumentów, które otrzymuje od strony lub innego podmiotu. Jeżeli zatem prawo do korzystania z karty traci jedna z osób ujętych we wniosku, wówczas taki wniosek powinien zostać usunięty dopiero wówczas, gdy wszystkie osoby, których dane ten wniosek zawiera, utracą prawo do korzystania z karty.

Warto nadmienić, że każda decyzja podjęta w tej materii przez administratora powinna uwzględniać zasadę rozliczalności sformułowaną w art. 5 ust. 2 RODO, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania danych określonych w ustępie 1 tego artykułu i musi być w stanie wykazać ich przestrzeganie. Pomocne w przestrzeganiu zasady ograniczenia przechowywania jest opracowanie i wdrożenie odpowiednich procedur związanych z usuwaniem danych osobowych.

Data wytworzenia informacji: 29.07.2021 r.

Czy broker ubezpieczeniowy ma status administratora?

Przedmiotem umowy urzędu z brokerem jest wykonywanie stałego pośrednictwa ubezpieczeniowego w zakresie ubezpieczeń osobowych oraz ubezpieczeń majątkowych oraz gwarancji ubezpieczeniowych. W tym celu broker otrzymuje od urzędu:

- **dane pracowników urzędu niezbędne w celu ubezpieczenia pracowników podczas zagranicznych delegacji służbowych,**

- **dane kierującego (pracownika urzędu) w przypadku szkody komunikacyjnej,**
- **dane osób, które ulegną wypadkowi na terenie miasta w ramach realizacji odszkodowań,**
- **wszelkie dane niezbędne do ubezpieczeń majątkowych.**

Czy w takiej sytuacji należy uznać, że broker, który działa na podstawie własnych, sektorowych przepisów prawa, jest odrębnym administratorem, czy jednak należy zawrzeć z nim umowę powierzenia przetwarzania danych osobowych?

Broker ubezpieczeniowy jest osobą pośrednicząca między klientem a firmą ubezpieczeniową. Działając na rzecz swoich klientów, wykonuje działalność na zasadach i w sposób określony przepisami prawa, przede wszystkim ustawą z dnia 15 grudnia 2017 r. o dystrybucji ubezpieczeń. Dlatego rozstrzygając, jaki status przysługuje temu podmiotowi w świetle przepisów o ochronie danych osobowych, należy odwołać się do przepisów określających zasady i sposób prowadzenia działalności przez brokerów ubezpieczeniowych (na analogiczne podejście wskazujemy w odpowiedzi na pytanie: CZY BIEGLI REWIDENCI MAJĄ STATUS ADMINISTRATORA W ZWIĄZKU ZE ŚWIADCZENIEM SWOICH USŁUG?)

Zgodnie z art. 4 ust. 4 ww. ustawy broker ubezpieczeniowy, w ramach prowadzonej działalności brokerskiej, **wykonuje czynności w zakresie dystrybucji ubezpieczeń w imieniu lub na rzecz klienta**, zwane dalej „czynnościami brokerskimi w zakresie ubezpieczeń".

Zgodnie z art. 4 ust. 1 powyższej ustawy **dystrybucja ubezpieczeń** oznacza działalność wykonywaną wyłącznie przez dystrybutora ubezpieczeń (tj. zakład ubezpieczeń, agenta ubezpieczeniowego, agenta oferującego ubezpieczenia uzupełniające lub brokera ubezpieczeniowego) polegającą na:

1. doradzaniu, proponowaniu lub wykonywaniu innych czynności przygotowawczych zmierzających do zawarcia umów ubezpieczenia lub umów gwarancji ubezpieczeniowych;
2. zawieraniu umów ubezpieczenia lub umów gwarancji ubezpieczeniowych w imieniu zakładu ubezpieczeń, w imieniu lub na rzecz klienta albo bezpośrednio przez zakład ubezpieczeń;
3. **udzielaniu pomocy przez** pośrednika ubezpieczeniowego (tj. agenta ubezpieczeniowego, agenta oferującego ubezpieczenia uzupełniające, **brokera ubezpieczeniowego** oraz brokera reasekuracyjnego, którzy wykonują dystrybucje ubezpieczeń albo dystrybucję reasekuracji za wynagrodzeniem) **w administrowaniu umowami ubezpieczenia lub umowami gwarancji ubezpieczeniowych i ich wykonywaniu, także w sprawach o odszkodowanie lub świadczenie.**

Zgodnie z art. 27 ust. 1 i 2 ustawy o dystrybucji ubezpieczeń **klient udziela brokerowi ubezpieczeniowemu, w formie pisemnej, pełnomocnictwa do wykonywania czynności**

brokerskich w zakresie ubezpieczeń w imieniu klienta, broker natomiast udostępnia zakładowi ubezpieczeń przy pierwszej czynności należącej do czynności brokerskich w zakresie ubezpieczeń ten dokument pełnomocnictwa. Zatem broker działa w imieniu i na rzecz swojego klienta na podstawie udzielonego pełnomocnictwa, ale - na co warto zwrócić uwagę - mandat ten nie jest nakierowany na przetwarzanie danych osobowych.

Stosownie do treści art. 32 ust.3 ww. ustawy broker ubezpieczeniowy:

1. **zachowuje w tajemnicy informacje uzyskane w związku z wykonywaniem czynności brokerskich** w zakresie ubezpieczeń, przy czym obowiązek ten ciąży na brokerze ubezpieczeniowym również po rozwiązaniu stosunku umownego ze zleceniodawcą;
2. okazuje zakładowi ubezpieczeń i klientowi na każde żądanie zezwolenie na wykonywanie działalności brokerskiej w zakresie ubezpieczeń;
3. prowadzi rejestr skarg i reklamacji;
4. **przechowuje dokumentację dotyczącą wykonywanej działalności brokerskiej w zakresie ubezpieczeń, w szczególności pełnomocnictwa do wykonywania czynności brokerskich w zakresie ubezpieczeń w imieniu klienta oraz dokumenty dotyczące wynagrodzenia brokera, przez okres 10 lat od dnia zakończenia współpracy z klientem.**

Powyższe przepisy określają zadania i obowiązki brokera ubezpieczeniowego oraz zasady świadczenia usług na rzecz klientów. Czynności brokera na rzecz klienta mogą polegać na wykonywaniu wszystkich albo tylko niektórych czynności w zakresie dystrybucji ubezpieczeń, np. na zebraniu i analizie dostępnych na rynku wariantów ubezpieczenia, doradztwie, zgłaszaniu i likwidacji roszczeń, układaniu się z zakładami ubezpieczeń co do wysokości świadczeń związanych z konkretnymi roszczeniami.

Zgodnie z przedstawionymi w pytaniu informacjami, przedmiotem umowy z brokerem jest prowadzenie serwisu brokerskiego polegającego na wykonywaniu stałego pośrednictwa ubezpieczeniowego w zakresie ubezpieczeń osobowych oraz ubezpieczeń majątkowych oraz gwarancji ubezpieczeniowych na rzecz zleceniodawcy, tj. gminy/urzędu. Takie czynności objęte są katalogiem zadań wskazanych w art. 4 ust. 1 pkt 3 ustawy o dystrybucji ubezpieczeń (udzielanie pomocy przez brokera w wykonywaniu umowy, także w sprawach o odszkodowanie lub świadczenie), co przemawiałoby za traktowaniem brokera - w zakresie przetwarzania danych osobowych w opisanym celu - jako administratora tych danych. Taki status brokera wynika również z innych obowiązków brokera określonych w przepisach powołanej ustawy, tj. obowiązek zachowania informacji w tajemnicy czy przechowywania dokumentacji dotyczącej wykonywanej działalności brokerskiej.

Data wytworzenia informacji: 06.09.2021 r.

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

Publiczna uczelnia wyższa planuje realizować monitoring karier zawodowych absolwentów zgodnie z art. 352 pkt 14 ustawy Prawo o szkolnictwie wyższym i nauce. Proszę o wyjaśnienie, czy wskazany powyżej przepis prawa stanowi podstawę prawną przetwarzania danych osobowych absolwentów (w celu monitoringu karier zawodowych) w myśl art. 6 ust. 1 lit. c RODO, czy też w tym celu należy uprzednio pozyskać stosowne zgody od studentów bądź absolwentów.

Administrator będący podmiotem publicznym, oceniając, czy przetwarzanie danych jest dopuszczalne w określonej sytuacji, powinien przede wszystkim kierować się przepisami prawa odnoszącymi się do jego działalności. Podmioty publiczne co do zasady przetwarzają dane na podstawie i w granicach określonych przez przepisy prawa.

W przypadku podmiotów publicznych - co do zasady - właściwymi podstawami do przetwarzania danych osobowych powinny być przesłanka określona w art. 6 ust. 1 lit. c i e RODO w połączeniu z właściwymi przepisami szczególnymi określającymi zadania konkretnych organów i instytucji, a zatem gdy przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze lub gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Natomiast zgoda osoby, której dane dotyczą, może być odebrana przez podmiot publiczny w sytuacjach przewidzianych w przepisach prawa. Wynika to z zasady praworządności, zgodnie z którą podmioty publiczne działają na podstawie przepisów prawa i w jego granicach.

Tymczasem zgodnie z brzmieniem art. 352 ust. 14 ustawy z dnia z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce „w celu dostosowania programu studiów do potrzeb rynku pracy uczelnia może prowadzić własny monitoring karier zawodowych swoich absolwentów”. Przepis ten nie nakłada na uczelnię obowiązku prowadzenia monitoringu karier, a jedynie daje jej taką możliwość.

Wobec powyższego zasadne jest przyjęcie, że podstawą przetwarzania danych absolwentów uczelni wyższej w związku z monitorowaniem karier zawodowych absolwentów w celu dostosowania programu studiów do potrzeb rynku pracy nie będzie art. 6 ust. 1 lit. c RODO, lecz art. 6 ust. 1 lit. e RODO, tj. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Data wytworzenia informacji: 06.09.2021 r.

Jakie rozwiązania są wystarczające w przypadku wykazu podmiotów podpowierzających?

Jako inspektor obsługujący podmioty przetwarzające działające w branży IT zwracam się z pytaniem dotyczącym klauzuli 7.7 pkt. A Decyzji Wykonawczej Komisji (UE) 2021/915 z dnia 4 czerwca 2021 r. w sprawie standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi na podstawie art. 28 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 oraz art. 29 ust. 7 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725. W naszej branży mamy do czynienia z pewną dynamiką zmian składu podmiotów przetwarzających. W opcji 2, klauzuli 7.7, pkt A znajdujemy zapis: "Podmiot przetwarzający ma ogólną zgodę administratora na korzystanie z usług podmiotów podprzetwarzających wpisanych do uzgodnionego wykazu.", a w załączniku nr 4 znajduje się zapis: "Niniejszy załącznik należy wypełnić w razie udzielenia szczegółowej zgody na korzystanie z usług podmiotów podprzetwarzających (klauzula 7.7 lit. a, opcja 1)."

Czy podmiot przetwarzający może zapewnić administratorowi jedynie ogólny dostęp do wykazu podprzetwarzających, który może być okresowo aktualizowany, bez wskazywania każdego nowego podmiotu przetwarzającego?

Czy wybór opcji 2 dla podmiotu przetwarzającego wiąże się z koniecznością posiadania "uzgodnionego wykazu" podprzetwarzających, ale nie musi to być to forma załącznika nr 4?

Czy przy przyjęciu następujących środków organizacyjnych:

- **umieszczenie w umowie powierzenia zapisu, że aktualny wykaz podmiotów podprzetwarzających podmiotu przetwarzającego znajduje się na jego stronie www,**
- **stała aktualizacja tego wykazu,**
- **zachowanie archiwalnych wersji strony www w celu zapewnienia rozliczalności,**
- **oraz poinformowanie administratorów na piśmie (wersja elektroniczna - automatyczny e-mail) o wszelkich zamierzonych zmianach w tym wykazie polegających na dodaniu lub zastąpieniu podmiotów podprzetwarzających z wyprzedzeniem co najmniej 7 dni, będą wystarczające dla zachowania zgodności z przepisami?**

Pomocne informacje w rozstrzygnięciu przedstawionych w pytaniu wątpliwości można znaleźć w Wytycznych EROD nr 7/2020 w sprawie pojęcia administratora oraz podmiotu przetwarzającego. Tekst ostatecznej wersji wytycznych w języku angielskim dostępny jest pod adresem: Guidelines 07/2020 on the concepts of controller and processor in the GDPR | European Data Protection Board (europa.eu), w chwili obecnej nie ma oficjalnego tłumaczenia na język polski.

Jak wskazała EROD w ww. wytycznych, umowa powierzenia musi określać:

- że podmiot przetwarzający nie może zatrudnić innego podmiotu przetwarzającego bez uprzedniej pisemnej zgody administratora oraz
- czy upoważnienie to będzie miało charakter szczególny czy ogólny.

W przypadku ogólnego upoważnienia podmiot przetwarzający musi poinformować administratora o każdej zmianie podmiotów podprzetwarzających na podstawie pisemnej zgody i umożliwić administratorowi zgłoszenie sprzeciwu.

Zaleca się, aby w umowie określono procedurę w tym zakresie. Należy zauważyć, że obowiązek podmiotu przetwarzającego polegający na informowaniu administratora o każdej zmianie podprzetwarzającego oznacza, że podmiot przetwarzający aktywnie wskazuje lub sygnalizuje takie zmiany administratorowi. Ponadto EROD w powołanych Wytycznych 7/2020 wskazała, że nie wystarczy, aby podmiot przetwarzający jedynie zapewnił administratorowi ogólny dostęp do wykazu podprzetwarzających, który może być okresowo aktualizowany, bez wskazywania każdego nowego podmiotu przetwarzającego. Innymi słowy, podmiot przetwarzający musi aktywnie informować administratora o wszelkich zmianach w wykazie (tj. o każdym nowym planowanym podpowierzeniu, pkt 128 Wytycznych 7/2020).

A zatem sposób, w jaki podmiot przetwarzający powiadomi administratora o dalszym podpowierzeniu powinien zapewniać mu realny wpływ na to, kto będzie „innym podmiotem przetwarzającym" i umożliwić administratorowi wyrażenie sprzeciwu zanim nastąpi podpowierzenie (art. 28 ust. 2 RODO). Procedura w tym zakresie powinna być uzgodniona przez strony umowy powierzenia i być objęta jej postanowieniami.

Data wytworzenia informacji: 06.09.2021 r.

Czy ze związkiem powiatowo-gminnym należy zawrzeć umowę powierzenia?

Powiat i gminy powiatu utworzyły związek celowy powiatowo–gminny, który realizuje określone przepisami Prawa oświatowego zadanie gminy polegające na zorganizowaniu bezpłatnego dowożenia dzieci objętych wczesnym wspomaganiem rozwoju i ich opiekunów z miejsca zamieszkania dziecka do szkoły lub placówki.

Moje wątpliwości jako inspektora ochrony danych dotyczą tego, czy w ww. przypadku będzie dochodziło do powierzenia przetwarzania danych osobowych uczniów między gminą i związkiem, czy raczej będzie tu miało miejsce udostępnienie danych osobowych.

W celu ustalenia, czy w danej sytuacji mamy do czynienia z odrębnym administratorem, czy jednak istnieje konieczność zawarcia umowy powierzenia, należy przede wszystkim dokonać analizy procesu przetwarzania z uwzględnieniem zadań określonych podmiotów wynikających m.in. z przepisów prawa czy z zawartej pomiędzy nimi umowy. Ocena ról w konkretnym przypadku będzie zależała bowiem od tego, o jakie dane osobowe oraz o jakie zadania chodzi. W wielu sytuacjach, gdy następuje przekazanie zadania innemu podmiotowi, który realizuje je (także w zakresie przetwarzania danych) w sposób niezależny, stosując się w tym zakresie do szczegółowych przepisów, uzasadnione jest uznanie tego podmiotu za odrębnego administratora. Powierzenie przetwarzania powinno mieć natomiast miejsce wówczas, jeśli zewnętrzny podmiot przetwarza dane w imieniu administratora i na jego polecenie, czyli w celach i w sposób przez niego określony.

W przypadku wskazanym w pytaniu należy zatem w pierwszej kolejności odwołać się do przepisów prawa określających zadania podmiotów lub organów publicznych, dla których realizacji niezbędne jest przetwarzanie danych osobowych.

Zgodnie z art. 127 ust. 7 Prawa oświatowego gmina może zorganizować bezpłatne dowożenie dziecka objętego wczesnym wspomaganiem rozwoju i jego opiekuna z miejsca zamieszkania dziecka do szkoły lub placówki, w której to wspomaganie jest prowadzone, a w razie potrzeby także bezpłatną opiekę nad dzieckiem w czasie dowożenia.

Art. 72a ust. 1 ustawy o samorządzie powiatowym stanowi natomiast, że w celu wspólnego wykonywania zadań publicznych, w tym wydawania decyzji w indywidualnych sprawach z zakresu administracji publicznej, powiaty mogą tworzyć związki z gminami, tworząc związek powiatowo-gminny. Zgodnie z ustępem 2 tego przepisu do związku powiatowo-gminnego stosuje się odpowiednio przepisy dotyczące związku powiatów, w tym przepis art. 65 ust. 3 ustawy o samorządzie powiatowym, zgodnie z którym prawa i obowiązki powiatów uczestniczących w związku, związane z wykonywaniem zadań przekazanych związkowi, przechodzą na związek z dniem ogłoszenia statutu związku.

Stosując zatem odpowiednio powyższy przepis można wskazać, że **prawa i obowiązki powiatów i gmin uczestniczących w związku powiatowo-gminnym, związane z wykonywaniem zadań przekazanych temu związkowi, przechodzą na związek**. Biorąc powyższe pod uwagę można zasadnie przyjąć, że w sytuacji utworzenia związku powiatowo-gminnego w celu wspólnego wykonywania określonego zadania publicznego, to ten związek staje się administratorem danych osobowych przetwarzanych w związku z **wykonywaniem przekazanych mu zadań** i wykonuje te zadania we własnym imieniu.

Wskazówki dotyczące określania statusu podmiotów w jednostkach samorządu terytorialnego znaleźć można w odpowiedziach na pytania zamieszczonych na stronie internetowej UODO

w zakładce Inspektor Ochrony Danych/Zadania, m.in. w odpowiedzi na pytanie: KTO JEST ADMINISTRATOREM DANYCH PRZETWARZANYCH W CELU WYDANIA KARTY SENIORA?

Data wytworzenia informacji: 08.10.2021 r.

Czy przedsiębiorstwo wodociągowe może udostępnić gminie dane na temat ilości zużytej wody?

Czy burmistrz, wójt, prezydent miasta w ramach kontroli, o której mowa w art. 6 ust. 5a ustawy o utrzymaniu czystości i porządku w gminach, dotyczącej przestrzegania przez mieszkańców obowiązków związanych z pozbywaniem się nieczystości ciekłych, może pozyskiwać od przedsiębiorstwa wodociągowego dane osobowe dotyczące zużycia wody? Czy nowe przepisy zmienią sytuację w tym zakresie?

Ze względu na określoną w art. 7 Konstytucji RP zasadę działania organów publicznych na podstawie i w granicach prawa, organ publiczny nie może domniemywać swoich kompetencji, jeśli nie wynikają one wprost z przepisu prawa. Pozyskanie danych osobowych przez podmiot realizujący zadania publiczne powinno zatem wynikać z przepisów prawa odnoszących się do zadań tego podmiotu.

Zgodnie z art. 5 ust. 6 ustawy z dnia 13 września 1996 r. o utrzymaniu czystości i porządku w gminach, nadzór nad wykonywaniem obowiązków nałożonych na właścicieli nieruchomości, tj. pozbywaniem się zebranych na terenie nieruchomości odpadów komunalnych oraz nieczystości ciekłych w sposób zgodny z przepisami ustawy i przepisami odrębnymi, w tym obowiązków określonych w regulaminie utrzymania czystości i porządku na terenie gminy, został powierzony wójtowi, burmistrzowi lub prezydentowi miasta. Wójt, burmistrz lub prezydent miasta kontroluje posiadanie umów i dowodów uiszczania opłat za usługi dotyczące pozbywania się zebranych na terenie nieruchomości odpadów komunalnych oraz nieczystości ciekłych lub inny sposób udokumentowania wykonania tych obowiązków (art. 6 ust. 5a).

Z przepisów powołanej ustawy wynika wprost zasada dokumentowania w formie umowy korzystania z usług wykonywanych przez gminną jednostkę organizacyjną lub przedsiębiorcę posiadającego zezwolenie na prowadzenie działalności w zakresie opróżniania zbiorników bezodpływowych i transportu nieczystości ciekłych lub gminną jednostkę organizacyjną lub przedsiębiorcę odbierającego odpady komunalne od właścicieli nieruchomości, wpisanego do rejestru działalności regulowanej – przez okazanie takich umów i dowodów uiszczania opłat za te usługi (art. 6 ust. 1).

Rada gminy może określić, w drodze uchwały, w zależności od lokalnych warunków, inne sposoby udokumentowania wykonania tych obowiązków (art. 6 ust. 1a ustawy). W tej sytuacji możliwość udokumentowania wykonania obowiązków określonych w art. 5 ust. 1 pkt 3b ustawy, w inny niż

określony przez ustawodawcę sposób, może nastąpić w sytuacji podjęcia przez radę gminy uchwały wydanej na podstawie art. 6 ust. 1a ustawy.

W przypadku właścicieli nieruchomości, którzy nie zawarli umów, o których mowa w art. 6 ust. 1 ustawy, gmina jest obowiązana zorganizować odbieranie odpadów komunalnych oraz opróżnianie zbiorników bezodpływowych (art. 6 ust. 6 ustawy). Na potrzeby realizacji tego obowiązku wójt, burmistrz lub prezydent miasta zobowiązany jest do wydania decyzji ustalającej: obowiązek uiszczania opłat za odbieranie odpadów komunalnych lub opróżnianie zbiorników bezodpływowych; wysokość opłat wyliczonych z zastosowaniem określonych stawek, terminy uiszczania opłat, sposób i terminy udostępniania pojemników lub zbiorników bezodpływowych, w celu ich opróżnienia, lub worków w celu ich odebrania (art. 6 ust. 7 ustawy). Wówczas do opłat stosuje się przepisy działu III ustawy z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa, z tym że uprawnienia organów podatkowych przysługują wójtowi, burmistrzowi lub prezydentowi miasta (art. 6 ust. 12 ustawy o utrzymaniu czystości i porządku w gminach). Jak wskazano w orzecznictwie, obowiązek wydania przez wójta decyzji powstaje nie tylko w odniesieniu do właścicieli nieruchomości, którzy nie zawarli umów korzystania z usług wykonywanych przez zakład będący gminną jednostką organizacyjną lub przedsiębiorcę posiadającego zezwolenie na prowadzenie działalności w zakresie opróżniania zbiorników bezodpływowych i transportu nieczystości ciekłych, ale także w przypadku właścicieli nieruchomości, którzy wprawdzie zawarli takie umowy, ale nie udokumentowali faktu ich wykonywania dowodami płacenia za usługi w zakresie opróżniania takich zbiorników i transportu takich nieczystości (wyrok WSA w Kielcach z 10 listopada 2010 r., sygn. akt II SA/Ke 628/10).

Wszystkie powyższe przepisy wskazują, w jaki sposób wójt, burmistrz lub prezydent mają realizować swoje zadanie w tym zakresie. Nie przewidują one możliwości pozyskiwania danych osobowych z innych źródeł niż od właściciela nieruchomości.

Warto nadmienić, że nowelizacja ustawy o utrzymaniu czystości i porządku w gminach (Dz. U. z 2021 r. poz. 1648; https://www.sejm.gov.pl) dokonała zmiany dotychczasowego brzmienia art. 6 ust. 5a. Zmiana dotyczy sposobu dokonywanej kontroli w odniesieniu do umów dotyczących obioru odpadów komunalnych. Wójt, burmistrz lub prezydent miasta kontroluje zgodność postanowień umów dotyczących obioru odpadów komunalnych z wymaganiami określonymi w regulaminie oraz ze sposobem określonym w przepisach wydanych na podstawie art. 4a ust. 1 ustawy. Ponadto nowa regulacja przewidziała dodanie nowych ust. 5b i 5c do tego artykułu, w których sformułowano uprawnienia wójta, burmistrza lub prezydenta miasta do wezwania stron umowy do usunięcia uchybień, w terminie określonym w tym wezwaniu, w przypadku gdy postanowienia umowy dotyczącej obioru odpadów komunalnych nie spełniają wskazanych w ustawie wymagań. Po bezskutecznym upływie terminu do usunięcia uchybień umowa wygasa, a wójt, burmistrz lub prezydent miasta wydaje decyzję, o której mowa w art. 6 ust. 7 ustawy.

Zmieniony art. 6 ust. 5a oraz nowo dodane ust. 5b i ust. 5c wchodzą w życie 1 stycznia 2022 r.

A zatem również i nowe przepisy nie dają wójtowi, burmistrzowi oraz prezydentowi miasta w związku z dokonywaną kontrolą przestrzegania przez mieszkańców obowiązków związanych z pozbywaniem się nieczystości ciekłych, o której mowa w art. 6 ust. 5a ustawy o utrzymaniu czystości i porządku w gminach, podstawy do pozyskiwania od przedsiębiorstwa wodociągowego danych osobowych w zakresie ilości wody zużytej przez właściciela danej nieruchomości.

Data wytworzenia informacji: 08.10.2021 r.

Jaki jest status rodziny sprawującej pieczę zastępczą?

W nawiązaniu do stanowiska Prezesa UODO w zakresie „Monitoringu wizyjnego w mieszkaniu rodziny sprawującej pieczę zastępczą" (https://uodo.gov.pl/pl/138/1544 **– tekst w ramce poniżej) zwracam się z prośbą o zajęcie stanowiska odnośnie do statusu rodziny sprawującej pieczę zastępczą względem danych osobowych dzieci umieszczonych w pieczy. W przywołanej interpretacji wskazali Państwo, iż „Osoby sprawujące pieczę zastępczą nie są wyłączone ze stosowania RODO. W ich przypadku nie można zastosować wyłączenia, które dotyczy sytuacji, gdy dane osobowe przetwarza osoba fizyczna w ramach czynności o osobistym lub domowym charakterze (art. 2 ust. 2 lit. c RODO)."**

Mam co do tego wątpliwości. Czy w zależności od rodzaju pieczy, nie będziemy mieli do czynienia raz z administratorem, raz z osobą przetwarzającą dane w ramach czynności o charakterze osobistym? Bezsprzecznie w przypadku pieczy instytucjonalnej (placówki opiekuńczo-wychowawcze) będziemy mieli do czynienia z administratorem. W mojej ocenie sytuacja wygląda jednak inaczej w przypadku rodzinnej pieczy zastępczej, na którą składają się rodziny zastępcze zawodowe i prowadzący rodzinny dom dziecka, którzy pobierają wynagrodzenie za świadczone usługi, a inaczej w przypadku rodzin zastępczych niezawodowych i rodzin zastępczych spokrewnionych, które nie pobierają wynagrodzenia. Czy należy przyjąć, że dla oceny, czy dana rodzina posiada status administratora w rozumieniu RODO, decydujący będzie fakt pobierania wynagrodzenia za sprawowanie pieczy? A zatem, czy rodziny spokrewnione lub niezawodowe niepobierające wynagrodzenia będą korzystały z wyłączenia, o którym mowa w art. 2 ust. 2 lit. c RODO?

Informacja ze strony archiwalnej UODO

Monitoring wizyjny w mieszkaniu rodziny sprawującej pieczę zastępczą

Procedury związane z wykorzystaniem monitoringu wizyjnego przez osoby sprawujące pieczę zastępczą tj. opiekę nad dziećmi w przypadku niemożności zapewnienia jej przez rodziców, nie są jednolite i budzą

wiele wątpliwości. Dlatego Prezes Urzędu Ochrony Danych Osobowych skierował wystąpienie do Ministra Rodziny, Pracy i Polityki Społecznej ws. uregulowania tej kwestii.

Prezes UODO we współpracy z Ministerstwem Rodziny, Pracy i Polityki Społecznej zgromadził materiał ze wszystkich województw dotyczący procedur związanych z monitoringiem wizyjnym stosowanym w placówkach pieczy zastępczej i dokonał jego analizy w kontekście legalności stosowania takich praktyk.

Przetwarzanie danych osobowych z wykorzystywaniem monitoringu wizyjnego, zdaniem UODO, powinno odbywać się z poszanowaniem zasad wynikających z RODO. Osoby sprawujące pieczę zastępczą nie są wyłączone ze stosowania tego rozporządzenia.

W ich wypadku nie można zastosować wyłączenia, które dotyczy sytuacji gdy dane osobowe przetwarza osoba fizyczna w ramach czynności o osobistym lub domowym charakterze (art. 2 ust. 2 lit. c RODO).

Zatem osoby sprawujące pieczę zastępczą, stosując monitoring wizyjny, nie mogą powoływać się na powyższe wyłączenie.

Dodatkowo są one administratorami i, wykorzystując monitoring wizyjny, powinni dysponować przesłanką do przetwarzania danych osobowych , czyli wskazać z jakiego powodu przetwarzają dane. Powinni także posiadać odpowiednie procedury, które zapewniłyby zgodność przetwarzania takich danych z przepisami o ochronie danych osobowych.

Ponadto należy zwrócić uwagę, że wykorzystywanie monitoringu wizyjnego wewnątrz budynku, w którym sprawowana jest piecza np. w mieszkaniu rodziny sprawującej pieczę, może stanowić bezprawną ingerencję w życie dziecka, o której mowa w art. 4 pkt 7 ustawy o wspieraniu rodziny i systemie pieczy zastępczej.

Co więcej, preambuła wspomnianej ustawy stanowi, że uchwalono ją dla dobra dzieci, które potrzebują szczególnej ochrony i pomocy ze strony dorosłych (…) dla zapewnienia **ochrony przysługujących im praw i wolności**. Jednym z praw, jakie powinno być zagwarantowane dzieciom objętym przepisami tej ustawy, jest to, które gwarantuje jasne i przejrzyste zasady przetwarzania ich danych osobowych w domach opieki zastępczej.

Organ nadzorczy dostrzega potrzebę stworzenia przepisów prawa, które określiłyby jednolite zasady wykorzystywania monitoringu wizyjnego w pieczy zastępczej, w tym m.in.: obszary w placówkach, które mogłyby zostać objęte monitoringiem, cel wykorzystywania monitoringu, okres przechowywania zgromadzonego z nagrań materiału.

Według UODO konkretne, dedykowane pieczy zastępczej przepisy prawa dotyczące monitoringu wizyjnego pozwoliłyby rozwiać wątpliwości podmiotów sprawujących tego typu formę pomocy rodzinie co do legalności i zakresu możliwości stosowania tego narzędzia.

Na problem związany ze stosowaniem monitoringu wizyjnego w pieczy zastępczej zwrócił uwagę Rzecznik Praw Dziecka. Zauważył on, że wykorzystywanie monitoringu wizyjnego w mieszkaniu niezawodowej rodziny zastępczej może stanowić bezprawną ingerencję w życie dziecka, o której mowa w art. 4 pkt 7 ustawy o wspieraniu rodziny i systemie pieczy zastępczej.

Informacje nt. dopuszczalnych form monitoringu wizyjnego są dostępne w opracowaniu pt. Wskazówki Prezesa Urzędu Ochrony Danych Osobowych dotyczące wykorzystywania monitoringu wizyjnego:

Stan prawny na: 15.06.20218

Nowe rozwiązania prawne dotyczące stosowania monitoringu wizyjnego wzbudziły u administratorów wiele wątpliwości interpretacyjnych i obawy o możliwość spełnienia nowych obowiązków w tak krótkim okresie. Dostrzegając te problemy, Prezes Urzędu Ochrony Danych Osobowych przygotował specjalne wskazówki i wyznacza administratorom okres przejściowy na dostosowanie się do nowych regulacji – koniec września 2018 r.

Od 25 maja 2018 r. stosowanie monitoringu wizyjnego podlega przepisom ogólnego rozporządzenia o ochronie danych (RODO) oraz uregulowaniom krajowym, które odnoszą się m.in. do: pracodawców, placówek oświatowych oraz jednostek samorządu terytorialnego. Te ostatnie zostały wprowadzone przepisami nowej ustawy o ochronie danych osobowych, w której nie przewidziano szczególnych okresów przejściowych. Prezes Urzędu Ochrony Danych Osobowych podkreśla, że brak okresów przejściowych na dostosowanie się do nowych regulacji nie zwalnia administratorów z realizacji tego obowiązku. Wskazuje jednocześnie, że obecnie funkcjonujące systemy monitorowania powinny zostać poddane aktualizacji i dostosowane do wymogów określonych nowymi przepisami do końca września 2018 r.

Biorąc zaś pod uwagę fakt, że nowe regulacje zrodziły u administratorów wiele wątpliwości interpretacyjnych, w celu ich rozwiania Prezes Urzędu Ochrony Danych Osobowych przygotował Wskazówki dotyczące stosowania monitoringu wizyjnego. Dokument ten w sposób kompleksowy omawia dopuszczalne cele stosowania monitoringu wizyjnego, prawa osób obserwowanych, obowiązki administratorów. Zawiera też odpowiedzi na często zadawane pytania.

Zważywszy na zróżnicowany charakter stosowanych obecnie systemów monitoringu wizyjnego, Prezes Urzędu Ochrony Danych Osobowych zachęca do udziału w konsultacjach niniejszego dokumentu. Mają one na celu jak najdokładniejsze poznanie potrzeb i opinii różnych środowisk w tej sprawie. Wszystkie zainteresowane osoby, w szczególności zrzeszenia branżowe i organizacje pozarządowe, mogą przedstawiać swoje stanowiska i uwagi. Wynikiem konsultacji będzie publikacja ostatecznej wersji wskazówek, która będzie operatorom monitoringu wizyjnego pomocna w dostosowaniu do obowiązujących przepisów. Uwagi należy przesyłać do 15 lipca 2018 r. na adres: desiwm@uodo.gov.pl. W tytule wiadomości prosimy wskazać hasło „Konsultacje Monitoring”.

Udział w konsultacjach jest dobrowolny. Podane dane kontaktowe (np. imię i nazwisko lub pseudonim, adres e-mail, funkcja pełniona w reprezentowanej organizacji) będą wykorzystane celem przygotowania raportu z konsultacji społecznych. Dane te mogą zostać udostępnione zgodnie z ustawą o dostępie do informacji publicznej, która przewiduje ograniczenie ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy (art. 5 ustawy) - dane osób, które nie wyrażą poniższej zgody, zostaną zanonimizowane.

Jeżeli zgadzają się Państwo na upublicznienie swoich danych kontaktowych, prosimy, by do przesyłanych uwag dołączyć poniższe oświadczenie zgody:

„Wyrażam zgodę na wykorzystanie moich danych osobowych przez Urząd Ochrony Danych Osobowych 00-193 Warszawa ul. Stawki 2 w celu publikacji na stronie internetowej Urzędu danych autorów uwag zgłoszonych w ramach konsultacji społecznych dokumentu Wskazówki dot. stosowania monitoringu wizyjnego."

Stosownie do treści art. 2 ust. 2 lit. c RODO, nie znajduje ono zastosowania m.in. w sytuacji przetwarzania danych osobowych przez osobę fizyczną, w ramach czynności o **czysto** osobistym lub domowym charakterze.

Tak jak miało to miejsce w przepisach art. 3 ust. 2 tiret drugie dyrektywy 95/46[17], a także w art. 3a ust. 1 pkt 1 ustawy o ochronie danych osobowych z 1997 r.[18], wyłączenie to jest zakreślone w sposób wymagający jego ścisłego i wąskiego traktowania. Trybunał Sprawiedliwości UE w wyroku z 11 grudnia 2014 r., C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů, odnoszącym się jeszcze do dyrektywy 95/46/WE podkreślił, że ochrona prawa podstawowego do prywatności, zagwarantowanego przez art. 7 Karty Praw Podstawowych Unii Europejskiej wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia były stosowane jedynie wtedy, gdy jest to absolutnie konieczne. Zwrócił uwagę, że z zakresu stosowania dyrektywy 95/46 wyłączono przetwarzanie danych wykonywane w trakcie czynności nie tylko o osobistym lub domowym charakterze, lecz o 'czysto' osobistym lub domowym charakterze. W związku z powyższym przetwarzanie danych osobowych jest objęte odstępstwem przewidzianym w art. 3 ust. 2 tiret drugie dyrektywy 95/46 jedynie w wypadku, gdy jest ono wykonywane w ramach sfery o czysto osobistym lub domowym charakterze, należącej do osoby, która dokonuje tego przetwarzania.

W doktrynie wskazuje się, że „czynności o <<czysto osobistym lub domowym charakterze>> są przeciwieństwem czynności o charakterze zawodowym lub aktywności gospodarczej (działalność profesjonalna). Jednak osobistego lub domowego charakteru nie wykazują również formy aktywności, które nie mają wymiaru zawodowego, a przybierają wymiar społeczny; nie mają charakteru działalności gospodarczej, a działalności *non profit*; podobnie mogą one nie mieć charakteru profesjonalnego, a amatorski (np. aktywność osoby fizycznej w stowarzyszeniu, fundacji itp.). W tym zakresie powoływanie się na omawiane wyłączenie nie jest zasadne"[19].

[17] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, art. 3 ust. 2 tiret drugie: Niniejsza dyrektywa nie ma zastosowania do przetwarzania danych osobowych (…) przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze.

[18] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, art. 3a ust. 1 pkt 1: Ustawy nie stosuje się do osób fizycznych, które przetwarzają dane wyłącznie w celach osobistych lub domowych (…).

[19] P. Fajgielski [w:] Komentarz do rozporządzenia nr 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy

Rodzina zastępcza w ramach sprawowanej opieki nad dzieckiem realizuje zadania w ramach systemu pieczy zastępczej, określone w ustawie z dnia 9 czerwca 2011 r. o wspieraniu rodziny i systemie pieczy zastępczej. Zarówno w przypadku rodzin zastępczych spokrewnionych, niezawodowych, czy zawodowych ich działalność wiąże się ze szczególnymi uregulowaniami dotyczącymi zasad pełnienia rodzinnej pieczy zastępczej, obejmującymi m.in. określone wymagania w stosunku do osób tworzących rodzinę zastępczą (art. 42), zakres opieki i zadania rodzin zastępczych (art. 40), zasady kontroli tych podmiotów (art. 38b), przekazywanie informacji i dokumentacji dotyczącej dziecka (art. 38a i art. 72).

Z analizy przepisów powyższej ustawy wynika zatem, że rodziny zastępcze (w tym również spokrewnione i niezawodowe), sprawując pieczę zastępczą i przetwarzając w tym celu dane osobowe dzieci i ich rodzin, realizują zadania w zakresie systemu pieczy zastępczej przewidziane w ww. ustawie. Dlatego nie można uznać, że przetwarzania tych danych osobowych dokonują w ramach czynności o czysto osobistym lub domowym charakterze. W takiej sytuacji bez znaczenia jest fakt, że niektóre z tych rodzin nie otrzymują w związku z realizacją tych zadań wynagrodzenia.

Data wytworzenia informacji: 08.10.2021 r.

Jaka jest podstawa przetwarzania przez szkołę danych uczniów w celu wydania mLegitymacji?

Patrząc na aktualne uregulowania, wydanie mLegitymacji (tj. elektronicznej wersji tradycyjnej legitymacji szkolnej wyświetlanej na ekranie telefonu) jest fakultatywne. Taka wersja legitymacji ma być jedynie ułatwieniem dla uczniów, bo i tak posiadają oni papierową wersję legitymacji. Nasza placówka zamierza umożliwić uczniom posiadanie takiej mobilnej legitymacji. Jaką podstawę prawną z art. 6 ust. 1 RODO (lit. a czy lit. c, czyli zgoda czy obowiązek prawny) szkoła powinna wskazywać w klauzuli informacyjnej dotyczącej usługi mLegitymacja?

W przypadku podmiotów publicznych oraz podmiotów, których działalność uregulowana została przepisami prawa co do zasady podstawę prawną przetwarzania (w tym udostępniania i pozyskiwania) danych osobowych powinno stanowić wykonanie obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO) lub wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO). W sytuacji, gdy przetwarzane będą szczególne kategorie danych, przesłanką dla ich przetwarzania zwykle będzie art. 9 ust. 2 lit. g RODO,tj. przetwarzanie jest niezbędne ze

95/46/WE (ogólne rozporządzenie o ochronie danych) [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, art. 2.

względów związanych z ważnym interesem publicznym na podstawie prawa Unii lub prawa państwa członkowskiego. Powołanie się na te przesłanki wymaga dodatkowo istnienia przepisów prawa wskazujących na zadania podmiotu publicznego, dla których realizacji niezbędne jest przetwarzanie danych osobowych.

Warunki i tryb wydawania mLegitymacji szkolnej uregulowane są w rozporządzeniu Ministra Edukacji Narodowej z 27sierpnia 2019 r. w sprawie świadectw, dyplomów państwowych i innych druków, wydanym na podstawie art. 11 ust. 2 ustawy z dnia 7 września 1991 r. o systemie oświaty.

Zgodnie z § 3 ust. 1 ww. rozporządzenia świadectwa szkolne promocyjne, świadectwa ukończenia szkoły, indeksy, **legitymacje szkolne i e-legitymacje szkolne wydają szkoły** publiczne i niepubliczne: szkoły podstawowe, szkoły ponadpodstawowe i placówki kształcenia ustawicznego.

W ust. 2 tego przepisu wskazano, że **szkoły**, wydając legitymację szkolną albo e-legitymację szkolną, **mogą wydać dodatkowo mLegitymację szkolną**, stanowiącą dokument elektroniczny przechowywany i prezentowany przy użyciu oprogramowania przeznaczonego dla urządzeń mobilnych, o którym mowa w art. 19e ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne.

Zgodnie z § 3 ust. 3 ww. rozporządzenia **mLegitymacja szkolna jest wydawana na wniosek pełnoletniego ucznia lub rodziców niepełnoletniego ucznia.**

W punkcie V załącznika nr 4 do powołanego rozporządzenia wskazano m.in. zakres informacji, jakie są widoczne w wizualizacji mLegitymacji szkolnej na ekranie urządzenia mobilnego. Wśród tych informacji są w szczególności następujące dane osobowe ucznia: numer legitymacji, który **w przypadku ucznia niepełnosprawnego jest uzupełniony dodatkowo oznaczeniem "-N",** kolorowe zdjęcie, imię lub imiona, nazwisko, data urodzenia, nr PESEL, wiek, nazwa i adres szkoły.

Zatem w treści mLegitymacji przetwarzane mogą być **zarówno dane osobowe zwykłe ucznia, jak i szczególne kategorie danych** (dane dotyczące zdrowia).

Mając na uwadze przytoczone powyżej przepisy prawa za właściwą przesłankę przetwarzania danych zwykłych w celu wydawania przez szkołę mLegitymacji uznać należy **art. 6 ust. 1 lit. e RODO w związku z przepisami ustawy o systemie oświaty oraz ww. rozporządzenia**. Zgodnie z tą przesłanką przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Przesłankę tę wskazuje się co do zasady w przypadkach, gdy ustawodawca przewidział możliwość, a nie obowiązek realizacji zadania przewidzianego w przepisie prawa.

Natomiast w przypadku przetwarzania szczególnej kategorii danych osobowych za właściwą przesłankę należy uznać tę wskazaną w **art. 9 ust. 2 lit. g RODO** (tj. przetwarzanie jest niezbędne

ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą) **w połączeniu z właściwymi przepisami ustawy o systemie oświaty oraz ww. rozporządzenia**. Przetwarzanie danych osobowych przez szkołę dla celów wydania mLegitymacji należy uznać za niezbędne dla wykonania obowiązków nałożonych na ten podmiot w ww. przepisach.

Jednocześnie należy zauważyć, że jeżeli podstawą prawną przetwarzania danych osobowych jest określony przepis prawa w związku z art. 6 ust. 1 lit. c lub art. 6 ust. 1 lit. e RODO, przesłanka zgody nie znajdzie zastosowania. W piśmiennictwie wskazuje się, że „w przypadku przesłanki zgody, w celu niezaburzenia elementu dobrowolności, nie jest co do zasady dopuszczalne niejako dodatkowe jej wykorzystywanie do legalizacji przetwarzania, w sytuacji gdy administrator dysponuje właśnie inną przesłanką przetwarzania danych w tym samym celu i zakresie, np. związaną z wykonywaniem umowy czy realizacją obowiązku wynikającego z przepisu prawa” (Chomiczewski Witold, Lubasz Dominik [w:] Bielak-Jomaa Edyta (red.), Lubasz Dominik (red.), RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Lex online, art. 6).

Data wytworzenia informacji: 03.11.2021 r.

Jakie dokumenty i przez jaki okres powinny być publikowane w BIP?

W związku z obowiązkiem udostępniania informacji publicznej prosimy o udzielenie wskazówek, czy na stronie internetowej urzędu powinniśmy zamieszczać: wnioski osób o dostęp do informacji publicznej i odpowiedzi na nie, skargi w rozumieniu działu VIII k.p.a. i odpowiedzi na nie, a także petycje. Czy dane osób fizycznych je składających należy zanonimizować? Jak długo informacje takie powinny być publikowane?

I. W odniesieniu do wątpliwości, **czy wnioski o udzielenie informacji publicznej składane w trybie ustawy o dostępie do informacji publicznej (dalej: u.d.i.p.) wraz z udzieloną odpowiedzią muszą być umieszczone na stronie urzędu**, wskazać należy, że podmiot zobowiązany do udostępnienia informacji publicznej, rozstrzygając o sposobie udostępnienia określonego zakresu danych w BIP, w pierwszej kolejności powinien ocenić, czy określone informacje mieszczą się w zakresie pojęcia informacji publicznej.

   Dokonując oceny, czy określone informacje (np. wnioski o dostęp do informacji publicznej) mieszczą się w zakresie pojęcia informacji publicznej warto zapoznać się z orzecznictwem sądów administracyjnych, zwłaszcza zaś z wyrokami zawierającymi rozstrzygnięcia dotyczące tego, czy dokument prywatny (np. pismo strony wnoszone w sprawie administracyjnej) jest dokumentem

urzędowym. Przykładowo w orzeczeniu I OSK 814/16 z dnia 26 stycznia 2018 r. NSA stwierdził: „zgodzić się należy ze stanowiskiem, że przymiot informacji publicznej bez wątpienia posiadają dokumenty urzędowe organu (będące dowodem tego, co w nich urzędowo stwierdzono, zatwierdzono lub podano), wytworzone w ramach realizacji powierzonych mu zadań, a więc dokumenty powstałe w związku z prowadzeniem konkretnych spraw. Natomiast przymiotu informacji publicznej nie mają dokumenty prywatne, które podmiot kieruje do organu administracji publicznej."

Wobec tego w kontekście przepisów ustawy o dostępie do informacji publicznej inaczej należy traktować pismo strony postępowania (np. wniosek o dostęp do informacji publicznej), a inaczej treść dokumentu urzędowego, w rozumieniu art. 6 ust. 2 tej ustawy.

Jeśli administrator oceni, że określona informacja stanowi informację publiczną, wówczas **w następnym kroku powinien ocenić, czy prawo dostępu do takiej informacji nie podlega ograniczeniu, np. z uwagi na prywatność osoby fizycznej.** Zgodnie z art. 5 ust. 2 u.d.i.p. prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy jednak informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. A zatem przepisy ustawy o dostępie do informacji publicznej wskazują na sytuacje oraz kategorie informacji, które mogą bądź muszą być wyłączone z udostępnienia.

Odnosząc się natomiast do kwestii obowiązku publikacji określonych informacji wskazać należy, że jedną z form udostępnienia informacji publicznej jest ogłaszanie informacji publicznej, w tym dokumentów urzędowych, w Biuletynie Informacji Publicznej (BIP), o którym mowa w art. 8 ust. 1 u.d.i.p. Katalog informacji podlegających obowiązkowemu udostępnieniu w BIP wskazany został w art. 8 ust. 3 tej ustawy. Niemniej organy władzy publicznej, do których zaliczają się również organy gminy, mogą udostępniać w Biuletynie także inne informacje publiczne, jak np. zarządzenia burmistrza (art. 8 ust. 3 zdanie drugie).

Ponadto prawo do informacji publicznej wynika również z art. 11b ustawy o samorządzie gminnym, który przewiduje jawność działalności organów gminy. Ograniczenia tej jawności mogą wynikać wyłącznie z ustaw (ust. 1). Zgodnie z tym przepisem jawność działania organów gminy obejmuje w szczególności prawo obywateli do uzyskiwania informacji, wstępu na sesje rady gminy i posiedzenia jej komisji, a także dostępu do dokumentów wynikających z wykonywania zadań publicznych, w tym protokołów posiedzeń organów gminy i komisji rady gminy (ust. 2). Zasady dostępu do dokumentów i korzystania z nich określa statut gminy (ust. 3). Jeżeli zatem w statucie gminy przewidziano obowiązek zamieszczania określonych informacji

publicznych w BIP (np. zarządzeń burmistrza), to wtedy informacje te podlegają obligatoryjnemu zamieszczeniu na stronie BIP urzędu danej gminy.

Opublikowanie przez urząd określonych informacji powinno być zatem poprzedzone staranną oceną, czy i w jakim zakresie należy je udostępnić.

II. Odnosząc się natomiast do kwestii okresu publikacji danych w BIP wskazać należy, że przepisy ustawy o dostępie do informacji publicznej, a także przepisy rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej nie precyzują okresu udostępniania informacji w BIP, zarówno minimalnego, jak i maksymalnego. Brak określonych przepisami prawa okresów przetwarzania (udostępniania) informacji zawierających dane osobowe, nie oznacza, że informacje takie można przetwarzać bezterminowo.

Do takich informacji zastosowanie bowiem znajduje zasada ograniczonego przechowywania, wynikającą z art. 5 ust. 1 lit. e RODO. Administrator powinien w tym zakresie kierować się przepisami, z których wynika czas, przez jaki może przetwarzać dane osobowe, a w przypadkach, w których prawo nie reguluje okresu retencji danych, po przeprowadzeniu analiz, określić ten okres tak, aby przetwarzanie danych było zgodne z celami, w których je pozyskano. Stanowisko takie zaprezentowane zostało także w uzasadnieniu wyroku Wojewódzkiego Sądu Administracyjnego w Lublinie z dnia 1 marca 2016 r., sygn. akt II SA/Lu 876/15: „[z] art. 26 ust. 1 pkt 4 ustawy o ochronie danych osobowych wynika zasada ograniczenia czasowego udostępnienia danych osobowych w Biuletynie Informacji Publicznej. Zasada ta oznacza, że nawet jeśli określone dane odpowiadają celowi, dla którego są zbierane, to nie powinny być przetwarzane, w tym udostępniane innym podmiotom ad finitum. Czasowym wyznacznikiem powinno być natomiast osiągnięcie celu przetwarzania.” Podkreślić należy, iż ww. wyrok zachowuje aktualność także przy obecnie obowiązujących przepisach o ochronie danych osobowych.

Podobnie wypowiedział się WSA w Warszawie w wyroku z dnia 29 stycznia 2020 r. (sygn. akt II SA/Wa 1810/19), wskazując, że brak regulacji nie oznacza, że dane mogą być publikowane bezterminowo. W takiej sytuacji znajduje bowiem zastosowania art. 5 ust. 1 lit. e RODO, co w konsekwencji nakłada obowiązek dokonania samodzielnej oceny okresu niezbędnego do osiągnięcia celu przetwarzania oraz zakreślenia precyzyjnego terminu usunięcia danych osobowych z BIP.

W decyzji z 18 października 2019 r. Prezes UODO wskazał, iż w celu zapewnienia przetwarzania danych zgodnie z zasadą ograniczonego przechowywania, administrator powinien stworzyć procedury, z których będzie wynikał termin i sposób usuwania informacji zawierających dane osobowe oraz zasady dokonywania przeglądów przetwarzanych danych w celu weryfikacji, czy określone w ten sposób terminy usuwania danych osobowych są przestrzegane.

Innymi słowy, jeżeli w tym zakresie brak jest określonych przepisami terminów, wzorów postępowania, to administrator musi przyjąć konkretne rozwiązania, które potrafi uzasadnić. Wynika to z przyjętej w art. 5 ust. 2 RODO zasady rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie zasad dotyczących przetwarzania danych wymienionych w art. 5 ust. 1 RODO i musi być w stanie to wykazać. Zasada rozliczalności wymaga też, aby administratorzy wykazywali logikę, na której opierają swoje decyzje, i potrafili uzasadnić, dlaczego przyjęli określone rozwiązania.

Pomocne informacje dotyczące tego zagadnienia znaleźć można również w odpowiedziach na znajdujące się w zakładce IOD pytania: CZY TRZEBA PRECYZYJNIE OKREŚLAĆ OKRES PRZECHOWYWANIA DANYCH?, JAK DŁUGO POWINNY BYĆ UDOSTĘPNIANE W BIP OŚWIADCZENIA MAJĄTKOWE, NP. RADNEGO, WÓJTA?

III. Wskazane powyżej informacje mogą być pomocne również w rozstrzygnięciu wątpliwości dotyczących skarg i wniosków w rozumieniu działu VIII k.p.a. Warto przy tym nadmienić, że problemem zamieszczania na stronie podmiotowej BIP danych osobowych wnoszącego taką skargę zajął się m.in. Naczelny Sąd Administracyjny w wyroku z 14 marca 2013 r. (I OSK 620/12). NSA stwierdził w nim, że „jeżeli celem zamieszczenia informacji publicznej w BIP-ie jest transparentność działalności publicznej Rady Gminy, w tym treść podejmowanych przez nią uchwał, to cel ten zostaje spełniony także wówczas, gdy chroniąc sferę prywatności z informacji usunięte zostaną dane dot. osób prywatnych.”

IV. Jeśli natomiast chodzi o petycje, to przy określaniu okresu przechowywania zastosowanie znajdą powyższe wskazówki. Nieco inaczej sytuacja wygląda natomiast w zakresie publikacji petycji i danych osobowych osób je wnoszących.

Zgodnie bowiem z art. 4 ust. 3 ustawy o petycjach, **petycja może zawierać zgodę na ujawnienie na stronie internetowej podmiotu rozpatrującego petycję** lub urzędu go obsługującego **danych osobowych podmiotu wnoszącego petycję** lub podmiotu, o którym mowa w art. 5 ust. 1 tej ustawy.

Zgodnie z art. 8 ust. 1 ww. ustawy, na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego niezwłocznie zamieszcza się informację zawierającą odwzorowanie cyfrowe (skan) petycji, datę jej złożenia oraz - **w przypadku wyrażenia zgody**, o której mowa w art. 4 ust. 3 - imię i nazwisko albo nazwę podmiotu wnoszącego petycję lub podmiotu, w interesie którego petycja jest składana.

Z treści powyższych przepisów wynika, że rozpatrujący petycję ma obowiązek zamieszczenia na swojej stronie internetowej informacji zawierającej odwzorowanie cyfrowe petycji, przy czym jeśli składający petycje wyrazi zgodę na ujawnienie jego imienia i nazwiska lub nazwy podmiotu, wówczas publikowana informacja o petycji może zawierać również te dane. Jeśli natomiast

składający petycje nie udzieli takiej zgody, wówczas adresat petycji nie może ujawnić jego danych, nie może też żądać wyrażenia takiej zgody.

Ponadto wskazać należy, że podstawą prawną do ujawnienia danych osobowych osoby składającej petycję na stronie internetowej organu rozpatrującego będzie zgoda w rozumieniu przepisów o ochronie danych osobowych. Skoro tak, to należy mieć na uwadze wymagania dotyczące zgody wskazane w RODO (art. 4 pkt 11 oraz art. 7-8).

Więcej informacji na temat ww. przesłanki przetwarzania znaleźć można na stronie internetowej UODO, w tym m.in. w materiale Zgoda nie zawsze jest podstawą przetwarzania danych – **tekst w ramce poniżej.**

Informacja ze strony archiwalnej UODO

Zgoda nie zawsze jest podstawą przetwarzania danych

Zgoda może być podstawą przetwarzania danych tylko wtedy, gdy nie występują inne przesłanki legalizujące. Gdy jednak zgoda ma zastosowanie, to musi spełniać określone warunki, by rzeczywiście była podstawą przetwarzania.

Wiele osób jest przekonanych, że jeśli nie wyraziło zgody na przetwarzanie swoich danych osobowych, to nie można tego robić. W praktyce jednak zgoda może być podstawą do przetwarzania naszych danych, gdy nie występują inne przesłanki legalizujące, które są określone w art. 6 ust. 1 RODO.

Przepis ten, oprócz zgody, określa, że nasze dane mogą być przetwarzane, gdy jest to niezbędne do wykonania umowy, do wypełnienia obowiązku prawnego ciążącego na administratorze, do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej. Nasze dane mogą być przetwarzane także wtedy, gdy jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi albo administrator musi zrealizować cel wynikający z prawnie uzasadnionych interesów.

Dopiero gdy nie mają zastosowania powyższe przesłanki, to podstawą do przetwarzania danych osobowych może być zgoda. Należy jednak pamiętać, że niedopuszczalne jest odbieranie zgody na przetwarzanie naszych danych osobowych w przypadku istnienia innej przesłanki legalizacyjnej upoważniającej administratora do przetwarzania danych osobowych w tym samym zakresie i celu. Takie działanie wprowadza w błąd osobę, która udziela zgody. Jest bowiem przekonana, że to na tej podstawie przetwarzane są jej dane i gdy ja wycofa, to administrator zaprzestanie dalszego przetwarzania. Tymczasem administrator może mieć wręcz obowiązek przetwarzania naszych danych, gdy mają zastosowania przedstawione powyżej przesłanki. Pozyskiwanie zgody w tej sytuacji może więc prowadzić do naruszenia zasady przejrzystości i rzetelności, o których mowa w art. 5 ust. 1 lit a RODO.

Warunki wyrażenia zgody

Zgoda, by mogła być podstawą przetwarzania danych, musi spełniać odpowiednie wymagania.
W przeciwnym razie może zostać zakwestionowana jako podstawa do przetwarzania danych osobowych.

Pojęcie zgody osoby, której dotyczą dane, definiuje art. 4 pkt 11 RODO i oznacza „dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych".

Zgoda udzielona przed rozpoczęciem przetwarzania danych osobowych powinna być: wyrażona wprost, określać osobę, która zgody udziela oraz której dane osobowe mają być udostępnione. Osoby te muszą wiedzieć, komu udzielają zgody na przetwarzanie danych, jaki jest ich zakres. Powinny też wiedzieć, przez jaki okres i w jakim celu dane te będą przetwarzane.

Administrator ma obowiązek zadbać o to, by jego działania były zgodne z zasadami przetwarzania danych osobowych, zwłaszcza z art. 5 oraz art. 7 RODO. Powinien ocenić, jakie ryzyka dla praw osób, mogą wiązać się z przetwarzaniem ich danych osobowych w konkretnym celu. Musi również przygotować jasne i rzetelne klauzule informacyjne.

Wymuszenie zgody

Należy pamiętać, że nikt nie ma prawa wymuszać na nikim wyrażenia zgody. Taka zgoda jest nieważna. Warto pamiętać, że z wymuszeniem zgody spotykamy się, gdy klauzula o wyrażeniu zgody znajduje się pomiędzy wieloma innymi punktami umowy. Przykładowo, klauzula o zgodzie na otrzymywanie informacji handlowych nie może znaleźć się we wzorcu wniosku o udzielenie pożyczki pomiędzy innymi postanowieniami oraz formularzem określającym m.in. dane osobowe kredytobiorcy. W tak skonstruowanym dokumencie konsument nie ma możliwości odmowy wyrażenia zgody, ponieważ składa podpis pod całością wniosku, przez co jego zgoda nie jest swobodna i niezależna od innych oświadczeń woli (art. 4 ustawy o świadczeniu usług drogą elektroniczną).

Z wymuszeniem zgody mamy również do czynienia, gdy instytucja publiczna lub niepubliczna realizująca zadanie publiczne uzależnia jego realizację od zgody, pomimo że z przepisów wynika uprawnienie lub obowiązek przetwarzania danych dla tych celów. Przykładowo: podczas rejestracji samochodu w urzędzie, urząd ten nie może żądać od nas wyrażenia zgody i uzależnić od niej wydanie decyzji o rejestracji pojazdu, bo z przepisów wynika obowiązek przetwarzania danych dla tego celu.

Wycofanie zgody

W myśl art. 7 ust. 3 RODO zgoda jest odwoływalna i uprawnienie to przysługuje osobie, której dane dotyczą, w każdym czasie. Osoba ta ma więc prawo w dowolnym momencie wycofać zgodę. Przepis nakłada na administratora obowiązek poinformowania osoby o tym prawie, zanim wyrazi zgodę. Wycofanie zgody musi być tak samo łatwe jak jej wyrażenie. Dlatego jeżeli np. na stronie internetowej istniał mechanizm do wyrażenia zgody, to powinien być również podobny do jej wycofania. Rozwiązanie takie nie powinno być w żaden sposób ukryte. Podobnie gdy administrator odbierał zgodę drogą mailową czy telefoniczną, to w tym wypadku jej odwołanie powinno być możliwe w ten sam sposób.

Uprawnienie osoby do rzeczywistego wycofania zgody łączy się z wymogiem dobrowolności zgody.

Zgoda na kontakt marketingowy

Szczególną czujnością kierujmy się, gdy mamy do czynienia z działaniami marketingowymi. O ile zgoda na marketing bezpośredni nie jest wymagana, o tyle sytuacja się zmienia, gdy taka forma komunikacji jest realizowana telefonicznie.

Prawo telekomunikacyjne w art. 172 zakazuje wykonywania połączeń do celów marketingu bezpośredniego, chyba że abonent lub użytkownik końcowy uprzednio wyraził na nie zgodę.

Ustawienia domyślne

Pamiętajmy również o tym, że wszelkie modele wykorzystujące bierność, milczenie osoby, której dane dotyczą, lub jej nieuwagę, a także ustawienia domyślne, domyślnie zaznaczone okienka zgód itp., są niedopuszczalne. Wskazał na to m.in. Europejski Trybunał Sprawiedliwości w wyroku z 1 października 2019 r. (sygn. akt. C-673/17).

Grupa Robocza Art. 29 w Wytycznych dotyczących zgody na mocy rozporządzenia 2016/679 wskazała, że osoba wyrażająca zgodę musi podjąć celowe działanie, aby wyrazić zgodę na określone przetwarzanie jej danych.

To my sami mamy decydować o tym na co się zgadzamy i świadomie to zaznaczać. Tymczasem domyślnie zaznaczone okienka możemy przez nieuwagę i pośpiech pominąć.

Przetwarzanie danych niezgodnie z prawem

Każdy, kto uważa, że jego dane osobowe są przetwarzane niezgodnie z prawem, może dochodzić swoich praw przed sądem powszechnym (art. 79 RODO). Jeżeli dana osoba uzna, że w wyniku naruszenia przepisów RODO poniosła szkodę majątkową lub niemajątkową, ma też prawo żądać od administratora lub podmiotu przetwarzającego odszkodowania (art. 82 RODO).

Możliwość skorzystania z powyższych praw w przypadku zgody może mieć miejsce, gdy np. wycofujemy zgodę, a administrator to utrudnia albo nie respektuje naszego żądania i w dalszym ciągu przetwarza nasze dane, a nie ma innej przesłanki legalizującej takie działanie. Również, gdy kwestionujemy dobrowolność wyrażonej zgody, to możemy skorzystać z przysługujących nam praw.

Data wytworzenia informacji: 03.11.2021 r.

Czy przedstawiciel związku zawodowego może mieć dostęp do danych we wnioskach o przyznanie świadczeń

Nasz pracodawca przyjął regulamin ZFŚS, który nie przewiduje powołania komisji socjalnej, a jedynie udział przedstawicieli związku zawodowego w procesie oceny wniosków o przyznanie świadczeń z tego funduszu. Zgodnie z tym regulaminem związki zawodowe pisemnie wyznaczają swojego przedstawiciela do udziału w opiniowaniu przyznawania indywidualnych świadczeń z ZFŚS. Zastanawiamy się (zwłaszcza w kontekście odpowiedzi na pytanie CZY ZWIĄZEK ZAWODOWY MOŻE MIEĆ DOSTĘP DO DANYCH Z WNIOSKÓW O PRZYZNANIE ŚWIADCZEŃ Z ZFŚS?**), czy w takim**

przypadku regulamin ZFŚS jako źródło prawa pracy może być podstawą udostępnienia danych zawartych we wnioskach pracowników przedstawicielom związku zawodowego.

Ponadto zastanawiamy się, czy jeżeli wniosek o przyznanie świadczeń z ZFŚS składa emeryt, to czy wówczas przedstawiciel związku zawodowego powinien mieć do dostęp do danych zawartych we wniosku?

W myśl art. 8 ust. 2 ustawy o zakładowym funduszu świadczeń socjalnych **zasady i warunki korzystania z usług i świadczeń finansowanych z Funduszu**, z uwzględnieniem ust. 1-lb, oraz **zasady przeznaczania środków Funduszu na poszczególne cele i rodzaje działalności socjalnej określa pracodawca** w regulaminie ustalanym zgodnie z art. 27 ust. 1 albo art. 30 ust. 6 ustawy z dnia 23 maja 1991 r. o związkach zawodowych. Pracodawca, u którego nie działa zakładowa organizacja związkowa, uzgadnia regulamin z pracownikiem wybranym przez załogę do reprezentowania jej interesów.

Postanowienia regulaminu ZFŚS określają zatem, na jakich zasadach, komu i w jaki sposób (w tym: z udziałem jakich osób) przyznawane są świadczenia z zakładowego funduszu świadczeń socjalnych.

Wiele podmiotów w postanowieniach regulaminu ZFŚS określa zadania i skład komisji socjalnych. W skład tych komisji często wchodzą również przedstawiciele związku zawodowego. W jednym z komentarzy wskazano, iż w przypadku, kiedy u pracodawcy funkcjonuje komisja socjalna, to „w celu prawidłowej realizacji zadań nałożonych na komisję, powinna ona mieć w swoim składzie pracodawcę lub jego przedstawiciela, przedstawiciela pracowników i przedstawiciela związków zawodowych." (Barbara Tomaszewska, Ustawa o zakładowym funduszu świadczeń socjalnych. Komentarz, komentarz do art. 8). Prawidłowość wydawania środków z ZFŚS podlega bowiem kontroli związków zawodowych na podstawie art. 8 ust. 3 ustawy o zakładowym funduszu świadczeń socjalnych. Zgodnie z tym przepisem związkom zawodowym przysługuje prawo wystąpienia do sądu pracy z roszczeniem o zwrot ZFŚS środków wydatkowanych niezgodnie z przepisami ww. ustawy lub o przekazanie należnych środków na ten Fundusz.

W sytuacji opisanej w przedstawionym pytaniu, pracodawca nie przewidział w regulaminie ZFŚS powołania komisji socjalnej, ale przewidział inne, zgodne z przepisami prawa pracy rozwiązanie, czyli udział przedstawicieli związków zawodowych w opiniowaniu przyznawania **indywidualnych** świadczeń poszczególnym osobom. Jeżeli regulamin ZFŚS przewiduje, że związki zawodowe pisemnie wyznaczają do tego zadania swojego przedstawiciela, wówczas taki przedstawiciel może i powinien mieć dostęp do danych osobowych zawartych we wniosku o przyznanie świadczenia.

Dodać należy, że odnośnie do regulaminu ZFŚS jako źródła prawa pracy i kwestii, które mogą być w nim uregulowane wypowiadał się Sąd Najwyższy w wyroku z 6 grudnia 2001 r. (I PKN 355/00), w którym wskazał, że: :„Regulamin zakładowego funduszu świadczeń socjalnych jest (…)

wewnątrzzakładowym aktem normatywnym, **konkretyzującym zasady** gospodarowania środkami funduszu, przeznaczania tych środków na różne rodzaje działalności socjalnej i przyznawania indywidualnych świadczeń socjalnych, w tym także o charakterze roszczeniowym."

Wyznaczony przez związek zawodowy przedstawiciel będzie również uprawniony do opiniowania wniosku o przyznanie świadczenia, który został **złożony przez emeryta**. Jak wskazuje art. 2 pkt 5 ustawy o zakładowym funduszu świadczeń socjalnych **osobami uprawnionymi do korzystania z ZFŚS są** pracownicy i ich rodziny, **emeryci** i renciści – byli pracownicy i ich rodziny oraz inne osoby, którym pracodawca przyznał, w regulaminie, o którym mowa w art. 8 ust. 2 ww. ustawy, prawo korzystania ze świadczeń socjalnych finansowanych z Funduszu.

Data wytworzenia informacji: 03.11.2021 r.

Jaki jest okres retencji danych zebranych w związku z rekrutacją na uczelnię wyższą?

Zwracam się z zapytaniem dotyczącym przetwarzania danych osobowych w systemach informatycznych uczelni osób, które uczestniczyły w procesie rekrutacyjnym, ale nie zostały studentami uczelni. Zgodnie z art. 83 ustawy Prawo o szkolnictwie wyższym i nauce, osoba przyjęta na studia nabywa prawa studenckie z chwilą złożenia ślubowania (podstawa prawna do procesu dalszego przetwarzania danych osobowych). Osoby te dostały się na wybrane wydziały, lecz nie podjęły studiowania (nie złożyły ślubowania). Czy w związku z takim stanem prawnym dane osobowe osób, które nie zostały studentami naszej uczelni, powinny być niezwłocznie usuwane z systemów informatycznych.

Kluczowe dla udzielenia odpowiedzi na tak sformułowane pytanie jest określenie, w jakim celu, w systemach informatycznych uczelni, przetwarzane są dane osobowe osób, które uczestniczyły w procesie rekrutacyjnym, ale nie zostały studentami uczelni. Czy ten cel związany jest jedynie z rekrutacją, czy też w grę mogą wchodzą inne cele przetwarzania danych osobowych.

Po ustaleniu, w jakim konkretnie celu określone dane są przetwarzane w systemach informatycznych uczelni, należy dokonać analizy, kiedy ten cel zostanie osiągnięty.

Zgodnie z art. 5 ust. 1 lit. b RODO dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami („ograniczenie celu"). Określenie celów przetwarzania danych osobowych ma zatem bezpośredni wpływ na zapewnienie zgodności operacji przetwarzania

danych z pozostałymi zasadami ochrony danych osobowych, takimi jak chociażby zasada minimalizmu, rzetelności i legalności oraz ograniczenia przechowywania.

Z zasady ograniczenia przechowywania (retencji) sformułowanej w art. 5 ust. 1 lit. e RODO wynika natomiast, że dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Zasada ta oznacza, że w każdym przypadku administrator musi ustalić, przez jaki okres może przetwarzać określone dane osobowe w określonym celu oraz jakie czynności musi podjąć po upływie tego okresu.

Kwestia ustalenia adekwatnego okresu przetwarzania jest kluczowa również z punktu widzenia spełnienia przez administratora innych obowiązków wynikających z przepisów RODO. Jest on zobowiązany wskazać okres, przez który dane osobowe będą przechowywane, w ramach realizacji obowiązków informacyjnych określonych w art. 13 ust. 2 i 14 ust. 2 RODO, oraz wskazać te okresy w prowadzonym przez siebie rejestrze czynności przetwarzania danych osobowych.

Administrator powinien dokonać analizy dotyczących jego działalności przepisów prawa, które mogą przewidywać określony termin przechowywania danych do realizacji określonego celu przetwarzania (np. ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach, których doprecyzowaniem jest instrukcja kancelaryjna, lub ustawy z dnia 29 września 1994 r. o rachunkowości).

W przypadku, gdy prawo nie reguluje okresu przechowywania danych należy, przy uwzględnieniu ogólnych zasad wynikających z RODO, samodzielnie ustalić termin ich przechowywania, biorąc pod uwagę cel przetwarzania. Brak określonych przepisami prawa okresów przetwarzania informacji zawierających dane osobowe, nie oznacza bowiem, że informacje takie można przetwarzać bezterminowo (tak też w odpowiedzi na pytanie CZY TRZEBA PRECYZYJNIE OKREŚLAĆ OKRES PRZECHOWYWANIA DANYCH?).

Zgodnie z art. 70 ust. 1 ustawy z dnia 20 lipca 2018 r. o szkolnictwie wyższym i nauce, uczelnia ustala warunki, tryb oraz termin rozpoczęcia i zakończenia rekrutacji oraz sposób jej przeprowadzenia. Artykuł ten stanowi delegację do określenia w uchwale senatu uczelni zasad i trybu rekrutacji, a także terminu rozpoczęcia i zakończenia rekrutacji na studia, jak również sposobu jej przeprowadzenia.

Mając na uwadze, że przepisy ustawy nie zawierają szczegółowych regulacji dotyczących okresu przechowywania danych w związku z przeprowadzaną rekrutacją na studia, a jedynie odsyłają do ustalenia przez uczelnię szczegółów dotyczących tego procesu, trzeba samodzielnie określić okres przechowywania danych osobowych, również w odniesieniu do danych przetwarzanych w systemach informatycznych. Konieczne jest uwzględnienie, że w odniesieniu do określonych danych osobowych przetwarzanych przez uczelnię publiczną mogą mieć zastosowanie przepisy

o narodowym zasobie archiwalnym i archiwach. Natomiast w sytuacji, gdy kandydat wniósł opłatę rekrutacyjną, przy ustaleniu okresu przechowywania danych należy także uwzględnić przepisy ustawy o rachunkowości (art. 74 tej ustawy).

Pomocne w przestrzeganiu zasady ograniczenia przechowywania jest opracowanie i wdrożenie odpowiednich procedur związanych z usuwaniem danych osobowych. W decyzji z dnia 18 października 2019 r. Prezes UODO wskazał, iż w celu zapewnienia przetwarzania danych zgodnie z zasadą ograniczonego przechowywania, administrator powinien stworzyć procedury, z których będzie wynikał termin i sposób usuwania informacji zawierających dane osobowe oraz zasady dokonywania przeglądów przetwarzanych danych w celu weryfikacji, czy określone w ten sposób terminy usuwania danych osobowych są przestrzegane (https://uodo.gov.pl/decyzje).

Warto wskazać, że UODO nie narzuca określonych wzorów postępowania, ale oczekuje od administratora przedstawienia argumentów, które przemawiają za przyjęciem określonych rozwiązań i wykazania spełnienia wynikających z RODO zasad, takich jak: zgodność z prawem, rzetelność i przejrzystość, celowość, minimalizacja danych, prawidłowość, integralność czy poufność. Powyższe wynika z określonej w art. 5 ust. 2 RODO zasady rozliczalności, zgodnie z którą administrator jest odpowiedzialny za przestrzeganie wymienionych w art. 5 ust. 1 RODO zasad dotyczących przetwarzania danych i musi być w stanie wykazać ich przestrzeganie. Zasada rozliczalności wymaga też, aby administratorzy wykazywali logikę, na której opierają swoje decyzje, i potrafili uzasadnić, dlaczego przyjęli określone rozwiązania.

Data wytworzenia informacji: 06.12.2021 r.

Czy pracodawca może pozyskiwać od pracownika informacje na temat powodów odejścia z pracy?

W celu podnoszenia jakości i poprawy warunków pracy oraz zaspokajania potrzeb pracowników w naszej firmie, przełożeni chcieliby mieć możliwość uzyskiwania od odchodzącego pracownika informacji na temat powodów jego decyzji. Na tej podstawie chcą zidentyfikować obszary wymagające poprawy. Zastanawiamy się, czy dopuszczalne jest pozyskiwanie takich informacji od pracownika oraz czy przetwarzanie takich danych pracowników można oprzeć na przesłance z art. 6 ust. 1 lit. f RODO.

W przedstawionej sytuacji w pierwszej kolejności należy odwołać się do przepisów Kodeksu pracy, ponieważ wskazują one, jakie informacje i w jakich celach pracodawca może pozyskiwać od pracownika. Zgodnie z art. 22^1 § 1 Kodeksu pracy pracodawca żąda od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko; datę urodzenia; dane kontaktowe wskazane przez taką osobę; wykształcenie; kwalifikacje zawodowe; przebieg dotychczasowego zatrudnienia. Natomiast zgodnie z art. 22^1 § 3, pracodawca żąda **od**

pracownika podania dodatkowo danych osobowych obejmujących: adres zamieszkania; numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość; inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy; wykształcenie i przebieg dotychczasowego zatrudnienia, jeżeli nie istniała podstawa do ich żądania od osoby ubiegającej się o zatrudnienie; numer rachunku płatniczego, jeżeli pracownik nie złożył wniosku o wypłatę wynagrodzenia do rąk własnych.

Natomiast zgodnie z art. 22^1 § 4 Kodeksu pracy pracodawca może żądać podania innych danych osobowych pracownika niż określone w § 1 i 3, **gdy jest to niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.** Obowiązek taki może wynikać zarówno z przepisów Kodeksu pracy, jak i z odrębnych przepisów prawnych. Przykładem takiej sytuacji może być przekazanie danych kontaktowych, np. prywatnego adresu e-mail i numeru prywatnego telefonu, w związku z obowiązkiem zawarcia umowy o prowadzenie Pracowniczych Planów Kapitałowych z wybraną instytucją finansową. Pracodawca ma bowiem obowiązek prawny, wynikający z ustawy o pracowniczych planach kapitałowych, przekazania danych osobowych m.in. w postaci adresu poczty elektronicznej i numeru telefonu od pracownika bez wyrażenia jego zgody do wybranej instytucji finansowej, o ile pracownik takie dane mu udostępni.

W Kodeksie pracy uregulowane są również przypadki, gdy zgoda kandydata do pracy lub pracownika pozwala na przetwarzanie innych danych niż wymienione w przepisach Kodeksu pracy, z wyłączeniem danych osobowych dotyczących wyroków skazujących oraz czynów zabronionych (art. 10 RODO). Należy jednak pamiętać, że zgoda taka musi odpowiadać wszystkim wymaganiom przewidzianym zarówno w RODO, jak i w przepisach Kodeksu pracy.
W szczególności należy mieć na uwadze, że pracownik ma prawo w dowolnym momencie udzieloną zgodę wycofać. Ponadto brak zgody, lub jej wycofanie, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenie umowy o pracę lub jej rozwiązanie bez wypowiedzenia przez pracodawcę (22^{1a} § 2 Kodeksu pracy).

Warto też przypomnieć , że zgoda pracownika może stanowić podstawę przetwarzania przez pracodawcę danych osobowych, o których mowa w art. 9 ust. 1 RODO (np. danych dotyczących zdrowia) wyłącznie w przypadku, gdy przekazanie tych danych osobowych następuje **z inicjatywy pracownika** (art. 22^{1b} § 1 Kodeksu pracy).

Odnosząc się natomiast do możliwości powołania się na art. 6 ust. 1 lit. f RODO wskazać należy, że przyjęcie tej przesłanki jako podstawy pozyskiwania od pracowników informacji dotyczących „obiektywnych powodów rozwiązania stosunku pracy" wymagałoby wnikliwego rozważenia.

Zwrócić należy uwagę, że pozyskiwane od pracowników informacje mają dotyczyć powodów rozwiązania stosunku pracy, zatem powody te mogą być bardzo różne i nie można wykluczyć, że czasami będą one dotyczyć względów pozazawodowych, a zatem dotykać bezpośrednio lub pośrednio sfery życia osobistego pracownika, np. stanu zdrowia. Natomiast ww. przesłanka może być podstawą do przetwarzania wyłącznie tzw. danych osobowych zwykłych.

Ponadto w opinii 2/2017 (WP 249) na temat przetwarzania danych w miejscu pracy Grupa Robocza Art. 29 wskazała, że niekiedy pracodawcy mogą powołać się na uzasadniony interes, wskazując go jako podstawę prawną podejmowanych działań, pod warunkiem że przetwarzanie danych jest **bezwzględnie konieczne ze względów prawnych i zgodne z zasadami proporcjonalności i pomocniczości**.

A zatem administrator, który zamierza przetwarzać dane osobowe (w tym dane osobowe pracowników) powinien kierować się zasadą minimalizacji (art. 5 ust.1 lit. c RODO), czyli gromadzić tylko takiego rodzaju dane i tylko o takiej treści, które są niezbędne ze względu na cel zbierania danych. **Ponadto, jak wskazano w motywie 39 RODO, dane osobowe powinny być przetwarzane wyłącznie w takich przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami**. Wobec tego administrator zanim podejmie decyzję o przetwarzaniu danych osobowych, powinien dokonać oceny, czy dane osobowe rzeczywiście są konieczne do osiągnięcia celu, czy nie istnieją inne, mniej inwazyjne, sposoby jego osiągniecia. Przetwarzanie danych w zakresie zbędnym dla osiągnięcia celu będzie sprzeczne z RODO.

Zastosowanie przesłanki z art. 6 ust. 1 lit. f RODO wymaga dokonania wcześniejszej starannej oceny, czy wskazane w tej przesłance kumulatywne warunki zostały spełnione. Zgodnie art. 6 ust. 1 lit. f RODO przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, **w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych**, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Po pierwsze należy ocenić, czy w konkretnej sytuacji występuje prawnie uzasadniony interes, który jest realizowany przez administratora lub przez stronę trzecią. Po drugie, niezbędna jest weryfikacja, czy przetwarzanie danych osobowych jest niezbędne dla realizacji celu wynikającego z prawnie uzasadnionych interesów. Następnie należy ocenić, czy nie jest spełniona przesłanka o charakterze negatywnym w postaci występowania w danym stanie faktycznym interesów lub podstawowych praw i wolności podmiotu danych, które mają charakter nadrzędny wobec

prawnie uzasadnionych interesów administratora lub strony trzeciej. W przypadku spełnienia tego warunku nie będzie można powołać się na przepis art. 6 ust. 1 lit. f jako uzasadnienie dla przetwarzania danych osobowych. Stosowanie tej negatywnej przesłanki polega w istocie na **wyważeniu dwóch dóbr chronionych prawem, tj. prawnie uzasadnionego interesu administratora lub strony trzeciej z jednej strony i interesów, podstawowych praw oraz wolności podmiotu danych z drugiej.**

Zatem aby można było oprzeć się na art. 6 ust. 1 lit. f RODO jako podstawie prawnej przetwarzania, należałoby przeprowadzić ważenie ww. interesów, nazywane też testem równowagi.

Na potrzebę przeprowadzenia takiego testu przed rozpoczęciem przetwarzania oraz udostępnienia jego wyników osobom, których dane dotyczą, wskazuje również Grupa Robocza Art. 29 w Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679 (WP 260). **W Wytycznych tych wskazano m.in., że w ramach najlepszej praktyki administrator może również przedstawić osobie, której dane dotyczą, informacje uzyskane w wyniku testu równowagi**, który należy przeprowadzić, aby można było oprzeć się na art. 6 ust. 1 lit. f jako podstawie prawnej przetwarzania, zanim jakiekolwiek dane osobowe osoby, której dane dotyczą, zostaną zebrane. (…) Jest to istotne dla skutecznej przejrzystości w przypadku gdy osoby, których dane dotyczą, **mają wątpliwości, czy test równowagi przeprowadzono rzetelnie** lub chcą złożyć skargę do organu nadzorczego.

Również w Wytycznych 4/2019 w sprawie uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych z artykułu 25, Europejska Rada Ochrony Danych wskazała, że w **przypadku gdy uzasadnione interesy stanowią podstawę prawną, administrator musi przeprowadzić ważenie interesów**, ze szczególnym uwzględnieniem nierównowagi władzy, w szczególności dzieci poniżej 18 roku życia i innych grup znajdujących się w trudnej sytuacji.

Wskazówki, w jaki sposób należy przeprowadzić test równowagi, znaleźć można m.in. w Opinii 06/2014 w sprawie pojęcia uzasadnionych interesów administratora danych zawartego w art. 7 dyrektywy 95/46/WE (WP 217).

Data wytworzenia informacji: 06.12.2021 r.

Czy art. 2 ust. 1 ust. o ochronie danych osobowych jest podstawą udostępnienia danych przez urząd?

Do naszego urzędu wpływają wnioski z prośbą o podanie informacji na temat osób dotychczas pełniących funkcje publiczne w samorządzie terytorialnym. Takie wnioski kierują np. dziennikarze, stowarzyszenia wydające publikacje związane np. z historią samorządu

terytorialnego itp. Wnioski te mogą dotyczyć różnych szczegółowych informacji odnoszących się do osób, które dotychczas pełniły funkcję publiczną, np. rok urodzenia, wykształcenie, przynależność do partii politycznej.

Podmioty występujące o powyższe dane jako podstawę ich udostępnienia wskazują artykuł 85 RODO oraz art. 2 ust. 1 ustawy o ochronie danych osobowych, wskazując, że do takich przypadków przepisy o ochronie danych osobowych nie mają zastosowania. Mamy jednak wątpliwości, czy to jest właściwa podstawa udostępnienia danych.

Czy art. 2 ust. 1 ustawy o ochronie danych osobowych stanowi podstawę udostępnienia danych przez urząd (np. gminy, starostwo powiatowe, urząd marszałkowski) – na wniosek podmiotu przygotowującego publikację (bądź dziennikarzowi, który przygotowuje artykuł) – o osobach pełniących dotychczas funkcję publiczną?

Warto zacząć od tego, że art. 2 ust. 1 ustawy o ochronie danych osobowych **nie jest podstawą udostępnienia danych osobowych**. Przepis ten bowiem wskazuje jedynie, **których z przepisów RODO** (art. 5-9, art. 11, art. 13-16, art. 18-22, art. 27, art. 28 ust. 2-10 oraz art. 30 RODO) **nie stosuje się do** działalności polegającej na redagowaniu, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych w rozumieniu ustawy z dnia 26 stycznia 1984 r. - Prawo prasowe, a także do wypowiedzi w ramach działalności literackiej lub artystycznej. Wyłączenie to - w zakresie wskazanych przepisów RODO - należy zatem odnosić do podmiotów, które dla wskazanej działalności (np. prasowej, literackiej) posługują się danymi osobowymi.

Podstawy (przesłanki dopuszczalności) przetwarzania, w tym udostępniania danych osobowych, określają inne przepisy RODO. Przetwarzanie tzw. danych zwykłych może się odbywać jedynie po spełnieniu jednego z warunków określonych w art. 6 RODO. Kryterium niezbędności przetwarzania danych osobowych występuje w większości wskazanych w art. 6 RODO przesłanek. Dodatkowo należy pamiętać o wyrażonym w art. 9 ust. 1 RODO zakazie przetwarzania (udostępniania) szczególnych kategorii danych osobowych, w tym danych osobowych ujawniających np. poglądy polityczne. Przetwarzanie szczególnych kategorii danych jest co do zasady zabronione, chyba że spełniony jest jeden z warunków wskazanych w ust. 2 tego artykułu.

W przypadku podmiotów publicznych co do zasady podstawę prawną przetwarzania danych osobowych powinno stanowić wykonanie obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c RODO) lub wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO), zaś w sytuacji, gdy przetwarzane będą szczególne kategorie danych - art. 9 ust. 2 lit. g RODO, tj. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym na podstawie prawa Unii lub prawa państwa członkowskiego. Wszelkie działania podejmowane przez podmioty publiczne powinny mieć bowiem oparcie w obowiązujących przepisach prawa regulujących ich działalność. Wobec tego podstawa prawna do przetwarzania (w tym

udostępniania) danych osobowych przez takie podmioty również powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami. Powołane przepisy RODO wymagają odwołania się do właściwych przepisów prawa krajowego (unijnego) szczegółowo regulujących zasady postępowania z danymi osobowymi lub obowiązki i zadania, dla których wykonania niezbędne jest przetwarzanie danych osobowych. W odniesieniu do przesłanek z art. 6 ust. 1 RODO mówi o tym ustęp 3 tego artykułu.

W przedstawionej sytuacji kwestię dopuszczalności udostępnienia danych osobowych przez organ publiczny innemu podmiotowi na jego wniosek należy przede wszystkim rozstrzygać na podstawie przepisów: ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej, ewentualnie ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego. Ponadto należy wskazać, że druga ze wskazanych ustaw utraciła moc, bowiem zastąpiła ją ustawa z dnia 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, która wchodzi w życie 8 grudnia 2021 r.

Jeśli chodzi o dostęp dziennikarzy do informacji będących w posiadaniu m.in. organów publicznych, to kwestię tę reguluje ustawa z dnia 26 stycznia 1984 r. Prawo prasowe. Zgodnie z art. 3a tej ustawy w zakresie prawa dostępu prasy do informacji publicznej stosuje się przepisy ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Zatem „(…) w zakresie informacji pozyskiwanych od podmiotów zobligowanych do udzielania informacji publicznej Prawo prasowe zostaje wyłączone, a dziennikarz ma takie same prawa i obowiązki jak każda inna osoba, która żąda dostępu do informacji publicznej.” (M. Brzozowska-Pasieka [w:] M. Olszyński, J. Pasieka, M. Brzozowska-Pasieka, Prawo prasowe. Komentarz praktyczny, Warszawa 2013, art. 3(a).).

Jednocześnie warto mieć na uwadze, iż informacje, o które wnioskuje podmiot, mogą mieć status materiału archiwalnego. **Zasady udostępniania materiałów archiwalnych określa ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach**. Dostęp do materiałów archiwalnych podlega ograniczeniu na podstawie art. 16b ww. ustawy w przypadkach w nim wskazanych (m.in. ze względu na ochronę dóbr osobistych i danych osobowych).

Data wytworzenia informacji: 06.12.2021 r.

Czy należy podpisać umowę powierzenia z firmą sprzątającą?

Czy UODO mógłby podać oficjalne stanowisko w sprawie podpisywania umów powierzenia przetwarzania danych osobowych z firmami świadczącymi usługi niewymagające przetwarzania danych osobowych, np. z zewnętrznymi firmami sprzątającymi. Jako inspektor ochrony danych mam z tym problem. Kancelarie prawne i serwisy internetowe specjalizujące się w ochronie danych osobowych wydają w tym zakresie różne opinie.

Z taką zewnętrzną firmą sprzątającą podpisywana jest umowa na świadczenie usług sprzątania. W trakcie wykonywania usług może dojść do przypadkowego kontaktu z danymi osobowymi przetwarzanymi u administratora. Czy z tego powodu należy podpisać umowę powierzenia przetwarzania danych osobowych, czy też wystarczy zawrzeć w umowie klauzulę o zachowaniu danych w poufności?

Ocena przedstawionego zagadnienia będzie zależała przede wszystkim od tego, jaki jest zakres usług świadczonych przez zewnętrzną firmę sprzątającą, tj. czy usługi te obejmują obok usług porządkowych również np. niszczenie dokumentów lub inne działania, które nie mogą być realizowane bez dostępu do dokumentów lub innych nośników danych osobowych.

Konieczność zawarcia umowy powierzenia przetwarzania danych osobowych istnieje wówczas, gdy administrator w celu realizacji swoich celów (zadań) **związanych z przetwarzaniem danych osobowych** posługuje się innym, zewnętrznym podmiotem. Jak wynika z art. 28 ust. 1 RODO, z powierzeniem przetwarzania danych osobowych mamy do czynienia, gdy **przetwarzanie** danych osobowych jest dokonywane przez zewnętrzny podmiot w imieniu administratora, w celach określonych przez administratora i zgodnie z jego poleceniami i instrukcjami.

Natomiast usługi sprzątania powierzchni danego obiektu (np. uczelni, biura) trudno zaliczyć do usług związanych z przetwarzaniem danych osobowych. Należy zatem przyjąć, że co do zasady usługi takie nie wymagają powierzenia przetwarzania danych osobowych.

Niemniej w przypadku korzystania przez administratora z takich usług (jak i innych usług wymagających dostępu do pomieszczeń administratora, w których przetwarzane są dane osobowe) – konieczne może się okazać zastosowanie odpowiednich środków technicznych i organizacyjnych, których celem będzie zapewnienie odpowiedniej ochrony danych osobowych, w tym przed nieuprawnionym ujawnieniem danych osobowych.

Administrator powinien bowiem analizować ryzyko związane z przetwarzaniem danych i podejmować środki, które będą je minimalizować. Działania te powinny dotyczyć zarówno pracowników administratora, jak i podmiotu zewnętrznego. Powinny one polegać m.in. na wprowadzeniu odpowiednich procedur i zadbanie o ich skuteczne wdrożenie i realizowanie przez cały cykl przetwarzania danych (art. 24 RODO, art. 32 RODO). W procedurach tych warto też przewidzieć, iż mogą zdarzyć się sytuacje, w których pracownicy firmy sprzątającej znajdą określony dokument lub inny nośnik zawierający dane osobowe. Jednocześnie w umowie z firmą sprzątającą należy określić sposób postępowania w takiej sytuacji oraz obowiązki pracownika, który uzyskał przypadkowy dostęp do danych osobowych.

Wiele pomocnych wskazówek dotyczących powierzenia przetwarzania danych osobowych znaleźć można m.in. w Wytycznych Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO. W ww. Wytycznych (pkt 79) wskazuje się, że

przetwarzanie danych osobowych w imieniu administratora wymaga przede wszystkim, aby odrębny podmiot przetwarzał dane osobowe na rzecz administratora. W art. 4 ust. 2 przetwarzanie definiuje się jako pojęcie obejmujące szeroki zakres operacji, począwszy od zbierania, przechowywania i konsultacji po wykorzystywanie, rozpowszechnianie lub udostępnianie i niszczenie w inny sposób. W rozdziale dotyczącym pojęcia „osoby trzeciej" podany jest następujący przykład związany z usługami sprzątania (pkt 89): „Przedsiębiorstwo A zawiera umowę z firmą sprzątającą na sprzątanie swoich biur. Pracownicy sprzątający zgodnie z umową mają zakaz uzyskiwania dostępu do danych osobowych lub ich przetwarzania w inny sposób. Nawet, jeśli mogą oni czasami natknąć się na takie dane podczas poruszania się po biurze, mogą wykonywać swoje zadania bez dostępu do danych. Osoby sprzątające nie są zatrudnione przez przedsiębiorstwo A ani nie są postrzegane jako podlegające bezpośredniemu zwierzchnictwu tej spółki. Przedsiębiorstwo A nie ma zamiaru angażować firmy sprzątającej ani jej pracowników w przetwarzanie danych osobowych. Firmę świadczącą usługi sprzątania i jej pracowników należy zatem postrzegać jako osobę trzecią, a administrator musi upewnić się, że istnieją odpowiednie środki bezpieczeństwa, aby uniemożliwić tej firmie i jej pracownikom dostęp do danych, oraz ustanowić obowiązek zachowania poufności w przypadku przypadkowego natknięcia się na dane osobowe."

Data wytworzenia informacji: 11.01.2022 r.

W jakim zakresie należy ujawniać dane przedsiębiorców prowadzących ośrodki szkolenia kierowców?

Do starostwa wpłynęło pismo właściciela firmy prowadzącego ośrodek szkolenia kierowców, zakazujące publikacji jego imienia i nazwiska oraz nazwy firmy w podawanych do publicznej wiadomości wynikach statystycznych w zakresie średniej zdawalności osób szkolonych w jego ośrodku. Przedsiębiorca wyraził zgodę na publikowanie tylko i wyłącznie numeru firmy pod jakim jest zarejestrowany ośrodek. Starosta - w ramach nadzoru w zakresie zgodności prowadzenia szkolenia osób ubiegających się o uzyskanie uprawnień do kierowania pojazdami silnikowymi lub motorowerem - sporządza analizę statystyczną oraz podaje do publicznej wiadomości jej wyniki m.in. w zakresie średniej zdawalności osób szkolonych w danym ośrodku (art. 43 ust. 1 pkt 6 lit. a ustawy o kierujących pojazdami). Upubliczniając ww. dane, starosta wskazuje firmę przedsiębiorcy wpisaną do rejestru przedsiębiorców prowadzących ośrodek szkolenia kierowców. Często firma przedsiębiorcy oznaczona jest imieniem i nazwiskiem osoby prowadzącej działalność, np. „Krzysztof Kowalski Ośrodek Szkolenia Kierowców Krzysztof".

Zgodnie z art. 28 ust. 1 ustawy o kierujących pojazdami działalność gospodarcza w zakresie prowadzenia ośrodka szkolenia kierowców jest działalnością regulowaną. Rejestry działalności

regulowanej zgodnie z art. 43 ust. 4 ustawy Prawo przedsiębiorców są jawne. Dane z rejestrów dotyczące firmy przedsiębiorcy oraz jego numeru identyfikacji podatkowej są udostępniane w sieci teleinformatycznej. Organ może udostępnić w sieci teleinformatycznej także inne dane, z uwzględnieniem przepisów o ochronie danych osobowych.

Art. 28 ust. 4 i ust. 7 ustawy o kierujących pojazdami wskazuje, jakie dane zamieszcza się w rejestrze przedsiębiorców prowadzących ośrodek szkolenia kierowców. Z publikacji wyłączony jest tylko adres zamieszkania przedsiębiorcy, jeżeli jest inny niż adres prowadzonej działalności gospodarczej.

Czy w związku z powyższym starosta, publikując ww. dane, uprawniony jest do oznaczenia ośrodka nazwą firmy przedsiębiorcy, nawet jeżeli zawiera ona w swej nazwie imię i nazwisko właściciela?

Dane osobowe osób fizycznych prowadzących jednoosobową działalność gospodarczą podlegają ochronie na mocy ogólnego rozporządzenia o ochronie danych (RODO), a podmioty, które chcą je przetwarzać, muszą spełnić wszystkie obowiązki wynikające z przepisów o ochronie danych osobowych, w tym legitymować się podstawą prawną do ich przetwarzania.

Administrator będący podmiotem publicznym, oceniając, czy przetwarzanie (w tym udostępnianie) danych jest w określonej sytuacji dopuszczalne, powinien w pierwszej kolejności kierować się przepisami prawa odnoszącymi się do jego działalności. Podmioty publiczne co do zasady przetwarzają dane na podstawie i w granicach określonych przez przepisy.

Przedstawione w pytaniu wątpliwości dotyczą tego, czy w celu realizacji obowiązku określonego w art. 43 ust. 1 pkt 6 lit. a ustawy o kierujących pojazdami starosta może udostępnić informacje o firmie przedsiębiorcy zawierającej imię i nazwisko osoby prowadzącej jednoosobową działalność, np. „Krzysztof Kowalski Ośrodek Szkolenia Kierowców Krzysztof”.

Zgodnie z art. 43 ust. 1 pkt 6 lit. a ustawy o kierujących pojazdami, starosta sprawuje nadzór w zakresie zgodności prowadzenia szkolenia osób ubiegających się o uzyskanie uprawnień do kierowania, w ramach którego w szczególności sporządza analizę, przetwarza oraz podaje do publicznej wiadomości wyniki analizy statystycznej, w zakresie średniej zdawalności osób szkolonych **w danym ośrodku szkolenia kierowców** oraz liczby uwzględnionych skarg złożonych **na dany ośrodek.**

Przywołany powyżej przepis nakłada na starostę obowiązek podania do publicznej wiadomości **wyników analizy statystycznej dotyczących danego ośrodka szkolenia kierowców**. Zatem podstawę do przetwarzania danych osobowych w tym celu stanowi ww. przepis ustawy o kierujących pojazdami, nie zaś zgoda osoby, której dane dotyczą.

Przepis ten (art. 43 ust. 1 pkt 6 lit. a ustawy o kierujących pojazdami) - zobowiązując starostę do podawania do publicznej wiadomości wyników analizy statystycznej - nie precyzuje, w jaki sposób

powinien zostać oznaczony taki ośrodek. Art. 28 ust. 7 w z związku z art. 28 ust. 4 ustawy o kierujących pojazdami stanowi, że w prowadzonym przez starostę rejestrze przedsiębiorców prowadzących ośrodek szkolenia kierowców (który jest jawny zgodnie z art. 43 ust. 4 ustawy Prawo przedsiębiorców) umieszcza się w szczególności **firmę przedsiębiorcy** oraz oznaczenie jego adresu i siedziby albo miejsca zamieszkania, a ponadto **oznaczenie** i adres **ośrodka szkolenia kierowców**. Aby zrealizować powyższy obowiązek starosta może zatem podać do wiadomości publicznej takie informacje dotyczące „danego" ośrodka, które go **jednoznacznie** identyfikują, łącznie z oznaczeniem i adresem ośrodka szkolenia kierowców nawet w przypadku, gdy oznaczenie to obejmuje firmę przedsiębiorcy[20], czyli w przypadku przedsiębiorcy będącego osobą fizyczną – jego imię i nazwisko.

Data wytworzenia informacji: 11.01.2022 r.

Jak postępować w przypadku otrzymywania tzw. niechcianych danych?

Jako inspektor ochrony danych pełniący swoją funkcję w ośrodku pomocy społecznej spotykam się z pytaniami pracowników, co robić z tzw. danymi niechcianymi. Chodzi o sytuacje, gdy kierowana jest do nas dokumentacja, o którą nie wnioskowaliśmy i której nie potrzebujemy, np. karty leczenia szpitalnego z ośrodków zdrowia czy innych instytucji. Zdarza się też, że zbędne dane - dotyczące osób trzecich albo niemające związku ze sprawą, która jest rozpatrywana - przekazywane są przez klientów. Czy taka dokumentacja i dane – zgodnie z zasadami określonymi w art. 5 ust. 1 lit. b i c RODO – powinny być odsyłane właściwym podmiotom lub usuwane?

Powyższe wątpliwości należy rozstrzygać, uwzględniając zarówno przytoczone w pytaniu zasady RODO, jak i przepisy prawa regulujące zasady i sposób realizacji określonych zadań przez ośrodki pomocy społecznej, np. Kodeks postępowania administracyjnego.

Rzeczywiście RODO wymaga, aby pozyskiwane (przetwarzane) dane osobowe były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane - tzw. zasada minimalizacji danych (art. 5 ust. 1 lit. c RODO). Ponadto dane osobowe powinny być zbierane w wyraźnie określonym i prawnie uzasadnionym celu (art. 5 ust. 1 lit. c). Niemniej kwestia ta powinna być rozstrzygana indywidualnie w każdej sprawie. Jest to spowodowane chociażby tym, że strona postępowania administracyjnego ma prawo przedstawienia wszelkich dowodów, np. dokumentów mających wpływ na jej sytuację, a w konsekwencji na treść wydanego przez organ rozstrzygnięcia. Organ dokonuje oceny tych dowodów, a następnie

[20] Zgodnie z art. 434 Kodeksu cywilnego firmą osoby fizycznej jest jej imię i nazwisko. Nie wyklucza to włączenia do firmy pseudonimu lub określeń wskazujących na przedmiot działalności przedsiębiorcy, miejsce jej prowadzenia oraz innych określeń dowolnie obranych.

w uzasadnieniu decyzji wskazuje okoliczności, które uznał za udowodnione, dowody, na których się oparł oraz przyczyny, z powodu których innym odmówił mocy dowodowej. Wobec powyższego wszelkie pisma strony składane w postępowaniu powinny zostać załączone do akt sprawy i ocenione w trakcie postępowania.

Wobec powyższego, mając na uwadze wskazane powyżej zasady RODO oraz przepisy prawa regulujące realizację określonych zadań przez ośrodki pomocy społecznej, np. Kodeks postępowania administracyjnego, administrator powinien dokonywać analizy, czy określony dokument zawierający dane osobowe istotnie został przesłany nadmiarowo lub pomyłkowo i w zależności od wyników takiej analizy np. pozostawić dokument w aktach sprawy, zwrócić lub przekazać zgodnie z właściwością do innego organu.

Data wytworzenia informacji: 11.01.2022 r.

Jak należy określać czas przechowywania upoważnień do przetwarzania danych byłego pracownika?

W związku z przechowywaniem upoważnień pracowników do przetwarzania danych osobowych wraz z oświadczeniami o przeszkoleniu i zachowaniu poufności, proszę o wskazówki, jak określać czas przechowywania upoważnień osób, z którymi pracodawca zakończył współpracę. Istnieją sprzeczne interpretacje w tym zakresie (od przechowywania upoważnień przez okres dotyczący archiwizowania akt osobowych pracownika do stanowiska mówiącego o konieczności usuwania upoważnień zaraz po zakończeniu zatrudnienia pracownika).

Decydujące dla udzielenia odpowiedzi na postawione pytanie jest określenie, na jakiej podstawie prawnej i w jakim celu przetwarzane są dane osobowe pracowników zawarte w upoważnieniach do przetwarzania danych osobowych.

Wydawanie upoważnień może być jednym ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych osobowych i kontroli nad tym, kto, z jakich powodów i w jaki sposób ma dostęp do przetwarzanych danych osobowych oraz jakich czynności może na nich dokonywać. Przyjmowane przez administratora środki (działania) powinny służyć m.in. zapobieganiu nieuprawnionemu wprowadzaniu danych osobowych oraz nieuprawnionemu oglądaniu, zmienianiu lub usuwaniu przechowywanych danych osobowych oraz zapewnieniu, że osoby uprawnione będą mieć dostęp wyłącznie do danych osobowych objętych posiadanym przez siebie uprawnieniem. Dzięki tym środkom osoby, które zostały dopuszczone do przetwarzania danych, zostają poinformowane, jaki jest zakres ich uprawnień co do przetwarzania danych osobowych. Więcej w tym zakresie wskazujemy w odpowiedzi na pytanie CZY ADMINISTRATOR POWINIEN UDZIELAĆ UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH?

Przepisy RODO nie wskazują na konieczność nadawania upoważnień w formie pisemnej, ale może to wynikać z przepisów szczególnych. Przykładem przepisu nakładającego obowiązek sporządzenia upoważnienia w formie pisemnej jest art. 22^{1b} § 3 Kodeksu pracy, który wskazuje, że do przetwarzania danych osobowych, o których mowa w art. 9 ust. 1 RODO, mogą być dopuszczone wyłącznie osoby posiadające pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy.

Jak wynika z § 3 pkt 2 rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej, w części B akt osobowych należy przetrzymywać oświadczenia lub dokumenty dotyczące nawiązania stosunku pracy oraz przebiegu zatrudnienia pracownika, w tym np. oświadczenia lub dokumenty dotyczące danych osobowych, gromadzone w związku z nawiązaniem stosunku pracy.

Przytoczony przepis jest podstawą do przechowywania w części B akt osobowych pracownika upoważnień nadawanych pracownikom zarówno w związku z wykonaniem obowiązku określonego w art. 22^{1b} § 3 Kodeksu pracy, jak i w przypadku gdy pracodawca nadaje upoważnienia do przetwarzania danych osobowych, traktując je jako jeden ze środków organizacyjnych, którego celem jest zapewnienie odpowiedniej ochrony danych i kontroli nad procesem ich przetwarzania.

W sytuacji, gdy upoważnienia stanowią część określonej dokumentacji, czas ich przechowywania może wynikać z przepisów określających zasady i sposób prowadzenia takiej dokumentacji. W przypadku, gdy są one częścią dokumentacji pracowniczej (akt osobowych) należy odwołać się do przepisów Kodeksu pracy oraz rozporządzenia Ministra Rodziny, Pracy i Polityki Społecznej z dnia 10 grudnia 2018 r. w sprawie dokumentacji pracowniczej oraz przepisów ustawy z 10 stycznia 2018 r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacją, które przewidują skrócenie (w zależności od tego, kiedy pracownik został zatrudniony) dotychczas obowiązujących terminów przechowywania dokumentacji pracowniczej.

Data wytworzenia informacji: 16.02.2022 r.

Czy wz. ze zmianą przepisów można udostępnić związkom zawodowym informację o wys. składki członkowskiej?

Z dniem 1 stycznia 2022 r. ustawą z dnia 29 października 2021 r. o zmianie ustawy o podatku dochodowym od osób fizycznych, ustawy o podatku dochodowym od osób prawnych oraz niektórych innych ustaw wprowadzono możliwość odliczenia od dochodu składek członkowskich uiszczonych przez członka związku zawodowego. W przypadku składek

potrącanych przez pracodawcę, dowodem wpłaty składek członkowskich na rzecz związku zawodowego jest oświadczenie organizacji związkowej o wysokości pochodzących od podatnika składek. Organizacje związkowe stoją na stanowisku, że aby wywiązać się z ciążącego na nich obowiązku, od 1 stycznia 2022 r. powinny prowadzić imienne ewidencje składek członkowskich wpłacanych na rzecz organizacji związkowej za pośrednictwem pracodawcy. Mając jednak na uwadze dotychczasowe stanowisko UODO (Newsletter, sierpień 2021 r.), powstały wątpliwości, czy w świetle ww. przepisów pracodawca na wniosek organizacji związkowej może przekazać informacje o wysokości składek związkowych za dany rok konkretnego pracownika w celach związanych z odliczeniem składki członkowskiej.

Stanowisko UODO zaprezentowane w Newsletterze dla IOD nr 8/2021 zostało przygotowane na podstawie obowiązujących wówczas przepisów prawa. Uprawnienie związku zawodowego do pozyskania od pracodawcy określonych informacji, niezbędnych do prowadzenia działalności związkowej, wynika z art. 28 ustawy o związkach zawodowych. Tak jak zostało wskazane w stanowisku, do niezbędnych informacji, o których mowa w art. 28, należy również zaliczyć to, czy dana osoba opłaciła składkę członkowską, czy też nie. W związku z tym pracodawca może przekazać do związku zawodowego listę wymienionych z imienia i nazwiska osób wraz z informacją, czy składka członkowska została odprowadzona.

Co zaś do udostępnienia informacji o wysokości odprowadzonej składki, to w ww. materiale wskazaliśmy, że istotny jest sposób jej ustalania. Jeżeli składka jest stała i jednakowa dla wszystkich członków, to pracodawca na żądanie związku zawodowego powinien przekazać mu listę zawierającą imię i nazwisko pracownika wraz z wysokością opłaconej składki. Jeśli jednak wysokość składki jest określana jako konkretny procent od wysokości wypłacanego wynagrodzenia, to jej ujawnienie może pośrednio doprowadzić do ujawnienia informacji o wysokości wynagrodzenia pracownika, a więc danych, do pozyskiwania których związek zawodowy nie jest uprawniony. W tej sytuacji podstawą uprawniającą pracodawcę do przekazania związkowi zawodowemu imienia i nazwiska pracownika wraz z wysokością odprowadzonej w jego imieniu składki, powinna być zgoda osoby, której dane dotyczą.

Ustawą z dnia 29 października 2021 r. o zmianie ustawy o podatku dochodowym od osób fizycznych, ustawy o podatku dochodowym od osób prawnych oraz niektórych innych ustaw dokonano zmiany w ustawie o podatku dochodowym od osób fizycznych poprzez wprowadzenie nowego odliczenia od dochodu, dotyczącego składek zapłaconych na rzecz związków zawodowych przez członków tych organizacji. Odliczeniu będą podlegać zapłacone w roku podatkowym składki członkowskie na rzecz związku zawodowego, udokumentowane dowodem wpłaty.

Jak wskazano w art. 26 ust. 7 pkt 5 ustawy o podatku dochodowym od osób fizycznych, wysokość wydatków będzie ustalana na podstawie dowodu wpłaty, z którego wynikają co najmniej: dane

identyfikujące członka związku zawodowego dokonującego wpłaty składek, organizacja związkowa, na rzecz której zapłacono składki, tytuł wpłaty i data oraz kwota składek, **a w sytuacji gdy pracodawca pośredniczy w przekazywaniu składek członkowskich pomiędzy związkowcem a związkiem zawodowym – na podstawie oświadczenia organizacji związkowej o wysokości pochodzących od podatnika składek.**

Przywołany wyżej przepis nie wprowadza obowiązku prowadzenia przez związki zawodowe imiennej ewidencji składek członkowskich wpłacanych na rzecz organizacji związkowej za pośrednictwem pracodawcy. Intencją prawodawcy było wprowadzenie możliwości odliczenia od dochodu składek uiszczanych przez związkowca (podatnika) na rzecz organizacji związkowej. Jest to uprawnienie podatnika, który może, ale nie musi z tego uprawnienia skorzystać.

Dlatego też obowiązek prawny nałożony na organizację związkową do wydania oświadczenia o wysokości pochodzącej od podatnika składki, ziści się wówczas, kiedy podatnik (związkowiec) zechce z tego rodzaju uprawnienia skorzystać oraz w sytuacji, gdy pracodawca pośredniczy w przekazywaniu składek członkowskich pomiędzy związkowcem a związkiem zawodowym. Wtedy to organizacja związkowa w celu realizacji nałożonego na nią obowiązku może pozyskać dane od pracodawcy w zakresie dotyczącym wysokości pochodzących od danego związkowca (podatnika) składek, o ile takich danych już nie posiada. W tym przypadku przetwarzanie danych (udostępnianie) przez pracodawcę odbywa się w związku z realizacją obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, zgodnie z art. 9 ust. 2 lit. b RODO.

Data wytworzenia informacji: 16.02.2022 r.

Czy OPS może weryfikować źródła ogrzewania z CEEB przy rozpatrzeniu wniosku o dodatek osłonowy?

Czy w celu rozpatrzenia wniosku o dodatek osłonowy OPS może weryfikować fakt zgłoszenia źródła ogrzewania do CEEB?

W związku z wejściem w życie ustawy o dodatku osłonowym ośrodek pomocy społecznej (któremu powierzono rozpatrywanie wniosków o dodatek osłonowy) zwrócił się do prezydenta miasta z pytaniem o możliwość weryfikacji oświadczeń złożonych przez osoby wnioskujące o dodatek osłonowy w wyższej wysokości poprzez porównanie ich z danymi zawartymi w bazie centralnej ewidencji emisyjności budynków (CEEB). Czy są podstawy prawne do dokonywania takiej weryfikacji?

Co do zasady wszelkie działania podejmowane przez podmioty publiczne (w tym ośrodki pomocy społecznej i gminy) powinny mieć oparcie w obowiązujących przepisach prawa regulujących ich

działalność. Wobec tego podstawa prawna do przetwarzania (w tym udostępniania i pozyskiwania) danych osobowych przez takie podmioty również powinna wynikać z przepisów prawa i być związana z realizowanymi przez nie zadaniami. Warto też pamiętać, że z uwagi na określoną w art. 7 Konstytucji RP zasadę działania organów publicznych na podstawie i w granicach prawa, organ publiczny nie może domniemywać swoich kompetencji, jeśli nie wynika to wprost z przepisu prawa.

Zasady i tryb przyznawania, ustalania wysokości i wypłacania dodatku osłonowego oraz właściwość organów w tych sprawach reguluje ustawa z dnia 17 grudnia 2021 r. o dodatku osłonowym.

Zgodnie z jej art. 3 ust. 1 wypłata dodatku osłonowego jest zadaniem z zakresu administracji rządowej, a dodatek osłonowy wypłacają gminy. Stosownie zaś do art. 2 ust. 11 ww. ustawy dodatek osłonowy przyznaje wójt, burmistrz lub prezydent miasta.

Artykuł 2 ust. 14 ustawy o dodatku osłonowym w związku z art. 411 ust. 10r ustawy Prawo ochrony środowiska przyznaje wójtowi (burmistrzowi lub prezydentowi miasta) kompetencję do przekazania realizacji zadania związanego z przyznawaniem dodatku osłonowego kierownikowi ośrodka pomocy społecznej (dyrektorowi centrum usług społecznych).

Dodatek osłonowy przysługuje osobie spełniającej kryteria dochodowe określone w art. 2 ust. 1 ww. ustawy.

Zgodnie natomiast z art. 2 ust. 6 ww. ustawy dodatek osłonowy w wyższej wysokości może być wypłacony w przypadku, gdy głównym źródłem ogrzewania gospodarstwa domowego jest: kocioł na paliwo stałe, kominek, koza, ogrzewacz powietrza, trzon kuchenny, piecokuchnia, kuchnia węglowa lub piec kaflowy na paliwo stałe, zasilane węglem lub paliwami węglopochodnymi, **zgłoszone do centralnej ewidencji emisyjności budynków (CEEB)**, o której mowa w art. 27a ust. 1 ustawy z dnia 21 listopada 2008 r. o wspieraniu termomodernizacji i remontów oraz o centralnej ewidencji emisyjności budynków.

W związku z tym częścią wniosku o dodatek osłonowy, którego wzór określony został w rozporządzeniu Ministra Klimatu i Środowiska z dnia 9 lutego 2022 r., jest m.in. oświadczenie wnioskodawcy, że spełnia ww. warunki.

Z przepisów ustawy o dodatku osłonowym oraz powyższego rozporządzenia nie wynika obowiązek załączania przez wnioskodawcę żadnych dokumentów potwierdzających to oświadczenie. Z przepisów tych nie wynika też wprost uprawnienie dla pomiotu rozpatrującego wniosek o dodatek osłonowy do weryfikacji faktu zgłoszenia ww. źródeł ogrzewania do CEEB.

Niektórzy administratorzy takiej podstawy dopatrują się w **art. 25 ust. 3** ustawy o świadczeniach rodzinnych, zgodnie z którym osoby otrzymujące świadczenia rodzinne, instytucje publiczne i organizacje pozarządowe są obowiązane do udzielania, na żądanie organu właściwego lub

wojewody, wyjaśnień oraz informacji co do okoliczności mających wpływ na prawo do świadczeń rodzinnych.

Ww. przepis stosuje się odpowiednio do postępowania w sprawie dodatku osłonowego na podstawie odesłania zawartego w **art. 2 ust. 14 ustawy o dodatku osłonowym,** a następnie odesłania z **art. 411 ust. 10n pkt 2** ustawy Prawo ochrony środowiska.

Należy jednak zwrócić uwagę, że zgodnie z art. 2 ust. 14 ustawy o dodatku osłonowym, przepisy art. 411 ust. 10j-10o oraz 10r ustawy z dnia 27 kwietnia 2001 r. - Prawo ochrony środowiska, a co za tym idzie również powołany wyżej art. 25 ust. 3 ustawy oświadczeniach rodzinnych stosuje się odpowiednio do **ustalenia** przez wójta, burmistrza lub prezydenta miasta **prawa do dodatku osłonowego, o którym mowa w art. 2 ust. 1 ustawy o dodatku osłonowym**.

Zgodnie natomiast z art. 2 ust. 1 ustawy o dodatku osłonowym, dodatek ten przysługuje osobom spełniającym kryteria **przeciętnego miesięcznego dochodu** w rozumieniu art. 3 pkt 1 ustawy z dnia 28 listopada 2003 r. o świadczeniach rodzinnych. Przepis ten (art. 2 ust. 1) odnosi się zatem wyłącznie do kryterium dochodowego, jakie należy spełnić, aby otrzymać dodatek osłonowy.

Wobec tego biorąc pod uwagę treść powołanych powyżej przepisów ustawy o dodatku osłonowym stwierdzić należy, że zawarte w art. 2 ust. 14 ustawy o dodatku osłonowym odesłanie do ww. przepisów (w tym art. 25 ust. 3 ustawy o świadczeniach rodzinnych) stosuje się wyłącznie do ustalenia przez wójta, burmistrza lub prezydenta miasta prawa do dodatku osłonowego, ale wyłącznie w zakresie ustalenia spełnienia kryterium dochodowego (o którym mowa w art. 2 ust. 1). Odesłania tego nie można zatem stosować do weryfikacji kryterium określonego w art. 2 ust. 6 ustawy o dodatku osłonowym, tj. kryterium posiadania określonego źródła ogrzewania zgłoszonego do CEEB.

Jednocześnie należy wskazać, że kwestia udostępniania informacji zgromadzonych w CEEB uregulowana jest w ustawie z dnia 21 listopada 2008 r. o wspieraniu termomodernizacji i remontów oraz o centralnej ewidencji emisyjności budynków. Zgodnie z jej art. 27d ust. 1 pkt 14 i pkt 16 dane i informacje zgromadzone w ewidencji udostępnia się, o ile są one niezbędne do realizacji ich ustawowych zadań, m.in.: ośrodkom pomocy społecznej lub centrom usług społecznych oraz wójtom, burmistrzom lub prezydentom miasta.

Należy jednak zauważyć, że ww. przepisy jeszcze nie obowiązują. Wejdą w życie z dniem wdrożenia rozwiązań technicznych, określonych w komunikacie ministra właściwego do spraw budownictwa, planowania i zagospodarowania przestrzennego oraz mieszkalnictwa, o którym mowa w art. 18 pkt 3 ustawy z dnia 28 października 2020 r. o zmianie ustawy o wspieraniu termomodernizacji i remontów oraz niektórych innych ustaw. Komunikat dotyczący wdrożenia rozwiązań technicznych umożliwiających udostępnianie danych i informacji z CEEB nie został dotychczas wydany.

Niezależnie od tego należy zauważyć, że przepisy powyższe normują udostępnianie danych zgromadzonych w CEEB, nie dotyczą natomiast zgłoszeń papierowych złożonych w gminach, a jeszcze niewprowadzonych do ewidencji.

Podsumowując: z powołanych powyżej przepisów prawa nie wynika uprawnienie dla podmiotu rozpatrującego wnioski o dodatek osłonowy (niezależnie od tego czy będzie to wójt, czy ośrodek pomocy społecznej) do weryfikowania faktu zgłoszenia źródła ogrzewania do CEEB.

Jednocześnie należy nadmienić, że w sytuacji, gdy podmioty stosujące w praktyce określone przepisy prawa dostrzegają, że przewidziane przez ustawodawcę unormowania są np. niewystarczające lub nieprecyzyjne, warto, aby sygnalizowały to właściwemu resortowi. Takie działania mogą przyczynić się do szybszego wprowadzenia niezbędnych zmian.

Data wytworzenia informacji: 16.03.2022 r.

Czy członkom wspólnoty mieszkaniowej można udostępnić dane innych jej członków?

Czy członkom wspólnoty mieszkaniowej można udostępnić dane innych jej członków?

Czy przekazanie członkom wspólnoty mieszkaniowej treści uchwał z podpisami członków wspólnoty stanowi naruszenie przepisów o ochronie danych osobowych? Według mojej oceny przekazywanie takich danych we wspólnocie mieszkaniowej jest niezbędne do wypełnienia obowiązku prawnego ciążącego na wspólnocie – wynikającego z ustawy o własności lokali oraz Kodeksu cywilnego. Ponadto zgodnie z ustawą o własności lokali każdy z właścicieli ma prawo zaskarżyć uchwałę do sądu. Wobec tego musi mieć możliwość skontrolowania, czy dana uchwała została podjęta w sposób prawidłowy. Musi też być poinformowany o jej podjęciu i sposobie głosowania.

Członkowie wspólnoty mieszkaniowej dla prawidłowego zarządzania współwłasnością **muszą znać dane osobowe pozostałych współwłaścicieli**. Członkowie wspólnoty mieszkaniowej mają prawo dostępu do danych osobowych pozostałych członków **w zakresie niezbędnym do wykonywania zarządu nieruchomością wspólną.**

Odnosząc się do zagadnienia dotyczącego przekazywania treści uchwał z podpisami członków wspólnoty wskazać należy, że przepisy prawa nie określają szczegółowo elementów treści uchwały. Niemniej zgodnie z art. 23 ust. 2 ustawy z dnia 24 czerwca 1994 r. o własności lokali, uchwały zapadają większością głosów właścicieli lokali, liczoną według wielkości udziałów, chyba że w umowie lub w uchwale podjętej w tym trybie postanowiono, że w określonej sprawie na każdego właściciela przypada jeden głos. Na podstawie zaś art. 23 ust. 3 tej ustawy, o treści

uchwały, która została podjęta z udziałem głosów zebranych indywidualnie, każdy właściciel lokalu powinien zostać powiadomiony na piśmie.

Jak słusznie wskazano w pytaniu, ma to o tyle znaczenie, że zgodnie z art. 25 ust. 1 ustawy o własności lokali właściciel lokalu może zaskarżyć uchwałę do sądu z powodu jej niezgodności z przepisami prawa lub z umową właścicieli lokali albo jeśli narusza ona zasady prawidłowego zarządzania nieruchomością wspólną lub w inny sposób narusza jego interesy. Powództwo w tym zakresie może być wytoczone przeciwko wspólnocie mieszkaniowej, w terminie 6 tygodni od dnia podjęcia uchwały na zebraniu ogółu właścicieli lokali albo od dnia powiadomienia wytaczającego powództwo o treści uchwały podjętej w trybie indywidualnego zbierania głosów (ust. 1a tego przepisu).

Sąd Okręgowy w Świdnicy w wyroku z 27 listopada 2018 r. (sygn. akt I C 1465/18) wyjaśnił, że niezgodność z przepisami prawa to przede wszystkim kolizja treści uchwały z przepisami ustawy oraz z przepisami Kodeksu cywilnego w zakresie, w jakim ma on zastosowanie do odrębnej własności lokali. Niezgodność uchwały z prawem może wynikać nie tylko z treści uchwały, ale także z powodu **wadliwości postępowania prowadzącego do podjęcia uchwały**. Oznacza to, że właściciel lokalu może podnosić obok zarzutów merytorycznych, również i zarzuty formalne, jeżeli uważa, że zostały naruszone przepisy postępowania określające tryb podejmowania uchwał we wspólnocie mieszkaniowej. Uchybienia mogą dotyczyć np. zasad głosowania. Jak pokazuje orzecznictwo, błędy dotyczące zasad głosowania mogą dotyczyć przykładowo: oddania głosu przez osobą inną niż właściciel, oddania głosu tylko przez jednego ze współwłaścicieli czy też nieprawidłowej reprezentacji podmiotu będącego członkiem wspólnoty. Błędy te z kolei mogą mieć wpływ przy ustalaniu ważności oddanego głosu i skuteczności podjęcia uchwały większością głosów.

W świetle wyżej wskazanego uprawnienia przekazanie członkowi wspólnoty mieszkaniowej treści uchwały wspólnoty mieszkaniowej wraz z podpisami jej członków nie może być zatem traktowane jako naruszenie przepisów o ochronie danych osobowych.

Jednocześnie należy pamiętać, że udostępnianie danych osobowych członków wspólnoty w zakresie szerszym niż konieczny do sprawowania zarządu nieruchomością wspólną może stanowić naruszenie przepisów o ochronie danych osobowych (zob. Sprawozdanie z działalności Generalnego Inspektora Ochrony Danych Osobowych w roku 2017, str. 44). W świetle przepisów RODO administrator jest zobowiązany do przetwarzania danych osobowych w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem. Przetwarzanie danych osobowych musi być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których te dane są przetwarzane (art. 5 ust. 1 lit. c RODO).

Data wytworzenia informacji: 16.03.2022 r.

Czy prawo dostępu do danych osobowych można realizować przez pełnomocnika?

Do placówki medycznej, w której pełnię funkcję IOD, wpływają wnioski dotyczące realizacji prawa określonego w art. 15 RODO. Są one składane przez pełnomocników osób, których dane dotyczą. Pracownicy, którzy zajmują się ich rozpatrywaniem, mają wątpliwości, czy mogą realizować wnioski dotyczące prawa dostępu do danych osobowych zgłaszane nie przez osobę, której dane dotyczą.

RODO nie odnosi się do kwestii wykonywania prawa dostępu do danych osobowych określonego w art. 15 RODO przez inną osobę niż ta, której dotyczy wniosek kierowany do administratora. Nie oznacza to jednak, by możliwość realizacji prawa dostępu danych osobowych przez pełnomocnika była wyłączona.

Rozpatrując przedstawione zagadnienie należy przede wszystkim wziąć pod uwagę treść art. 12 ust. 1 i 2 RODO wskazującego na konieczność łatwej dostępności do informacji na temat przetwarzania danych (zasada przejrzystości) oraz ułatwiania wykonywania praw osoby, której dane dotyczą, w tym prawa określonego w art. 15 RODO. Zgodnie z motywem 63 RODO: „Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem”.
Z powyższego wnioskować można, że „możliwość łatwego wykonywania prawa dostępu do danych osobowych” oznacza również wykonywanie tego prawa przez pełnomocnika.

Z tych samych powodów należy przyjąć, że nie jest tu wymagane pełnomocnictwo (upoważnienie) mające szczególną formę. Niemniej treść pełnomocnictwa powinna pozwolić na weryfikację, kto złożył oświadczenie uprawniające inną osobę do działania w jej imieniu.

Europejska Rada Ochrony Danych (EROD) w projekcie wytycznych nr 1/2022 w sprawie praw osób, których dane dotyczą – prawo dostępu w rozdziale 3.4 pt.„Requests made via third parties / proxies”[21] wskazała, że z prawa dostępu do danych osobowych najczęściej korzystają osoby, których dane dotyczą, jednak dopuścić należy również możliwość złożenia wniosku w imieniu osoby, której dane dotyczą np. przez pełnomocnika. Zgodnie ze wskazówkami znajdującymi się w powyższym projekcie wytycznych, w przypadku gdy wniosek nie jest składany przez osobę, której dane dotyczą, należy wziąć pod uwagę przepisy krajowe dotyczące działania przez pełnomocnika/

[21] Projekt wytycznych w wersji angielskiej przed konsultacjami publicznymi 1/2022 znajduje się pod następującym linkiem: https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-012022-data-subject-rights-right_pl (Dostęp do wytycznych z dnia 11 marca 2022 r.). Natomiast wersja wytycznych po konsultacjach publicznych będzie dostępna pod następującym linkiem: https://edpb.europa.eu/our-work-tools/general-guidance/guidelines-recommendations-best-practices_pl

przedstawiciela ustawowego — w celu sprawdzenia, czy osoba ta jest prawidłowo umocowana i czy może występować w imieniu osoby, której dane dotyczą.

W doktrynie prezentowane jest stanowisko tożsame z tym, które prezentuje EROD w projekcie ww. wytycznych. Jeden z jej przedstawicieli wskazuje, że uprawnienia przyznane na podstawie art. 15 RODO mogą być również „realizowane przez podmiot danych zarówno osobiście, jak i przez jego przedstawiciela ustawowego czy pełnomocnika”[22].

W przypadku rozpatrywania wniosku na podstawie art. 15 RODO przez podmioty z sektora medycznego (np. szpitale) należy zwrócić uwagę, iż dostęp do danych osobowych będzie obejmował również dane dotyczące zdrowia, a więc dane szczególnej kategorii. Jak wyjaśnia się w motywie 63 RODO, prawo określone w art. 15 RODO obejmuje „prawo dostępu osób, których dane dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania”.

Z treści pełnomocnictwa dotyczącego wykonania prawa dostępu do danych osobowych w imieniu innej osoby powinno wynikać, iż obejmuje ono realizację prawa dostępu do danych osobowych przetwarzanych przez konkretnego administratora bądź kategorię administratorów przetwarzających dane o stanie zdrowia (np. szpitale, przychodnie).

Ważne jest też ustalenie, czy pełnomocnictwo (upoważnienie) obejmuje działanie do realizacji praw przysługujących podmiotowi danych na mocy RODO czy innej ustawy (np. ustawa z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta). Należy odróżnić sytuację, gdy wniosek o realizację prawa określonego w art. 15 RODO jest składany przez osobę, która została umocowana do takiego działania w imieniu innej osoby, od sytuacji, gdy osoba działa na podstawie upoważnienia, o którym mowa w art. 26 ust. 1 ustawy z dnia 6 listopada 2008 r. o prawach pacjenta i Rzeczniku Praw Pacjenta. W myśl tego przepisu podmiot udzielający świadczeń zdrowotnych udostępnia dokumentację medyczną pacjentowi lub jego przedstawicielowi ustawowemu, bądź osobie upoważnionej przez pacjenta.

Kolejną ważną kwestią jest weryfikacja tożsamości zarówno osoby, która składa pełnomocnictwo, jak również osoby, której danych dotyczy wniosek. EROD w ww. projekcie wytycznych zwróciła

[22] J. Łuczak [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 15

uwagę, że udostępnienie danych osobowych osobie, która nie jest uprawniona do dostępu do nich, może stanowić naruszenie ochrony danych osobowych. RODO w motywie 64 wskazuje, że administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Zasadę tę należy odnieść również do weryfikacji tożsamości pełnomocnika osoby, której dane dotyczą. (zob. W JAKI SPOSÓB IDENTYFIKOWAĆ OSOBY, KTÓRE ZWRACAJĄ SIĘ DO IOD JAKO PUNKTU KONTAKTOWEGO?).

Jak wynika z brzmienia motywu 59 RODO administrator powinien przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy RODO, w tym mechanizmy żądania - i gdy ma to zastosowanie bezpłatnego uzyskiwania - w szczególności dostępu do danych osobowych. Wobec powyższego administrator powinien zastanowić się, w jaki sposób będzie obsługiwał wnioski osób, których dane dotyczą, w tym, jak będzie weryfikować, czy osoba, która składa wniosek w imieniu innej osoby jest umocowana do złożenia wniosku o dostęp do danych na podstawie art. 15 RODO (np. jakie dane będą niezbędne do ustalenia tożsamości osoby, której dane dotyczą, jak również jej pełnomocnika).

W ww. projekcie wytycznych EROD zwróciła uwagę na jeszcze jedną istotną kwestię. Celem prawa dostępu do danych osób, których dane dotyczą, jest zapewnienie osobom fizycznym wystarczających, przejrzystych i łatwo dostępnych informacji o przetwarzaniu ich danych osobowych, tak aby osoby te mogły być świadome i weryfikować zgodność z prawem przetwarzania oraz dokładność przetwarzanych danych. Realizowanie prawa określonego w art. 15 RODO przez pełnomocnika stanowić może gwarancję, że prawa tego nie zostaną pozbawione osoby, które nie mogą go wykonać ze względu na swój stan zdrowia. Natomiast uznanie, iż prawo dostępu do danych może być realizowane wyłącznie osobiście byłoby dla podmiotu danych nieuzasadnionym ograniczeniem w szczególności w sytuacji, gdy z przyczyn obiektywnych nie mógłby tego prawa zrealizować (m.in. z uwagi na stan zdrowia albo brak umiejętności i z tego powodu potrzebne byłoby działanie przez pełnomocnika).

Data wytworzenia informacji: 07.04.2022 r.

Czy szkoła może udostępnić CUW kopię rejestru czynności przetwarzania?

Uchwałą rady miasta powołane zostało centrum usług wspólnych (CUW) w celu świadczenia usług na rzecz jednostek obsługiwanych – m.in. wszystkich szkół w mieście. Do zadań Centrum należy m.in. świadczenie usług i wdrażanie standardów z zakresu informatyki dla jednostek obsługiwanych, jak również wspieranie rozwoju i dostępu do infrastruktury informatycznej, w tym pomoc przy tworzeniu i częściowej obsłudze stron internetowych obsługiwanych

jednostek, zakładanie poczty służbowej pracownikom jednostek, pomoc techniczna przy obsłudze programów. Z treści przedstawionego przez CUW do podpisu projektu porozumienia wynika, że szkoła powierza Centrum przetwarzanie danych osobowych. Natomiast moje wątpliwości budzi zakres dokumentów wymienionych w jednym z załączników do ww. porozumienia, które szkoła jest zobowiązana przekazać do Centrum, a mianowicie wyciąg z rejestru czynności przetwarzania. Pracownik CUW udzielił informacji, że Centrum będzie przygotowywać ujednolicony rejestr czynności przetwarzania. W związku z powyższym uprzejmie proszę o udzielenie odpowiedzi, czy szkoła powinna przekazać do Centrum wyciąg z rejestru czynności przetwarzania oraz kopię rejestru zbiorów?

W pierwszej kolejności warto wskazać, że przepisy RODO nie przewidują obowiązku udostępniania poprzez administratora podmiotowi przetwarzającemu prowadzonego przez niego rejestru czynności przetwarzania. Z art. 30 ust. 4 RODO (motywu 82 RODO) wynika, że takie rejestry mają być udostępniane jedynie na żądanie organu nadzorczego. Ponadto zgodnie z art. 29 RODO, podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego.

Niemniej może zaistnieć sytuacja, kiedy informacje zawarte w rejestrze w całości bądź w ograniczonym zakresie są potrzebne podmiotowi przetwarzającemu do realizacji powierzonych mu zadań z uwagi na charakter tych zadań. W przedstawionej sprawie nie jest jednak jasne, na jakiej podstawie oraz w jakim celu miałby powstać „ujednolicony rejestr czynności przetwarzania" i kto miałby z niego korzystać, a także dla jakich zadań podmiotu przetwarzającego konieczne było udostępnienie takiego rejestru. Nie jest też wiadome, na czym ma polegać ujednolicenie rejestru czynności przetwarzania. Jeżeli miałby powstać jedynie ujednolicony szablon rejestru, to do tego celu nie jest potrzebne przekazywanie zawartości poszczególnych pól rejestru. A zatem ostateczne przesądzenie, czy i w jakim zakresie istnieje konieczność udostępnienia rejestru czynności przetwarzania wymagałoby wyjaśnienia powyższych okoliczności w kontekście zadań CUW określonych m.in. w uchwale rady miasta dotyczącej powołania CUW.

W przedstawionej sytuacji celowe byłoby dokładne omówienie i ustalenie przez strony zawieranego porozumienia wszystkich kwestii, w tym tych budzących wątpliwości czy też wymagających uzupełnienia. Takie działania pozwolą na wyeliminowanie wątpliwości i wypracowanie dokumentu spełniającego wymogi określone przepisami RODO.

Na zakończenie warto zwrócić uwagę, że przewidziana w RODO zasada rozliczalności wymaga, aby administratorzy wykazywali logikę, na której oparli swoje decyzje, i potrafili uzasadnić, dlaczego przyjęli określone rozwiązania. Pomocne w takich sytuacjach jest przeprowadzanie

starannych analiz i ocen w zakresie podejmowanych rozstrzygnięć, a w uzasadnionych przypadkach - ich udokumentowanie.

Data wytworzenia informacji: 07.04.2022 r.

W jakim języku należy wypełnić obowiązek informacyjny?

Wśród administratorów, których obsługuję jako IOD, pojawiają się wątpliwości, w jakim języku powinny być formułowane klauzule informacyjne kierowane do obywateli Ukrainy w kontekście pozyskiwania od nich danych osobowych, np. w związku z przyjęciem do szkoły? Czy wszystkie klauzule informacyjne funkcjonujące w szkole należy przetłumaczyć na język ukraiński (np. klauzula dot. monitoringu wizyjnego, ogólna klauzula informacyjna, klauzula dot. udostępniania danych na podstawie zgody)? W jaki sposób i przez kogo klauzule te powinny zostać przetłumaczone, czy konieczne jest tłumaczenie przysięgłe?

Wypełniając obowiązek informacyjny, należy wziąć pod uwagę zasadę przejrzystości. Została ona wyrażona w art. 5 ust. 1 lit. a RODO, a rozwinięta w art. 12 ust. 1 RODO. Zgodnie z drugim z wymienionych przepisów administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności, gdy informacje są kierowane do dziecka – udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

Powyższa zasada wraz z zasadami zgodnego z prawem i rzetelnego przetwarzania (art. 5 ust. 1 lit. a RODO) nie bez powodu zajmuje pierwszą pozycję w katalogu zasad dotyczących przetwarzania danych osobowych (więcej o zasadzie przejrzystości: „Obowiązek informacyjny" - szkolenie dla IOD, 28 lutego 2019 r.). W praktyce oznacza ona, że osoba, której dane dotyczą, powinna zostać poinformowana o podjęciu operacji przetwarzania i jej celach, a także o ryzyku, zasadach, zabezpieczeniach i prawach związanych z przetwarzaniem danych osobowych.

Dlatego, jeżeli administrator przetwarza dane osób nieposługujących się językiem polskim, powinien zapewnić, aby klauzule informacyjne były dla nich zrozumiałe, czyli sporządzone w języku, jakiego zwykle używa w komunikacji z tymi osobami. Grupa Robocza Art. 29 w Wytycznych w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP260 rev. 01 (zob: Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679, WP260 rev.01) wskazała, że „jeżeli administrator kieruje informacje do osób, których dane dotyczą i które posługują się innym językiem lub innymi językami, należy zapewnić tłumaczenie w tym języku lub tych językach".

W przypadku, gdy administrator przetwarza dane wielu osób posługujących się różnymi językami możliwym rozwiązaniem jest stworzenie - oprócz klauzuli informacyjnej w języku polskim - klauzuli informacyjnej w języku uniwersalnym takim, jak np. język angielski. W sytuacji gdy administrator będzie przetwarzał dane obywateli jednego kraju, np. Ukrainy, powinien zapewnić, aby informacje, o których mowa w art. 13 lub 14 RODO były przekazywane tym osobom w języku dla nich zrozumiałym.

Brak jest przepisów prawa, które wskazywałyby, w jaki sposób powinny zostać przetłumaczone klauzule informacyjne. Jednakże - jak wskazała Grupa Robocza Art. 29 w ww. Wytycznych w sprawie przejrzystości (str. 11) - jeżeli informacje są tłumaczone na język obcy, administrator danych powinien zapewnić, by wszystkie tłumaczenia były wierne oraz by frazeologia i składnia tekstów w języku obcym były zrozumiałe, tak by nie trzeba było rozszyfrowywać znaczenia przetłumaczonego tekstu lub dokonywać jego reinterpretacji. Administrator jest zobowiązany podejmować odpowiednie decyzje co do szczegółowych, przyjmowanych w konkretnej organizacji rozwiązań.

Analogicznie należy się odnieść do pytania, które klauzule powinny być przetłumaczone, ponieważ zależy to od tego, w jakich rzeczywistych celach dane osobowe Ukraińców będą przetwarzane. Również i w tym zakresie administrator musi dokonać analizy i oceny, uwzględniając konkretne okoliczności przetwarzania danych oraz wyżej wskazane zasady rzetelności, zgodności z prawem i przejrzystości. W dużej mierze zależy to od tego, jakie zadania administrator realizuje i jakie dane oraz jakiej kategorii osób - w związku z tymi zadaniami - przetwarza.

Data wytworzenia informacji: 07.04.2022 r.

Czy administrator może przerzucać swoje obowiązki na IOD?

Rolą IOD jest wspieranie administratora w przestrzeganiu i właściwym stosowaniu przepisów o ochronie danych osobowych. Czy administrator może przerzucać swoje obowiązki wynikające z RODO na IOD? Czy IOD może wyręczać administratora w realizacji jego zadań?

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). 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.

Potwierdzeniem powyższego jest jedna z decyzji, w której organ nadzorczy udzielił upomnienia podmiotowi, który zobowiązał IOD do nadawania pracownikom upoważnień do przetwarzania danych osobowych (sygn. sprawy ZWAD.405.31.331.2019).

W decyzji tej wskazano, 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 RODO, niemniej jednak zgodnie z art. 38 ust. 6 RODO 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) RODO, doprowadziłoby w efekcie do sytuacji, gdzie IOD sprawowałby nadzór nad własną działalnością, a więc do konfliktu interesów, czego wprost zakazuje art. 38 ust. 6 RODO. 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 RODO. 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 RODO, 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 RODO, 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 RODO. 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".

Na niewłaściwość takiej praktyki, jako powodującej konflikt interesów, zwracaliśmy uwagę również w zamieszczonej na stronie internetowej urzędu odpowiedzi na pytanie „CZY IOD MOŻE NADAWAĆ UPOWAŻNIENIA?". Wskazujemy tam, 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 osobą 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 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".

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.

Więcej wskazówek dotyczących zadań IOD znaleźć można ponadto w odpowiedziach na następujące pytania:

- JAKIE ZADANIA MA IOD?

- KTO POWINIEN OPRACOWAĆ WEWNĘTRZNĄ POLITYKĘ OCHRONY DANYCH OSOBOWYCH? ADMINISTRATOR CZY IOD?
- CZY PROWADZENIE REJESTRU CZYNNOŚCI POWINNO BYĆ ZALICZANE DO ZADAŃ IOD?
- CZY IOD POWINIEN SPORZĄDZIĆ PLAN AUDYTÓW?
- CZY NARUSZENIE PRZEPISÓW ODNOSZĄCYCH SIĘ DO IOD MOŻE SKUTKOWAĆ ADMINISTRACYJNYMI KARAMI PIENIĘŻNYMI?

Data wytworzenia informacji: 10.05.2022 r.

Czy okręgowa izba inżynierów budownictwa może udostępnić inwestorowi dane projektanta?

Pełnię funkcję IOD w okręgowej izbie samorządu zawodowego inżynierów budownictwa. Izba otrzymuje wnioski od inwestorów o udostępnienie danych projektantów (członków izby samorządu zawodowego). Jako uzasadnienie inwestorzy wskazują brak możliwości kontaktu z projektantem. Zastanawiam się, czy w takiej sytuacji izba może udostępnić dane projektanta.

Każdy wniosek o udostępnienie danych osobowych wymaga indywidualnej analizy. Rozpatrujący go administrator, który podejmuje ostateczną decyzję w tej sprawie, musi wziąć pod uwagę konkretne okoliczności faktyczne i prawne, w tym obowiązujące przepisy prawa, rodzaj danych osobowych, cel oraz uzasadnienie potrzeby posiadania danych przez podmiot, który występuje o ich udostępnienie.

Zgodnie z art. 20 ust. 1 pkt 3 ustawy z dnia 7 lipca 1994 r. Prawo budowlane do podstawowych obowiązków projektanta należy wyjaśnianie wątpliwości dotyczących projektu i zawartych w nim rozwiązań. Projektant pełni zatem istotną rolę w procesie budowlanym, a możliwość łatwego kontaktu z nim jest nieodzownym elementem prawidłowego wykonania projektu budowlanego. Jak wskazuje się w doktrynie, „Rola projektanta jako uczestnika procesu budowlanego w zakresie wyjaśniania wątpliwości dotyczących projektu i zawartych w nim rozwiązań trwa już od chwili podjęcia czynności przygotowawczych związanych z wystąpieniem o pozwolenie na budowę (tj. od zawarcia umowy z inwestorem) przez postępowanie administracyjne o pozwolenie na budowę, a także w toku realizacji budowy i jej zakończenia. Nie można też wykluczyć, że również podczas użytkowania obiektu budowlanego, np. w razie potrzeby zmiany sposobu użytkowania obiektu związanej z dokonaniem robót budowlanych.” [23]

Ponadto w doktrynie zwraca się uwagę, że „Nałożenie w art. 20 ust. 1 pkt 3 na projektanta obowiązku wyjaśniania wątpliwości dotyczących projektu i zawartych w nim rozwiązań jest kolejnym przykładem modyfikacji wzajemnych obowiązków i uprawnień inwestora i projektanta

[23] A. Plucińska-Filipowicz, T. Filipowicz [w:] Prawo budowlane. Komentarz aktualizowany, red. M. Wierzbowski, LEX/el. 2021, art. 20

jako stron umowy o przygotowanie projektu w interesie publicznym, mianowicie po to, aby zapewnić udział czynnika fachowego także przy wykładni projektu budowlanego. Określony w komentowanym przepisie obowiązek projektanta jest niezależny od tego, czy został ujęty w umowie, odmowa zaś jego wykonania może być uznana za naruszenie obowiązków zawodowych projektanta i z tego powodu poddana sankcji administracyjnej na podstawie art. 95 pkt 4."[24]

Wobec powyższego w każdym przypadku, gdy inwestor wnosi do okręgowej izby samorządu budownictwa wniosek o przekazanie danych kontaktowych projektanta odpowiedzialnego za realizację projektu budowlanego, należy dokonać analizy, dlaczego inwestor prosi o te dane. Inwestor powinien uprawdopodobnić, czy utrudniony jest kontakt z projektantem i czy w związku z tym istnieje zagrożenie dla prawidłowej i bezpiecznej realizacji procesu budowlanego inwestora.

Do zadań samorządu zawodowego inżynierów budownictwa należy w szczególności sprawowanie nadzoru nad należytym i sumiennym wykonywaniem zawodu przez członków izb, reprezentowanie i ochrona interesów zawodowych swoich członków, ustalanie zasad etyki zawodowej i nadzór nad jej przestrzeganiem (art. 8 pkt. 1-3 ustawy z dnia 15 grudnia 2000 r. o samorządach zawodowych architektów oraz inżynierów budownictwa). Dodać należy, że okręgowa rada izby wykonuje zaś zadania samorządu zawodowego na obszarze działania izby, w tym prowadzi listę członków okręgowej izby (art. 19 ust. 1 pkt 8 ww. ustawy).

W kontekście powyższych zadań okręgowej izby inżynierów budownictwa oraz obowiązków projektanta jako członka tej izby, jak również jego obowiązków określonych w Prawie budowlanym należy uznać za zasadne udostępnienie danych projektanta przez ww. izbę samorządu zawodowego, gdy przeprowadzona przez nią ocena wykaże, że jest to konieczne dla prawidłowej realizacji procesu budowlanego.

Data wytworzenia informacji: 12.05.2022 r.

Na co zwrócić szczególną uwagę przy powierzeniu danych osobowych w sektorze medycznym?

W działalności podmiotów leczniczych, z którymi współpracuję jako IOD, zdarzają się wątpliwości co do potrzeby zawierania umowy powierzenia przetwarzania danych osobowych. Ponadto wątpliwości budzi, czy takie powierzenie przetwarzania powinno odpowiadać dodatkowym warunkom, skoro mamy do czynienia z sektorem medycznym.

Powierzenie przetwarzania danych osobowych powinno mieć miejsce wówczas, jeśli zewnętrzny podmiot przetwarza dane w imieniu administratora, w celach określonych przez administratora

[24] Z. Kostka [w:] Prawo budowlane. Komentarz, wyd. III, red. A. Gliniecki, Warszawa 2016, art. 20

i zgodnie z jego poleceniami i instrukcjami. W przypadku powierzenia przetwarzania danych to administrator musi legitymować się podstawą prawną do przetwarzania wynikającą z art. 6 lub art. 9 RODO oraz ponosi odpowiedzialność za zgodność tego przetwarzania z przepisami o ochronie danych osobowych, również w zakresie przetwarzania, które powierzył innemu podmiotowi. W motywie 79 RODO podkreślono, że ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora.

To, czy w danej sytuacji należy skorzystać z powierzenia przetwarzania danych wymaga przeprowadzenia analizy uwzględniającej przepisy prawa regulujące działalność podmiotów leczniczych oraz o stan faktyczny, w którym funkcjonują podmioty, pomiędzy którymi dochodzić będzie do przepływu danych. Na tej podstawie należy ustalić, jakie dane osobowe są przetwarzane, jakie zadania/cele są realizowane, do którego z podmiotów one należą, a w związku z tym, który podmiot decyduje o celach przetwarzania, a także, czy któryś z nich działa na zlecenie administratora i realizuje jego cele, czy też wspólnie ustalają cele i sposoby przetwarzania.

Ponadto, tak jak wskazujemy w odpowiedzi na pytanie CZY LEKARZOM NALEŻY NADAWAĆ UPOWAŻNIENIA?, jednym z warunków kwalifikowania danej relacji jako relacji administrator - podmiot przetwarzający jest posiadanie przez podmiot przetwarzający statusu odrębnego (zewnętrznego) podmiotu od administratora. Między innymi dlatego pracownicy i inne osoby, które działają pod bezpośrednim zwierzchnictwem administratora (na przykład tymczasowo zatrudnieni pracownicy) nie są podmiotami przetwarzającymi, ponieważ przetwarzają dane, będąc częścią organizacji administratora. Zgodnie z art. 29 RODO są one również związane instrukcjami administratora.

Gdy działalność jest wykonywana przez lekarza w siedzibie podmiotu leczniczego, na warunkach techniczno-organizacyjnych określonych przez ten podmiot i w związku z przetwarzaniem danych osobowych klientów podmiotu leczniczego jako świadczeniodawcy, dochodzi do quasi-zatrudnienia. Ponieważ działalność ta może być wykonywana wyłącznie w zakładzie leczniczym na podstawie kontraktu umowy z podmiotem leczniczym, stanowi ona substytut zatrudnienia. Inny słowy w sytuacji lekarza zatrudnionego na kontrakcie, tj. na podstawie umowy cywilnej, mamy do czynienia z relacją podobną do tej, jaka występuje w przypadku pracodawcy i pracownika. Lekarz nie ma wówczas statusu podmiotu odrębnego od administratora i nie należy go traktować ani jako osobnego administratora, ani jako podmiotu przetwarzającego. Niemniej w praktyce

podmiotów leczniczych mogą występować również inne modele współpracy. Dlatego ustalenie wzajemnych relacji pomiędzy podmiotami zawierającymi kontrakt powinno następować na podstawie analizy danego przypadku. Umowy cywilnoprawne, w zależności od uregulowań, mogą różnić się od siebie zarówno zakresem obowiązków, jak i stopniem zależności od podmiotu leczniczego.

Pytanie dotyczy podmiotów leczniczych, a zatem dodatkowo należy mieć na uwadze, że zgodnie z przepisami ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta (art. 24 ust. 5-7) w przypadku powierzenia przetwarzania danych osobowych zawartych w dokumentacji medycznej, poza warunkami przewidzianymi w art. 28 ust. 3 RODO muszą być spełnione dodatkowe wymagania wskazane w ww. ustawie:

1. realizacja tej umowy nie może powodować zakłócenia udzielania świadczeń zdrowotnych, w szczególności w zakresie zapewnienia, bez zbędnej zwłoki, dostępu do danych zawartych w dokumentacji medycznej,
2. podmiot, któremu powierzono przetwarzanie danych osobowych w związku z realizacją umowy o powierzeniu przetwarzania danych osobowych jest obowiązany do zachowania w tajemnicy informacji związanych z pacjentem uzyskanych w związku z realizacją tej umowy. Podmiot ten jest związany tajemnicą także po śmierci pacjenta,
3. w przypadku zaprzestania przetwarzania danych osobowych zawartych w dokumentacji medycznej przez podmiot, któremu powierzono takie przetwarzanie, w szczególności w związku z jego likwidacją, jest on zobowiązany do przekazania danych osobowych zawartych w dokumentacji medycznej podmiotowi, o którym mowa w ust. 1, który powierzył przetwarzanie danych osobowych.

W uzasadnieniu do wprowadzenia powyższych przepisów do ustawy o prawach pacjenta i Rzeczniku Praw Pacjenta wskazano: „w art. 24 ust. 4-6 wprowadzone zostały przepisy umożliwiające podmiotom udzielającym świadczeń zdrowotnych zawieranie umów z podmiotami zajmującymi się przechowywaniem i archiwizacją dokumentacji medycznej. W wielu przypadkach przechowywanie i archiwizowanie elektronicznej dokumentacji medycznej będzie wiązało się z dużymi nakładami inwestycyjnymi i technicznymi. W przypadku małych podmiotów wykonujących działalność leczniczą zlecenie ww. usług może być uzasadnione względami bezpieczeństwa i efektywności finansowej. Przechowywanie dokumentacji przez podmiot zewnętrzny nie będzie mogło wpływać na ograniczenie prawa pacjenta do dostępu do jego dokumentacji. Ponadto wprowadzono przepis regulujący postępowanie w przypadku zaprzestania, w tym także nagłego, działalności przez podmiot, który przetwarzał dane osobowe zawarte w dokumentacji medycznej, na podstawie umowy zawartej z podmiotem udzielającym świadczeń zdrowotnych.”

Dodać należy, że wiele pomocnych wskazówek w zakresie rozstrzygania kwestii statusu podmiotów zawierają Wytyczne Europejskiej Rady Ochrony Danych w sprawie pojęć administratora i podmiotu przetwarzającego na gruncie RODO. Szczególnie pomocny może okazać się schemat zamieszczony w załączniku nr 1, zawierający pytania ułatwiające dokonywanie tej oceny (robocze tłumaczenie Wytycznych).

Data wytworzenia informacji: 12.05.2022 r.