Uniwersytet Wrocławski

Mariusz Jabłoński, Marlena Sakowska-Baryła, Krzysztof Wygoda

Czy jesteśmy gotowi na stosowanie RODO?

Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej

Wrocław 2018

Czy jesteśmy gotowi na stosowanie RODO?

Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej

Prace Naukowe
Katedry Prawa Konstytucyjnego
Wydziału Prawa, Administracji i Ekonomii
Uniwersytetu Wrocławskiego

Seria: **eMonografie Katedry Prawa Konstytucyjnego** Nr 2

Dostęp online: http://www.bibliotekacyfrowa.pl/publication/100568

Czy jesteśmy gotowi na stosowanie RODO?

Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej

Mariusz Jabłoński
Uniwersytet Wrocławski
https://orcid.org/0000-0001-8347-1884

Marlena Sakowska-Baryła
SBC Kancelaria Radców Prawnych
https://orcid.org/0000-0002-3982-976X

Krzysztof Wygoda
Uniwersytet Wrocławski
https://orcid.org/0000-0002-0997-5512

Wrocław 2018

Publikacja ukazała się dzięki finansowemu wsparciu
Urzędu Marszałkowskiego Województwa Dolnośląskiego

Recenzent: *prof. zw. dr hab. Andrzej Szmyt, Wydział Prawa i Administracji, Uniwersytet Gdański*

Korekta: *Magdalena Wojcieszak*
Projekt i wykonanie okładki: *Andrzej Malenda*
Skład i opracowanie techniczne: *Aleksandra Kumaszka*

Druk: *Drukarnia Beta-druk, www.betadruk.pl*

ISBN 978-83-65653-41-3 (druk)
ISBN 978-83-65653-42-0 (online)

Wydawnictwo eBooki.com.pl
tel.: +48 602 606 508
email: biuro@ebooki.com.pl
WWW: http://www.ebooki.com.pl

Spis treści

Słowo wstępne

Wydawać się może, że ponad dwa lata po wejściu w życie 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; RODO) na poziomie ustawodawstwa każdego z państw członkowskich Unii Europejskiej w kompleksowy sposób uregulowane zostały wszystkie kwestie istotne z punktu widzenia stworzenia kompletnego normatywnie systemu ochrony danych osobowych. Niestety nie możemy tego powiedzieć o naszym porządku prawnym. Jedynie tytułem przykładu można wskazać, że do dnia dzisiejszego nie doszło do uchwalenia istotnej z punktu widzenia zarówno zobowiązanych, jak i uprawnionych osób ustawy „wdrożeniowej", czyli takiej, która według samego projektodawcy „[…] musi zapewniać skuteczne stosowanie przepisów RODO"[1]. Projekt ustawy o zmianie niektórych ustaw w związku z zapewnieniem

[1] Jak podkreśla się w uzasadnieniu do kolejnego projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 z dnia 22 października 2018 r., „W tym celu konieczne stało się, poza uchwaleniem nowej ustawy z dnia 8 maja 2018 r. o ochronie danych osobowych, także dokonanie licznych zmian w innych ustawach. Z uwagi liczbę i charakter koniecznych zmian, a także w trosce o zapewnienie spójnego podejścia, zdecydowano się dokonać ich w jednym projekcie ustawy. Celem projektu jest dostosowanie polskiego porządku prawnego do RODO m.in. przez usunięcie przepisów, które są sprzecznie z RODO lub które powielają rozwiązania RODO. Celem projektu jest też dostosowanie RODO (przez implementację przepisów tego wymagających) do specyfiki polskiego porządku prawnego" – uzasadnienie dostępne na stronie: http://legislacja.rcl.gov.pl/projekt/12302951/katalog/12457738#12457738 [dostęp 10.11.2018].

stosowania rozporządzenia 2016/679 do dnia przesłania do druku niniejszej monografii nie trafił jeszcze nawet do Sejmu[2].

Oczywiście opieszałość krajowego prawodawcy nie zwalnia administratorów od realizacji wszystkich obowiązków, które zostały sprecyzowane w RODO, jak również tych, które wynikają z uchwalonej dnia 10 maja 2018 r. ustawy o ochronie danych osobowych. Nie budzi bowiem wątpliwości, że wdrożone (najpóźniej od 25 maja 2018 roku) przez szereg administratorów rozwiązania mają – przynajmniej w części – charakter przejściowy. Owa przejściowość nie może być też traktowana wyłącznie jako konsekwencja braku prawotwórczej działalności ustawodawcy krajowego czy unijnego (a także krajowego organu nadzoru). Wynika ona raczej z tego, iż przepisy RODO w wielu obszarach jedynie kierunkowo definiują działania, które podjąć musi administrator. W szczególności dotyczy to identyfikacji samego administratora, jego relacji z inspektorem ochrony danych, jak i wielu aspektów proceduralnych, nieodłącznie wiążących się z realizacją praw przez osoby, których dane dotyczą. Można też odnieść wrażenie, że upływ ostatnich kilku miesięcy z jeszcze większą siłą uświadomił praktykom ochrony danych osobowych wielość spraw, które będą musiały zostać poddane gruntownej analizie i to zarówno punktu widzenia specyfiki charakteryzujących organizacyjne formy funkcjonowania administratorów, jak i realizacji poszczególnych obowiązków wskazanych w RODO.

Cykliczne konferencje, które Katedra Prawa Konstytucyjnego wraz z Urzędem Marszałkowskim Województwa Dolnośląskiego (na przestrzeni ostatnich 12 miesięcy odbyły się trzy takie konferencje) oraz Generalnym Inspektorem Danych Osobowych organizowała we Wrocławiu, pozwoliły na wypracowanie propozycji wstępnych rozwiązań, również w okresie tzw. przejściowym, tzn. charakteryzującym się funkcjonowaniem

[2] W dniu 10 listopada 2018 r. nie doszło jeszcze do notyfikacji projektu.

systemu, w ramach którego nie wszystkie elementy składowe zostały w sposób dostateczny skonkretyzowane.

Upływ kilku miesięcy od momentu, gdy postanowienia RODO są bezpośrednio stosowane w polskim porządku krajowym, pozwolił nam na weryfikację części pierwotnych ustaleń oraz poglądów. Mając więc na względzie konieczność poszukiwania rozwiązań praktycznych i zarazem racjonalnych (zarówno z punktu widzenia administratora, jak i osoby, której dane dotyczą), podjęliśmy się próby przygotowania monografii dotyczącej istotnych problemów związanych z problematyką ochrony danych osobowych. Mamy nadzieję, że poruszone zagadnienia – choć oczywiście jedynie w zakresie wybranych kwestii – a przede wszystkim wskazane sposoby interpretacji postanowień RODO i ustawy o ochronie danych osobowych pozwolą na eliminację pojawiających się rozbieżności interpretacyjnych oraz problemów organizacyjnych i proceduralnych towarzyszących ciągłemu (dynamicznemu) procesowi kształtowania kompletnego systemu ochrony danych osobowych.

Mariusz Jabłoński
Marlena Sakowska-Baryła
Krzysztof Wygoda

Wrocław – Łódź, listopad 2018 r.

Rozdział I

Administrator danych w administracji publicznej

(dr Krzysztof Wygoda)

1. Pojęcie administratora na gruncie RODO – zagadnienia wprowadzające

Sfera administracji publicznej jest niewątpliwie jednym z głównych adresatów 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, dalej: RODO)[3]. Z faktu tego nie wynika jednak, że akt ten dostosowany jest wyłącznie do potrzeb, jakie pojawiają się w związku z działalnością administracji. Wręcz przeciwnie, ambicją prawodawcy było ustanowienie aktu generalnego, uniwersalnie regulującego zagadnienia przetwarzania danych osobowych bez względu na status podmiotu i sposoby owego przetwarzania. Jednakże łącząc sferę prywatną i publiczną, zazwyczaj nie sposób osiągnąć wystarczającej, do celów łatwej interpretacji przepisów, precyzji regulacji.

Nie wydaje się być zatem nadużyciem stwierdzenie, że reforma ochrony danych osobowych, choć zmieniła podejście do budowy systemu ochrony danych, nie przyniosła istotnej zmiany w sposobie funkcjonowania

[3] Dz. Urz. UE z 4.5.2016, L119, s. 1.

organów i podmiotów publicznych w związku z przetwarzaniem danych osobowych. Prawodawca w dalszym ciągu posługuje się też pojęciami wymagającymi wielopłaszczyznowej interpretacji, a zauważalna w regulacjach swoboda decydowania w zakresie formalnych aspektów systemu służącego przetwarzaniu jedynie wzmaga niepewność co do właściwego wdrażania postanowień RODO.

Zastanawiając się nad statusem, jaki posiadać mogą w procesie przetwarzania danych podmioty przynależące do szeroko ujętej administracji publicznej, można posłużyć się ogólnym stwierdzeniem, że RODO „[…] mówi o administratorze i podmiocie przetwarzającym zwykle jako o rolach, w których każdy podmiot może się znaleźć. Jednak często też ma na myśli podstawowe funkcje spełniane przez poszczególne organizacje”[4]. Zwłaszcza bowiem w tej sferze funkcjonowania państwa można dostrzec pewien dualizm w odniesieniu do organów czy podmiotów publicznych, które dla różnych realizowanych przez siebie zadań wiążących się z przetwarzaniem danych będą raz administratorem (dalej ADO) a innym razem podmiotem przetwarzających (dalej PP) w zależności od tego, który proces przetwarzania będziemy analizować. Ta wielość ról i statusów z uwagi na różny charakter i zakres obowiązków wymaga każdorazowego wyraźnego rozgraniczenia. Nie zawsze jest to jednak tak proste, jak być powinno. Dzieje się tak za sprawą przyjętej koncepcji odpowiedzialności, w której dominującą postacią jest administrator. Samo w sobie nie jest to kontrowersyjnym rozwiązaniem, niestety trudności rodzi praktyczne stosowanie definicji administratora, którą posługuje się prawodawca.

Konieczna jest zatem odpowiedź na pytanie, kim jest administrator danych w RODO. Wobec istnienia definicji legalnej wskazanej w art. 4 pkt. 7 RODO odpowiedź na to pytanie powinna być prosta, aczkolwiek w sferze publicznej okazuje się nieoczywista. Jedną z głównych przyczyn

[4] M. Gawroński, K. Kloc, M. Wojtas, [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018, s. 145.

takiego stanu rzeczy jest ponad dwudziestoletni okres funkcjonowania zbliżonej definicji administratora i praktyka, która w tym czasie została ukształtowana. Warto zatem zastanowić się, kim był „administrator danych osobowych" na gruncie ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[5] (dalej s.u.o.d.o.), przy czym należy zacząć od wskazania, że akt ten, podobnie jak RODO, zakładał prawie pełną swobodę co do statusu prawnego ADO. Odwołanie się do wypowiedzi doktryny i judykatury, poczynionych na gruncie s.u.o.d.o., pozwoli bowiem ocenić, czego można spodziewać się w trakcie stosowania samego RODO, gdzie wobec dodatkowego ryzyka generowanego jego naruszeniem ustalenie statusu administratora w przypadku szeroko pojętych organów i podmiotów publicznych wydaje się być jeszcze ważniejsze.

Zgodnie z definicją zawartą w art. 7 pkt 4 starej ustawy o ochronie danych osobowych „Ilekroć w ustawie jest mowa o: administratorze danych – rozumie się przez to organ, jednostkę organizacyjną, podmiot lub osobę, o której mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych".

Sam art. 3 s.u.o.d.o. dotyczący podmiotowego zakresu stosowania przepisów o ochronie danych osobowych wskazuje, że ustawę stosowało się do:

- organów państwowych,
- organów samorządu terytorialnego,
- państwowych i komunalnych jednostek organizacyjnych,
- podmiotów niepublicznych realizujących zadanie publiczne,
- osób fizycznych,
- osób prawnych,
- jednostek organizacyjnych niebędących osobami prawnymi.

[5] T. j. Dz. U. z 2016 r., poz. 922 ze zm.

Przy czym cztery ostatnie kategorie musiały przetwarzać[6] dane osobowe w związku z działalnością zarobkową, zawodową lub dla realizacji celów statutowych (jeśli mają one siedzibę albo miejsce zamieszkania terytorium Rzeczypospolitej Polskiej, albo w państwie trzecim, o ile przetwarzają dane osobowe przy wykorzystywaniu środków technicznych znajdujących się na terytorium Rzeczypospolitej Polskiej).

W definicji tej kluczowym kryterium kwalifikacji statusu administratora wydaje się być zatem **samodzielne decydowanie o celach i środkach przetwarzania danych osobowych,** a kwestie prawne dotyczące ich organizacji czy struktury są, wobec szerokiego wachlarza możliwości zaprezentowanych przez ustawodawcę, drugorzędne.

Tak skonstruowany model administratora w praktyce funkcjonowania krajowego organu nadzorczego i sądów nie był jednak prostym narzędziem kwalifikacji statusu podmiotów przetwarzających dane. Oczywistą niekonsekwencję stosowania kryteriów widać choćby po przeprowadzeniu analizy wpisów w rejestrze zbiorów danych, prowadzonym do 25 maja 2018 r. przez Generalnego Inspektora Danych Osobowych (dalej GIODO), gdzie dla takich samych sytuacji (w ujęciu faktycznym i normatywnym) wskazywano różnych ADO. Dobrym przykładem podsumowującym istniejące kontrowersje są wypowiedzi doktrynalno-jurydyczne, w których wskazano, że „[...] w przypadku podmiotów publicznych, ustalenie, kto jest administratorem danych, nie zawsze jest jednoznaczne. Trudność taka wynika z dwóch przyczyn: po

[6] Samo pojęcie przetwarzania danych nie było zasadniczo sporne na gruncie s.u.o.d.o., a rozumiano przez nie, stosownie do art. 7 pkt 2 tej ustawy, „[…] jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Należy podkreślić, że ustawa używa pojęcia «przetwarzanie danych osobowych», a zatem posługuje się określeniem wskazującym na dokonywanie (tu i teraz) czynności czy operacji na danych osobowych[…]" (I OSK 945/13 – wyrok NSA z dnia 1 stycznia 2014 r.). Należy przypuszczać, że również praktyka stosowania RODO nie będzie budziła większych kontrowersji w tej materii (oczywiście o ile uda się jasno wykazać, że mamy do czynienia z danymi osobowymi).

pierwsze, w odniesieniu do podmiotów publicznych o celu i środkach przetwarzania danych osobowych decyduje zazwyczaj ustawodawca, stanowiąc przepisy prawa, a po drugie, art. 7 pkt 4 powołanej wyżej ustawy stanowi, iż administratorem może być organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3.

Pierwsza ze wskazanych powyżej kwestii jest konsekwencją zasady legalizmu, zgodnie z którą organy władzy publicznej (administracji publicznej) działają na podstawie i w granicach określonych przepisami prawa. Podmioty publiczne są zobowiązane do przetwarzania danych osobowych dla realizacji określonych ustawowo celów. Zazwyczaj także środki, jakie służyć mają przetwarzaniu danych osobowych, wskazane są w przepisach ustawowych lub w wydanych na ich podstawie przepisach aktów wykonawczych. Stąd też możność decydowania przez podmioty publiczne o celu i środkach przetwarzania danych osobowych jest stosunkowo niewielka**.** Jak stwierdza R. Hauser (*Przetwarzanie danych osobowych: cel i środki*, „Rzeczpospolita" z 6 kwietnia 1999 r.), „[…] cel przetwarzania danych osobowych będzie mniej lub bardziej ogólnie wyznaczony przepisami prawa, a określony ich administrator, decydując o celu przetwarzania danych, będzie jedynie konkretyzował jego zakres, aby odpowiadał on potrzebom bardziej szczegółowo określonego zadania publicznego..."[7].

Przy czym bezwzględnie należy pamiętać, że nie jest natomiast administratorem ten, „[...] kto przetwarza dane w pełni według poleceń, wskazówek innego podmiotu, na jego zlecenie. Nie jest również administratorem danych osoba, której administrator powierzył przetwarzanie

[7] Wyrok NSA z dnia 28 sierpnia 2009 r., I OSK 1472/08. Ten fragment uzasadnienia wyroku jest też cytatem z: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. 4, Warszawa 2007, s. 375-376 (i w następnych, np. w wyd. 6, Warszawa 2015, s. 332). Na wypowiedź R. Hausera powoływali się często zarówno przed, jak i po 25 maja 2018 r. również inni komentatorzy i przedstawiciele doktryny, np. A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2005, s. 64 czy P. Fajgielski, *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz,* Warszawa 2018, s. 123.

danych, co wynika z art. 31 ustawy o ochronie danych osobowych, w szczególności z jego ust. 4, który przewiduje sytuacje, w których administrator danych powierza innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych[...]”[8].

By dookreślić, czym tak naprawdę zajmuje się ADO (w kontekście kwalifikowania go do tej kategorii), należy wskazać na bardzo szerokie ustawowe, ale wynikające również z Dyrektywy 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[9], ujęcie zjawiska przetwarzania danych „[...] gdyż «cel» i «środki» należy odnieść do procesu przetwarzania danych osobowych. Zgodnie z art. 7 pkt 2 ustawy przez przetwarzanie danych osobowych rozumie się jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych. Regulacja w art. 7 ust. 4 ustawy o ochronie danych osobowych nie stanowi regulacji pełnej. Podstawą wypełniającą regulację art. 7 ust. 4 tej ustawy jest regulacja materialnoprawna, która normuje działalność związaną z przetwarzaniem danych osobowych[...]”[10], a za takie regulacje można uznać zazwyczaj skierowane do podmiotów publicznych regulacje materialne i proceduralne określające zakres ich obowiązków związanych z wypełnianiem zadań czy funkcji.

Bez wątpienia problem uznania za ADO wzbudza jeszcze większe kontrowersje w bardzo wielu przypadkach, gdzie mamy do czynienia ze związaniem z konkretnym zbiorem (utworzonym dla realizacji prawnego obowiązku, który implikuje konieczność współdziałania, przy czym prawo wprost nie wskazuje/nazywa jego administratora) dwu lub większej

[8] Wyrok NSA z dnia 28 sierpnia 2009 r., I OSK 1472/08.
[9] Dz. Urz. UE L281, poz. 31.
[10] Wyrok NSA z dnia 01 października 2014 r., I OSK 945/13.

ilości pomiotów. Jak wskazują J. Barta, P. Fajgielski i R. Markiewicz, „[...] taka sytuacja może nastąpić wówczas, gdy zbiór pozostaje we wspólnej dyspozycji więcej niż jednego podmiotu. W tym przypadku [...] mogą oni działać wspólnie (a więc decyzje dotyczące zbioru podejmować we wzajemnym uzgodnieniu, w tym także opartym na podziale kompetencji) albo samodzielnie (i wtedy każdy z nich miałby status samodzielnego administratora łącznie z wiążącymi się z tym uprawnieniami i obowiązkami)."[11].

Problem ten nie został niestety rozwiązany przez dodanie[12] do s.u.o.d.o. art. 23 ust. 2a wskazującego, że podmioty, o których mowa w art. 3 ust. 1 s.u.o.d.o., „[...] uważa się za jednego administratora danych, jeżeli przetwarzanie danych służy temu samemu interesowi publicznemu". Przepis ten wzbudził ogromne kontrowersje w praktyce i szeroką dyskusję w doktrynie. Syntetycznie kwestię tę opisali P. Barta i P. Litwiński, wskazując na dwie potencjalnie możliwe interpretacje[13]. Jedna z nich wskazująca, że mamy wówczas do czynienia z kilkoma organami będącymi jednocześnie administratorami tych samych danych, jeżeli przetwarzanie danych „służy temu samemu interesowi publicznemu" wydaje się być do pogodzenia z brzmieniem art. 7 pkt 4 i z przepisem zawartym w art. 2 lit. d Dyrektywy 95/46/WE. Konsekwencją uznania wielości administratorów (współadministratorów) będzie konieczność wspólnego określania celów i sposobów przetwarzania w ramach tej wspólnoty, przy czym nic nie stoi na przeszkodzie, by jeden z nich odgrywał większą rolę niż pozostali. Z uwagi na wskazywaną wyżej właściwość organów związaną z wynikaniem celów przetwarzania z przepisów prawa owo uzgodnienie dotyczyć będzie więc wyłącznie szeroko

[11] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, wyd. 6, Warszawa 2015, s. 335.

[12] Co wynika z ustawy z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz. U. 2016 poz. 195).

[13] Zob. szerzej P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, wyd. 4, Warszawa 2016, s. 129-135.

pojętych sposobów przetwarzania obejmujących wspólne części (współwykorzystywanie) zbioru.

Jak wynika ze wskazanych wyżej wypowiedzi doktryny i rozstrzygnięć sądowych, na gruncie s.u.o.d.o. istniało wiele wątpliwości co do rozumienia pojęcia ADO, szczególnie w odniesieniu do sfery publicznej, nie da się jednak nie zauważyć pewnych zbieżnych poglądów zakładających, że ADO musi w jakimś, choćby niewielkim, zakresie decydować o celach i środkach przetwarzania danych osobowych, przy czym dla organów i podmiotów publicznych wystarczającym obszarem decyzyjnym jest sfera środków przetwarzania, gdyż co do zasady cele (w ich przypadku) powinny być określone prawem, a zatem podmioty te mogą co do zasady jedynie konkretyzować ich realizację, a nie dokonywać ich wyznaczenia *sensu stricto.*

Analizując już samo RODO, nie sposób nie zauważyć jeszcze większej elastyczności pojęcia administratora, które wskazano 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.

Prawodawcy z jednej strony zachowali neutralność statusu organizacyjno-prawnego administratora, a jednocześnie dostrzegli, że czasem na decyzji o sposobach lub celach przetwarzania waży zdanie wielu podmiotów. Za wystarczający warunek wpływający na przyznanie statusu administratora uznano zatem wspólne z innymi ustalanie celów i sposobów[14] przetwarzania. W tej sytuacji, jak słusznie zauważa

[14] Nastąpiła zamiana pojęcia „środki" na „sposoby", jednak, jak się wydaje, nie ma ona większego znaczenia merytorycznego. Bez wątpienia decydowanie o środkach przetwarzania mieści się w szerokiej kategorii określania sposobów przetwarzania.

K. Witkowska-Nowakowska[15], należy brać pod uwagę konsekwencje wynikające z art. 26 RODO[16], który obejmuje zjawisko współadministrowania, zwłaszcza „[...] że ten współudział przy decydowaniu może przybierać różne formy, w tym formę bardzo ścisłej współpracy lub wprost przeciwnie – jedynie częściowego wspólnego działania. Może zachodzić zatem wówczas, gdy administratorzy wspólnie określają i dzielą wszystkie cele oraz sposoby przetwarzania w równych proporcjach, jak i wtedy, kiedy podział jest niesymetryczny"[17].

Uznanie za administratora, na gruncie RODO, organu lub podmiotu ze sfery publicznej, nie wymaga już zatem nawet jego symbolicznej niezależności czy samodzielności decyzyjnej od innych, a za warunek wystarczający można będzie uznawać przyznanie mu – w oparciu o przepisy materialne prawa krajowego (lub materialne i formalne) – jakiegoś (choćby minimalnego) zakresu swobody decydowania o sposobach przetwarzania. W szczególności o terminach podejmowania czynności,

[15] Zob. szerzej K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 215-217; konieczność łącznego odczytywania definicji administratora i art. 26 RODO wskazują również P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Komentarz,* Warszawa 2018, s. 225.

[16] Art. 26 Współadministratorzy: „1. Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, 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". 2. Uzgodnienia, o których mowa w ust. 1, należycie odzwierciedlają odpowiednie zakresy obowiązków współadministratorów oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą. Zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą. 3. Niezależnie od uzgodnień, o których mowa w ust. 1, osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia wobec każdego z administratorów.

[17] K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *op. cit.*, s. 215.

sposobach/kanałach pozyskiwania/udostępniania informacji, narzędziach zabezpieczających przetwarzanie itp. Uogólniając powyższe, tak w kontekście współdecydowania, jak i samodzielnego przekazywania części decyzji innym uczestnikom procesów przetwarzania, można stwierdzić, że „[...] ustalanie przez administratora sposobów przetwarzania obejmuje zatem tak kwestie techniczne, jak i organizacyjne. Nie oznacza to jednak, że decydując o sposobie przetwarzania danych osobowych, wszystkie czynności na tym zasobie administrator musi wykonywać samodzielnie. Zdecydowanie o sposobie przetwarzania danych może sprowadzać się do decyzji o powierzeniu przetwarzania danych zewnętrznemu podmiotowi oraz o tym, że podmiot ten może korzystać z podwykonawcy (subprocesora). Administrator nie musi bowiem fizycznie posiadać danych, dla których ustala cele i sposoby przetwarzania, ani wykonywać samodzielnie wszystkich czynności potrzebnych dla osiągnięcia konkretnego celu; najistotniejsze jest to, że to podejmuje decyzje w procesie przetwarzania danych”[18].

Paradoksalnie podejście to, choć niewątpliwie bardziej uwzględnia realia funkcjonowania sfery publicznej, nie przynosi poprawy jednoznaczności regulacji. Z jednej strony powoduje ono jeszcze większą elastyczność w potencjalnym kwalifikowaniu do kategorii administratora, z drugiej generuje możliwość zbędnego pomnożenia ilości ADO, gdy mieć będą oni jakiś udział decyzyjny w procesach przetwarzania. Prawdopodobnie w większości przypadków, wobec braków kadrowych związanych choćby z niedoborem osób spełniających wymogi kwalifikacyjne na funkcję Inspektora Ochrony Danych (dalej IOD), w sferze publicznej takie rozdrobnienie nie tylko nie poprawi nadzoru nad procesami przetwarzania i ochrony praw osób, których dane dotyczą ale wręcz doprowadzi do pogorszenia się niewysokiego standardu istniejącego przed 25 maja 2018 r.

[18] M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red. nauk.), *Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 103.

Skalę potencjalnych problemów łatwo dostrzec na przykładzie funkcjonowania samorządu terytorialnego choćby w przypadku gminy, która może być ADO jako jednostka samorządu terytorialnego – osoba prawna działająca przez swoje organy (wójta i radę gminy). Jednak administratorami mogą być również jej organy – wójt (burmistrz, prezydent) i rada gminy. Nie wolno też zapominać o możliwości uznania za ADO urzędu gminy jako jednostki organizacyjnej. (powszechnie traktuje się go jako administratora z uwagi na funkcję pracodawcy). W gminie możemy również wskazać na występowanie jednostek pomocniczych, np. osiedli. Wobec otwartości RODO problemem jest zatem możliwość potraktowania ich jako ADO, w oderwaniu od miasta, organu wykonawczego burmistrza/prezydenta miasta oraz urzędu, który wspiera logistycznie ich funkcjonowanie, przy czym jednostki te mają własne organy, radę osiedla i zarząd osiedla, co jedynie multiplikuje możliwości. Podobnie rzecz wygląda na poziomie sołectw i sołtysa oraz wielu innych podmiotów, np.: rad seniorów, młodzieżowych rad miejskich, czy związków międzygminnych, Problemem są również gminne jednostki organizacyjne, takie jak miejskie ośrodki pomocy społecznej, zarządy dróg, inwestycji, zieleni, lokali, jednostki dedykowane świadczeniom rodzinnym, urbanistyce, geodezji, usługom komunalnym, centra usług wspólnych, itp.

Potencjalny stopień skomplikowania, widoczny choćby w opisanym przypadku, jest więc duży, a dotychczasowa praktyka określania tego, kto, w sektorze publicznym jest ADO, wynikała głownie z samopostrzegania się podmiotów, które w oparciu o różne uwarunkowania uznawały się za ADO, oraz z zapadających *a casu ad casum* rozstrzygnięć GIODO i sądów. Niestety trudno było się w niej dopatrzyć jednolitości stanowisk podmiotów rozstrzygających oraz konsekwentnego stosowania jasnych kryteriów. Bywały więc przypadki, w których dla takich samych zasobów informacji/zbiorów danych przyjmowano odmienne koncepcje wskazania ADO.

2. Podmiot realizujący obowiązki administratora – elementy definiujące ADO

Jak wskazano wyżej, przed 25 maja 2018 r., trudno było uznać status administratora za oczywisty, a obecnie rozwiązania normatywne nie poprawiają znacząco tego stanu. W pewnym kontekście wydają się nawet utrudniać rozwiązywanie problemów związanych ze wskazywaniem ADO. Teoretycznie można bowiem widzieć ADO w szerszym kręgu bytów biorących udział w procesach przetwarzania przy czym dziać się tak będzie nawet na poziomie wewnętrznej struktury istniejących obecnie podmiotów.

Zarówno RODO, jak i nowa ustawa o ochronie danych osobowych[19] (dalej u.o.d.o.) nie kwestionują wprost dotychczasowych ustaleń statusu ADO poczynionych w konkretnych przypadkach. Szczególnie w u.o.d.o. widoczny jest nawet trend do utrzymania *status quo* (o czym świadczy praktycznie cały jej rozdział 13), co podtrzymywać może często nielogiczne czy irracjonalne podejście do wskazywania ADO mające długie korzenie w dotychczasowej praktyce.

W tym stanie rzeczy zasadną wydaje się próba wypracowania systemowego podejścia do problemu określenia ADO, wykorzystująca okazję, jaką niesie RODO. Próbując w tym celu sięgnąć do najnowszego dorobku doktryny, spotkamy się zazwyczaj z dokładną analizą definicji zawartej w art. 4 pkt 7 RODO. Autorzy konsekwentnie podkreślają znaczenie elementów statusu wyartykułowanych w definicji legalnej. Działanie takie jest oczywiście racjonalne, gdyż to z niej wyprowadzić należy przesłanki wpływające zasadniczo na możliwość uzyskania statusu ADO. Tendencję tę można zaprezentować na przykładzie wskazania K. Witkowskiej-Nowakowskiej, która podkreśla, że w „[…] definicji z art. 4 pkt 7 wyróżnić należy trzy podstawowe komponenty: 1) element podmiotowy, czyli adresata przepisu, tj. osobę fizyczną lub osobę prawną, organ

[19] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz. 1000).

publiczny, jednostkę lub inny podmiot: 2) sposób działania dopuszczający model kontroli pluralistycznej: samodzielnie lub wspólnie z innymi; 3) zakres decyzyjny odróżniający administratora od innych podmiotów: ustala on cele i sposoby przetwarzania”[20].

Większość przedstawicieli doktryny podkreśla też, że w przypadku organów i podmiotów publicznych ustawodawca krajowy może wprowadzić inne kryteria warunkujące uzyskanie pozycji ADO. Co ciekawe, dostrzegając potrzebę uściślenia czy zracjonalizowania procesu uznawania za ADO w sferze publicznej, nie formułują w tym zakresie żadnych uwag *de lege ferenda*, które można uznać za propozycję owych dodatkowych kryteriów. Najczęściej spotykany jest postulat sprowadzający się do konieczności skorzystania przez ustawodawcę z możliwości, jaką pozostawił prawodawca unijny, polegającej na bezpośrednim wskazaniu ADO.

W tym kontekście na szczególną uwagę zasługuje analiza dokonana przez M. Sakowską-Baryłę, która podkreśla, że „[…] takie «ustawowe» wyznaczenie administratora nie może być dowolne i nie może następować w każdych okolicznościach. Jak bowiem wynika z treści tego przepisu, w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania, jeżeli cele i sposoby przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego. Stąd też wyznaczenie administratora w przepisach prawa nie może się obyć bez określenia w przepisach celów i sposobów przetwarzania. […] Należy uznać, że dopuszczalne jest zarówno łączne uregulowanie wszystkich tych kwestii, jak i ujęcie ich w osobnych aktach. Analogicznie rzecz się ma

[20] K. Witkowska-Nowakowska, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *op. cit.*, s. 213-214. Wskazania te pokrywają się ze stanowiskiem Grupy Roboczej art. 29 (sformułowanym wprawdzie na kanwie poprzednio obowiązujących przepisów, które w kwestii definicji administratora są jednak zasadniczo zbieżne z obecną definicją) zawartym w Opinii 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający” 00264/10/PL WP 169, przyjętej w dniu 16 lutego 2010 r., s. 34 (dla dalszego oznaczenia tego ciała używany będzie skrót GR29).

w przypadku ustawowego określenia «konkretnych kryteriów wyznaczania» administratora”[21]. Co istotne, autorka ta przedstawia rozwiązanie pozwalające na określenie ADO, do którego można sięgnąć w konkretnym stanie faktycznym, gdzie „[…] w braku przepisu szczególnego jednoznacznie przesądzającego o tym, komu w danym przypadku przysługuje taki status, administratora powinno się poszukiwać spośród tych podmiotów, które będą zdolne do ponoszenia odpowiedzialności, a więc którym przysługuje zdolność prawna”[22].

Wprawdzie nie zawsze wnioski wyciągane przez innych autorów są tak jasno podawane, widać jednak, że wielu z nich, dostrzegając pewne trudności w praktycznym stosowaniu definicji opierającej się głównie na analizie samego przepisu zawartego w art. 4 pkt 7 RODO, stara się włączyć doń szersze spektrum przesłanek. Dobrą ilustracją tego trendu jest wypowiedź P. Fajgielskiego, który stwierdza, że „[…] w świetle definicji zawartej w rozporządzeniu dla wskazania, kto jest administratorem, kluczowe jest stwierdzenie, kto decyduje o celu i sposobach przetwarzania danych (kto ustala cele i sposoby przetwarzania danych). Zazwyczaj kompetencje w tym zakresie posiadają podmioty kierujące działalnością. Stwierdzenie, kto jest administratorem, jest niezwykle istotne ze względu na to, że większość wymogów określonych przepisami komentowanego rozporządzenia ciąży na administratorze, jego także obarcza się odpowiedzialnością za naruszenie przepisów”[23]. Cytowana już M. Sakowska-Baryła podtrzymuje stanowisko prezentowane we wcześniejszych publikacjach, sprowadzające się do uznania, że ADO „[…] wyróżniają dwie podstawowe cechy: władztwo w procesie przetwarzania danych, a więc faktyczne podejmowanie we własnym imieniu i na własną rzecz decyzji o procesach przetwarzania danych – o tym, w jakim celu i w jaki sposób dane są przetwarzane, oraz specyficzna dla niego odpowiedzialność za zgodność

[21] M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 98.
[22] *Ibidem,* s. 104-105.
[23] P. Fajgielski, *Ogólne rozporządzenie…,* s. 122.

przetwarzania z przepisami o ochronie danych osobowych, która na gruncie RODO nie sprowadza się wyłącznie do odpowiedzialności administracyjnej”[24]. Stanowisko to jest niewątpliwie zgodne z wypowiedziami GR29, która podkreśla, że konieczność jednoznacznego określenia ADO „[…] w kontekście ochrony danych będzie w praktyce wiązać się z przepisami prawa cywilnego, administracyjnego lub karnego odnoszącymi się do powierzania obowiązków lub stosowania sankcji”[25].

Można jednak odnieść wrażenie, że również wypowiedzi innych autorów, nawiązujące do kryterium odpowiedzialności ADO nieco mniej bezpośrednio, nie są bynajmniej wynikiem odrzucenia tej koncepcji, a wynikają głównie z miejsca omówienia tego problemu powiązanego z systematyką wewnętrzną RODO. Wszyscy bowiem podkreślają, że ten aspekt realizacji obowiązków administratora wydaje się być jedną z istotnych gwarancji przestrzegania zasad RODO.

Na marginesie obecnych problemów interpretacyjnych warto dodać, że definiowanie ADO uwzględniające wymogi zdolności prawnej nie jest koncepcją nową. Wskazuję na to choćby wypowiedź M. Krzysztofka, który wskazuje na ADO jako podmiot funkcjonujący w dowolnej formie prawnej dającej mu zdolność do nabywania praw i zaciągania zobowiązań i związaną z tym możliwość ustalania celów i sposobów przetwarzania[26]. Do podobnych wniosków doszedł też wcześniej A. Drozd, który wprost postulował dokonywanie rekonstrukcji definicji ADO o elementy spoza tekstu samego przepisu zawartego w słowniczku (ówcześnie był to art. 7 pkt 4 s.u.o.d.o.). Zwracał on przy tym uwagę na niedoskonałości implementacji dyrektywy 95/46/WE, jak i podkreślał nieracjonalność działania, obejmującego zwłaszcza sferę publiczną, zmuszającego do uznania za ADO organ wydający akty normatywne, „[…] gdyż to właśnie

[24] M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red.), *op. cit.,* s. 101.

[25] Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający” 00264/10/PL WP 169, przyjęta w dniu 16 lutego 2010 r., s. 18.

[26] Por. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014, s. 204.

w tych aktach rozstrzyga się niekiedy o celach, a czasem także o środkach przetwarzania danych osobowych"[27]. Należy dodać, że ten ostatni argument nie stracił nic ze swej aktualności na gruncie nowych rozwiązań wynikających z RODO, a praktyka pokazała, że w kontekście decyzji prawotwórczych organy takie jak Sejm nigdy nie były traktowane jako administrator, mimo rzeczywistego dominującego wpływu na wskazanie calu działania podmiotów przynależących do szeroko pojętej administracji publicznej.

Za uznaniem kryterium posiadania przez ADO zdolności do ponoszenia odpowiedzialności we wszystkich obszarach – zarówno administracyjnym, jak i cywilnym – przemawia również stanowisko judykatury wypracowane pod rządami s.u.o.d.o. Jak słusznie podnosili D. Klimas i P. Wróbel, pomimo faktu, że s.u.o.d.o. nie zawierała odniesienia do kwestii „[…] odpowiedzialności cywilnej administratora, poruszając co do zasady jedynie kwestie odpowiedzialności administracyjnej i karnej, a mimo to SN dążąc do zagwarantowania ochrony praw osób których dane są przetwarzane, powiązał wymogi zakreślone w u.o.d.o. z odpowiedzialnością na gruncie cywilnoprawnym. Unijny prawodawca, kształtując odpowiedzialność cywilnoprawną podmiotów zaangażowanych w procesy przetwarzania danych, skupił się na odpowiedzialności odszkodowawczej. Jej podstawę stanowi art. 82 RODO, a motyw 146 zawiera wskazówki interpretacyjne w zakresie jego stosowania"[28]. Rozwijając swą wypowiedź zauważyli też, że „RODO czyni odpowiedzialnym za nieprawidłowości nie tylko samego administratora danych, ale także procesora, podmioty wspólnie administrujące bądź przetwarzające dane oraz podmiot przetwarzający na zlecenie procesora (tzw. subprocesor lub podprocesor). Chociaż każdy z wyżej wymienionych ponosi odpowiedzialność w innym

[27] A. Drozd, *Ustawa o ochronie…,* s. 62.

[28] D. Klimas, P. Wróbel, *Cywilnoprawna odpowiedzialność za naruszenie ochrony danych osobowych na gruncie RODO – wstęp do zagadnienia*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017, s. 106.

zakresie, podmiotowi danych umożliwia się wysunięcie roszczeń do szerszego kręgu podmiotów, co stanowi dla niego niebagatelne ułatwienie w dochodzeniu swoich praw”[29]. Stanowisko takie nie budzi najmniejszych wątpliwości a jego logiczną konsekwencją jest przyjęcie założenia o konieczności przypisania ADO zdolności sądowej w rozumieniu art. 64 k.p.c.[30] Co stanowi immanentny, choć nieujęty w definicji z art. 4 pkt 7 RODO element określający status ADO.

Być może takie stwierdzenie jest obecnie trudno akceptowalne, niemniej nie sposób uznać je za nieuzasadnione, gdyż od początku budowy systemu ochrony danych osobowych istotą tworzenia kategorii podmiotów, jakimi są ADO, było uczynienie ich odpowiedzialnymi za prawidłowość procesu przetwarzania. Odpowiedzialność ta przekładała się oczywiście na podległość rozstrzygnięciom krajowych organów nadzorczych, które miały charakter administracyjny, i na tej płaszczyźnie konieczna jest zatem odpowiednia zdolność sądowa – tym razem w rozumieniu art. 25 p.p.s.a.[31]

Należy uznać, że również po 25 maja 2018 r., próbując zrekonstruować pojęcie ADO, nie możemy opierać się wyłącznie na brzmieniu

[29] *Op. cit.*

[30] (Dz. U. 2018 poz. 1360 t. j. – Ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego) „Art. 64 § 1. Każda osoba fizyczna i prawna ma zdolność występowania w procesie jako strona (zdolność sądowa).

§ 1^1. Zdolność sądową mają także jednostki organizacyjne niebędące osobami prawnymi, którym ustawa przyznaje zdolność prawną. § 2. (uchylony)”.

[31] (Dz. U. 2018, poz. 1302 t. j. – Ustawa z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi) „Art. 25. Pojęcie i zakres zdolności sądowej § 1. Osoba fizyczna, osoba prawna lub organ administracji publicznej mają zdolność występowania przed sądem administracyjnym jako strona (zdolność sądowa). § 2. Zdolność sądową mają także państwowe i samorządowe jednostki organizacyjne nieposiadające osobowości prawnej oraz organizacje społeczne nieposiadające osobowości prawnej. § 3. Zdolność sądową mają także inne jednostki organizacyjne nieposiadające osobowości prawnej, jeżeli przepisy prawa dopuszczają możliwość nałożenia na te jednostki obowiązków lub przyznania uprawnień lub skierowania do nich nakazów i zakazów, a także stwierdzenia albo uznania uprawnienia lub obowiązku wynikających z przepisów prawa. § 4. Zdolność sądową mają ponadto organizacje społeczne, choćby nie posiadały osobowości prawnej, w zakresie ich statutowej działalności w sprawach dotyczących interesów prawnych innych osób”.

definicji zawartej w art. 4 pkt 7 RODO, ale powinno się sięgnąć do całości przepisów odnoszących się do funkcjonowania tego podmiotu. Zważywszy na możliwość realizacji wobec niego uprawnień Prezesa UODO, które gwarantować mają przestrzeganie regulacji prawnych poświęconych ochronie danych osobowych, nie wydaje się możliwe odrzucenie wniosku, że jednym z atrybutów ADO jest podległość środkom prawnym i sankcjom określonym w wielu przepisach (art. 77, 78, 79, 82, 83, 84 RODO). Zatem bez najmniejszej wątpliwości podmiot pretendujący do tej roli musi mieć zdolność podlegania im. Innymi słowy działania podmiotów mogących korzystać z tych środków i nakładać sankcje muszą być kierowane bezpośrednio do ADO, a nie innego podmiotu. W konsekwencji to właśnie ADO ma odpowiadać za ich zrealizowanie, a przynajmniej ma mieć taką prawną możliwość. W przypadku braku możliwości rzeczywistych (np. brak wystarczających środków na zaspokojenie administracyjnej kary pieniężnej) decydujące okażą się bowiem elementy normatywne, pozwalające uznać, że co do zasady ADO mógłby samodzielnie karę ową zapłacić.

Konsekwencją takiego podejścia jest *de facto* uznanie, że osoby fizyczne lub prawne, organy publiczne, jednostki lub inne podmioty, który samodzielnie lub wspólnie z innymi ustalają cele i sposoby przetwarzania danych osobowych mogą stać się ADO jedynie wtedy, gdy jednocześnie posiadają prawne możliwości wywiązywania się z obowiązków przypisanych administratorowi i samodzielnego ponoszenia konsekwencji ich łamania. W przypadku braku takich przymiotów należałoby uznać, że mamy do czynienia z pierwotnym brakiem legitymacji do pełnienia funkcji ADO[32].

[32] Co ciekawe, teza taka raczej nie będzie budzić wątpliwości w przypadku osób fizycznych, których status nie obejmuje pełnej zdolności do czynności prawnych. Nie można bowiem wykluczyć, że osoby takie potencjalnie mogłyby podlegać regulacjom RODO, przetwarzając dane w ramach czynności innych niż te o czysto osobistym lub domowym charakterze. Sytuacją tego typu jest choćby prowadzenie nawet częściowo skomercjalizowanego bloga. Na gruncie wyroku TSUE z dnia 19 października 2016 r. w sprawie C-582/14,

Trudne do zaakceptowania byłoby też przyjęcie, że ADO będzie działał na „koszt" innego ponoszącego zań odpowiedzialność bytu. Przyjęcie takiego założenia wydaje się pozostawać w sprzeczności z tezą, iż „[…] podmiotem o najszerszym zakresie odpowiedzialności pozostaje administrator danych, czyli, jak wskazuje definicja z art. 4 pkt 7 RODO, podmiot decydujący o celach i sposobie przetwarzania danych osobowych. Jego odpowiedzialność wynika z udziału w procesie przetwarzania danych w sposób naruszający przepisy RODO, a swoje roszczenie może wysunąć względem niego każda osoba fizyczna, której dane dotyczą, a która poniosła z tego powodu szkodę majątkową lub niemajątkową"[33]. Takie właśnie podejście zbieżne jest z poglądami GR29, która w kontekście decyzyjności ADO podkreślała, że „ważne jest, aby nawet w przypadkach przetwarzania danych niezgodnego z prawem zapewnić możliwość łatwego odnalezienia administratora danych i uznania go za odpowiedzialnego za przetwarzanie"[34]. A co za tym idzie, konieczność jasnego określenia ADO „[…] będzie w praktyce wiązać się z przepisami prawa cywilnego, administracyjnego lub karnego odnoszącymi się do powierzania obowiązków lub stosowania sankcji, którym osoba fizyczna lub prawna może podlegać"[35].

W kontekście takiego stanowiska znamienny jest jednak fakt, że w swych opiniach GR29 nie analizowała *de facto* przypadków innych niż osoba prawna i fizyczna oraz szczątkowo organ publiczny. Można

w którym stwierdzono, że adres IP, nawet dynamiczny, może stanowić dane osobowe, dochodzimy do wniosku, że osoba (np. dziecko powyżej 16 roku życia) będzie teoretycznie mogła podlegać RODO i uzyskać status ADO pomimo braku pełnej zdolności do czynności prawnych. Chyba że zastosujemy jednak reguły ogólne prawa cywilnego i odpowiedzialność przeniesiona zostanie na opiekunów prawnych, a nie tego, kto faktycznie decyduje o celach i sposobach przetwarzania. Poszukiwać zatem będziemy legitymacji ADO nie tylko w art. 4 pkt 7 RODO, ale i poza nim – właśnie we wskazanej (choćby teoretycznie) możności realizowania obowiązków ADO.

[33] *Op. cit.*, s. 107.

[34] Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" 00264/10/PL WP 169, przyjęta w dniu 16 lutego 2010 r.

[35] *Op. cit.*, s. 18.

zatem przyjąć, że twierdzenia te są modelowym ujęciem właśnie w odniesieniu do tych podmiotów, a inne formy organizacyjne ADO mają być traktowane „odpowiednio" przy uwzględnieniu ich specyfiki. Można też teoretycznie zakładać, że tam, gdzie występuje osoba prawna, nie należy próbować doszukiwać się odrębnych ADO w ramach różnych aspektów jej działania – w szczególności nie powinny być za ADO uważane jej wewnętrzne organy czy jednostki organizacyjne. Oczywiście tam, gdzie mamy do czynienia z organem – jako takim – nic nie stoi na przeszkodzie, by traktować go jako ADO. Również gdy mamy samodzielną (w sensie prawnym) i posiadającą zdolność sądową jednostkę organizacyjną czy nawet spełniający te kryteria podmiot, uznawanie ich za ADO mieści się w logice wywodu GR29.

W przypadku organów wewnętrznych, jednostek organizacyjnych itd. nie mających zdolności sądowej można by stosować istniejące i opisywane w doktrynie, na gruncie s.u.o.d.o., rozróżnienie na ADO i podmioty administrujące danymi na jego „rachunek" i w jego imieniu, przy czym nie mielibyśmy do czynienia z relacją powierzenia danych – gdyż działania odbywałyby się w ramach jednej struktury (organizacji). Oczywiście odrywamy w tym momencie szczegółową, bezpośrednią decyzyjność od ADO – ale pozostaje ona na poziomie ogólnym. Taki sposób zarządzania procesami przetwarzania można by zatem traktować jako wybór sposobu przetwarzania. Pamiętać bowiem należy, że w przypadku administracji publicznej cele przetwarzania zasadniczo wynikają z przepisów i wiążą podmioty je realizujące zgodnie z zasadą legalizmu.

Brak zdolności sądowej podmiotu, który w świetle reguł wprost wskazanych w art. 4 pkt 7 RODO traktowano lub zamierza się traktować jako ADO, winien zatem być sygnałem ostrzegawczym i zmuszać do głębszego zastanowienia nad słusznością takiej kwalifikacji. Prawdopodobnie istnieje bowiem jakiś „wspólny mianownik", w ramach którego można wskazać tego, kto odpowiedzialność będzie ponosił. Tytułem przykładu można by tu przywołać gminę – jako osobę prawną. Zazwyczaj

samodzielne organy czy urzędy (na czele których stoi jakiś prezes/dyrektor itp.) mają jednak legitymację procesową, zatem uznanie ich za ADO nie stanowiłoby najmniejszego problemu systemowego. Co więcej, zarówno gminy, jak i organy oraz urzędy dysponują budżetem, w którym znajdują się szeroko pojęte środki na ich działalność (są tam też takie pozycje, jak „pozostała działalność", a w niej środki kwalifikowane jako „§ 4590 – Kary i odszkodowania wypłacane na rzecz osób fizycznych"), z których teoretycznie można zaspokajać roszczenia odszkodowawcze.

Problemem będzie zaś niewątpliwie to, że powyższe rozróżnienie nie sprawdzi się w przypadku przetwarzania danych pracowniczych. Panuje bowiem jednolite przekonanie, poparte zresztą treścią przepisów prawa, że w zakresie stosunków pracy pracodawcą w samorządzie jest jednostka organizacyjna zatrudniająca pracowników i to nawet wtedy, gdy nie posiada ona osobowości prawnej. Pracodawcą jest więc niewątpliwie urząd miejski, szkoła czy przedszkole. Zatem ADO danych pracowniczych będą te właśnie jednostki, a skoro czynności z zakresu prawa pracy w odniesieniu do pracowników tam zatrudnionych wykonują kierownicy tych jednostek, będą też oni osobami decydującymi w kwestiach przetwarzania danych pracowniczych w imieniu pracodawcy[36]. Wniosek ten nie przeczy jednak ogólnemu założeniu o konieczności posiadania zdolności sądowej przez ADO – gdyż paradoksalnie w sprawach pracowniczych taką legitymację podmioty będące pracodawcami

[36] Wynika to z ustawy z dnia 21 listopada 2008 r. o pracownikach samorządowych (t. j. Dz. U. z 2018 r. poz. 1260, 1669) „Art. 7. Czynności w sprawach z zakresu prawa pracy za jednostki, o których mowa w art. 2, z zastrzeżeniem art. 8 ust. 2, art. 9 ust. 2 i 3 oraz art. 10 ust. 2 i 3, wykonują: 1) wójt (burmistrz, prezydent miasta) – wobec zastępcy wójta (burmistrza, prezydenta miasta), sekretarza gminy, skarbnika gminy oraz kierowników gminnych jednostek organizacyjnych; 2) przewodniczący zgromadzenia związku jednostek samorządu terytorialnego – wobec członków zarządu tego związku; 3) wójt (burmistrz, prezydent miasta), starosta, marszałek województwa w urzędzie jednostki samorządu terytorialnego – wobec pozostałych pracowników urzędu oraz wobec kierowników samorządowych jednostek organizacyjnych innych niż wymienione w pkt 1 i 2; 4) kierownik jednostki organizacyjnej – za inne niż wymienione w pkt 1–3 jednostki".

posiadają[37]. Można pokusić się zatem o postawienie tezy, że przetwarzanie danych pracowniczych legitymuje przedmiotowo pracodawcę do występowania w sporach związanych z naruszeniami RODO i ewentualnymi kwestiami odszkodowawczymi również przed sądami cywilnymi.

Pamiętać jednak należy, że w obrocie cywilnoprawnym jednostki organizacyjne nieposiadających osobowości prawnej (są to np.: urząd gminy czy miasta, starostwo powiatowe i urząd marszałkowski, miejski ośrodek pomocy społecznej, powiatowy urząd pracy, dom dziecka, dom pomocy społecznej czy szkoła publiczna) działają jedynie w zastępstwie jednostki samorządu terytorialnego. Jednostki te (określane mianem *stationes municipii*) zawsze działają w imieniu i na rachunek organu

[37] Tytułem przykładu można przywołać wyrok z dnia 4 stycznia 2008 r., I PK 187/07, w którym SN stwierdził, że „dla dyrektora domu pomocy społecznej stanowiącego jednostkę organizacyjną powiatu pracodawcą jest ten dom pomocy społecznej, natomiast uprawniony do dokonywania za tę jednostkę czynności z zakresu prawa pracy wobec kierownika samorządowej jednostki organizacyjnej jest starosta powiatu". W procesie ustalania, kto jest rzeczywistym pracodawcą danej osoby, nie ma zatem większego znaczenia fakt, że to gmina (czy powiat) posiada osobowość prawną, a jednostka organizacyjna bezpośrednio zatrudniająca pracownika nie posiada takiego statusu. W opinii SN, niezależnie od tego, jaki organ zatrudnił danego pracownika oraz na jakim stanowisku jest on zatrudniony, składając pozew, jako pozwanego powinien wskazać tę jednostkę organizacyjną, w której był zatrudniony, i to ta jednostka ma siłą rzeczy legitymację procesową. Pamiętać bowiem należy, że określenie w pozwie w sposób niewłaściwy strony pozwanej powoduje poważne konsekwencje procesowe. W przypadku gdyby pracownik przedszkola złożył pozew np. przeciwko burmistrzowi jako organowi gminy, a organ ten nie posiada zdolności sądowej ani procesowej, to burmistrz (jako pozwany) może domagać się odrzucenia pozwu (wyrok SN z dnia 25 września 2008 r., II PK 36/08). Gdyby zamiast przedszkola jako strona pozwana została wskazana gmina lub urząd gminy, powództwo podlegałoby oddaleniu z uwagi na brak legitymacji procesowej pozwanego. Analogicznie do powyższego w przypadku decyzji PUODO wskazującej na złamanie przez ADO zasad RODO jeśli pozwany nie będzie miał zdolności sądowej, to wskazanie w pozwie kogoś innego, np. gminy może okazać się przesłanką do oddalenia powództwa, gdyż ta, nie będąc ADO, powoła się na brak legitymacji procesowej. Cała sprawa nabiera zaś dodatkowego wymiaru poprzez wskazanie, że zgodnie z art. 97 u.o.d.o. o faktach decyduje PUODO – „Art. 97. Ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia 30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów".

założycielskiego, zatem gminy, powiatu czy województwa. Jeśli zatem w wyniku działania nieposiadającej osobowości prawnej jednostki organizacyjnej miałby powstać stosunek prawny, to zawsze jest on zawierany przez jednostkę samorządu terytorialnego, a nie przez tę jednostkę organizacyjną. Nic jednak nie stoi na przeszkodzie, aby obok gminy, powiatu czy województwa wskazywać taką jednostkę jako faktycznego realizatora stosunku prawnego (np. Gmina X – Urząd Miejski, Powiat Y – Powiatowe Centrum Pomocy Rodzinie, Województwo Z – Wojewódzki Zarząd Dróg). Byłoby to zbieżne ze znanym polskiej doktrynie statusem podmiotu administrującego danymi w imieniu jednostki posiadającej osobowość prawną – a kierujący tą jednostką, jeśli miałby decydować o przetwarzaniu, działałby na podstawie określonego rodzajowo upoważnienia – nie byłoby jednak mowy o stosunku powierzenia przetwarzania.

Reasumując dotychczasowe wątki, należałoby stwierdzić, że modelowe wskazywanie ADO powinno przebiegać według następującego schematu:

1. Zbadanie, czy podmiot uznawany za ADO, samookreślający się jako ADO lub „przymierzany" do statusu ADO spełnia kryteria wprost wskazane w art. 4 pkt 7 RODO.
2. Jeśli pierwszy etap zostanie zweryfikowany pozytywnie, sprawdzeniu powinna podlegać jego zdolność do realizacji wszystkich obowiązków ADO (w tym odszkodowawczych) wynikających z RODO a następnie u.o.d.o. (zatem również zbadać należy jego zdolność sądową na tle art. 25 p.p.s.a. i art. 64 k.p.c.).
3. W przypadku stwierdzenia niemożliwych do przezwyciężenia wad, uniemożliwiających realizację obowiązków przez badanego „ADO" należy sprawdzić inne możliwości – badając podmioty realizujące warunek pierwszy i dążąc jednocześnie do odnalezienia najbliższego „wspólnego mianownika", w ramach którego mieści się „niezaakceptowany ADO" – najczęściej powiązanie występować będzie

równolegle na płaszczyźnie organizacyjnej i funkcjonalnej (związanej z realizacją kompetencji przez „niezaakceptowane ADO")[38].

4. Po odnalezieniu właściwego ADO konieczne będzie sprawdzenia, a być może i ułożenie relacji z „niezaakceptowanym ADO", które jednak co do zasady nie będą opierać się na powierzeniu przetwarzania, ale raczej na cedowaniu części kompetencji (decyzyjnych czy zarządczych w wymiarze konkretyzującym podejmowane działania mieszczące się w pojęciu przetwarzania) w ramach rozstrzygania, przez rzeczywistego ADO, o sposobach przetwarzania.

Zarysowana wyżej koncepcja nie znajduje jednak dotychczas odzwierciedlenia w działaniach podejmowanych przez Prezesa UODO, a wcześniej GIODO. Wraz z napływem pozwów przeciwko ADO sądy cywilne, ale przede wszystkim osoby pozywające będą się jednak musiały skonfrontować z problemem potencjalnego braku zdolności sądowej pewnej części ADO. Brak tej zdolności bywał i bywa dominującym aspektem wielu spraw[39], a orzeczenia uzależnione były w efekcie od rozstrzygnięcia tej pierwotnej kwestii.

3. ADO w administracji publicznej

Jak wiadomo, grupa podmiotów tworzących administrację publiczną jest dość mocno zróżnicowana. Bez wątpienia realizuje ona swoje zadania w oparciu o zasadę legalizmu, z prawa więc wynikać będzie

[38] Tytułem przykładu można zakładać, że zarówno dla rady gminy, jak i wójta tym „wspólnym mianownikiem" powiązanym organizacyjnie i funkcjonalnie będzie gmina jako osoba prawna, w imieniu której działają oba organy.

[39] Zob. np.: postanowienie SN z dnia 16 kwietnia 2015 r., I CSK 396/14, postanowienie SN – Izba Cywilna z dnia 10 sierpnia 2017 r., II CSK 765/16, postanowienie SN – Izba Cywilna z dnia 30 marca 2017 r., V CZ 23/17, wyrok WSA w Gliwicach z dnia 10 lutego 2017 r., SA/Gl 1166/16, postanowienie SN – Izba Cywilna z dnia 25 stycznia 2017 r., IV CSK 149/16, postanowienie SA w Krakowie z 5 lutego 2014 r., I ACz 133/14, postanowienie SN – Izba Cywilna z dnia 26 września 2012 r., II CSK 722/11, wyrok SN z dnia 25 września 2008 r., II PK 36/08, wyrok SN z dnia 4 stycznia 2008 r., I PK 187/07.

status ADO, gdyż to ono wskazywać będzie cele i określać zasady większości procesów przetwarzania danych, które będą miały miejsce w przypadku tej grupy podmiotów. Do jej opisu, z punktu widzenia realizacji obowiązków ADO rekonstruowanych w oparciu RODO, warto podzielić ją co najmniej na dwie części, w których osią podziału mógłby być stopień i sposób regulowania jej działalności, a ściślej rzecz ujmując, stopień swobody decydowania o celach przetwarzania. Tą bardziej doprecyzowaną normatywnie grupą podmiotów jest niewątpliwie administracja rządowa, a działającą z nieco większym luzem (oczywiście tylko w niektórych obszarach) będzie administracja samorządowa. Zakres działań władczych podejmowanych przez oba rodzaje administracji będzie jednak miał swe pierwotne źródło w przepisach prawa powszechnie obowiązującego, w tym w limitującym działania władzy publicznej art. 51 konstytucji. Oczywiście część organów władzy nie jest doktrynalnie zaliczana do sfery administracji (ta jest bowiem ściśle powiązana z tzw. władzą wykonawczą). Organy pozostałych władz, czyli zasadniczo Sejm, Senat, Sądy i Trybunały (oraz Krajowa Rada Sądownictwa) nie zostały jednak, przynajmniej co do zasady, wyłączone spod działania RODO. Dotyczyć ich zatem będą te same reguły, gdyż i one działają w granicach i na podstawie prawa, mając mocno ograniczoną sferę wpływu na wybór celu przetwarzania danych odbywającego się w ramach powierzonych im kompetencji.

Wracając do administracji należy podkreślić, że w myśl reguł obowiązujących w RODO, o tym, kto może być traktowany jako organ lub podmiot publiczny (bo tak klasyfikujemy właściwie wszystkie podmioty mieszczące się ściśle w pojęciu organów administracji publicznej), decydować może kraj członkowski (definiując tę kategorię na potrzeby realizacji obowiązków wynikających z art. 37 RODO czy ograniczając wobec nich stosowanie administracyjnych kar pieniężnych, a nawet mając możliwość pewnego ograniczenia realizacji praw jednostki wskazanych w przepisach RODO). Zgodnie z art. 9 u.o.d.o. (i tożsamymi

rozwiązaniami art. 101 i 102 u.o.d.o.) pod pojęciem organów i podmiotów publicznych kryją się wyłącznie:

1) jednostki sektora finansów publicznych;
2) instytuty badawcze;
3) Narodowy Bank Polski.

W tym miejscu nie sposób uciec od wskazania, że jeszcze w końcowych projektach u.o.d.o. kategoria tych podmiotów była nieco bardziej dookreślona. Wskazywano bowiem na „l) jednostki sektora finansów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych; 2) instytuty badawcze, o których mowa w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2017 r. poz. 1158 oraz 1452 i 2201); 3) Narodowy Bank Polski". Odesłanie do ustawy o finansach publicznych (dalej u.f.p.) dawało nieco większą pewność przy wskazywaniu na podmioty przynależące do tej grupy (również w ramach tych zaliczanych do administracji publicznej), niemniej nawet taka redakcja przepisu nie wydawała się wystarczająco precyzyjna.

Kwestią wartą zasygnalizowania są wyłączenia przedmiotowe stosowania RODO, co powoduje, że mamy też takie organy szeroko pojętej administracji publicznej, które, będąc zasadniczo jednostkami sektora finansów publicznych, w zakresie realizacji swoich kompetencji nie podlegają RODO. Chodzi tu o służby specjalne w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu czyli samych ABW, AW, oraz Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralne Biuro Antykorupcyjne. Wyłączenie dokonane przez polskiego prawodawcę ma bowiem podmiotowy charakter obejmujący całą działalność wskazanych podmiotów, co może rodzić wątpliwości w zakresie właściwego użycia techniki legislacyjnej. O ile obecne działania tej grupy organów zdają się mieścić w zakresie art. 2 ust. 2 lit. a) i d) RODO, to w przypadku legislacyjnej zmiany obszarów ich zainteresowania należało będzie dokonać

ewentualnych korekt przepisu zawartego w u.o.d.o.[40] Sama nazwa służby czy agencji nie przesądza bowiem o jej rzeczowej właściwości, zwłaszcza że zazwyczaj mogą one podejmować działania określone w odrębnych ustawach i umowach międzynarodowych (zob. np. art. 5 ust. 1 pkt 5) ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[41].

Innym podziałem organów mogącym mieć wpływ na funkcjonowanie w ramach zasad ustalonych przez RODO będzie oparty o kryterium liczebności – dychotomiczna klasyfikacja wyróżniająca organy monokratyczne i kolegialne.

Chodzi oczywiście o jedność personalną w zakresie decyzyjności w przypadku piastunów organów monokratycznych i jej rozbicie w organach kolegialnych. Będzie ono skutkowało wyraźnym odróżnieniem ADO – jak traktować będziemy taki organ – i jego piastunów, którzy do realizacji swych zadań zmuszeni będą działać w określonych ramach formalnych. Kwestia właściwej reprezentacji, kworum, właściwej formy zwołania i trybu procedowania będą bowiem oddziaływać na skuteczność prawną podejmowanych decyzji – również w sferze ochrony danych. Dodatkowo należy brać pod uwagę fakt, że prawo zazwyczaj określa jakieś szczególne uprawnienia przewodniczącego czy też prezydium takiego organu, które to podmioty nie powinny być jednak utożsamianie z ADO jako takim.

[40] Chodzi oczywiście o „Art. 6. Ustawy oraz rozporządzenia 2016/679 nie stosuje się do: 1) przetwarzania danych osobowych przez jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 1, 3, 5, 6 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r. poz. 2077 oraz z 2018 r. poz. 62 i 1000), w zakresie, w jakim przetwarzanie to jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego, jeżeli przepisy szczególne przewidują niezbędne środki ochrony praw i wolności osoby, której dane dotyczą; 2) działalności służb specjalnych w rozumieniu art. 11 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz. U. z 2017 r. poz. 1920 i 2405 oraz z 2018 r. poz. 138, 650, 723 i 730)".

[41] T. j. Dz. U. z 2017 r. poz. 1920, 2405, z 2018 r. poz. 138, 650, 723, 730, 1544, 1560, 1669.

Osobną grupę organów administracji wartą wzmiankowania stanowią wszelkiego rodzaju „urzędy". Niektóre z nich działać będą jak organy i to im przypisywać będziemy funkcję/status ADO, w innych przypadkach ich rola sprowadzać się będzie do „obsługiwania" właściwego organu mającego przymiot ADO. Co ciekawe, „urzędy" (bez względu na ich nazwę) jako jednostki organizacyjne będą pełnić funkcję pracodawcy i w związku z tym przymiot ADO będzie przypisany w tej wąskiej sferze właśnie im. Siłą rzeczy właściwa realizacja obowiązków ADO wymagała będzie działań organów wewnętrznych kierujących pracą „urzędu", przy czym może nastąpić oddzielenie procesu decyzyjnego związanego z zarządzaniem obiema sferami przetwarzania (gdyż w niektórych przypadkach za sferę pracowniczą odpowiada dyrektor urzędu, którego nie będzie można utożsamiać z organem obsługiwanym przez taki urząd). Dojdzie wówczas do multiplikacji ADO w ramach jednej struktury, co zasadniczo nie sprzyja procesom decyzyjnym. Sytuacje takie wymagać będą zatem możliwie ścisłej współpracy decyzyjnej, najlepszym bowiem rozwiązaniem jest ujednolicanie zasad i procedur przetwarzania danych.

Bez względu na formę i typ organu dochodzić będzie również do sytuacji, w której status ADO wynikać będzie ze wskazania prawodawczego. Przypisanie normatywne roli ADO odbywa się na poziomie ustawowym i modelowo wiązać się powinno z wyposażeniem przypisanego podmiotu/organu we właściwe kompetencje i środki pozwalające mu realizować obowiązki ADO. Niestety to modelowe założenie nie zawsze będzie się sprawdzać w praktyce, również na poziomie sygnalizowanego w poprzedniej części problemu zdolności sądowej wskazanego normatywnie ADO. Być może racjonalnym wyjściem z tej sytuacji będzie uznanie, że ustawowe określenie ADO spełnia wymóg określony w art. 64 § 1^1 k.p.c. (zdolność sądową mają także jednostki organizacyjne niebędące osobami prawnymi, którym ustawa przyznaje zdolność prawną), gdyż bez wątpienia zauważalna jest funkcjonalna konieczność

posiadania takiej zdolności przez ADO. Dodatkowo założenie uznające potrzebę wyposażenia w odpowiednie środki rodzi wątpliwości, czy w przypadku ich braku podmiot przekazujący kompetencje ADO na mocy aktu prawnego nie czyni z siebie co najmniej współadministratora odpowiadającego za określenie sposobów przetwarzania – w szczególności wtedy, gdy owo wydzielenie funkcji ADO nie będzie się wiązać z odpowiednią pulą pieniędzy umożliwiającą realizację zadania.

Jeszcze inne problemy pojawiać się będą na kanwie realizacji przez organy administracji zadań zleconych – tu zasadniczo nie powinny mieć one statusu ADO, ale powierzenie przetwarzania winno modelowo mieć swe źródło w innym środku prawnym niż umowa[42]. *Nota bene* również w tym przypadku nieodzowne wydaje się być zabezpieczenie odpowiednich środków finansowych umożliwiających właściwe wywiązywanie się z obowiązków podmiotu przetwarzającego.

Kolejną płaszczyznę analizy obszarów generującą potencjalne problemy systemowe są powiązania różnego rodzaju uprawnień organów wewnętrznych danego podmiotu, na co dodatkowo nakładać się może rozdzielenie pozycji i uprawnień piastunów organów kolegialnych. Splot ten ilustrować mogą relacje istniejące w ramach samorządu terytorialnego. Na poziomie gminy w interakcję w ramach przetwarzania danych wchodzić będą wójt (burmistrz czy prezydent) z radą/przewodniczącym rady, a nawet radnymi jako samodzielnie działającymi przedstawicielami gminy uprawnionymi do przetwarzania danych (choćby w ramach tworzenia i prowadzenia biura radnego i zajmowania się sprawami mieszkańców). Zakładając, że mamy do czynienia z gminą jako ADO, to właściwe relacje wymagają, by organ wykonawczy (wójt, burmistrz czy prezydent) zapewnił właściwą organizację urzędu (ustanowił odpowiednie procedury, narzędzia przetwarzania itp.). Z kolei rada ma ustalić regulamin prac z określeniem zasad ochrony danych w ramach prac na

[42] Na temat powierzenia zob. Rozdział IV. Powierzenie przetwarzania w administracji publicznej.

posiedzeniach rady i komisji – osobą odpowiedzialną za czuwanie nad przestrzeganiem tych zasad będzie oczywiście prowadzący obrady (zazwyczaj odpowiada za to przewodniczący czuwający nad przestrzeganiem regulaminu/porządku obrad). Z kolei radny, z jednej strony działając jako członek organu kolegialnego, z drugiej jako samodzielnie uprawniony podmiot i posiadający biuro radnego, gdzie samodzielnie zbiera dane i za nie odpowiada, musi przestrzegać zasad wypracowanych przez gminę/radę, dysponując jednocześnie środkami zapewnianymi przez urząd obsługujący radę i jego samego. Jak się wydaje, działania związane z przetwarzaniem danych zawsze podejmowane są w celu przypisanym wspólnocie samorządowej utożsamianej z gminą, zatem nie ma powodu, by doszukiwać się w tego typu rozdzielonych funkcjonalnie procesach przetwarzania działań odrębnych administratorów czy nawet współadministrowania.

Ostatnią kwestią niezbędną do właściwego uregulowania w ramach funkcjonowania ADO jest potrzeba wyraźnego zdefiniowania obszarów i osób odpowiedzialnych w ramach potrzeb wynikających z przypisanej do procesów przetwarzania danych odpowiedzialności administracyjnej, odpowiedzialności cywilnej i odpowiedzialności karnej (przy czym ta ostatnia może, a *de facto* musi być zindywidualizowana i spersonalizowana). Linie podziału i obszary odpowiedzialności zależeć będą oczywiście od konkretnych uwarunkowań związanych z każdym ADO, jednak brak właściwego wyznaczenia ról poszczególnych osób i organów biorących udział w przetwarzaniu danych na każdym jego etapie będzie się niewątpliwie przyczyniał do zwiększonego ryzyka zaistnienia zdarzeń generujących każdy z rodzajów odpowiedzialności. Należy mieć na uwadze, że odpowiedzialność ADO, w ramach poprzednio obowiązującego sytemu, który w tym kontekście nie uległ ograniczeniu (a nawet można mówić o jego rozszerzeniu), generowana była na zasadzie, którą NSA wyartykułował w wyroku z dnia 4 kwietnia 2003 r., wskazując, że „administrator odpowiada więc za czyny swoich pracowników

w zakresie naruszenia ustawy o ochronie danych osobowych. Nie może się przy tym ekskulpować, na podstawie art. 26, że dołożył szczególnej staranności w celu ochrony tych danych"[43].

[43] Wyrok NSA z dnia 4 kwietnia 2003 r., II SA 2935/02, zob. też. wyrok NSA z dnia 31 stycznia 2012 r., I OSK 1318/11, wyrok NSA z dnia 1 grudnia 2009 r., I OSK 227/2009.

Rozdział II

Proces przetwarzania danych osobowych i jego legalizacja w sektorze publicznym

(dr Marlena Sakowska-Baryła, dr Krzysztof Wygoda)

1. Przetwarzanie danych w sektorze publicznym

W przypadku przetwarzania podejmowanego w sektorze publicznym zazwyczaj nie pojawiają się wątpliwości, że mamy do czynienia z tym właśnie zjawiskiem. Należy jednak pamiętać, że nie każda sytuacja wiążąca się z przetwarzaniem danych osobowych będzie, nawet w przypadku administracji publicznej, podlegała zasadom RODO. Działania nieobjęte RODO wskazane zostały głównie w art. 2 ust. 1 RODO, jednak również w innych przepisach tego aktu można doszukać się pewnych ograniczeń, których świadomość powinien mieć ADO.

Część z nich wynika z samych definicji – np. definicji danych osobowych – gdzie przetwarzanie danych osób obejmuje wyłącznie osoby fizyczne (a zatem w świetle prawa polskiego żyjące w chwili przetwarzania), tym samym przetwarzanie informacji o osobach prawnych nie jest poczytywane za przetwarzanie danych osobowych[44]. Nie należy jednak dokonywać prób rozszerzenia wskazanej reguły, co w szczególności dotyczy danych osobowych osób prowadzących działalność

[44] Trzeba jednak zwrócić uwagę, że informacje o reprezentantach takiej osoby – prezesach, pełnomocnikach, piastunach organów itd. stanowią jednak dane osobowe.

gospodarczą (na gruncie RODO dane przedsiębiorców – osób fizycznych – to bez wątpienia dane osobowe).

Inne ograniczenia są konsekwencją wskazanego w przepisach RODO zakresu stosowania poszczególnych praw jednostki i zasad przetwarzania wyartykułowanych w postaci powiązanych ze sobą przesłanek pozytywnych i negatywnych. Tak np. uregulowane jest nośne prawo do „zapomnienia" opisane w art. 17 RODO, którego w praktyce funkcjonowania administracji publicznej właściwie nie będzie można realizować z uwagi na wpisaną do tegoż przepisu regułę wynikającą z ustępu 3 zakładającą brak możliwości realizacji żądania osoby fizycznej w sytuacji, gdy zgodnie z lit. b) przetwarzanie jest niezbędne: do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Z uwagi na fakt, iż jest to wiodąca przesłanka legalizująca przetwarzanie w ramach działań podejmowanych przez ADO w analizowanym sektorze w większości przypadków uprawnienie do usunięcia danych nie będzie realizowalne wobec przetwarzania dokonywanego przez administrację publiczną w ramach realizacji jej kompetencji.

Należy jednak zauważyć, że również definicja przetwarzania[45] niesie w sobie pewne niebezpieczeństwa – tym razem prowadzące do szerszego ujęcia tego zjawiska, niż miało to początkowo miejsce na gruncie s.u.o.d.o. Wprawdzie wypowiedzi doktryny, GIODO i sądów, pojawiające się po korekcie, nie pozostawiały wątpliwości, że podleganie s.u.o.d.o. z uwagi na prowadzenie przetwarzania nie wymaga budowy

[45] „Art. 4 pkt 2) «przetwarzanie» oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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".

zbiorów danych w sytuacji, gdy przetwarzanie ma miejsce w systemie informatycznym, ale znaczna część administratorów ograniczała się do analizy art. 2 ust. 1 s.u.o.d.o., pomijając jego dalszą część. Pewne znaczenie dla zmian w świadomości ADO mieć będzie zapewne zmiana używanego w polskim ustawodawstwie desygnatu przetwarzania danych odbywającego się w systemie informatycznym (który, zgodnie z art. 7 pkt 2a) s.u.o.d.o., stanowił zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych) na przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany. Pojęcie występujące w RODO jest szersze i można oczekiwać objęcia zasadami ochrony danych również tych sytuacji, w których w procesie brać będą udział pojedyncze urządzenia „inteligentne" (np. liczniki, zamki, klucze) i inne urządzenia mechaniczne.

Problem inteligencji urządzeń służących do przetwarzania danych osobowych zyska jednak nowy wymiar, gdy starać się będziemy uznać za przetwarzanie zautomatyzowanie operacji podejmowanych w niedalekiej przyszłości przez działającą SI. Zagadnienie to stanowi poważny problem w sytuacji błyskawicznie rozwijających się technologii tworzenia autonomicznych urządzeń (np. samochodów, dronów, automatów bojowych itd.), które nie tylko przetwarzają dane, ale również wpływają bezpośrednio na wolności i prawa osób fizycznych mających z nimi kontakt – w jakimś stopniu i obszarze dotykać to będzie w przyszłości również sfery administracji publicznej.

Należy wskazać, że zautomatyzowane lub częściowo zautomatyzowane przetwarzanie jako niewymagające tworzenia zbioru danych wpisuje się w filozofię dążenia do szerokiej ochrony praw jednostki. Zaistnienie jakiegokolwiek przetwarzania danych osobowych odbywającego się w sposób całkowicie lub częściowo zautomatyzowany potencjalnie wymusza stosowanie RODO, o ile nie zaistnieje wyłączenie takiego obowiązku z uwagi na cel przetwarzania. Bez względu na sekwencję

występujących po sobie operacji mieszczących się w pojęciu przetwarzania, jeśli choć jedna z nich odbywa się w sposób zautomatyzowany, to całość procesu należy uznać za częściowo zautomatyzowany i jako taki podlegający zasadom RODO.

W przypadku przetwarzania odbywającego się w sposób inny niż zautomatyzowany będzie ono objęte regułami RODO, jeśli dotyczyć będzie danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Stosowanie reguł ochrony danych do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych, sugeruje konieczność występowania elementu wolicjonalnego (decydujący ma być zamiar umieszczenia danych w zbiorze, choćby nawet ostatecznie do tego nie dochodziło) po stronie potencjalnego administratora. Oznacza to, że ADO podlega RODO również wtedy, gdy jeszcze nie pozyskał danych mających trafić do zbioru. Wpisuje się to w szersze zjawisko widoczne na gruncie RODO – a mianowicie w dbałość o ochronę danych na każdym etapie procesu – w tym w trakcie jego projektowania. Jest to oczywiste również dlatego, że tylko wtedy, gdy administrator ma zamiar tworzyć zbiór, może spełnić wymogi art. 25 RODO nakazującego uwzględniać ochronę danych również przy określaniu sposobów przetwarzania, co bezsprzecznie obejmuje fazę projektowania i budowy struktury zbioru. Należy mieć nadzieję, że normy prawne określające cele przetwarzania narzucane ADO ze sfery publicznej będą uwzględniać takie założenia.

Należy też pamiętać, że tworzenie nawet chwilowo istniejącego zbioru doraźnego jest przesłanką wymuszającą działanie zgodne z RODO. Szczególnie ostrożnie należy podchodzić do procesów przetwarzania danych osobowych, realizowanych w sposób inny niż zautomatyzowany, które nie mają prowadzić do tworzenia zbiorów. Największym problemem może się w ich wypadku okazać niekonsekwentne trzymanie się technik manualnych i użycie w trakcie realizowania celów, dla których je

pozyskano, narzędzi służących do zautomatyzowanego przetwarzania danych (np. digitalizacja zasobów papierowych).

Rezygnacja z konieczności budowy zbioru w przypadku przetwarzania zautomatyzowanego lub częściowo zautomatyzowanego może powodować daleko idące konsekwencje, przekładające się również na brak wymogu utrwalenia przetwarzanych danych. Podejście takie wpisuje się w zasadę minimalizacji przetwarzania, a rezygnacja ze zbędnych elementów procesu przetwarzania, jeśli nie przyczyniają się one do osiągnięcia jego celu, wydaje się oczywista.

Przykładem takiego przetwarzania może być monitoring dokonywany w czasie rzeczywistym bez nagrywania obrazu, gdzie cel (np. zapewnienie bezpieczeństwa osobom lub ochrona mienia) osiągnięty zostaje dzięki bezpośredniej obserwacji nadzorującego monitory strażnika. Działania ADO również w takiej sytuacji mają jednak wpływ na prawa osób, których dane dotyczą – w tym wypadku dochodzić może choćby do naruszenia prywatności. W przypadku przesyłania danych (obrazu) pomiędzy urządzeniami, co jest istotą monitoringu, dochodzić może również do przechwycenia transmisji, co dodatkowo może wpływać na ryzyko naruszenia wolności i praw osób obserwowanych. Należy zatem przyjąć i wdrożyć odpowiednie zabezpieczenia dla takiego procesu przetwarzania – będzie on jednak prowadzony w warunkach ograniczenia (w sposób immanentnie wynikający z jego natury) realizacji praw jednostki wynikających z RODO. W praktyce ADO, w tym też ten ze sfery publicznej, zmuszony będzie jedynie do dopełnienia obowiązku informacyjnego z art. 13 RODO. Ciekawym studium z pogranicza takiej sytuacji będzie np. internetowa transmisja obrad rady miejskiej – również takie działania wymagają spełnienia wymogów, jakie niesie RODO.

Oczywiście biorąc pod uwagę specyfikę sektora przetwarzanie danych osobowych, i tak najczęściej będzie w nim przybierać formę prowadzącą do tworzenia zbiorów danych.

2. Podstawowe przesłanki legalizujące przetwarzanie w administracji publicznej

Już na wstępie należy podkreślić, że chociaż przesłanki legalizujące procesy przetwarzania wymieniane są w pewnym porządku, to nie ma on jakiegokolwiek znaczenia w kontekście hierarchizowania ich wagi. Wszelkie przesłanki zawarte w art. 6 i 9 oraz 10 mają taką samą wartość legalizującą, a różnice między nimi polegają jedynie na użyteczności w konkretnym procesie przetwarzania. Nie sposób jednak nie wspomnieć, że bez względu na użytą do legalizacji procesu przesłankę nie będzie on za taki uznawany, jeśli przetwarzanie obejmie dane inne niż niezbędne w kontekście realizacji celu tego procesu. Przy czym cel najczęściej nie występuje pojedynczo a raczej, w szczególności w administracji publicznej, mamy całą wiązkę częstokroć powiązanych ze sobą celów, które mogą uzasadniać konieczność przetwarzania różnego zakresu danych – sumarycznie dają jednak szerokie spektrum kategorii informacji mieszczących się w celu procesu.

Obowiązek wykazania kryterium „niezbędności", który zwykle obciąża ADO, w przypadku administracji publicznej będzie w znaczącej mierze „przerzucony" na prawodawcę określającego szczegóły i zasady procedur oraz przepisów materialnych, którymi taki ADO zmuszony jest się posługiwać. Samo pojęcie to występuje wprost w treści podstaw prawnych przetwarzania danych, wymienionych po przesłance zgody, czyli w art. 6 ust. 1 lit. b-f, a zatem ściśle ogranicza okoliczności, w jakich mogą one mieć zastosowanie. W przypadku gdy ADO nie działa w myśl szczegółowych przepisów (np. nie używa w procesie pozyskiwania danych normatywnie określonego formularza), wkraczanie w sferę prywatności osoby fizycznej powinno pozostawać w odpowiedniej proporcji do celów, których ochrona uzasadnia dokonane ograniczenie. To, co mieści się w kryterium niezbędności, należy ustalać jednak w każdym konkretnym przypadku, z uwzględnieniem celu, potrzeb i kontekstu przetwarzania

danych osobowych oraz wiążących administrację reguł sprawnego i terminowego realizowania powierzonych ich kompetencji. Brak jasnych wzorów limitujących kategorie i terminy przetwarzania zmusza niewątpliwie do dokonania przeglądu przynajmniej części procedur przetwarzania realizowanego przez administrację.

2.1. Art. 6 ust. 1 lit. a

Przesłanka, jaką jest zgoda, nie powinna być zasadniczo używana przez organy publiczne z uwagi na jej niską stabilność (możliwość cofnięcia zgody w każdym czasie) i wątpliwości co do realnej dobrowolności udzielenia w warunkach choćby względnej równości podmiotu danych i ADO. Zgodnie z treścią art. 6 ust. 1 lit. a dopuszczalne jest przetwarzanie danych, jeśli osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów. Pojęcie zgody zostało sformułowane w art. 4 pkt 11, warunki prawidłowości wyrażonej zgody określono w art. 7, natomiast warunki wyrażenia zgody przez dziecko w przypadku usług społeczeństwa informacyjnego wskazano w art. 8 RODO.

Należy też podkreślić, że założenie legalizmu, które limituje działania podejmowane przez administrację, *de facto* powoduje nieużyteczność zgód w procesach związanych z władztwem państwowym. W szczególności nie wolno używać zgody obok przesłanek wynikających z lit. c) i e) art. 6 RODO – gdyż żądanie takiej zgody w procesie opartym na tych właśnie przesłankach jest wprowadzaniem w błąd osoby, której dane przetwarzamy.

Powyższe uwagi nie implikują jednak braku konieczności uzyskiwania zgód na wszelkie działania, jeśli wymaga tego wprost przepis prawa. Przy czym nie będą to najczęściej zgody *sensu stricto* na przetwarzanie danych osobowych, ale raczej na realizację jakichś innych czynności (np. w niektórych przypadkach komercyjne wykorzystanie

wizerunku), z którymi z kolei może wiązać się konieczność przetwarzania danych osobowych.

2.2. Art. 6 ust. 1 lit b

Zgodnie z art. 6 ust. 1 lit. b RODO przetwarzanie jest zgodne z prawem w przypadkach, gdy przetwarzanie jest niezbędne do wykonania umowy, gdzie stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Z tak określonej przesłanki dopuszczalności przetwarzania danych osobowych podmioty publiczne mogą korzystać wówczas, gdy spełnione są wszystkie wynikające z niej kryteria. Nie każda zatem umowa zawierana przez publiczną osobę prawną czy jednostkę organizacyjną niemającą osobowości prawnej zawierana jest w warunkach, o których stanowi przywołany przepis, choć – rzecz jasna – podmioty te zawierają umowy. Ta forma kształtowania stosunków prawnych wchodzi w rachubę w tych przypadkach, gdy rzeczone podmioty publiczne nie działają w sposób władczy, ale występują w obrocie prawnym jako podmioty prawa cywilnego – w obrębie ich sfery dominium.

Gdyby przyjrzeć się bliżej umowom zawieranym przez publicznych administratorów, można dojść do wniosku, że w wielu przypadkach dysponowanie danymi osobowymi konkretnych osób fizycznych przy ich zawieraniu i realizacji nie następuje wcale na podstawie art. 6 ust. 1 lit b RODO, ale w oparciu o inne przesłanki legalizujące, w tym zwłaszcza prawnie uzasadniony interes (art. 6 ust. 1 lit. f RODO). Po przesłankę z art. 6 ust. 1 lit. b dla usprawiedliwienia przetwarzania danych osobowych nie sięgamy bowiem wówczas, gdy dane osobowe w umowach pojawiają się dla oznaczenia osób reprezentujących osoby prawne lub jednostki organizacyjne nieposiadające osobowości prawnej, osób, które strony umowy dedykowały do jej wykonania (tzw. osób kontaktowych), czy też osób, których w jakimś zakresie umowa dotyczy – jak choćby: pracowników urzędu marszałkowskiego skierowanych na szkolenie, osób,

na których rzecz kontrahent ma dokonać określonego świadczenia, osób, dla których dotyczy konkretna usługa, np. zaopatrzenie urzędnika w podpis elektroniczny.

Należy skupić uwagę na tym, że analizowany przepis art. 6 ust. 1 lit b RODO legalizuje przetwarzanie danych osobowych w dwóch sytuacjach:

1) gdy przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy lub
2) gdy przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą.

Niemniej za każdym razem chodzi o stosunek umowny, którego stroną jest skonkretyzowana osoba fizyczna, bądź kiedy ta osoba żąda zawarcia umowy. W konsekwencji przesłanka ta legalizuje przetwarzanie tylko wówczas, gdy stroną umowy pozostaje lub ma pozostać osoba fizyczna działająca we własnym imieniu i jej dane jako strony umowy podlegają operacjom przetwarzania niezbędnym odpowiednio do wykonania umowy lub czynności przygotowawczych przed jej zawarciem. Stąd jeżeli stroną umowy z publicznym administratorem pozostaje spółka osobowa czy kapitałowa, fundacja, stowarzyszenie, partia polityczna, uniwersytet, instytucja kultury itp., nietrafne jest wskazywanie na analizowany tu przepis. Natomiast, gdy przetwarzanie danych odbywa się przy zawarciu umowy najmu czy dzierżawy z osobą fizyczną, gdy taka osoba – także w ramach prowadzonej działalności gospodarczej – wykonuje usługę na rzecz administratora czy dostarcza jemu określone dzieło chociażby w postaci sporządzonej opinii prawnej, projektu graficznego, pieczątek czy tym podobnych, można uzasadniać je treścią art. 6 ust. 1 lit. b RODO. Dla zastosowania tego przepisu osoba, której dane dotyczą, musi być stroną umowy, co oznacza, że zakres tego przepisu nie obejmuje przetwarzania danych osobowych innych osób, które nie są stronami umowy, choć umowa może dotyczyć ich szeroko pojmowanych interesów. Można tu zwrócić uwagę choćby na przetwarzanie danych osób, które

objęte są działaniem umowy o świadczenie na rzecz osoby trzeciej, której konstrukcja wynika z art. 393 k.c. Poprzez jej zawarcie będąca stroną umowy osoba, której dane dotyczą, może umówić się z drugą stroną – administratorem na gruncie RODO, że spełni on świadczenie na rzecz osoby trzeciej bliżej oznaczonej w umowie. Oznacza to, że w takim przypadku administrator będzie nie tylko przetwarzał dane osobowe tej osoby fizycznej, z którą umowę zawarł, ale również innej osoby, na rzecz której ma obowiązek świadczyć, ale z którą umowy nie zawierał.

Preambuła RODO w motywie 40 (*in fine*) wskazuje, że aby przetwarzanie danych było zgodne z prawem, powinno odbywać z poszanowaniem umowy, gdzie stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. W to poszanowanie umowy wpisana jest konieczność dokonywania ustaleń co do dopuszczalności przetwarzania danych osobowych z uwzględnieniem istoty i charakteru konkretnego stosunku umownego, zamiaru stron oraz okoliczności, w jakich umowa jest zawierana i wykonywana. Wszystko to ma bowiem wpływ na zakres danych osobowych przetwarzanych przy zawieraniu i realizacji umowy. Zakres danych podlegających przewarzaniu w znaczącej mierze uzależniony jest od przedmiotu świadczenia, kontekstu oraz przepisów prawa dotyczących umów konkretnego rodzaju i ciężarów publicznych z nimi związanych. Chodzi tu zwłaszcza o obowiązki podatkowe czy obowiązki z zakresu ubezpieczeń społecznych.

Analizowana przesłanka dopuszczalności przetwarzania nie będzie dotyczyć osób działających w ramach przedstawicielstwa uregulowanego w art. 95 i nast. k.c., a więc przetwarzania danych osobowych osób fizycznych działających na rzecz i w imieniu innej osoby fizycznej. Czynności prawnej bowiem można dokonać przez przedstawiciela, przy czym umocowanie do działania w cudzym imieniu może opierać się na ustawie (przedstawicielstwo ustawowe) albo na oświadczeniu reprezentowanego (pełnomocnictwo) i przetwarzanie ich danych osobowych w związku z działaniem przy zawieraniu umowy w imieniu i na rzecz

w imieniu osoby reprezentowanej nie jest objęte zakresem art. 6 ust. 1 lit. b, ale odbywa się na podstawie art. 6 ust. 1 lit. f RODO. Tak też rzecz się ma z przetwarzaniem danych osobowych przedstawiciela ustawowego osoby ograniczonej w zdolności do czynności prawnych w związku z wyrażaniem przez niego zgody na dokonanie czynności prawnej, w na tym zawarcie umowy z administratorem, bez której czynność jest nieważna (art. 17 k.c.)[46].

Podkreślić trzeba, że w przepisach legalizujących przetwarzanie danych osobowych, w tym w art. 6 ust. 1 lit. b RODO, akcentuje się zawsze, by przetwarzanie danych spełniało kryterium niezbędności. W przypadku analizowanej podstawy przetwarzania należy oczekiwać, że „niezbędność" dotyczyć będzie zarówno zakresu danych osobowych, którymi dysponuje się przed zawarciem umowy lub przy jej wykonaniu, jak i zakresu wykonywanych operacji przetwarzania. Ma to uzasadnienie nie tylko w treści art. 6 ust. 1 lit. b, ale i art. 5 ust. 1 lit. c, z którego wynika zasada minimalizacji danych, z którą spójna jest wytyczna wynikająca z motywu 39 preambuły RODO, iż dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane, a także przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Przetwarzanie danych w celu wykonania umowy nie powinno być przy tym okazją dla administratora, w tym administratora z sektora publicznego, do przetwarzania przy tej sposobności danych w szerszym zakresie czy w ramach szerszych operacji przetwarzania niż to adekwatne dla tego celu, chyba że jednocześnie administrator jest w stanie wykazać się spełnieniem innej przesłanki legalizującej przetwarzanie danych osobowych. Pamiętać jednak należy, że każdy z takich celów przetwarzania powinien być zakomunikowany podmiotowi danych zwłaszcza w ramach spełnianego obowiązku informacyjnego wynikającego z art. 13 lub art. 14 RODO.

[46] Zob. A. Nerka, M. Sakowska-Baryła, *Komentarz do art. 6*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 159.

Należy zwracać uwagę na ten standard, ponieważ wszelkie przetwarzanie danych osobowych powinno być przejrzyste dla osób fizycznych. Osoby te powinny wiedzieć, że informacje o nich są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane (art. 5 ust. 1 lit. a RODO oraz motyw 39). Nie jest możliwe uniwersalne określenie, jakie dane osobowe czy jakie operacje przetwarzania mogą być wykorzystywane przez administratora dla wykonania umowy lub do podjęcia działań przed zawarciem umowy. Wydaje się, że także pod rządami RODO aktualne pozostają w tym względzie ustalenia judykatury poczynione jeszcze w poprzednim stanie prawnym, gdy stosowano art. 23 ust. 1 pkt 3 s.u.o.d.o., który określał zbliżoną przesłankę legalizującą przetwarzanie danych osobowych. Sięgnąć tu można choćby po następujące wyroki: wyrok NSA z dnia 13 lipca 2004 r., OSK 420/04; wyrok WSA we Wrocławiu z dnia 9 października 2009 r., I SA/Wr 945/09; wyrok WSA w Warszawie z dnia 27 lutego 2004 r., II SA 291/03; wyrok WSA w Warszawie z dnia 29 lipca 2010 r., II SA/Wa 539/10, na których tle kształtowała się praktyka posługiwania się danymi osobowymi przy zawieraniu i realizacji stosunków umownych z osobami fizycznymi.

2.3. Art. 6 ust. 1 lit. c

Bez najmniejszych wątpliwości główną przesłanką legalizująca procesy przetwarzania w administracji publicznej jest wskazana w art. 6 ust. 1 lit. c niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze. Przy czym należy pamiętać, że prawodawca doprecyzował warunki, które są wspólne dla obu przypadków przetwarzania występującego w sektorze publicznym (lit. c i e) i założył, iż podstawa prawna przetwarzania musi zostać określona w prawie UE lub w prawie państwa członkowskiego, na podstawie którego działa administrator. Co oznacza, że zasadniczo przetwarzanie powinno opierać się bezpośrednio o normę wywiedzioną z przepisu prawa, który, zważywszy na regulacje

konstytucyjne (art. 31 ust. 3 Konstytucji RP), powinien znajdować się w akcie rangi ustawy. Należy zakładać, że warunek ten dotyczy wyartykułowania w niej obowiązku (lub w przypadku przesłanki opisanej w lit. e) tegoż artykułu zadania realizowanego w interesie publicznym czy w ramach sprawowania władzy publicznej). Z faktu wskazania w przepisie obowiązku prawnego może wynikać chęć kierowania się precyzyjnymi wskazaniami nakazującymi podejmowanie określonych działań podmiotom zobligowanym do podporządkowania się takiemu prawu. W odróżnieniu od wcześniej obowiązującej regulacji, odwołującej się do przesłanki realizacji ogólnie określonego uprawnienia przewidzianego przepisem prawa, nowa reguła mówi wprost o konieczności wyartykułowania celu przetwarzania objętego obowiązkiem. Można zatem stwierdzić, że każdorazowo wyprowadzając przesłanki legalizujące z tej opisanej w literze c), należy wskazać również inny przepis opisujący ów cel, w związku z którym pojawia się obowiązek przetwarzania danych. W praktyce może się zapewne zdarzyć, że będą to także przepisy samego RODO, które nakładają na administratora szereg obowiązków, z którymi musi wiązać się przetwarzanie danych osobowych. Artykulacja celu i obowiązku nie musi być łączna – zatem przy ogólnym, normatywnym sformułowaniu celu może być precyzowana szczegółowo wyartykułowanymi obowiązkami albo przy jasno wskazanym celu obowiązek można wyprowadzić z reguł ogólnych**.** Jak podnosi doktryna sytuacja pierwsza może dotyczyć np. obowiązków pojawiających „… się w przy:

1) realizacji praw osób, których dane dotyczą, związane z ustaleniem tożsamości osoby żądającej realizacji uprawnienia;
2) adekwatnym umocowaniem personelu administratora do przetwarzania, w tym z upoważnianiem i poleceniem przetwarzania oraz zobowiązaniem do zachowania odpowiedniego rodzaju tajemnicy czy weryfikacją, czy konkretna osoba spełnia kryteria wykonywania zawodu, z którym związana jest tajemnica zawodowa;

3) powierzaniu przetwarzania, które zazwyczaj wymaga zawarcia umowy, a co za tym idzie przetwarzania danych osób reprezentujących jej strony;
4) współadministrowaniu, które wymaga dokonania wspólnych ustaleń przez administratorów, gdzie udokumentowanie takich ustaleń powoduje konieczność przetwarzania informacji o osobach fizycznych działających w imieniu każdego ze współadministrujących podmiotów;
5) wyznaczaniu inspektora ochrony danych i informowaniu o nim organu nadzorczego, gdzie nieodzowne jest posługiwanie się danymi osobowymi konkretnej osoby fizycznej wykonującej taką funkcję u administratora itp."[47]

Przy konkretnie wskazanym celu charakter przepisu bądź jego usytuowanie w dziedzinie prawa nie ma istotnego znaczenia, jeżeli jego adresatem jest administrator. W tym miejscu mogą pojawiać się wątpliwości co do możliwości działania na podstawie aktów rzędu niższego niż ustawa. Należy założyć, że nie powinno się wykluczać aktów niższego rzędu (rozporządzenia i akty prawa miejscowego), jeżeli traktować je będziemy jako przepisy uzupełniające określające „[…] ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX" RODO. Przy czym należy, jeszcze raz podkreślić, że sam cel i obowiązek działania nałożony na ADO musi być wyprowadzony z przepisów rangi ustawy[48].

[47] A. Nerka, M. Sakowska-Baryła, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 162.

[48] Warto wskazać, że nawet na gruncie s.u.o.d.o. NSA uznał za nieważną uchwałę rady miejskiej w sprawie regulaminu utrzymania czystości i porządku na terenie miasta,

Nakładając na ADO konieczność szukania podstawy w celach wyprowadzonych z aktów normatywnych, prawodawca wyklucza zasadniczo jako wyłączne podstawy przetwarzania danych osobowych akty stosowania prawa (decyzje, postanowienia itp.). Z drugiej strony będą one stanowiły częstokroć impuls rozpoczynający proces przetwarzania na określonym jego etapie – należy jednak mieć na uwadze, że za ich wydaniem stoją przepisy rangi ustawy i wskazane w nich cele, obowiązki itd., a samo realizowanie wskazań wynikających z takiego aktu stosowania prawa (szczególnie wyroku) jest obowiązkiem jego adresata.

Istnienie konkretnych przepisów dookreślających zadania ADO może mu ułatwić realizację zasady minimalizacji przetwarzania, ponieważ w tym wypadku konkretny przepis często będzie wyznaczał zakres niezbędności przetwarzania. W konsekwencji przetwarzanie dokonywane z naruszeniem ram wyznaczonych przez treść takiego przepisu zasadniczo nie będzie spełniało waloru niezbędności. W przypadku braku przepisów szczegółowych – czego RODO zasadniczo nie wymaga[49] – ADO będzie zobowiązany do ustalenia związku między zakresem przetwarzania danych a realizacją obowiązku wynikającego z przepisu. Poza tym warto zwrócić uwagę, iż motyw 45 wskazuje na możliwość realizacji zadań podmiotów publicznych nawet przez osoby fizyczne: „Prawo Unii lub prawo państwa członkowskiego powinno określać także, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ

nakładającą obowiązek znakowania psów i rejestrowania danych ich właścicieli. W ocenie NSA nałożenie takiego obowiązku w drodze uchwały rady miasta narusza art. 51 Konstytucji RP – również wymagającego ustawowej regulacji obowiązków związanych z ujawnianiem informacji – por. wyrok NSA z dnia 1 marca 2012 r., II OSK 2599/11.

[49] Należy zwrócić uwagę, że w również w motywie 45 wskazano, iż RODO nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, albo że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu [...]". Sytuacje takie są spotykana również na gruncie prawa polskiego np. w przypadku realizowania zadań związanych z ochroną zdrowia publicznego przez lekarzy i to nawet wtedy, gdy nie korzystają oni ze środków publicznych (np. w ramach realizacji obowiązków określonych w ustawie z dnia 5 grudnia 2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi[50].

Wymóg istnienia obowiązku prawnego ciążącego na konkretnym administratorze nie musi każdorazowo implikować powiązanego z nim obowiązku podania danych osobowych przez osobę, której dane podlegać mają przetwarzaniu. Zwłaszcza w przypadku istnienia zobowiązania nałożonego na organ lub podmiot publiczny może on dysponować innymi sposobami pozyskiwania informacji o podmiotach danych, wykorzystywanymi priorytetowo w procesie ich przetwarzania, dającymi dodatkowo pewność co do poprawności użytych w procesie przetwarzania informacji (chodzi np. o dostęp do zasobów zawartych w Systemie Rejestrów Państwowych poprzez aplikację ŹRÓDŁO) – konieczność weryfikacji danych wskazanych przez osobę, których dane dotyczą, co zasadniczo jest warunkiem ich pełnej wiarygodności i poprawności, winna zawsze ograniczać chęć gromadzenia danych niesprawdzalnych. Weryfikacja owa może napotykać w praktyce nieprzezwyciężalne przeszkody i musi się odbywać w formach przewidzianych prawem.

2.4. Art. 6 ust. 1 lit. d

Przesłanka legalizująca przetwarzanie w związku z ochroną żywotnych interesów osoby fizycznej zakłada (w myśl art. 6 ust. 1 lit. d RODO) dopuszczalność przetwarzania nie tylko wtedy, gdy jest to niezbędne do

[50] T. j. Dz. U. z 2018 r., poz. 151. Por. K. Wygoda, *Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych w oparciu o art. 6 RODO a działania podmiotów sektora publicznego*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *op. cit*., s. 38.

ochrony żywotnych interesów osoby, której dane dotyczą, ale również w ochronie takich interesów innej osoby fizycznej. W poprzednim stanie prawnym przesłanka ta wymagała „wtórnej" legalizacji poprzez uzyskanie następczej zgody podmiotu danych na przetwarzanie jego danych osobowych. Możliwość oparcia czynności przetwarzania na tej przesłance była zatem ograniczona czasowo do momentu, gdy uzyskanie zgody znów stało się możliwe.

W literaturze jako przykład na wykorzystanie tej przesłanki wskazuje się okoliczność podania do publicznej wiadomości informacji dotyczących osoby stwarzającej zagrożenie dla życia i zdrowia innych w związku z popełnieniem przez nią przestępstwa i trwającymi poszukiwaniami[51].

Bez wątpienia wykładnia przesłanki wymaga poddania analizie zwrotu: „żywotne interesy" osoby fizycznej, który nie ma obecnie w pełni zdefiniowanego zakresu znaczeniowego. Występuje on również w treści art. 9 ust. 2 lit. c, jednakże na kanwie żadnego z nich prawodawca nie wskazał sposób jego rozumienia. W związku z tym w poszukiwaniu wskazówek interpretacyjnych należy sięgnąć do motywu 46 preambuły, który jako rodzaje przetwarzania służące żywotnym interesom wskazuje przykładowo: niezbędność przetwarzania do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych, w szczególności w przypadku klęsk żywiołowych i katastrof spowodowanych przez człowieka. W tym kontekście nie ulega wątpliwości, że chodzi o interesy związane z ratowaniem życia bądź zdrowia (z zastrzeżeniem, że dane o zdrowiu należą do szczególnych kategorii danych objętych ochroną na gruncie art. 9 ust. 2 lit. c). Można to odnieść do sytuacji klęski żywiołowej i podjęcia działań w celu ratowania zdrowia lub życia (np. lokalizacji tych osób w celu ewakuacji, dostarczenia leków, żywności itp.), które wiążą się z niezbędnością przetwarzania danych osobowych tych

[51] Por. D. Lubasz, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *op. cit.*, komentarz do art. 6.

osób, albo ustalenia przyczyn utraty przytomności przez osobę fizyczną, np. choroba[52].

Tak nadany kontekst wskazuje, że przesłanka ta jest potencjalnie przydatna również w przypadku działania administracji publicznej, ale sytuacje jej użycia nie będą raczej obejmować zwykłych/rutynowych zadań ADO należącego do sfery publicznej.

2.5. Art. 6 ust. 1 lit. e

Wykonywanie zadania publicznego lub władzy publicznej jako przesłanka legalizująca wskazane zostało jako przesłanka legalizująca w art. 6 ust. 1 lit. e. Stanowi podstawę przetwarzania danych w przypadku organów i podmiotów publicznych, które działają, co do zasady, w celu realizacji zadań „[...] w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi". Rozwiązanie to jest przykładem wykorzystania przez ustawodawcę tzw. zwrotów niedookreślonych. W literaturze przedmiotu zauważa się, że „O klauzulach generalnych w klasycznym rozumieniu tego terminu mówi się bowiem właśnie wtedy, gdy niespornie choćby zinterpretowany przepis prawny głosi, że sposób stosowania prawa w określonych wypadkach ma być uzależniony od oceny organu co do słuszności takiego czy innego rozstrzygnięcia w danej konkretnej sytuacji, czy też od odniesienia do jakiegoś zespołu wartości bezpośrednio niewyznaczonych w samym tekście prawnym, wartości pozaprawnych, albo szerzej – obejmuje się tym mianem również wypadki, gdy przepisy zawierają zwroty niedookreślone znaczeniowo, które w funkcjonowaniu systemu prawnego mają rolę analogiczną do roli klauzul klasycznych", z jednoczesnym podniesieniem, że zwroty takie

[52] Por. B. Kaczmarek-Templin, *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych –wybrane zagadnienia*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *Polska i europejska reforma ochrony danych osobowych,* Warszawa 2016, s. 122.

(pojęcie nieostre) powinny być rozpatrywane, „gdy tylko jest to możliwe, z punktu widzenia praw obywatela”[53].

Nie mniej ważne staje się podkreślenie reguły wskazującej, że organy publiczne są związane przepisami prawa, które wyznacza kryteria ich działania, zatem „w poszukiwaniu zdefiniowania interesu publicznego w konkretnej sytuacji (podobnie jak i celu publicznego) konieczne jest w pierwszej kolejności przeanalizowanie wypowiedzi ustawodawcy na ten temat. Dopiero w razie stwierdzenia, że ustawodawca milczy w tym względzie, a zwłaszcza nie wyjaśnia, jak należy rozumieć i realizować interes publiczny w danej sytuacji, uzasadnione staje się odwołanie do kategorii celu, do jakiego ma zmierzać administracja, a który to cel polega właśnie na realizowaniu ogólnie rozumianego interesu publicznego”[54].

Generalnie interes publiczny identyfikuje się z pojęciem interesu ogółu, a w jeszcze szerszym znaczeniu z dobrem wspólnym[55]. Mówiąc więc o interesie publicznym, myślimy o interesie wspólnoty, którą tworzą np. mieszkańcy osiedla, dzielnicy, jednostki samorządu terytorialnego (np. gminy, powiatu, województwa) czy obywatele (Rzeczpospolita Polska).

Mając na względzie wymóg uwzględnienia interesu publicznego, istotne staje się podniesienie, że w zakresie oceny konkretnej sytuacji faktycznej niezbędne jest podjęcie takich działań (bądź ich zaniechanie), których zakres i charakter uwzględniać będzie troskę o należyte, harmonijne współżycie członków danej społeczności (czy szerzej, gdy chodzi o państwo polskie czy społeczeństwo), co obejmuje zarówno ochronę interesów poszczególnych osób, jak i określonych dóbr społecznych, w tym i mienia publicznego[56]. Jednocześnie ochrona czy uwzględnienie

[53] W. Jakimowicz, *Wykładnia w prawie administracyjnym*, Kraków 2006.
[54] *Ibidem*.
[55] Wyrok TK z dnia 27 stycznia 1999 r., K 1/98.
[56] Por. wyrok TK z dnia 8 października 2007 r., K 20/07.

interesu publicznego, „nie może przybierać postaci, która polegałaby na naruszeniu niezbywalnej godności człowieka”[57].

Regulacja ta daje bardzo szerokie możliwości wykazania legalności przetwarzania, nie skierowane bezpośrednio na ustanowienie kompetencji organu lub podmiotu powołującego się na ich istnienie jako uzasadnienie występowania interesu publicznego. Jeśli przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, jak i wówczas, gdy jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, konieczne staje się, by podstawa prawna takiego przetwarzania była określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator. W dotychczasowych wypowiedziach doktryny bezspornie wyraża się stanowisko, że chodzi o działania prowadzone w interesie publicznym przy użyciu form niewładczych, np. świadczenie pomocy socjalnej, pomocy ofiarom klęsk żywiołowych, walka z terroryzmem, z działającymi niezgodnie z prawem sektami, przeciwdziałanie praniu brudnych pieniędzy itp. I choć w całym przepisie mowa o przetwarzaniu danych „w ramach sprawowania władzy publicznej”, w tym przypadku owego sprawowania władzy nie będziemy utożsamiać z takimi aktami władztwa publicznego, jak decyzje administracyjne, wyroki sądowe czy innego rodzaju akty indywidualno-konkretne stanowiące przejawy władztwa publicznego wobec osób fizycznych czy podmiotów prywatnych, z którymi wiąże się przetwarzanie danych osobowych. Formy władcze stanowią na tyle silną ingerencję w prawa jednostki, że dla realizacji właściwie bezwzględnie wymagają konkretnych w swej treści przepisów rangi ustawy.

Z kolei przetwarzanie danych w ramach sprawowania władzy publicznej powierzonej administratorowi stanowi pewne *novum*. Przesłankę tą należy interpretować z uwzględnieniem przepisów konstytucyjnych,

[57] Wyrok TK z dnia 20 marca 2006 r., K 17/05.

w szczególności art. 51 Konstytucji RP stanowiącego dyrektywę dla ustawodawcy zwykłego w zakresie stosowania zasady proporcjonalności. Należy zatem obligatoryjnie uwzględniać przepisy regulujące zakres dopuszczalnych działań organów wyznaczony normatywnie. Oznacza to, że przetwarzanie określonych danych powinno mieścić się w ramach rzeczowej i miejscowej właściwości podmiotu, który tego dokonuje. W praktyce przypadki stosowania tej przesłanki zapewne często będą zbieżne z tymi, które w poprzednim stanie prawnym znajdowały podstawę w przesłance określonej w art. 23 ust. 1 pkt 4 s.u.o.d.o., zgodnie z którym przetwarzanie danych było dopuszczalne, gdy było niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego. Wydaje się, że w bieżącym stanie prawnym, podobnie jak poprzednio, analizowana przesłanka ma charakter otwarty; nie sposób bowiem z góry określić katalogu zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej w przypadku jakiegokolwiek administratora. Katalogu takich administratorów także zresztą nie sposób określić. Aktualność zachowuje tu stanowisko wyrażone przez NSA na tle art. 23 ust. 1 pkt 4 s.u.o.d.o., iż chodzi tu o zadania, które zostały zlecone przez prawo temu podmiotowi, który dane przetwarza, oraz że mogą to być zadania z zakresu bezpieczeństwa publicznego, walki z przestępczością, udzielania pomocy ofiarom klęsk żywiołowych itd., a podmiotami wykonującymi zadania publiczne mogą zaś być organy państwowe, samorządowe lub komunalne jednostki organizacyjne, a także inne podmioty wykonujące zadania publiczne, w tym podmioty niepubliczne[58]. Bez wątpienia natomiast chodzi tu o takie zadania, które administrator wykonuje – nawiązując do tradycyjnego podziału obszarów działalności podmiotów publicznych – w sferze imperium, a nie sferze dominium, a więc tam, gdzie realizuje swoje kompetencje z zakresu przyznanej mu władzy, nie zaś z zakresu działalności ściśle

[58] Zob. wyrok NSA z dnia 5 lutego 2008 r., I OSK 37/07.

cywilnoprawnej, w tym zwłaszcza właścicielskiej w odniesieniu do majątku, którym dysponuje, czy też w sferze prawnopracowniczej wobec członków swojego personelu. Użytecznym przykładem tego typu zadań mogą być zadania publiczne wyszczególnione w każdej z ustaw samorządowych jako zadania danej wspólnoty. W każdym z tych przypadków zadania określone zostały w taki sposób, że w zależności od konkretnej sytuacji, stanu prawnego w danym czasie, kontekstu realizacyjnego mogą one wymagać przetwarzania danych osobowych bądź nie, a jeżeli tak, na warunkach określonych w RODO potencjalnie można poszukiwać dla nich oparcia w treści art. 6 ust. 1 lit. e.

2.6. Art. 6 ust. 1 lit. f

Przesłanka legalizująca przetwarzanie danych osobowych, gdy przetwarzanie odbywać się ma dla prawnie uzasadnionych interesów, po myśli art. 6 ust. 1 lit. f RODO, adresowana jest zasadniczo do podmiotów sektora gospodarczego i nakierowana na ochronę ich interesów.

Zgodnie z tym przepisem przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy 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, z tym zastrzeżeniem poczynionym *in fine*, że reguła ta nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Oznacza to, że organy władzy publicznej pozostają znacząco ograniczone w możliwości legalizowania za pomocą tak określonej przesłanki dysponowania danymi osobowymi, choć bezwzględnie nie można wykluczyć jej stosowania przez te podmioty. Zasadne wydaje się uznać że dopuszczalne jest jej stosowanie tam, gdzie przetwarzanie danych osobowych odbywa się w celach innych niż te,

które łączą się bezpośrednio z realizacją zadań organów publicznych, na co zdaje się wskazywać motyw 49. Dlatego też przyjmować należy, że organy publiczne mogą korzystać z przedmiotowej przesłanki poza tymi przypadkami, gdy przetwarzanie danych osobowych odbywa się w celu wykonywania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi[59], choć w literaturze napotkać można także stanowisko, wedle którego „[o]mawiana tu przesłanka może być stosowana jedynie przez podmioty prywatne (np. przedsiębiorców), natomiast nie mogą się na nią powoływać podmioty publiczne"[60]. Tymczasem praktyka pokazuje, że wcale nierzadko podmioty publiczne na równi z podmiotami prywatnymi sięgają po tę właśnie przesłankę legalizującą przetwarzanie w przypadkach, gdzie poruszają się w sferze dominium, nie wykonując swojego władztwa. Jako przykład posłużyć nam może wspominane już wskazywanie w umowach danych osobowych osób odpowiedzialnych za realizację umowy, udostępnianie nagrań z monitoringu zamieszczonego na urzędowym parkingu osobom, które brały udział w kolizji itp.

Niewątpliwie jednak każdorazowo przy stosowaniu tej przesłanki konieczne jest dokonanie swoistego testu proporcjonalności. Może mieć on charakter sformalizowany dla celów dowodowych, może też przybrać formę nieudokumentowanej analizy, której odzwierciedlenie znajdzie jedynie wzmianka o tej podstawie prawnej w rejestrze czynności przetwarzania (art. 30 RODO), niemniej jednak test taki należy wykonać. Chodzi o to, że art. 6 ust. 1 lit. f RODO pozwala na przetwarzanie danych osobowych w zakresie niezbędnym do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter

[59] Zob. K. Wygoda, *Modyfikacja...*; M. Gumularz, *Uzasadniony interes w sektorze publicznym – na przykładzie monitoringu*, „ABI Expert" 2018, nr 2, s. 18; A. Nerka, M. Sakowska-Baryła, *op. cit.*, s. 163.

[60] Zob. P. Fajgielski, *Ogólne rozporządzenie...*, s. 176.

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. Warunkiem prawidłowości powołania się na tak określoną przesłankę jest spełnienie łączne następujących kryteriów: po pierwsze – identyfikacja prawnie uzasadnionego interesu, który jest realizowany przez administratora lub przez stronę trzecią; po drugie – zweryfikowanie niezbędności przetwarzania dla realizacji celu wynikającego z przedmiotowego interesu; po trzecie – ocena, 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[61].

Wskazać tu jednocześnie wypada, że zgodnie z motywem 47 RODO administrator przy analizie i dokonywaniu ważenia dóbr powinien wziąć pod uwagę rozsądne oczekiwania osób, których dane dotyczą, oparte na ich powiązaniach z administratorem, czyli np. uwzględnić pozostawanie w relacji z klientem administratora lub gdy osoba działa na jego rzecz.

Biorąc pod uwagę treść 6 ust. 1 lit. f RODO, należy stwierdzić, iż prawodawca unijny, wprowadzając kategorię „uzasadnionego interesu administratora", ustanowił szerszą przesłankę przetwarzania danych osobowych niż miało to miejsce w art. 23 ust. 1 pkt. 5 s.u.o.d.o. z 1997 r., który wprowadzał zbliżoną instytucję „prawnie usprawiedliwionego celu". Odnotować trzeba, że pojęcie „interes" jest szerszą kategorią niż pojęcie „cel". Interes administratora może być określany jako pewna relacja między jakimś stanem obiektywnym a oceną tego stanu z punktu widzenia korzyści, jaką on przynosi lub może przynieść administratorowi, przy czym musi być uzasadniony, co więcej, kategoria ta jest

[61] Szerzej zob. M. Więckowska, *Przetwarzanie danych na podstawie prawnie uzasadnionego interesu*, „ABI Expert" 2018, nr 3, s. 10 i n.; M. Więckowska, *Prawnie uzasadniony interes – test badania równowagi*, „ABI Expert" 2018, nr 3, s. 48-49.

zróżnicowana W RODO nie przesądza się, co taki interes stanowi. W ten sposób stwarza się możliwość *interesu* przez samych zainteresowanych z uwzględnieniem okoliczności każdego przypadku, pod warunkiem spełnienia pozostałych kryteriów określonych w przepisie oraz przy respektowaniu wymagań art. 5 RODO[62]. W sektorze publicznym baczyć należy jednak, by ów interes nie wkraczał w obszar władztwa organów władzy publicznej, bo wówczas korzystanie z analizowanej tu przesłanki jest wyłączone. Warto w tym miejscu odnotować, że zgodnie z motywem 47 zakres klauzuli uzasadnionego interesu administratora obejmuje marketing bezpośredni oraz zapobieganie oszustwom[63]. Względy takie w pewnej mierze wystąpić mogą także po stronie podmiotu publicznego.

2.7. Art. 10 RODO

Na podkreślenie zasługuje fakt, że RODO, odwołując się w art. 10 do kategorii informacji „dotyczących wyroków skazujących i naruszeń prawa" oraz innych informacji o adekwatnej wartości (np. orzeczeń o umorzeniu postępowania, zawieszeniu wykonania kary, ułaskawieniu itd.) dopuszcza przetwarzanie tych dość specyficznych informacji (pojawiających się jako efekt końcowy działalności m.in. sądownictwa) w innych okolicznościach, niż wskazuje to dyrektywa 2016/680. Należy podkreślić, że co do zasady nie chodzi tu jo wszelkie dane zebrane w trakcie postępowań, a jedynie o informacje obejmujące ich końcowy efekt. Nie można jednak wykluczyć, że przynajmniej część z rozstrzygnięć zapadających w trakcie postępowania (np. postanowienie o tymczasowym aresztowaniu) również powinno być postrzegane jako mieszczące się w granicach art. 10 RODO[64]. W odróżnieniu od s.u.o.d.o. (w formie, jaką

[62] Zob. A. Nerka, M. Sakowska-Baryła, *op. cit.*, s. 166-168.

[63] Zob. P. Barta, *Prawnie uzasadniony interes w działalności marketingowej*, „ABI Expert" 2018, nr 3, s. 15 i n.

[64] Podobnie wskazują P. Litwiński, P. Barta i M. Kawecki, omawiając użyte w art. 10 RODO pojęcie „powiązanych środków bezpieczeństwa". Uznają oni, że powinno się je

przyjęto po nowelizacji z 25 sierpnia 2001 r.)[65] RODO, uznając je za specyficzny rodzaj danych, nie przynależących jednak do kategorii danych szczególnych, wskazuje jako właściwe przesłanki legalizujące proces ich przetwarzania te ujęte w art. 6. a nie w art. 9 RODO.

Na relatywnie szerokie możliwości przetwarzania tej grupy informacji wskazuje choćby treść motywu 97 RODO[66]. Odnosząc się bezpośrednio do potrzeby powołania inspektora danych, prawodawca dał w nim wyraźnie do zrozumienia, że może istnieć bliżej nieokreślona grupa podmiotów publicznych (choć teoretycznie dotyczy to również sektora prywatnego), których główna działalność polegać będzie na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa. Bez wątpienia w przypadku organów i podmiotów publicznych swoboda ich

interpretować zbieżnie ze „środkami karnymi" w rozumieniu art. 30 k.k. – P. Litwiński (red.), *op. cit.*, s. 346-347.

[65] Dz. U. Nr. 100, poz. 1087 – ustawodawca dokonał wówczas włączenia tej kategorii informacji do art. 27, który regulował przetwarzanie danych szczególnie wrażliwych objętych generalnym zakazem przetwarzania. Pomimo tego zabiegu prawidłowa wykładnia zmuszała do sięgania po dyrektywę 95/46/WE i traktowania ich jako szczególnej grupy informacji, przetwarzanych wyłącznie w oparciu o przepisy wskazujące taką możliwość.

[66] Motyw 97) RODO: Jeżeli przetwarzania dokonuje organ publiczny z wyjątkiem sądów lub niezależnych organów wymiaru sprawiedliwości w ramach sprawowania wymiaru sprawiedliwości lub jeżeli w sektorze prywatnym przetwarzania dokonuje administrator, którego główna działalność polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, to w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. W sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający. Tacy inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.

przetwarzania nie będzie jednak pełna, w szczególności gdy podmioty te uznamy za synonimiczne określenie władz publicznych[67], które, jak wielokrotnie podkreślano, co do zasady działają na podstawie i w granicach prawa.

Co ciekawe, pojawia się tu swoisty paradoks, gdyż biorąc pod uwagę wymogi, jakie stawia się w art. 10 RODO, skupiające się na tym, by przetwarzania dokonywać wyłącznie pod nadzorem władz publicznych lub podejmować je w sytuacji, gdy jest ono dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą, można by założyć, że w przypadku podmiotów zaliczanych do władz publicznych oba te warunki spełnione będą jednocześnie. Nie można jednak uznać takiego stwierdzenia za w pełni właściwą interpretację, trudno bowiem automatycznie utożsamić przetwarzanie dokonywane przez podmioty publiczne – realizowane dla własnych potrzeb, niezwiązanych bezpośrednio z realizacją zadań władzy (np. w sferze zatrudnienia, gdzie ustawowo wskazany wymóg niekaralności jest dość często spotykany w sektorze publicznym) – z działaniami dokonywanymi pod nadzorem władz publicznych. Warto wspomnieć, że wymóg działania podejmowanego pod nadzorem władz zdaje się obligatoryjnie dotyczyć jedynie tych przypadków, w których budowane są rozbudowane czy, jak wskazuje prawodawca, kompletne rejestry[68] przeznaczone do gromadzenia tego typy informacji.

W przypadku podmiotów i organów publicznych dość bezpiecznym założeniem będzie przyjęcie, że spośród pełnego katalogu przesłanek legalizujących przetwarzanie danych w oparciu o art. 6 ust. 1 RODO będą się one mogły posługiwać się ujętą na trzecim miejscu zasadą wskazującą, że przetwarzanie jest niezbędne do wypełnienia obowiązku

[67] O dużych problemach i wątpliwościach interpretacyjnych, związanych z tą kategorią administratorów i podmiotów przetwarzających, pisze np. M. Jabłoński, [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *op. cit*., s. 76-82.

[68] W Polsce oznacza to *de facto* działania podejmowane w granicach opisanych w ustawie z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2017 r., poz. 678).

prawnego ciążącego na administratorze. Z natury swej zdaje się to dobrze korespondować z regułą podejmowania działań w granicach i na podstawie prawa – choć w tym wypadku dotyczyć to będzie nie tylko realizacji kompetencji organów władzy. Dobrą egzemplifikacją takiego działania będą, wskazywane już wcześniej, sytuacje przetwarzania danych przez pracodawców należących do sfery publicznej, dotyczące karalności osób będących np. pracownikami samorządowymi. W odróżnieniu od dość prostego do interpretacji stanu, w którym przetwarza się jakieś wybrane kategorie danych, objętych art. 10 RODO bezpośrednio w oparciu o przepis prawa, wątpliwości zdaje się budzić sytuacja przetwarzania tych danych w oparciu o zgodę osoby, której one dotyczą. Typowym tego przykładem jest przekazanie ich pomiędzy innymi informacjami w dokumentach składanych do podmiotu publicznego np. przez kandydatów do pracy (gdy konkretne stanowisko nie wymaga niekaralności) lub inne osoby, które z faktu osadzenia w więzieniu czy konieczności zapłaty grzywny wywodzą swoje wnioski – uzasadniając tym choćby niedotrzymanie jakiegoś terminu czy brak realizacji płatności. Wobec szeregu obowiązków ciążących na organach publicznych, zwłaszcza tych związanych z realizacją zadań w aspekcie proceduralnym, nie jest możliwe niszczenie zawierających te informacje dokumentów lub ich selektywne usuwanie nawet wówczas, gdy dane takie w najmniejszym nawet stopniu nie przyczyniają się do załatwienia konkretnej sprawy[69].

[69] Warto w tym wypadku odesłać do poradnika przygotowanego przez Ministerstwo Cyfryzacji, który wprawdzie dotyczy ADO ze sfery prywatnej ale wskazane w nim poglądy zdają się być aktualne również w sferze publicznej. W odniesieniu do ADO, który otrzymuje informacje bez własnej woli, wskazano, że nie ma on „obowiązku usunięcia danych (w tym danych wrażliwych wykraczających poza dane, które miał zamiar zebrać), jeżeli z przyczyn technicznych nie jest możliwe ich usunięcie bez jednoczesnego usunięcia danych, które administrator ma prawo przetwarzać (np. kiedy dane wrażliwe znajdują się w jednym piśmie z żądaniem klienta lub jego danymi kontaktowymi). W takim wypadku wystarczające dla ochrony danych osobowych jest, jeżeli administrator:

- nie ma możliwości i nie będzie podejmował próby użycia tych danych osobowych w stosunku do osoby, której dane dotyczą ani też
- przechowywanie danych nie będzie miało wpływu na tę osobę,

2.8. Art. 9 RODO

Poprzednio omawiane przesłanki legalizujące przetwarzanie dotyczyły procesów, w których administratorzy mają do czynienia z tzw. danymi zwykłymi (oraz przetwarzanymi w oparciu o te same podstawy dane penalne, o których mowa w art. 10 RODO). Należy jednak podkreślić, że w RODO (podobnie jak to miało miejsce na gruncie wcześniejszych regulacji) mamy również do czynienia z innym rodzajem danych, które uznawano powszechnie za dane szczególnie wrażliwe. Na gruncie rozporządzenia ogólnego noszą one miano „danych szczególnych kategorii", a ich przetwarzanie jest objęte zakazem, który podlega uchyleniu w oparciu o przesłanki wyartykułowane w art. 9 ust. 2 RODO.

Do „szczególnych kategorii danych" zaliczamy informacje ujawniające:

- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych.

Zakazem objęte jest również przetwarzanie:

- danych genetycznych,
- danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej,
- danych dotyczących zdrowia,
- seksualności lub orientacji seksualnej konkretnej osoby[70].

- nie udostępnia tych danych ani nie umożliwia dostępu do nich innemu podmiotowi,
- zabezpiecza dane osobowe odpowiednimi środkami technicznymi i organizacyjnymi, usuwa dane niezwłocznie, kiedy jest to możliwe", Ministerstwo Cyfryzacji, *RODO. Poradnik dla sektora Fintech*, Warszawa 2018, s. 12.

[70] Szerszą analizę treści i zakresu stosowania art. 9 RODO zob. P. Fajgielski, *op. cit.*, s. 193-216; P. Litwiński (red.), *op. cit.*, s. 326-344; M. Kuba, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *op. cit.*, s. 437-454; A. Nerka, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 178-188.

W sferze publicznej przetwarzanie tego rodzaju danych będzie mieć miejsce w wielu sytuacjach, jednak modelowo należy poszukiwać dodatkowego prawnego uzasadnienia (czy nawet wprost wyartykułowanej podstawy) dla procesów przetwarzania realizowanych w ramach sprawowania władzy. Inaczej rzecz ujmując, można przyjąć, że ich przetwarzanie nie będzie możliwe, jeśli nie stanowią one jednej z przesłanek realizacji kompetencji takiego podmiotu. Chodzi tu zwłaszcza o sytuacje, w których przepis prawa wymusza zbadanie określonego stanu faktycznego obejmującego informacje mieszczące się w grupie „szczególnych kategorii danych" jako element procesu decyzyjnego w ramach sprawowania władzy publicznej. Ta perspektywa wskazuje, że tylko część przesłanek znoszących zakaz przetwarzania danych tej kategorii[71] będzie właściwa dla grupy zaliczanej do administracji publicznej. Oczywiście w stosunkach pracowniczych organy i podmioty publiczne mogą być jednak traktowane jak zwykli administratorzy.

Można zgodzić się z poglądem wyrażonym w doktrynie[72], że dla sektora publicznego podstawowe znaczenie powinny mieć przesłanki wskazane w art. 9 ust. 2 lit. b) oraz od e) do h). Przy czym część z tych przesłanek nie powinna być jbrana pod uwagę w sytuacjach realizacji kompetencji władczych. Szczególnie dotyczy to podejmowania przetwarzania niezbędnego do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej oraz tego, co uznane zostanie za niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej

[71] Poza wskazanymi wyżej publikacjami syntetyczną analizę przesłanek umożliwiających przetwarzanie „szczególnych kategorii danych" przedstawia A. Krasuski, *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018, s. 226-236.

[72] M. Gumularz, *Ochrona danych osobowych w sektorze publicznym,* Warszawa 2018, s. 130-131.

lub zabezpieczenia społecznego (mieści się to w art. 9 ust. 2 lit. b) i h) RODO).

W stosunku do przesłanki zgody (art. 9 ust. 2 lit. a) RODO), która nie została wskazana wyżej, należy wyrazić daleko idące zastrzeżenia i bez wyartykułowanego *expressis verbis* wymogu uzyskania jej przez podmioty zaliczane do szeroko pojętej administracji publicznej nie traktować jako dopuszczalnej przesłanki legalizującej proces przetwarzania tej kategorii danych w sferze imperium państwa.

Bez wątpienia szczególną rolę w ramach realizacji kompetencji władczych administracji publicznej odgrywać będą przesłanki f) i h) wskazujące na możliwość przetwarzania, gdy jest ono niezbędne do ustalenia, dochodzenia lub obrony roszczeń albo w ramach sprawowania wymiaru sprawiedliwości przez sądy, a także z uwagi na niezbędność ze względów związanych z ważnym interesem publicznym. Przy czym ten ostatni warunek wymaga, by interes był identyfikowalny na podstawie prawa Unii lub prawa państwa członkowskiego, a zakres przetwarzania obejmował to, co jest proporcjonalne do wyznaczonego celu, nie naruszając istoty prawa do ochrony danych. Działanie to odbywać się musi w ramach określonej procedury, gdyż tylko ona zapewnia odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą. Co niezwykle istotne, realizacja celu publicznego nie upoważnia ADO do swobodnego wyznaczania osób dokonujących operacji przetwarzania, gdyż zgodnie z art. 9 ust. 3 RODO jest to możliwe „jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe".

Podsumowując zagadnienie przetwarzania „szczególnych kategorii danych" przez administrację publiczną, należy jeszcze raz podkreślić, że ich wykorzystanie w ramach realizacji kompetencji organów wymaga, by w ustawach szczególnych wskazywano taką konieczność co najmniej w ramach wymogów materialnych szeroko ujętego procesu decyzyjnego. Pożądane jest również formalne/proceduralne określenie zasad podejmowanych działań, co jednak zasadniczo nie powinno być większym problemem w ramach działań podejmowanych przez organy administracji publicznej.

Rozdział III

Inspektor Ochrony Danych a obowiązki administratora

(dr Marlena Sakowska-Baryła)

Funkcjonowanie inspektora ochrony danych (dalej: inspektor, IOD) w systemie ochrony danych osobowych poprzedzało wyznaczanie administratora bezpieczeństwa informacji (ABI) przez administratora danych na warunkach określonych w ustawie o ochronie danych osobowych z 1997 r. jako urzędnika ds. ochrony danych osobowych (ang. *data protection official*), o którym stanowił art. 18 ust. 2 oraz art. 20 ust. 2 dyrektywy 95/46/WE Parlamentu Europejskiego i Rady. Inspektor jest właściwie sukcesorem ABI, choć treść przepisów RODO określających status IOD, jego zadania, usytuowanie w strukturze organizacyjnej, a wreszcie kwestie jego pojawienia się w organizacji w pewnym zakresie różni się od stanu poprzedniego. Na pierwszy plan wysuwa się zagadnienie obowiązkowego wyznaczania IOD w przypadkach określonych w art. 37 ust. 1 rozporządzenia, następnie warunki dopuszczalności wyznaczenia jednego IOD dla więcej niż jednego podmiotu, a także same zadania przypisane temu podmiotowi, które określone są z jednej strony dość szeroko, ale z drugiej pozostawiają spore pole do uszczegółowienia w wewnętrznych procedurach (politykach) administratora. W literaturze i praktyce wielokrotnie podkreśla się, że instytucja IOD ma kluczowe znaczenie w nowym modelu ochrony danych osobowych, a sam IOD odgrywać ma w tym systemie kluczową rolę. Zapewne jest tak, ponieważ,

na gruncie przepisów RODO, IOD określać można jako „gwaranta" właściwego stosowania przepisów tego rozporządzenia. Temu celowi służą wymagania stawiane osobie wykonującej funkcję inspektora odnośnie kwalifikacji zawodowych, wiedzy, doświadczenia, umiejętności, warunku dokształcania się, rozwijania kompetencji społecznych i spełniania standardów etycznych. Przepisy RODO dotyczące IOD są skonstruowane w taki sposób, że podkreślają ważną rolę tej instytucji, kompetencji, które ma posiadać IOD, oraz niezbędnych działań, aby do tego się przygotować. Przepisy kreujące IOD jako gwaranta należytego wykonywania przepisów z zakresu ochrony danych osobowych należy oceniać jako szansę na profesjonalizację osób pełniących tę funkcję, jak również całej grupy zawodowej[73]. Osiągnięcie tego celu zależy jednak od rzetelnego doboru osób pełniących tę funkcję, zadbania o ich odpowiednie przygotowanie oraz możność utrzymywania standardu fachowości, co uzależnione jest tak od uwarunkowań organizacyjnych, jak i środków finansowych przeznaczonych na utrzymanie IOD w konkretnej jednostce organizacyjnej – u danego administratora czy podmiotu przetwarzającego. W znacznej części za osiągnięcie należytego stanu w tym względzie odpowiedzialne będą podmioty z sektora publicznego, bo to one mają obowiązek wyznaczenia IOD. W tym stanie rzeczy, jeśli dobór IOD będzie odbywał się przypadkowo – na zasadzie dodania wybranemu pracownikowi zadań IOD bez względu na jego wiedzę i umiejętności z zakresu ochrony danych osobowych albo gdy za wyborem konkretnego IOD przemawiać będzie wyłącznie niska cena oferowanej przez niego usługi, nie wydaje się, by funkcjonowanie takiego inspektora w organizacji w istocie miało gwarancyjny charakter. Obserwacja praktyki pierwszych miesięcy stosowania RODO pokazuje, że zapewnienie inspektora ochrony danych u publicznych administratorów niekiedy powodowało znaczne trudności finansowe i organizacyjne.

[73] Zob. A. Nerka, *Komentarz do art. 37*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 405.

Konieczność wyznaczenia IOD uczyniła bowiem niezbędnym zapewnienie odpowiednich środków finansowych w budżecie, dokonania „przesunięć" tych środków, wymusiła zdecydowanie o organizacyjnej formule wykonywania funkcji przez IOD, a więc chociażby o tym, czy powołuje się jednego inspektora dla kilku podmiotów i jak właściwie się tego dokonuje, czy IOD jest „wewnętrzny", czy „zewnętrzny", a więc czy wchodzi w skład personelu pracowniczego jednostki, czy świadczy usługi na podstawie umowy cywilnoprawnej.

1. Obowiązek wyznaczenia IOD

Zgodnie z art. 37 ust. 1 RODO administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych zawsze, gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
b) 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; lub
c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9, lub danych osobowych dotyczących wyroków skazujących i czynów zabronionych, o czym mowa w art. 10.

Treść art. 37 ust. 1 RODO pozostaje w powiązaniu z motywem 97 preambuły RODO, gdzie klaruje się, że jeśli przetwarzania dokonuje organ publiczny z wyjątkiem sądów lub niezależnych organów wymiaru sprawiedliwości w ramach sprawowania wymiaru sprawiedliwości lub

jeżeli w sektorze prywatnym przetwarzania dokonuje administrator, którego główna działalność polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę, lub jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, to w monitorowaniu wewnętrznego przestrzegania RODO administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych.

Dla prowadzonych tu analiz istotne znaczenie ma, że RODO wymaga, aby IOD był wyznaczony zawsze, gdy przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości[74]. Kategoria „organy lub podmioty publiczne" nie została sprecyzowana w RODO. W opinii Grupy Roboczej art. 29 dotyczącej inspektorów ochrony danych (*Wytyczne dotyczące inspektorów ochrony danych ('DPO'). Przyjęte w dniu 13 grudnia 2016 r.* przez Grupę Roboczą Art. 29 Ds. Ochrony Danych, WP 243) wskazano, że pojęcie to powinno zostać określone na poziomie przepisów krajowych, a do podmiotów takich najczęściej zalicza się organy władzy krajowej, organy regionalne i lokalne, a jednocześnie, z mocy właściwego prawa krajowego, może być zaliczonych także wiele innych podmiotów prawa publicznego. Z art. 9 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000) wynika, że do grona organów i podmiotów publicznych zobowiązanych do wyznaczenia IOD należą:

a) jednostki sektora finansów publicznych;
b) instytuty badawcze;
c) Narodowy Bank Polski.

[74] Szerzej zob. M. Sakowska-Baryła, *Obowiązek wyznaczenia IOD w podmiotach publicznych*, „ABI Expert" 2017, nr 2, s. 10 i n.

Zgodnie z art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. z 2017 r., poz. 2077 ze zm.), do jednostek sektora finansów publicznych zalicza się:

1) organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;
2) jednostki samorządu terytorialnego oraz ich związki;
3) związki metropolitalne;
4) jednostki budżetowe;
5) samorządowe zakłady budżetowe;
6) agencje wykonawcze;
7) instytucje gospodarki budżetowej;
8) państwowe fundusze celowe;
9) Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego;
10) Narodowy Fundusz Zdrowia;
11) samodzielne publiczne zakłady opieki zdrowotnej;
12) uczelnie publiczne;
13) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne;
14) państwowe i samorządowe instytucje kultury;
15) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego.

Tak ukształtowany zakres podmiotowy jednostek sektora finansów publicznych pozwala stwierdzić, że należą do nich tzw. podmioty instytucjonalne – jednostki organizacyjne, a więc osoby prawne lub jednostki organizacyjne niemające osobowości prawnej, utworzone przez państwo

lub jednostkę samorządu terytorialnego, wykonujące zadania publiczne, całkowicie lub częściowo finansowane ze środków publicznych

Obowiązek wyznaczenia IOD dotyczy tak określonych podmiotów publicznych niezależnie od charakteru ich działalności i skali przetwarzania danych osobowych, jak również wielkości, rodzaju czy zastosowanych w nich rozwiązań organizacyjnych. W efekcie wyznaczenie IOD to zadanie między innymi gminnej biblioteki zatrudniającej trzy osoby czy małego przedszkola, którego personel przetwarza dane osobowe kilkanaściorga dzieci, a liczebność personelu nie przekracza kilku osób. Od strony praktycznej to istotny problem zwłaszcza dla jednostek samorządu terytorialnego, które wraz rozpoczęciem stosowania RODO musiały zapewnić inspektorów dla dużej liczby podmiotów, w tym także odpowiednie środki finansowe na ich zaangażowanie, oraz zapewniać na to odpowiednie finansowanie w przyszłości.

Choć taki obowiązek nie wynika z przepisów RODO, Grupa Robocza Art. 29 we wspomnianych wytycznych WP 243 zaleca, aby prywatne jednostki realizujące zadania w interesie publicznym lub sprawujące władzę publiczną także powoływały inspektora. Takie rozwiązanie należałoby zalecać z należytą rozwagą, bowiem kwalifikowanie zadania jako „publicznego" nie oznacza, że automatycznie mamy do czynienia z przetwarzaniem danych osobowych o podwyższonych standardach bezpieczeństwa czy podwyższonym ryzyku naruszeń wolności lub praw osoby fizycznej. Takimi podmiotami mogą być m.in. fundacje przetwarzające dane osobowe wielu osób np. dotkniętych różnymi chorobami czy wymagających pomocy w zakresie mocno wkraczającym w sferę prywatności osoby fizycznej, jak i punkty przedszkolne, które przetwarzają dane niewielkiej grupy uczniów i ich rodziców.

Obserwując praktykę stosowania RODO, można też podawać w wątpliwość trafność konceptu prawodawcy unijnego wynikającego z omawianego tu art. 37 ust. 1 lit. a, by IOD pojawiał się w każdym podmiocie wyłącznie dlatego, można mu przypisać przymiot „publiczności"

w rozumieniu tego przepisu, i dookreślającego jego desygnaty art. 9 u.o.d.o., bez możliwości wzięcia pod uwagę dodatkowych kryteriów dotyczących przetwarzania danych osobowych lub czynników mających wpływ na jego zakres, charakter, kontekst i cele. Nie sposób też jednoznacznie stwierdzić, czy formalne wyznaczenie w nich IOD realnie wpływa na podwyższenie standardów ochrony danych osobowych, zwłaszcza gdy, korzystając z możliwości przewidzianej w art. 37 ust. 3 RODO, wyznacza się jednego inspektora dla wielu podmiotów bez uwzględniania ich faktycznych potrzeb i specyfiki działania.

Na odnotowanie zasługuje jednocześnie swoiste wyłączenie spod obowiązku wyznaczenia IOD w odniesieniu do sądów w zakresie sprawowania wymiaru sprawiedliwości i niewyrażony wprost, ale dający się wyprowadzić w drodze interpretacji art. 37 ust. 1 lit. a RODO powrót do reguły ogólnej wyznaczania IOD tam, gdzie w sądach wymiaru sprawiedliwości się nie stosuje, a działania sądu nakierowane są np. na warstwę organizacyjną i administracyjną, w tym na zatrudnianie pracowników, obsługę praktyk, realizację dostępu do informacji publicznej, prowadzenie list biegłych i dokonywanie z nimi odpowiednich rozliczeń, realizację zamówień publicznych, zawieranie umów cywilnoprawnych, obsługę wideomonitoringu, kontrolę wejść i wyjść itp.[75] W tych wszystkich przypadkach bowiem nie mamy do czynienia ze sprawowaniem wymiaru sprawiedliwości, a skoro tak, uzasadnione jest wyznaczenie w sądzie IOD, który swym nadzorem obejmować będzie tak zarysowany obszar procesów przetwarzania danych osobowych. Oznacza to, że także w sądach – z uwagi na ich „publiczny" charakter – wyznaczenie IOD jest obligatoryjne.

[75] Zob. *ibidem* s. 13; P. Fajgielski, *Ogólne rozporządzenie...*, s. 416; K. Wójcik-Prządka, *Sądy Powszechne a rodo*, „ABI Expert" 2018, nr 2, s. 61.

2. Obowiązek wyznaczenia IOD w ujęciu podmiotowym

Z art. 37 ust. 1 lit. a RODO wynika, że obowiązek wyznaczenia inspektora przepis ten nakłada na administratora w rozumieniu art. 4 pkt 7 RODO oraz na podmiot przetwarzający (procesora), o którym mowa w art. 4 pkt 8 rozporządzenia.

Zgodnie z art. 4 pkt 7 RODO wynika, że „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. Niestety tak określony zakres podmiotowy pojęcia „administrator" w dalszym ciągu – analogicznie, jak miało to miejsce w poprzednim stanie prawnym pod rządami s.u.o.d.o. z 1997 r. – nie do końca czyni jasnym, kogo w publicznych jednostkach uznać za administratora. Problem ten aktualizuje się już przy elementarnej kwestii ustalenia, czy administratorem w danym przypadku jest organ czy obsługujący go urząd, a w przypadku samorządu terytorialnego – czy administratorem jest jednostka samorządu terytorialnego, czy odpowiednio organ uchwałodawczy oraz organ wykonawczy, wyodrębnione komunalne jednostki budżetowe, a w przypadku gmin także rady osiedli, zarządy osiedli, itp. Najbardziej efektywne byłoby w tym przypadku, aby kwestia owego administrowania rozwiązana była w przepisach ustawowych choćby „wdrażających" przepisy RODO, bo takie dostosowanie prawa krajowego jest nieodzowne. Tyle że polski prawodawca z rzadka korzysta z możliwości ustawowego określenia administratora, co właśnie w okresie dostosowywania organizacji do spełniania wymogów RODO w sektorze publicznym szczególnie doskwierało. Oto bowiem w podobnych

okolicznościach prawnych i faktycznych obserwować można różne ujęcia. Najbardziej jest to widoczne w sektorze samorządowym, gdzie niekiedy samą jednostkę samorządu terytorialnego traktuje się jako administratora albo przymiot administratora przypisuje się wyodrębnionym w jej ramach jednostkom organizacyjnym, a także jej organom – każdemu z osobna. Nie przesądzając jednoznacznie o słuszności tych rozwiązań, w kontekście analiz dotyczących wyznaczenia inspektora ochrony danych, wskazać należy, że pierwszy model – potraktowanie gminy, powiatu czy województwa jako „globalnego" administratora w jednostce samorządowej nie zawsze jest rozwiązaniem usprawiedliwionym. Nadto w kontekście wyznaczania IOD bywa mocno problematyczne. Jeśli bowiem przyjąć, że administrator wyznacza jednego IOD, to wyznaczenie takiego IOD w ramach odpowiednio urzędu gminy, starostwa powiatowego czy urzędu marszałkowskiego oznaczałoby, że ów inspektor jednocześnie pozostaje IOD dla licznych jednostek budżetowych powołanych do życia w rzeczonych jednostkach samorządowych. Tymczasem nie sposób określić, w jaki sposób takiemu „zbiorczemu" inspektorowi można by zapewnić rzeczywiste wykonywanie zadań określonych w art. 39 RODO we wszystkich jednostkach organizacyjnych jednostki samorządu, które na dodatek na gruncie RODO mogą występować wobec siebie w charakterze administratorów i podmiotów przetwarzających. W takim przypadku może być trudno ustrzec się konfliktu interesów i pozorności działań nadzorczych.

Podmiot przetwarzający natomiast, to – po myśli art. 4 pkt 8 RODO – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. „Publiczne" podmioty mogą pozostawać w stosunku powierzenia w charakterze procesora zarówno wobec „publicznych" administratorów, jak i administratorów „prywatnych". Szczególnie często występującym w ostatnim okresie przypadkiem powierzenia jest przetwarzanie przez centra usług wspólnych danych osobowych, które pozostają w dyspozycji jednostek obsługiwanych będących administratorami.

Z treści art. 37 ust. 1 lit. a RODO wywodzić należy, że chodzi w nim o podmiot przetwarzający, który jednocześnie posiada przymiot bycia „organem lub podmiotem publicznym". Nie chodzi tu zatem o podmiot przetwarzający związany stosunkiem powierzenia przetwarzania z „publicznym" administratorem, ale procesora, który sam ma „publiczny" charakter i jest zaliczany do jednostek organizacyjnych określonych w art. 9 u.o.d.o.

W literaturze napotkać jednak można stanowisko, zgodnie z którym „[a]naliza komentowanego przepisu może prowadzić do wątpliwości, czy obowiązek wyznaczenia inspektora ochrony danych ciąży również na podmiotach przetwarzających dane na zlecenie administratorów będących podmiotami publicznymi. Pomimo tego, że w ust. 1 lit. a komentowanego artykułu nie wskazano podmiotów przetwarzających dane na zlecenie administratora będącego podmiotem publicznym, to należy przyjąć, iż w tym przypadku wyznaczenie inspektora ochrony danych przez podmioty przetwarzające jest wymagane, gdyż przetwarzanie odbywa się w imieniu (na zlecenie) administratora, a podmiot przetwarzający jako adresat obowiązku został wskazany w ust. 1 komentowanego artykułu"[76]. Z tak postawioną tezą trudno się jednak zgodzić. Po pierwsze, literalnie art. 37 ust. 1 lit. a RODO nie wprowadza tak określonego wymagania, a więc wyznaczania IOD przez procesora, o ile tylko świadczy usługi na rzecz publicznego administratora. Po drugie zaś, tak wykreowane wymaganie ograniczałoby znacząco swobodę działalności gospodarczej i swobodę wyboru podmiotów przetwarzających do takich, które korzystają z obsługi wyznaczonego przez siebie IOD, a nadto prowadziłoby do kłopotliwych sytuacji, bo charakter, zakres, kontekst i cel powierzonego przetwarzania częstokroć w żadnej mierze nie wymagają objęcia ich nadzorem IOD. Przykładowo, jeżeli przedmiotem powierzenia przez publicznego administratora – wójta – jest

[76] P. Fajgielski, *Ogólne rozporządzenie…*, s. 416.

wykonanie przez grafika imiennych okolicznościowych dyplomów dla osób wyróżnionych za zasługi dla gminy bądź jeśli przedmiotem powierzenia przez szkołę jest skorzystanie z usługi introligatora oprawiającego dzienniki lekcyjne czy inne dokumenty prowadzone przez szkołę, nie sposób twierdzić, że odpowiednio grafik czy introligator mają na potrzeby realizacji tej konkretnej usługi wyznaczać IOD. Przecież przez fakt realizacji usługi dla organu czy podmiotu publicznego takim podmiotem się nie stają.

3. Wyznaczenie IOD wielu podmiotów

W RODO przewidziano możliwość wyznaczenia IOD dla więcej niż jednego podmiotu, a mianowicie dla grupy przedsiębiorstw (art. 37 ust. 2) oraz dla kilku organów lub podmiotów publicznych będących administratorami lub procesorami (art. 37 ust. 3)[77].

Zgodnie z 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. Stosowanie tego rozwiązania wymaga jednak rozwikłania kilku wątpliwości, co jednak nie jest proste i póki co nie znajduje wsparcia w orzecznictwie ani praktyce Prezesa UODO. Po pierwsze, trzeba zmierzyć się z problemem odpowiedniego wyłożenia znaczenia terminu „kilka"; po drugie, kłopotliwe jest ustalenie, w jaki sposób należałoby usytuować owego wspólnego IOD organizacyjnie. W tym drugim przypadku pojawia się jeszcze kwestia tego, jak to wyznaczenie IOD dla wielu sformalizować – z kim ma on zawrzeć umowę, w przypadku wskazania tej samej osoby jako IOD w kilku wyodrębnionych jednostkach organizacyjnych który

[77] Szerzej zob. P. Litwiński, *Wyznaczenie jednego IOD przez grupę podmiotów,* „ABI EXPERT" 2017, nr 2, s. 17 i n.

podmiot miałby prawo do wyznaczenia IOD dla kilku podmiotów lub organów, kiedy ta decyzja miałaby być wiążąca, czy znaczenie powinny mieć stosunki panujące między tymi podmiotami, a wreszcie jaki wpływ może mieć taki IOD na działanie podmiotu, z którym nie wiąże go stosunek prawnopracowniczy lub umowy i czy jako pracownik jednego podmiotu – przy IOD zatrudnionym na etacie – może mieć wpływ na działanie podmiotów, z którymi nie pozostaje w takim samym stosunku.

Słownikowo i w języku potocznym „kilka" znaczy więcej niż jeden i mniej niż dziesięć, a więc maksymalnie dziewięć, jednak przy stosowaniu RODO pierwsze być powinny względy celowości. W konsekwencji pojęcie to powinno być interpretowane poprzez odwołanie się do celu regulacji. W tym przypadku należy przyjmować, że w tym przypadku wyznaczenie IOD dla kilka podmiotów niekoniecznie musi być rozumiane jako maksymalnie dziewięć[78]. Chodzi tu bowiem o to, by wyznaczyć IOD z uwzględnieniem struktury organizacyjnej i wielkości takich podmiotów, aby było możliwe spełnienie wymogów wynikających z art. 37-39 RODO i aby taki inspektor mógł rzetelnie wykonywać zadania. Należy przy tym zaakcentować, że IOD wyznaczony dla kilku administratorów czy podmiotów przetwarzających działa w interesie każdego z nich osobno. Dlatego też przed jego wyznaczeniem w tej formule konieczne jest dokonanie ustaleń co do struktury i wielkości podmiotów objętych wspólną obsługą, ażeby świadczący ją IOD mógł rzeczywiście należycie wykonywać przypisane mu zadania. Istotne jest także takie ułożenie relacji obsługiwanych przez „jednego" IOD podmiotów, aby nie powstawał po jego stronie konflikt interesów.

Wzgląd na strukturę organizacyjną podmiotów i ich wielość, zgodnie z art. 37 ust. 3 RODO powoduje, że te właśnie czynniki w pierwszej kolejności należy brać pod uwagę przy decydowaniu się na wyznaczenie IOD dla większej liczby podmiotów. To one bowiem decydująco

[78] Tak też A. Nerka, *op. cit.*, s. 410-411; P. Fajgielski, *Ogólne rozporządzenie*…, s. 421.

wpływają na ustalenia co do dopuszczalności zgrupowania ich dla sprawowania nadzoru w systemach ochrony danych osobowych każdego z nich przez tego samego IOD. Wyklucza to stosowanie omawianego rozwiązania w takich przypadkach, gdzie wielkość i rozbudowana struktura publicznych administratorów lub podmiotów przetwarzających powodowałaby problemy w należytym wykonywaniu obowiązków przez IOD w równym stopniu na rzecz wszystkich podmiotów, dla których został wyznaczony. Należy przyjąć, że taka konstrukcja nie powinna być stosowana, np. łącznie dla kilku gmin czy kilku powiatów albo kilku ministerstw właśnie ze względu na rozbudowaną strukturę tych podmiotów i bardzo dużą liczbę realizowanych przez nie zadań, których rozmiar powoduje, że ta sama osoba nie mogłaby równocześnie wykonywać zadań IOD we wszystkich tych podmiotach.

Jednocześnie przy wyznaczaniu IOD dla kilku podmiotów należy dołożyć należytej staranności w takim doborze podmiotów do grupy wspólnie obsługiwanych i tak zaplanować realizację zadań przez inspektora, aby uniknąć konfliktu interesów. Poszczególne podmioty mogą bowiem pozostawać ze sobą w takich stosunkach prawnych, organizacyjnych, faktycznych, że wykonywanie zadań przez wspólnego inspektora i dysponowanie przez niego wiedzą co do pewnych okoliczności może powodować napięcie i prowadzić do sytuacji konfliktu.

Z konstrukcji przewidzianej w art. 37 ust. 3 RODO nie można jednak wywodzić, że pomiędzy kilkoma podmiotami, o których mowa w tym przepisie, może powstać taka zależność, iż podmioty te wyznaczają (wyznacza się dla nich) wspólnie jednego IOD, zaś w każdej z tych jednostek odrębnie funkcjonuje osobny – niejako lokalnie wyznaczony IOD, zaś łącznie ci „lokalni" inspektorzy podlegają wspólnemu, który stoi na ich czele. Takie rozwiązane nie wydaje się zgodne z treścią art. 37 ust. 3 RODO. W tym przepisie bowiem chodziło o pewną ekonomikę działania i ustanowienie jednego inspektora dla kilku jednostek organizacyjnych, nie zaś o to, by „mnożyć" inspektorów, a przez to komplikować ich

obsługę. Ponadto przy takim rozwiązaniu trudno byłoby ustalić zakres odpowiedzialności IOD i lokalnych inspektorów oraz źródło ich podporządkowania, w tym wydawania im poleceń przez IOD głównego.

4. Wymogi kwalifikacyjne wyznaczenia inspektora ochrony danych

W art. 37 ust. 5 RODO określono wymagania stawione kandydatowi na inspektora. To wymagania o charakterze merytorycznym odnoszące się do 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. W RODO nie skonkretyzowano tych wymagań, pozostawiając to administratorowi lub podmiotowi przetwarzającemu, który angażuje inspektora. W przypadku IOD w sektorze publicznym należałoby stawiać wymóg dysponowania przez niego wiedzą na temat przepisów regulujących funkcjonowanie organów lub podmiotów, które obsługuje. Chodzi tu zarówno o specyfikę ochrony danych osobowych poszczególnych sektorach administracji publicznej, jak i o znajomość zagadnień ustrojowych, materialnych i proceduralnych. I nie chodzi tu wyłącznie o znajomość k.p.a. czy procedury postępowania przed Prezesem Urzędu Ochrony Danych Osobowych. Z pewnością inspektor musi posiadać wiedzę w obszarze europejskich i krajowych przepisów dotyczących ochrony danych osobowych – wskazuje na to motyw 97 preambuły RODO, podkreśla to także Grupa Robocza Art. 29 w wytycznych dotyczących IOD. Wykonywanie zadań IOD wymaga także praktycznego przygotowania popartego odpowiednim doświadczeniem zawodowym. Charakter obowiązków IOD oraz charakter administratora lub podmiotu przetwarzającego wyznaczają, o jaką wiedzę i o jakie doświadczenie chodzi w konkretnym przypadku.

5. Podstawa sprawowania funkcji IOD

Zgodnie z art. 37 ust. 6 RODO inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego, lub wykonywać zadania na podstawie umowy o świadczenie usług. Wybór podstawy sprawowania funkcji przez inspektora należy do podmiotu, który go wyznacza, i dotyczy w równym stopniu sektora publicznego, jak i prywatnego. Inspektor może być pracownikiem zatrudnionym w jednostce albo osobą zewnętrzną. Inspektora można wyznaczyć w ramach zatrudnienia pracowniczego, podporządkowanego przepisom prawa pracy bądź zatrudnienia cywilnoprawnego ze wskazaniem na umowę zlecenie – zgodnie z potrzebami administratora lub procesora w zakresie ochrony danych osobowych, z uwzględnieniem przyjętych zasad polityki kadrowej, analizy kosztów zatrudnienia, kwestii odpowiedzialności prawnej itp. Podstawowym kryterium wyboru inspektora powinien być profesjonalizm w wykonywaniu zadań[79]. Niemniej niezależnie od wyboru podstawy zatrudnienia RODO nie przewiduje możliwości przeniesienia odpowiedzialności w zakresie ochrony danych osobowych ciążącej z mocy prawa na administratorze czy procesorze na inspektora, nawet wówczas, jeśli IOD pełni funkcję na zasadzie outsourcingu. W obu wariantach czas trwania nawiązanego stosunku prawnego jest uzależniony od woli stron, aczkolwiek w przypadku prawnopracowniczego stosunku prawnego należy brać pod uwagę uwarunkowania i ograniczenia wynikające z kodeksu pracy.

Przywołany art. 37 ust. 6 RODO nie precyzuje, co oznacza pozostawanie „członkiem personelu" oraz nie klaruje, o jaką „umowę o świadczenie usług" chodzi i nie określa jej stron.

Zwłaszcza w przypadku wykonywania zadań IOD „na podstawie umowy o świadczenie usług" powstają istotne kwestie interpretacyjne.

[79] A. Nerka, *op. cit.*, s. 404-405.

Nadto usługa IOD może być dostarczana konkretnemu administratorowi czy podmiotowi przetwarzającemu, którzy dokonali indywidualnego wyboru, i wyznaczenia IOD, ale i przypadku określonego w art. 37 ust. 3 RODO, gdy jeden IOD ma być wyznaczony dla więcej niż jednego podmiotu w sektorze publicznym.

Analogicznie jak Grupa Robocza Art. 29 należy przyjąć, że umowa dotycząca świadczenia usług przez IOD może być zawarta zarówno bezpośrednio z osobą fizyczną, która świadczy usługi jako IOD, jak i z innym podmiotem spoza organizacji administratora lub podmiotu przetwarzającego, który na podstawie tejże umowy „dostarczać będzie" IOD do konkretnego podmiotu. Niezbędne jest, aby każda osoba działająca jako IOD na rzecz podmiotu sprawującego funkcję IOD spełniała wszystkie odpowiednie wymogi określone przez RODO dla IOD. Wymagane jest także, aby taki podmiot oraz każda z osób świadczących usługi jako IOD korzystała z gwarancji, jakimi RODO obejmuje osobę pełniącą funkcję inspektora. Nie może mieć zatem miejsca nieuzasadnione rozwiązanie umowy o świadczenie usług w zakresie pełnienia funkcji IOD czy też niezgodne z prawem zwolnienie osoby będącej członkiem podmiotu realizującego zadania inspektora ochrony danych. Każda z osób wykonujących funkcję IOD musi unikać konfliktu interesów. Powinien to zapewnić podmiot dostarczający usługi IOD administratorom lub podmiotom przetwarzającym. Zaakcentować przy tym trzeba, że RODO nie określa rodzaju stosunku prawnego, jaki ma łączyć osobę fizyczną wykonującą funkcję IOD u administratora lub procesora z podmiotem związanym z administratorem lub procesorem umową o świadczenie usługi IOD. Dlatego też z aprobatą podchodzić należy do praktyki, że osoby te mogą być zarówno zatrudniane przez ten podmiot na podstawie umowy o pracę, jak i wykonywać te czynności na

podstawie umowy cywilnoprawnej[80]. Taki stan rzeczy istniał także pod rządami poprzedniej s.u.o.d.o. z 1997 r.[81]

Dobrą stroną świadczenia usługi IOD przez podmiot instytucjonalny jest to, że w pracy zespołowej można połączyć indywidualne atuty i umiejętności tak, aby zapewnić wydajniejszą obsługę swoich klientów, –na co zwraca uwagę Grupa Robocza Art. 29 w Wytycznych WP 243. Jednak, jak podkreśla Grupa, w celu zapewnienia przejrzystości prawnej, dobrej organizacji i uniknięcia konfliktów interesów wśród członków zespołu, zalecany jest wyraźny podział zadań w jego ramach oraz wyznaczenie jednej osoby jako wiodącej osoby kontaktowej i osoby odpowiedzialnej za każdego klienta, a określenie tych kwestii byłoby wskazane w umowie o świadczenie usług[82].

Przedmiotem świadczenia w umowie o świadczenie usługi IOD, o której mowa w art. 37 ust. 6 RODO, jest wykonywanie zadań IOD określonych w art. 38-39 RODO, a także innych przepisach tego rozporządzenia. Niemniej zadania wykonywane przez IOD w konkretnym przypadku mogą być określone w taki sposób, że ich treści wykraczały poza te wymienione wprost w przywołanych przepisach, byleby ich określenie nie powodowało konfliktu interesów w rozumieniu art. 38 ust. 6 RODO. Jeśli umowa dotyczy świadczenia usługi IOD przez podmiot inny niż osoba fizyczna faktycznie wykonująca te czynności, umowa powinna zawierać albo imienne wskazanie osoby IOD wykonującej zadania na rzecz usługodawcy, albo określać zasady jej wyznaczenia. Jednocześnie umowę o świadczenie usługi IOD kwalifikować należy jako umowę powierzenia przetwarzania, co oznacza, że powinna spełniać wymogi art. 28 RODO.

[80] A. Nerka*, op. cit.*, s. 413-414.

[81] Zob. M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 178.

[82] Zob. Wytyczne WP 243 GR 29.

6. Obowiązki związane z wyznaczeniem IOD

Na podstawie art. 37 ust. 7 RODO administrator lub podmiot przetwarzający zawiadamiają organ nadzorczy o danych kontaktowych inspektora, a tym samym o jego wyznaczeniu. Z rozporządzenia nie wynika, jakie konkretnie dane powinny być przekazane organowi nadzorczemu, określa to natomiast art. 10 ust. 1 u.o.d.o. z dnia 10 maja 2018 r., przewidując, że podmiot, który wyznaczył inspektora, zawiadamia Prezesa UODO o jego wyznaczeniu w terminie 14 dni od dnia wyznaczenia, wskazując imię, nazwisko oraz adres poczty elektronicznej lub numer telefonu inspektora. Zawiadomienie może zostać dokonane przez pełnomocnika podmiotu, wówczas do zawiadomienia należy pełnomocnictwo udzielone w formie elektronicznej. W treści zawiadomienia wskazuje się ponadto:

1) imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna;
2) firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą;
3) pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt 1 i 2;
4) numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.

Na podmiocie, który wyznaczył inspektora, ciąży obowiązek zawiadamiania Prezesa UODO o każdej zmianie danych objętych zakresem art. 10 ust. 1 i 3 u.o.d.o. oraz o odwołaniu inspektora, w terminie 14 dni od dnia zaistnienia zmiany lub odwołania. Poza tym w razie wyznaczenia jednego inspektora przez organy lub podmioty publiczne albo przez

grupę przedsiębiorców każdy z tych podmiotów dokonuje stosownego zawiadomienia. Zawiadomienie sporządza się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP.

Zgodnie z art. 11 u.o.d.o. podmiot, który wyznaczył inspektora, udostępnia dane inspektora, o których mowa w art. 10 ust. 1, niezwłocznie po jego wyznaczeniu, na swojej stronie internetowej, a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

7. Status IOD i miejsce w strukturze organizacyjnej

Status IOD i miejsce w strukturze organizacyjnej w głównej mierze określa art. 38 RODO. Po jego myśli administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 1), nadto IOD ma podlegać bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego (art. 38 ust. 3).

Status IOD w określają obowiązki, które względem niego ma spełniać administrator i procesor. Należą do nich:

1) zapewnienie niezależności, w tym poprzez takie usytuowanie w strukturze organizacyjnej, by IOD podlegał bezpośrednio najwyższemu kierownictwu administratora lub podmiotu przetwarzającego;
2) właściwe i niezwłoczne włączanie we wszystkie sprawy dotyczące ochrony danych osobowych;
3) zapewnienie wsparcia IOD w wypełnianiu przez niego zadań, o których mowa w art. 39;
4) zapewnienie niezbędnych zasobów do wykonywania zadań IOD;

5) zapewnienie dostępu do danych osobowych i operacji przetwarzania;
6) zapewnienie zasobów niezbędnych do utrzymania wiedzy fachowej IOD;
7) zapewnienie, by IOD nie otrzymywał instrukcji dotyczących wykonywania jego zadań;
8) zapewnienie, by IOD nie był odwołany ani karany za wypełnianie swoich zadań;
9) zapewnienie zachowania przez IOD tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego;
10) niepowierzanie IOD zadań powodujących konflikt interesów;
11) zapewnienie kontaktu z osobami, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO[83].

Jednym z podstawowych przymiotów IOD jest gwarantowana mu niezależność[84]. Z motywu 97 RODO wynika, że inspektorzy ochrony danych bez względu na to, czy są pracownikami administratora, powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny. Niezależność sprowadza się do braku podporządkowania, wyłączenia spod wpływów, wolności od nacisków, a przez to obiektywizmu w ocenach i działaniach.

Prawny wymóg niezależności działań IOD oznacza, że pracodawca nie będzie mógł w pełni korzystać z uprawnień kierowniczych w zakresie określania przedmiotu wykonywania pracy przez IOD. Jego możliwości działań władczych doznają ograniczeń, co na płaszczyźnie

[83] Zob. M. Sakowska-Baryła, *Komentarz do art. 38*, [w:] M. Sakowska-Baryła (red nauk.), *op. cit.*, s. 419-420.

[84] E. Bielak-Jomaa, *Komentarz do art. 38*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *op. cit*.

stosunków pracy można uzasadniać, odwołując się do koncepcji „autonomicznego podporządkowania”[85]. Niezależność IOD sprowadzać należy do autonomii działania w zakresie zadań określonych w art. 39 RODO. To nieuleganie wpływom, zarówno z zewnątrz, jak i wewnątrz organizacji, i działanie w sprawach dotyczących ochrony danych w sposób wolny od nacisków. Tak określona pozycja umożliwi IOD wolne od ingerencji i nacisków, oparte na wiedzy i doświadczeniu dokonywanie ustaleń i formułowanie zaleceń w ramach realizowanych zadań i pełnionych obowiązków. Jednakże w przypadku IOD zatrudnionego w charakterze pracownika należy wskazać, że „praca” w rozumieniu prawa pracy musi być w jakimś zakresie podporządkowana i regułą jest, że powinna być świadczona na ryzyko pracodawcy. Ustawodawca wyposażył przecież pracodawcę w prawo do kierowania procesem pracy (art. 22 k.p.).

Włącznie IOD we wszelkie sprawy dotyczące ochrony danych osobowych zakwalifikować należy jako założenie spójne z wymogiem uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych wynikającym z art. 25 RODO, które odnoszą się także do podmiotów z sektora publicznego. Dlatego też także te podmioty przy planowaniu zadań związanych z przetwarzaniem danych osobowych czy realizacji procesów wymagających przetwarzania zobowiązane są uwzględniać 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 wynikających z przetwarzania, w których to kwestiach najlepiej powinien orientować się IOD. Publiczny administrator i podmiot przetwarzający powinien zadbać o to, aby zaangażowanie IOD miało następujące cechy:

1) powinno być „właściwe”, a więc adekwatne, odpowiednie, w sposób zapewniający możliwie kompleksowe zapoznanie się IOD z okolicznościami przetwarzania danych osobowych – kontekstem,

[85] Zob. B. Bury, *Podporządkowanie pracownika pracodawcy*, „Państwo i Prawo” 2006, nr 9, s. 63.

celami, zakresem, charakterem, uwarunkowaniami czasowymi, technicznymi, prawnymi;
2) powinno odbywać się niezwłocznie – a więc bez nieuzasadnionej zwłoki, możliwie szybkie, na możliwie najwcześniejszym etapie – najlepiej – o ile to możliwe – zanim jeszcze zaczną być dokonywane operacje przewarzania;
3) powinno dotyczyć wszystkich spraw ochrony danych osobowych.

Ze względu na powyższe IOD należy informować i angażować we wszystkie sprawy z zakresu ochrony danych osobowych bez względu na to, jakich kategorii danych i kategorii osób dotyczą, oraz czy należą do istoty działalności administratora lub podmiotu przetwarzającego, czy też mają wyłącznie charakter pomocniczy. Przykładowo zaangażowanie IOD powinno być podstawową procedurą przy w przygotowaniu zamówienia publicznego, przy planowaniu nowych zadań, funkcjonalności systemów informatycznych, zmian w organizacji lub zabezpieczeniach.

8. Zapewnienie IOD wsparcia w wykonywaniu zadań

Zgodnie z art. 37 ust. 2 RODO administrator oraz podmiot przetwarzający wspierają 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, a także zasoby niezbędne do utrzymania jego wiedzy fachowej. Grupa Robocza art. 29 w wytycznych nr 243 określiła ogólne zasady wspierania IOD w wykonywaniu przez niego zadań poprzez:

1) wsparcie IOD ze strony kadry kierowniczej jednostki organizacyjnej;
2) zapewnienie IOD aktywnego udziału w działaniach na rzecz ochrony danych osobowych, propagowanie działań, zachowań, postaw etycznych i praktyk odpowiadających wymogom ochrony

danych osobowych, nadawanie odpowiednio wysokiej rangi wytycznym, zaleceniom, przedsięwzięciom inspektora, liczenie się z jego stanowiskiem, a przynajmniej branie go pod uwagę;

3) zapewnienie IOD odpowiedniego wymiaru czasu pracy umożliwiającego wykonywanie powierzonych mu zadań i odpowiednie ustalenie priorytetów zwłaszcza, gdy ta osoba łączy je z jeszcze innymi zadaniami w organizacji – w takich przypadkach należałoby odpowiednio oszacować czas potrzebny na wykonywanie poszczególnych obowiązków;
4) zapewnienie wsparcia finansowego, organizacyjnego, odpowiedniego kolportażu istotnych informacji.

Zgodnie z art. 38 ust. 3 RODO IOD ma nie otrzymywać instrukcji dotyczących wykonywania jego zadań. Nadto nie może być odwołany ani karany za wypełnianie swoich zadań. Nie chodzi tu o brak nadzoru nad wykonywaniem zadań przez IOD, bezkrytyczne podejście do wykonywania tych zadań w sposób niezgodny z prawem, zasadami przetwarzania danych osobowych czy też na szkodę administratora lub podmiotu przetwarzającego. Grupa Robocza Art. 29 w wytycznych 243 wskazuje, że kary, o których tu mowa, są niedozwolone tylko w przypadkach, gdy ich nałożenie byłoby w związku z wypełnianiem przez IOD jego zadań, np. w związku z przedłożonymi przez niego rekomendacjami czy zaleceniami, dokonywanymi przez niego ustaleniami audytu, nieustępliwym raportowaniem o nieprawidłowościach w procesie przetwarzania, którego dopuszczają się wciąż te same osoby, określaniem planu audytów czy kontroli nie po myśli kierownictwa jednostki organizacyjnej, itp. Chodzi tu o niedopuszczalność wszelkich form karania – bezpośrednich i pośrednich, takich jak choćby obniżenie premii, opóźnienie awansu, utrudnienie rozwoju zawodowego, ograniczeniu dostępu do korzyści oferowanych pozostałym pracownikom. Jeśli natomiast IOD narusza porządek w pracy, nie wykonuje swoich obowiązków pracowniczych czy wynikających

z umowy cywilnoprawnej, wówczas może ponosić konsekwencje jak każdy inny pracownik czy usługodawca.

9. Zapobieganie konfliktowi interesów

Jak stanowi art. 38 ust. 6 RODO, inspektor ochrony danych może wykonywać inne zadania i obowiązki, jednakże administrator lub podmiot przetwarzający mają zapewnić, by takie zadania i obowiązki nie powodowały konfliktu interesów. Rozporządzenie nie precyzuje jednak, na czym miałby on polegać. Taki stan rzeczy bywa kłopotliwy także w sektorze publicznym, ponieważ wykonywanie każdej pracy czy zadania w jakimś stopniu wiąże się z przetwarzaniem danych osobowych i każde to przetwarzanie może potencjalnie wymagać nadzoru. Przykładowego wyliczenia zadań pozostających w konflikcie i wyjaśnienia, kiedy taki konflikt może zaistnieć, podjęła się GRUPA 29 w wytycznych WP 243. Wskazuje w nich, że IOD nie może zajmować w organizacji stanowiska pociągającego za sobą określanie sposobów i celów przetwarzania danych, a ponieważ każda jednostka organizacyjna posiada pewną specyfikę, kwestię tę należy przeanalizować indywidualnie. Jedynie przykładowo GRUPA uznała, że zasadniczo „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”[86].

[86] Zob. Wytyczne WP 243.

10. Zadania IOD

Zasadniczy zakres zadań IOD określa art. 39 ust. 1 RODO, niemniej jego zadania mogą być rekonstruowane także na podstawie innych przepisów RODO oraz kształtowane przez administratora lub procesora w takim zakresie, aby odpowiednio wykonywać przepisy RODO i sprawować nad tym wykonywaniem należyty nadzór. Katalog określony w art. 39 ust. 1 ma charakter otwarty.

Wspomniany przepis pozwala na wyodrębnienie następujących zadań inspektora ochrony danych:

1) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych;
2) doradzanie administratorowi, podmiotowi przetwarzającemu oraz ich pracownikom w sprawie obowiązków z zakresu ochrony danych osobowych;
3) monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych;
4) podział obowiązków z zakresu monitorowania ochrony danych osobowych;
5) działania zwiększające świadomość administratora, procesora i ich personelu;
6) szkolenia personelu uczestniczącego w operacjach przetwarzania;
7) audyty powiązane z monitorowaniem przestrzegania przepisów, polityk, wykonywaniem obowiązków z zakresu ochrony danych osobowych, szkoleniami i działaniami zwiększającymi świadomość;

8) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
9) współpraca z organem nadzorczym;
10) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36;
11) w stosownych przypadkach prowadzenie konsultacji z organem nadzorczym we wszelkich innych sprawach niż wynikające z art. 36 RODO;
12) uwzględnianie przy wykonywaniu zadań ryzyka związanego z operacjami przetwarzania, w okolicznościach determinowanych określonym charakterem, zakresem, kontekstem i celami przetwarzania.

Do zadań IOD należy także zapewnienie kontaktu z podmiotami danych. Zgodnie z art. 38 ust. 4 osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO. Należy przyjąć, że kontakt z osobą, której dane dotyczą, IOD realizuje w imieniu i na rzecz administratora (odpowiednio procesora). Istotą tego rozwiązania jest to, iż w sprawach ochrony danych osobowych kontakt z podmiotem danych ma być realizowany przez profesjonalistę.

Zasadne jest postulować, by procedury wykonywania zadań przez IOD zostały określone w ramach odpowiednich wewnętrznych procedur obowiązujących u podmiotu, który go wyznaczył. Chodzi tu choćby o procedury realizacji kontaktu z podmiotem danych, dokumentowania faktu jego dokonania lub przebiegu, procedury przebiegu sprawdzeń, audytów, monitorowania zgodności z RODO, jakie kompetencje ma IOD w ramach kontaktu z personelem administratora czy procesora, jak często ma realizować poszczególne zadania, jak dokumentować ich realizację,

jak ma wyglądać proces zaznajamiania personelu z zasadami ochrony danych osobowych, czy jak zapewnić włączanie IOD w sprawy ochrony danych osobowych na najwcześniejszym możliwym etapie.

Obserwacja praktyki pozwala na stwierdzenie, że częstokroć przyjmowane polityki w tym względzie są nader ogólne i nie precyzują takich kwestii lub czynią to w taki sposób, że nie jest możliwe skonkretyzowanie sposobu i trybu działania przez IOD.

11. Odpowiedzialność IOD

Zasadniczo odpowiedzialność IOD wyznacza charakter stosunku prawnego, na którego podstawie wykonuje on zadania. Pod uwagę należy tu brać odpowiedzialność prawnopracowniczą lub odpowiedzialność kontraktową (cywilną). Niemniej na zakres tej odpowiedzialności istotny wpływ może mieć standard wykonywania zadań IOD określony w art. 39 ust. 2 RODO. Zgodnie z tym przepisem inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania. Przepis ten musi być brany pod uwagę w przypadku określania odpowiedzialności osoby wykonującej funkcję inspektora na podstawie umowy o świadczenie tego rodzaju usług lub w ramach stosunku pracy. Inspektor ma bowiem wykonywać nie tylko konkretne zadania, ale także wykonywać je z „należytym uwzględnieniem ryzyka". Przywodzi to na myśl wynikające z art. 355 k.c. ramy staranności dłużnika przy wykonywaniu zobowiązań[87]. Obiektywizacja wzorca staranności zakłada posługiwanie się pewnym modelem postępowania dłużnika

[87] Zgodnie z tym przepisem dłużnik przy wykonywaniu zobowiązań obowiązany jest do należytej staranności, a więc staranności ogólnie wymaganej w stosunkach danego rodzaju (§ 1), z tym że należytą staranność dłużnika w zakresie prowadzonej przez niego działalności gospodarczej określa się przy uwzględnieniu zawodowego charakteru tej działalności (§ 2).

w ramach istniejącego stosunku zobowiązaniowego, który jest następnie porównywany z zachowaniem dłużnika na tle konkretnej sytuacji, więc w praktyce konieczne będzie konstruowanie miernika obiektywnie należytego wykonywania zadań przez IOD, w tym należytego uwzględniania ryzyka związanego z operacjami przetwarzania w odniesieniu do skategoryzowanych charakteru, zakresu, kontekstu i celów przetwarzania[88]. Założyć trzeba, że tego rodzaju kategoryzacja standardu należytej staranności nastąpi także w odniesieniu do wykonywania funkcji IOD w sektorze publicznym, tudzież w poszczególnych podkategoriach tego sektora. W przypadku inspektorów – pracowników na kształt tego standardu wywierać wpływ będą zapewne także pragmatyki służbowe, które określają częstokroć sposób zachowania i świadczenia pracy takich pracowników.

[88] Zob. M. Sakowska-Baryła, *Komentarz do art. 39*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 433-434.

Rozdział IV

Powierzenie przetwarzania w administracji publicznej

(dr Marlena Sakowska-Baryła)

1. Powierzenie przetwarzania w administracji publicznej

Przygotowanie do stosowania RODO, a następnie wykonywanie zawartych w nim postanowień dotyczy także outsourcingu, którego przedmiotem głównym lub akcesoryjnym przedmiotem pozostaje przetwarzanie danych osobowych. Obserwacja praktyki pozwala stwierdzić, że z rzadka chodzi wyłącznie o zlecanie na zewnątrz czynności przetwarzania danych osobowych. Z reguły owo przetwarzanie dokonywane przez zewnętrzny podmiot lub grupę zewnętrznych podmiotów stanowi niezbędny element uzupełniający stosunku łączącego podmiot, który usługę zleca, oraz tego, który ją wykonuje. Przykładowo w zleceniu zewnętrznemu podmiotowi takich usług, jak skonstruowanie i prowadzenie strony BIP, ochrona osób i mienia wraz z obsługą systemu monitoringu, wydawaniem i przechowywaniem przepustek oraz legitymowaniem osób wchodzących na teren jednostki organizacyjnej, obsługa księgowa wykonywana przez samorządowe centrum usług wspólnych albo biuro księgowe, dostarczanie usługi prowadzenia elektronicznych dzienników lekcyjnych itp., nie tyle chodzi o samo przetwarzanie danych osobowych, ale o osiągnięcie wskazanych efektów, celów, stanów, których nie sposób zrealizować bez korzystania z danych osobowych. Obserwacja praktyki

stosowania RODO przez pierwszych kilka miesięcy, pozwala wysnuć wniosek, że obok rzetelnego przeglądu procesów powierzenia do przetwarzania danych osobowych i ich dostosowania do nowych wymogów prawnych wciąż jeszcze mamy do czynienia z pomijaniem tego zagadnienia albo – odwrotnie – z jego nadużywaniem i wadliwą interpretacją, gdzie powierzenie myli się z udostępnieniem danych osobowych albo doszukuje się go tam, gdzie od strony podmiotowej nie sposób stwierdzić jego istnienia[89]. Przygotowanie do stosowania RODO powinno zatem objąć:

1) zrozumienie istoty „powierzenia przetwarzania";
2) inwentaryzację zawartych umów oraz analizę relacji z podmiotami zewnętrznymi, także wówczas, gdy stron nie łączy pisemna umowa, a opierają się one na innych podstawach lub pozostają jedynie stosunkiem faktycznym;
3) ustalenia co sposobu weryfikacji podmiotów przetwarzających z punktu widzenia gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą;
4) analizę umów czy innych instrumentów prawnych, wziąwszy pod uwagę kryteria określone w art. 28 ust. 3 i 9 RODO.

To zadanie, którego podjąć się zmuszony jest każdy administrator i każdy podmiot przetwarzający, także w sektorze publicznym.

2. Istota powierzenia

Powierzenie przetwarzania danych osobowych to stan faktyczny istniejący w konkretnych okolicznościach relacji pomiędzy administratorem lub współadministratorami a podmiotem przetwarzającym (niekiedy

[89] Szerzej zob. K. Wygoda, *Czy potrzebne są umowy powierzenia przetwarzania?*, „ABI Expert" 2018, nr 3, s. 27 i n.

podmiotami przetwarzającymi). Istotą powierzenia jest zlecenie podmiotowi zewnętrznemu wobec administratora – „podmiotowi przetwarzającemu" w rozumieniu art. 4 pkt 8 RODO operacji na danych osobowych. Operacje te podmiot przetwarzający podejmuje na rzecz i w imieniu administratora, który zleca owemu podmiotowi takie właśnie czynności. Zlecenie, o którym tu mowa, należy uznać za powierzenie przetwarzania danych osobowych, jeśli jego treścią pozostaje przetwarzanie danych osobowych w rozumieniu art. 4 pkt 2 RODO, choć rozporządzenie to nie posługuje się tym pojęciem, a sam art. 28 RODO nie jest zatytułowany „Powierzenie przetwarzania", ale „Podmiot przetwarzający"[90].

W omawianej relacji podmiot przetwarzający w imieniu administratora „przetwarza" dane osobowe. Oczywiste jest zatem, że czynności, które wykonuje, określać należy mianem „przetwarzania" i rozumieć je w taki sposób, w jaki pojęcie to zdefiniowane zostało w art. 4 pkt 2 RODO[91]. Zgodnie z tą definicją przez „przetwarzanie" należy rozumieć operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką 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. Tak więc istotą powierzenia przetwarzania danych osobowych jest zlecenie na zewnątrz czynności przetwarzania danych osobowych – usługi wymagającej przetwarzania danych, w ramach której przetwarzanie to jest elementem podstawowym lub co najmniej niezbędnym. Powierzenie przetwarzania danych osobowych zaistnieje zatem np. w przypadku zlecenia zewnętrznemu podmiotowi obsługi w zakresie bhp,

[90] Zob. M. Sakowska-Baryła, *Komentarz do art. 28 uwaga 2*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 315.

[91] Szerzej zob. K. Wygoda, *Komentarz do art. 4 pkt 2*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 78 i n.

dostarczenia i bieżącego serwisu systemu elektronicznego do elektronicznego zarządzania dokumentami, wyprodukowania okolicznościowych imiennych dyplomów dla osób wyróżnionych odznaką za zasługi dla powiatu, organizacji konferencji w zakresie wysyłki zaproszeń do referentów i innych gości oraz zapewnienia im noclegów, ponieważ we wszystkich przypadkach korzystanie z danych osobowych stanowi niezbędny element wykonania zlecenia. Do powierzenia przetwarzania nie dojdzie natomiast chociażby wówczas, gdy przedmiotem zlecenia jest zapewnienie sprzątania pomieszczeń urzędu gminy czy ministerstwa, dostarczenie produktów żywnościowych do szkoły czy szpitala albo zapewnienie ochrony fizycznej terenu starostwa powiatowego poprzez montaż rolet antywłamaniowych i patrolowanie terenu wokół budynku. Z powierzeniem nie mamy również do czynienia, gdy zawierające umowę strony w treści tejże imiennie wyznaczają osoby odpowiedzialne za jej realizację. Praktyka pokazuje jednak, że stosunkowo często zawiera się umowy nazywane „powierzeniem przetwarzania" także w przypadkach odpowiadającym ostatnim z przytoczonych, choć w żadnej mierze nie mają one takiego charakteru.

Ustalenie istoty rozważanej tu instytucji ma tym większe znaczenie, że w odnoszących się do niej: motywie 81 preambuły RODO oraz w art. 28 w ust. 1, 2, 3 lit. d i g oraz ust. 4 jest mowa o korzystaniu z „usług" podmiotów przetwarzających, a nie o „powierzeniu przetwarzania" lub „zlecaniu przetwarzania". Niemniej jednak brzmienie przepisów RODO nie pozostawia wątpliwości, że chodzi tu o „usługi" przetwarzania danych osobowych, gdzie przetwarzanie to jest przedmiotem świadczenia.

Używanego w przywołanej treści RODO pojęcia „usługa" nie powinno się rozumieć wyłącznie w kategoriach cywilistycznych, chodzi tu zdecydowanie o kategorię w znaczeniu funkcjonalnym. Wniosek taki wywodzić należy z treści art. 28 ust. 3 RODO, który podstawą przetwarzania danych osobowych przez podmiot przetwarzający czyni umowę lub inny instrument prawny. Rozporządzenie nie przesądza o komercyjnym

bądź niekomercyjnym charakterze owej „usługi", o tym, czy ma ona charakter odpłatny, czy nieodpłatny itp. Nie wydaje się, by uzasadnione było zrównywanie „usługi" z art. 28 RODO z usługą, o której mowa w art. 750 k.c., w myśl którego do umów o świadczenie usług, które nie są uregulowane innymi przepisami, stosuje się odpowiednio przepisy o zleceniu. Te dwa pojęcia mogą bowiem, ale nie muszą, mieć wspólny zakres podmiotowy, to znaczy „usługa" w rozumieniu art. 750 k.c. może polegać między innymi na przetwarzaniu danych osobowych na rzecz usługobiorcy, który w tym ujęciu będzie administratorem, zaś usługodawca – „podmiotem przetwarzającym", ale nie musi. Tak samo „usługa", o której stanowi art. 28 RODO, może być tą, która wynika również z art. 750 k.c., ale wielokrotnie wcale nią nie jest. O usłudze w rozumieniu art. 750 k.c. można mówić np. w odniesieniu do przetwarzania danych osobowych przez centrum usług wspólnych, gdy jednostka obsługująca przetwarza dane osobowe w zakresie i celu niezbędnych do wykonywania zadań w ramach wspólnej obsługi tej jednostki, choć z punktu widzenia RODO mamy tu do czynienia ze stosunkiem powierzenia przetwarzania[92].

3. Charakter czynności powierzenia przetwarzania

Powierzenie przetwarzania danych osobowych ma charakter mieszany, biorąc pod uwagę podział czynności prawnych na konsensualne – skuteczne na skutek złożenia oświadczenia woli i realne – wymagające faktycznego władztwa nad rzeczą dla ich dokonania. Umowa powierzenia przetwarzania danych osobowych czy też „inny instrument prawny" (inny akt prawny) nie zawsze wymaga bowiem faktycznej zmiany w zakresie władztwa nad danymi osobowymi. Nie w każdym też przypadku dla skuteczności powierzenia wystarczające będzie wyłącznie złożenie

[92] Szerzej zob. M. Sakowska-Baryła, *Organizacja ochrony danych osobowych w ramach wspólnej obsługi w centrum usług wspólnych,* [w:] M. Sakowska-Baryła, M. Górski (red.), *Samorządowe centra usług wspólnych,* Warszawa 2017, s. 177 i n.

oświadczenia woli. Wiele w tym względzie zależy od tego, jaka jest podstawa i cel stosunku powierzenia. Trzeba też brać pod uwagę wymogi wynikające z art. 28 ust. 3 RODO i określone w nim *essentialia negotii* treści umowy powierzenia (innego instrumentu prawnego) oraz szerszy kontekst powierzonego przetwarzania. Warto w tym miejscu zaznaczyć, że zgodnie z art. 28 ust. 3 zd. 2 RODO świadczenie podmiotu przetwarzającego obejmuje szereg czynności organizacyjno-technicznych, zabezpieczających i przygotowawczych, a także informacyjnych, których nie można zaliczyć do czynności o charakterze realnym. W większości mają one charakter konsensualny, a więc i umowa lub inny akt, z których wynikają w przeważającym stopniu, mają ten właśnie charakter.

4. Strony stosunku powierzenia przetwarzania

Powierzenie przetwarzania danych osobowych to stosunek prawny pomiędzy administratorem a podmiotem przetwarzającym. 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. „Podmiot przetwarzający" natomiast – w myśl art. 4 pkt 8 RODO – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Jak można wywnioskować z przytoczonych tu definicji – niezależnie od sposobu ich statuowania i podstaw prawnych ich działania w danej roli czy charakterze, zarówno administratorzy, jak i podmioty przetwarzające mogą należeć do tych samych kręgów podmiotowych – osób

fizycznych, prawnych, organów publicznych, jednostek lub innych podmiotów. To katalog otwarty podmiotów, które w zależności od okoliczności faktycznych mogą być kwalifikowane jako „administratorzy" albo jako „podmioty przetwarzające"[93]. Różnią się natomiast znacząco w zakresie władztwa w procesie przetwarzania danych osobowych.

Administratorem jest bowiem ten, kto decyduje o celach i sposobach przetwarzania danych osobowych, a więc także o tym, w jaki sposób to przetwarzanie danych osobowych się odbywa, czy operacje na danych osobowych wykonuje samodzielnie, w tym za pośrednictwem własnego personelu, czy też ceduje je na zewnątrz. To także ten, na którego przepisy prawa nakładają określone obowiązki czy zadania dotyczące przetwarzania danych osobowych lub z którymi przetwarzanie danych osobowych jest nierozłącznie związane, jak też taki podmiot, który „administratorem" został określony bezpośrednio w przepisach prawa i z tego też względu jako posiadający ten status wykonuje przypisane mu czynności. Podkreślenia wymaga, że status administratora może być przypisany organowi publicznemu, jeżeli z przepisów prawa wynika, że organ ten decyduje o celach i sposobach przetwarzania danych. Jak jednak wskazuje się w literaturze, zazwyczaj przepis prawa choćby ogólnie reguluje te kwestie, a organ publiczny jedynie je precyzuje i uszczegóławia[94]. Decydujące znaczenie mają tu rodzaj i charakter kompetencji z zakresu spraw publicznych, jak również zadania wyznaczone podmiotom z sektora publicznego. W takim ujęciu w sektorze publicznym, w tym samorządowym, administrowanie danymi osobowymi jest nie tyle elementem stanu faktycznego, jakim pozostaje władztwo w procesie

[93] Zob. P. Litwiński, P. Barta, P. Kawecki, *Komentarz do art. 4 pkt 7, uwaga 92*, [w:] P. Litwiński (red.), *op. cit.*, s. 222.

[94] Zob. P. Fajgielski, *Komentarz do art. 4 uwaga 31*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 122.

przetwarzania danych osobowych, ale rola, jaką w tym procesie danemu podmiotowi przyznają właściwe przepisy prawa[95].

Podmiotem przetwarzającym, określanym często jako „procesor", jest natomiast ten, który nie posiada władztwa nad celami i sposobami przetwarzania danych osobowych lub którego władztwo jest znacząco ograniczone, ponieważ przetwarza dane osobowe wyłącznie w imieniu administratora. Ten podmiot nie dokonuje przetwarzania danych osobowych dla siebie, ale dla administratora, który to określa cel przetwarzania lub któremu ów cel jest przypisany. Przykładowo to podmiot zobowiązany na gruncie ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej[96] ma prowadzić Biuletyn Informacji Publicznej, ale czynności faktyczne w zakresie prowadzenia tego BIP, redagowania jego treści, dokonywania publikacji na stronie, anonimizacji zamieszczanych tam dokumentów, uzupełniania tzw. metryczek o dane osobowe może dokonywać podmiot zewnętrzny, który dostarcza usługi dedykowane zapewnieniu realizacji tego zadania. Procesor w „warstwie wykonawczej" w pewnej, często znaczącej, mierze decyduje o sposobach przetwarzania danych, ponieważ to on, wykonując usługę, dobiera środki, personel, metody potrzebne do jej wykonania. Niemniej na wstępie o sposobie przetwarzania decyduje administrator poprzez ustalenie, że przetwarzanie danych osobowych w konkretnym przypadku odbywać się będzie przy udziale podmiotu przetwarzającego.

Zaznaczyć przy tym należy, że administrator może korzystać z usług więcej niż jednego podmiotu przetwarzającego, co może mieć miejsce niezależnie od innych trwających powierzeń, także w obrębie jednego celu przetwarzania. Dotyczy to również nałożonych na administratora zadań publicznych. Między innymi administrator samorządowy może wykonywać to samo zadanie publiczne przy udziale więcej niż jednego

[95] Zob. P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 4 pkt 7, uwaga 96*, [w:] P. Litwiński (red.), *op. cit.*, s. 223-224.

[96] T. j. Dz. U. z 2018 r. poz. 1330 ze zm.

procesora. Dopuszczalne jest też, że tego samego procesora z administratorem łączyć będzie kilka umów powierzenia w zakresie jednej lub kilku usług[97].

Po stronie procesora wystąpić może więcej niż jeden podmiot Obok podmiotu przetwarzającego, któremu administrator zleca usługę przetwarzania, wystąpić może podwykonawca – zgodnie z terminologią art. 28 ust. 2 i 4 RODO – „inny podmiot przetwarzający" – bądź nawet swoisty łańcuszek subprocesorów. Każdy z nich przetwarza dane osobowe na rzecz administratora, ale podstawą tego przetwarzania jest strunek prawny (umowa) łączący go z pierwotnym podmiotem przetwarzającym, a nie z administratorem bezpośrednio. Dla wskazania owego subprocesora czy podprzetwarzającego RODO używa określenia „inny podmiot przetwarzający", nie definiuje zatem osobno tego pojęcia, a tym samym nie nadaje mu odrębnej nazwy. Za zasadne należy zatem przyjąć, że „inny podmiot przetwarzający" pozostaje „podmiotem przetwarzającym" w rozumieniu art. 4 pkt 8 RODO, a więc osobą fizyczną lub prawną, organem publicznym, jednostką lub innym podmiotem, który przetwarza dane osobowe w imieniu administratora, z tym zastrzeżeniem, że w ramach usług realizowanych dla „pierwotnego" podmiotu przetwarzającego. Jak wynika to z art. 28 ust. 2 i 4 RODO, przetwarzanie danych osobowych przez subprocesora odbywa się w imieniu administratora, a nie w imieniu pierwotnego podmiotu przetwarzającego. Nie formułuje zakazu dalszego powierzenia przetwarzania danych osobowych przez „subprocesora pierwotnego", a wręcz – przez wzgląd na treść przywołanych tu art. 28 ust. 2 i 4 RODO – pozwala na zastosowanie takiego rozwiązania organizacyjnego. Z uwagi na reguły odpowiedzialności wynikające z art. 28 ust. 4 RODO w praktyce tworzenie łańcuszka podwykonawców przy przetwarzaniu danych

[97] J. Byrski, *Umowne powierzenie do przetwarzania danych osobowych w ustawie o ochronie danych osobowych, dyrektywie 95/46/WE i w ogólnym rozporządzeniu o ochronie danych*, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych*, Warszawa 2016, s. 37.

osobowych można uznać za ryzykowne zwłaszcza dla pierwotnego podmiotu przetwarzającego[98].

5. Podmiot przetwarzający a współadministrator

Podmiot przetwarzający nie jest współadministratorem. Instytucję współadministrowania reguluje art. 26 RODO, choć właściwie zapowiada ją już regulacja art. 4 pkt 7 RODO w definicji pojęcia „administrator" poprzez wskazanie, że jest nim podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Zgodnie zaś z art. 26 ust. 1 zd. 1 RODO jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. Do takich podmiotów procesor z pewnością nie należy, ponieważ nie uczestniczy w podejmowaniu decyzji co do celów i sposobów przetwarzania. Umowne uzgodnienia pomiędzy procesorem a administratorem lub grupą administratorów nie mają takiej treści i mają zgoła odmienny charakter, ponieważ nie chodzi tu o działania wspólne, ale o usługi na rzecz tego, kto administruje.

Natomiast działający wspólnie współadministratorzy – w sposób opisany w art. 26 ust. 1 i 2 RODO – mogą powierzyć przetwarzanie danych osobowych procesorowi, który wówczas dokonuje przetwarzania w ich imieniu i na ich rzecz. Te wspólne uzgodnienia co do powierzenia przetwarzania danych mogą następować *ad hoc* lub też zostać określone w umowie o współadministrowanie. Nie ma bowiem przeszkód, a właściwie wręcz jest pożądane, by umowa określała zasady powierzania przetwarzania przez współadministratorów. Jej przedmiotem może być w szczególności rozstrzygnięcie, czy o powierzeniu współadministratorzy decydują wspólnie, czy cedują to zadanie na któregoś z nich. Jeśli nie

[98] M. Sakowska-Baryła, *Komentarz do art. 4 pkt 8*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 110.

dokonano umownych ustaleń w tym przedmiocie, a z przepisów prawa to nie wynika, zasadne jest przyjmować, że każdy ze współadministratorów powinien zawierać umowy powierzenia w zakresie przypisanych mu celów i sposobów przetwarzania pod warunkiem, że wspólne uzgodnienia – w praktyce najpewniej umowa o współadministrowanie – nie wyłączają powierzenia bądź też powierzenia przetwarzania w danym zakresie[99]. W praktyce pierwszych miesięcy stosowania RODO jako nieczęste odnotowywać należy formalizowanie stosunków współadministrowania w sektorze publicznym, w tym w samorządzie terytorialnym. Teoretycznie rzecz ujmując, współadministrowania należałoby doszukiwać się tam, gdzie kilka podmiotów wspólnie realizuje pewne zadania. Nie jest jednak ani łatwe, ani oczywiste wskazywanie na takie właśnie. Można przyjąć, że ze współadministrowaniem mamy do czynienia, gdy dwa gminne przedszkola organizują konkurs rysunkowy lub gdy cztery szkoły decydują się na wspólną organizację zajęć z gry w piłkę siatkową, ale obserwacja praktyki pozwala twierdzić, że nie za każdym razem w tych przypadkach placówki te dokonują ustaleń odpowiadających opisanym w art. 26 RODO i nie każdorazowo dbają o odpowiednie udokumentowanie tej relacji z punktu widzenia wymogów RODO.

6. Powierzenie a zapewnienie dostępu do danych osobowych

Pierwsze miesiące stosowania RODO pokazały, że wielokrotnie błędnie o powierzeniu mówi się lub wręcz się je stosuje poprzez zawieranie umów tak właśnie nazwanych i nawiązujących swą treścią do wymogów wynikających z art. 28 ust. 3 RODO, w tych przypadkach, gdy administrator z jakichś względów umożliwia dostęp do danych

[99] M. Sakowska-Baryła, *Komentarz do art. 4 pkt 8, uwaga 86 i 87*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 108; P. Litwiński (red.), *op. cit.*, s. 476-477; J. Byrski, *op. cit.*, s. 39.

osobowych. Tymczasem nie każde udostępnienie danych osobowych czy zapewnienie do nich dostępu w jakiejś formie jest równoznaczne z powierzeniem przetwarzania danych osobowych. Nie każde też powierzenie przetwarzania jest równoznaczne z udostępnieniem, bo powierzyć podmiotowi przetwarzającemu można także operację polegającą na zbieraniu danych w imieniu i na rzecz administratora, których siłą rzeczy administrator wcześniej nie posiadał, więc i nie może ich udostępnić. Pamiętać należy, że zgodnie z treścią 4 pkt 2 RODO jako udostępnienie danych osobowych kwalifikuje się w szczególności takie operacje, jak ujawnianie poprzez przesłanie, rozpowszechnianie, a także inne operacje, które prowadzą do ujawnienia danych, ale przecież nie zawsze wykonuje się je w ramach powierzenia przetwarzania danych osobowych. Jeśli bowiem jeden podmiot w jakikolwiek sposób udostępnia dane osobowe drugiemu, może to czynić choćby dlatego, że wynika to z ich wspólnych prawnie uzasadnionych interesów bądź z prawnie uzasadnionych interesów jednego z nich (zob. art. 6 ust. 1 lit. f RODO) dlatego, że to udostępnienie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na dokonującym go administratorze (zob. art. 6 ust. 1 lit. c RODO) czy dlatego, że takie przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (zob. art. 6 ust. 1 lit. e RODO), a może i dlatego, że osoba, której dane dotyczą, zwyczajnie tego oczekuje i wyraziła na udostępnienie jej danych zgodę na warunkach określonych w art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a w związku z art. 4 pkt 11 oraz art. 7 RODO.

Obserwując praktykę stosowania przepisów rozporządzenia, także przez jednostki organizacyjne samorządu terytorialnego, wysnuć można wniosek, że powierzenie przetwarzania niesłusznie i błędnie dostrzega się np. we:

1) wzajemnym przekazywaniu przez strony umów w ich treści danych osób odpowiedzialnych za realizację umowy;

2) udostępnianiu danych osobowych innemu podmiotowi, np. danych osobowych pracowników, którzy oddelegowani zostali do obsługi jakiegoś odcinka zadań (np. inspektorów odpowiedzialnych za kontakt z placówkami oświatowymi w gminie) albo pracowników wysłanych na szkolenie organizowane przez podmiot zewnętrzny, który ma wystawić im certyfikaty uczestnictwa;
3) wymianie informacji pomiędzy szkołą a ośrodkiem pomocy społecznej dotyczących dziecka korzystającego z dożywiania na terenie szkoły;
4) oddawania do dyspozycji pracowników administratora lub innych członków jego personelu pewnego zakresu danych osobowych, które są niezbędne do wykonywania powierzonych im zadań na określonym stanowisku pracy.

Tymczasem w trzech pierwszych sytuacjach w żadnym razie nie mamy do czynienia z relacją administrator – procesor oraz z przetwarzaniem danych osobowych w imieniu i na rzecz administratora przez podmiot przetwarzający, ponieważ we wszystkich tych przypadkach mamy do czynienia z dwoma administratorami, którzy w oparciu o przesłanki określone odpowiednio w art. 6 lub art. 9 ust. 2 RODO dokonują operacji przetwarzania danych osobowych we własnym imieniu i na własną rzecz. Nadto czynności udostępnienia danych przez jedną ze stron, a następnie przetwarzanie danych osobowych w postaci różnych operacji wykonywanych przez drugą stronę nie są podejmowane na polecenie jednego z administratorów kierowane do drugiego podmiotu.

Czwarty zaś z wymienionych przypadków, a mianowicie umożliwienie dostępu do danych osobowych pracownikom administratora bez wątpienia to sytuacja, w której przetwarzanie odbywa się w imieniu administratora i na jego rzecz, ale nie na warunkach powierzenia, lecz w ramach czynności samego administratora. Operacje przetwarzania dokonywane przez pracowników administratora lub innych członków jego personelu uznać należy za czynności jego samego. Nie ma tu przy

tym znaczenia podstawa prawna wykonywania czynności. Za zasadne należy uznać zaliczenie do personelu administratora jego pracowników, wykonujących zadania na podstawie umowy o pracę, na podstawie umów cywilnoprawnych, w ramach stażu absolwenckiego, praktyk studenckich czy wolontariatu. Istotne jest to, że operacje przetwarzania w danym przypadku wykonywane są pod kierunkiem administratora, w jego infrastrukturze lub w infrastrukturze, za którą on ponosi odpowiedzialność albo korzystanie z której wyraźnie dopuszcza, podejmując ryzyko naruszenia praw lub wolności osób fizycznych związanych z przetwarzaniem danych osobowych[100]. W ramach eliminacji niepotrzebnych umów powierzenia należy zawsze zbadać, jaka jest swoboda podmiotu przetwarzającego w ramach realizacji „umowy powierzenia" – czy może on podejmować swobodnie, na gruncie obowiązującego go prawa, czynności przetwarzania nieobjęte umową. Postulować wypada dokonanie analiz wcześniejszych praktyk w zakresie zawierania umów powierzenia choćby z podmiotami profesjonalnie zajmującymi się świadczeniem usług wymagających przetwarzania danych, których celem nie jest jednak bezpośrednio ich przetwarzanie, a dane osobowe pojawiają się w tych relacjach z uwagi na wymogi prawne lub prakseologiczne. W nadmiernym i zbędnym zawieraniu umów powierzenia można wręcz dopatrzeć się utrudnienia przepływu danych pomiędzy administratorami, czemu – w myśl art. 1 ust. 3 – RODO ma służyć. Trzeba uznać za co najmniej osobliwe przypadki, gdy dochodzi do zawarcia umowy powierzenia tylko dlatego, że w dokumentacji przekazywanej na potrzeby wykonania umowy znajdują się dane osób uprawnionych do reprezentowania drugiej strony umowy czy wykonujących określone zadania wynikające z umowy, a nawet jedynie tzw. osób kontaktowych,. Biorąc pod uwagę zasadę adekwatności i minimalizacji przetwarzania, wynikającą z art. 5 RODO, oraz wymogi wskazane w art. 24 i 25 tego rozporządzenia, procesy

[100] Podobnie zob. P. Fajgielski, *Ogólne rozporządzenie…,* s. 124.

udostępniania danych nie powinny nadmiernie ingerować w prawa osób, których dane będą udostępniane. Również w ramach samego powierzenia nie posiadają one bowiem praktycznych środków kontroli, a tym bardziej nie muszą wyrażać zgody na takie działanie podejmowane przez administratora[101].

7. Weryfikacja podmiotu przetwarzającego

Zgodnie z art. 28 ust. 1 RODO jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą. To przepis, nakładający na administratora obowiązek odpowiedniego zweryfikowania podmiotu, któremu ma być powierzone przetwarzanie danych osobowych. Obowiązek ten dotyczy administratorów niezależnie od sektora, do którego można ich zaliczyć. Dotyczy to także administratorów publicznych, w tym samorządowych, bez względu na to, jak kształtuje się podstawa powierzenia – czy wynika ono z umowy cywilnoprawnej, czy z tzw. innego instrumentu prawnego. Sensem tego wymogu jest zapewnienie danym osobowym powierzonym do przetwarzania przez podmiot zewnętrzny standardów ochrony nie niższych niż te, których prawo wymaga od administratora. Chodzi tu o odpowiednie zabezpieczenie prywatności informacyjnej jednostki i zagwarantowanie możliwości realizacji jej praw. Jak wynika z motywu 81 preambuły RODO, „[a]by zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu

[101] Zob. K. Wygoda, *Czy potrzebne…*, s. 29.

czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania". Konsekwencją tego założenia jest także treść art. 28 ust. 3 zd. 2 i określony tam zakres obowiązków podmiotu przetwarzającego, który powinien być ustalony odpowiednio w umowie lub w innym akcie, z którego powierzenie wynika.

Biorąc pod uwagę zasady rozliczalności przetwarzania, administrator jest zobowiązany wykazać spełnienie wymogu wynikającego z art. 28 ust. 1 RODO. Sposób owego wykazywania zgodności z RODO nie jest opisany, a administratorowi pozostawiono w tym zakresie dowolność. Z pewnością zmuszony on będzie sprawdzić, czy potencjalny procesor zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą, a następnie wykazać, że takiego sprawdzenia dokonał.

Przed każdym, w tym publicznym, administratorem stoi zatem zadanie zaplanowania procesu weryfikacji procesorów, określenia adekwatnych i efektywnych sposobów jego dokonywania. Praktyka pokazuje, że następuje to między innymi poprzez:

1) tworzenie tzw. list kontrolnych dotyczących potencjalnego procesora oraz świadczonych przez niego usług;
2) przeprowadzenie audytu u potencjalnego kontrahenta, który może być dokonywany przez personel administratora, personel przetwarzającego lub niezależnego audytora;
3) odpowiednie włączenie procesu weryfikacji procesora w procedury zamówień publicznych – stawianie odpowiednich wymogów w specyfikacji istotnych warunkach zamówienia, stawianie odpowiednio sformułowanych pytań w zapytaniach ofertowych itp.;

4) żądanie wykazania, że procesor przeszedł pozytywnie audyt przetwarzania danych osobowych[102].

Rozporządzenie nie określa jednak, jakie gwarancje po stronie procesora są „wystarczające". Uzasadnione jest przyjmować, że chodzi tu o takie gwarancje, które dotyczą środków technicznych i organizacyjnych, a ich poziom powinien być oceniany w konkretnych okolicznościach, wziąwszy pod uwagę cel, charakter, zakres i kontekst przetwarzania. Ocena i wymogi co do gwarancji są różne w zależności od tego, jak skonkretyzuje się powyższe czynniki. Praktyka pokazuje, że zwyczajnie nie sprawdzają się zunifikowane listy kontrolne w sektorze samorządowym. Nie istnieje bowiem ani perfekcyjna, ani uniwersalna lista kontrolna. Jeśli procesy przetwarzania danych osobowych, konteksty, cele, zakresy i charakter przetwarzania są podobne, można próbować tworzyć podobne instrumenty weryfikacji. Jednak z pewnością lista kontrolna tworzona w celu weryfikacji introligatora nie będzie adekwatna do weryfikacji podmiotu dostarczającego system informatyczny do rozliczeń budżetowych czy elektronicznego obiegu dokumentów i odwrotnie. Przeprowadzenie wnikliwej, specjalistycznej analizy pozwoli dopiero na osiągnięcie wyniku, na którego podstawie możliwe będzie podjęcie decyzji o wdrożeniu odpowiednich środków technicznych i organizacyjnych, które są niezbędne, aby zapewnić stopień bezpieczeństwa danych osobowych przed potencjalnymi zagrożeniami[103].

Niezależnie od powyższego, zgodnie z treścią motywu 81 preambuły RODO „[s]tosowanie przez podmiot przetwarzający zatwierdzonego

[102] Zob. M. Krzysztofek*, Warunki dopuszczalności powierzenia – lista kontrolna*, „ABI Expert" 2017, nr 4, s. 18-20; T. Izydorczyk, *Działania organizacyjne*, „ABI Expert" 2017, nr 4, s. 36-37.

[103] M. Jabłoński, J. Węgrzyn, *Zmiana modelu ochrony danych osobowych – podejście oparte na ryzyku, privacy by design i privacy by default,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017, s. 77-78, http://www.biblioteka-cyfrowa.pl/dlibra/docmetadata?id=89093&from=publication [dostęp: 27.11.2018].

kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora". W konsekwencji także w art. 28 ust. 5 RODO przewidziano, że wystarczające gwarancje, o których mowa w art. 28 ust. 1 i 4, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42[104].

8. Umowa powierzenia lub inny instrument prawny i ich zakres

Powierzenie powinno mieć swoje sformalizowane źródło w pisemnej lub mającej formę elektroniczną umowie lub w innym instrumencie prawnym. Zawarcie umowy lub wykreowanie (podjęcie) „innego instrumentu prawnego" stanowi wynikający z RODO wymóg legalizujący przetwarzanie danych osobowych na zasadzie powierzenia. Wywodzić to należy z treści motywu 81 oraz art. 28 ust. 3 i 9 RODO.

W motywie 81 czytamy, że „[p]rzetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym instrumentem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby, której dane dotyczą".

[104] Szerzej zob. T. Osiej, *Mechanizmy certyfikacji, znaki jakości i oznaczenia w zakresie ochrony danych w świetle przepisów ogólnego rozporządzenia o ochronie danych,* [w:] M. Kawecki, T. Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017, s. 173 i n.; J. Anisimowicz, *Akredytacja dla podmiotów certyfikujących oraz przebieg procesu certyfikacji*, „ABI Expert" 2017, nr 4, s. 30-32.

Zgodnie z treścią art. 28 ust. 3 RODO przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora. Jednocześnie rzeczone umowa lub inny instrument prawny mają podlegać prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora. Kryterium odpowiedniego umocowania w przepisach prawa odnosi się do obu tych przypadków legalizacji przetwarzania danych na zasadzie powierzenia. Co więcej, art. 28 ust. 3 RODO wskazuje obowiązkowy zakres ich treści. Zgodnie z art. 28 ust. 3 RODO ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

a) przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki wymagane na mocy art. 32;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na

żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;

f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32-36;

g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;

h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Przy czym w związku z obowiązkiem określonym w akapicie pierwszym lit. h) podmiot przetwarzający ma niezwłocznie informować administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

9. Umowa

Powierzenie przetwarzania danych osobowych w pierwszej kolejności może wynikać z umowy. Umowa jest czynnością prawną dwustronną lub wielostronną. Powszechnie przyjmuje się, że obejmuje ona zgodny zamiar stron skierowany na wywołanie powstania, zmiany lub ustania skutków prawnych[105]. W przypadku stosunku powierzania

[105] Zob. W Czachórski, *Zobowiązania. Zarys wykładu*, Warszawa 1999, s. 129; Z. Radwański, *Prawo cywilne – część ogólna*, Warszawa 2007, s. 220.

przetwarzania danych osobowych zgodny zamiar stron określony będzie przez administratora lub współadministratorów i podmiot przetwarzający lub podmioty przetwarzające, a także przez subprocesora lub subprocesorów względem procesora.

Wspomniana umowa może, ale nie musi dotyczyć wyłącznie powierzenia przetwarzania danych osobowych. Treść odpowiadająca wymogom wynikającym z art. 28 ust. 3 RODO może stanowić element szerszej umowy określającej warunki współpracy między jej stronami. Może także być ujęta w osobnym dokumencie określanym często mianem „umowy powierzenia przetwarzania danych osobowych" lub „umowy o powierzenie przetwarzania danych osobowych".

10. Inny instrument prawny

Inny instrument prawny legalizujący powierzenie przetwarzania danych osobowych to zapewne czynność prawna inna od umowy, choć RODO nie określa w żadnej mierze jej charakteru. Uzasadnione jest założenie, że może to być nie tylko zgodne oświadczenie dwóch stron, ale i jednostronna czynność prawna, uchwała, obejmująca oświadczenia woli więcej niż jednego podmiotu. W RODO nie dokonano jednak wskazania, w jaki sposób interpretować pojęcie „innego instrumentu prawnego", co może być kłopotliwe, zwłaszcza że w dalszej części art. 28 RODO – w ust. 4, 6 i 9 – w polskiej wersji językowej mowa już nie o „instrumencie", ale o „akcie prawnym", co zbieżne jest z określaniem tej instytucji w innych wersjach językowych RODO. Zasadne wydaje się wzięcie pod uwagę przewidzianej prawem formy działania organów i podmiotów publicznych, które w zakresie swoich kompetencji decydują o nawiązaniu stosunku powierzenia przetwarzania danych pomiędzy administratorem danych a podmiotem przetwarzającym. Można tu brać pod uwagę ustawy określające prawne formy działania określonych

organów i podmiotów, ale też przesądzające o treści nawiązywanych przez nie stosunków prawnych. Powierzenie może wynikać także z różnych form działania organów i podmiotów publicznych przewidzianych dla nich w przepisach prawa, które jednak trudno skonkretyzować. W rachubę będą mogły tu wchodzić akty kreujące byt publicznych jednostek organizacyjnych, określające jednocześnie ich statuty, zasady, zakres i formy działania, a także zawierane w granicach prawa porozumienia między takimi jednostkami[106]. W samorządzie – o czym już wspomniano – za powierzenie na podstawie „innego instrumentu prawnego" uznać należy powierzenie przetwarzania jednostce obsługującej danych osobowych, w stosunku do których administratorem pozostaje jednostka obsługiwana w przypadku utworzenia centrum usług wspólnych na podstawie ustaw samorządowych[107] – w zależności od przypadku – odpowiednio na szczeblu gminnym, powiatowym, wojewódzkim. Kwestię takiego powierzenia ustawy samorządowe regulują niemal jednobrzmiąco. Nie jest to jednak wyłączna podstawa powierzenia. Konkretyzuje je bowiem akt powołujący do życia wspólną obsługę, którym będzie odpowiednio albo uchwała organu uchwałodawczego danej jednostki samorządu terytorialnego albo porozumienie o przystąpieniu do wspólnej obsługi[108]. Inny instrument prawny powinien odpowiadać co do treści wymogom wynikającym art. 28 ust. 3 RODO.

Jak jednak wskazuje się w literaturze, modelowa konstrukcja instrumentu prawnego ma jednak poważne ograniczenie, ponieważ

[106] M. Sakowska-Baryła, *Powierzenie przetwarzania danych osobowych w sektorze publicznym*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *op. cit.*, s. 19-21, http://www.bibliotekacyfrowa.pl/dlibra/docmetadata?id=89093&from=publication [dostęp: 27.11.2018]; M. Sakowska-Baryła, *Komentarz do art. 28, uwaga 11*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 321-322.

[107] Zob. ustawa z dnia 8 marca 1990 r. o samorządzie gminnym (Dz. U. z 2018 r. poz. 994 ze zm.); ustawa z dnia 5 czerwca 1998 r. o samorządzie powiatowym (t. j. Dz. U. z 2018 r. poz. 995 ze zm.); ustawa z dnia 5 czerwca 1998 r. o samorządzie województwa (Dz. U. z 2018 r. poz. 913 ze zm.).

[108] Zob. M. Sakowska-Baryła, *Organizacja ochrony...*, s. 177 i n.

przyjmując za punkt wyjścia treść RODO, należy podkreślić, że wszystkie składniki instrumentu prawnego muszą wiązać zarówno administratora, jak i podmiot przetwarzający lub podmioty przetwarzające. Tyle tylko, że istniejące obecnie tego rodzaju akty, w tym uchwały kreujące samorządowe centra wspólne (CUW), najczęściej wymagają uzupełnienia ich treści w „obudowujących je aktach wykonawczych" (choćby o charakterze wewnętrznie obowiązującym wiążącym jednostki organizacyjne korzystające, np. CUW), ale nie zawierają jednocześnie norm delegujących na organy wykonawcze określenie szczegółowego zakresu powierzenia w akcie ustanawianym przez te pomioty, uniemożliwiając takie rozwiązanie. Tymczasem zakładać trzeba, że bez stosownej delegacji organy stanowiące nie mają możliwości podejmowania działań prawotwórczych w tym zakresie. Jedynym zatem wyjściem stosowanym na szeroką skalę, nie uwzględniającym interwencji prawodawczej uzupełniającej treść dotychczasowych podstaw prawnych, jest podążanie drogą wypracowaną jeszcze w oparciu o s.u.o.d.o. z 1997 r. i zawieranie umów powierzenia dookreślających treści wymagane w art. 28 RODO. Idąc dalej, można zastanowić się nad generalnym zakwestionowaniem ułomnego (niepełnego) instrumentu prawnego jako legalnej podstawy powierzenia wskazanej w art. 28 RODO, ale rzeczone modelowe ujęcie zderza się najczęściej z rzeczywistością, w której przy braku pełnego dookreślenia treści innego instrumentu wiążącego pomioty znajdują się w sytuacji znaczącego wpływu czy nawet uzależnienia jednego z nich od drugiego, owocującej zawarciem umowy powierzenia. To stan niepożądany i niepokojący, bo relacje w ramach powierzenia powinny być określane na zasadzie wyłączności albo przez umowę lub inny instrument wiążący i nie powinno się ich łączyć. W systemie prawa zakładamy bowiem związanie w ramach obowiązków z niego wynikających i nie

powinny być one uzależnione od późniejszego zawarcia umowy. chyba że okoliczność taka wprost wynika z samego instrumentu[109].

11. Forma umowy lub innego aktu prawnego

Z art. 28 wynika, że umowa lub inny akt prawny, regulujące powierzenie oraz podpowierzenie musi mieć formę pisemną, w tym formę elektroniczną. Choć interpretacja owej pisemności i elektronicznej formy może budzić wątpliwości interpretacyjne, zasadne wydaje się przyjąć, że „forma elektroniczna" powinna być rozumiana w sposób autonomiczny, bez odwoływania się do przepisów k.c. Wykładać je należy, biorąc pod uwagę zasadę efektywności oraz uwzględniając *ratio legis* poszczególnych przepisów o formie. Zasadne jest, aby za wystarczające uznać użycie formy dokumentowej zgodnie z art. 77^2 k.c., z mocy którego do zachowania dokumentowej formy czynności prawnej wystarcza złożenie oświadczenia woli w postaci dokumentu, w sposób umożliwiający ustalenie osoby składającej oświadczenie. Warunkiem tu pozostaje jednak, że użyte rozwiązana zapewnią integralność oraz autentyczność umowy lub innego aktu regulującego powierzenie[110].

12. Podpowierzenie

Zgodnie z art. 28 ust. 2 RODO podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych

[109] Zob. K. Wygoda, *Czy potrzebne*…, s. 28.

[110] K. Witkowska-Nowakowska, *Komentarz do art. 28, uwaga 16*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *op. cit.*; P. Litwiński (red.), *op. cit.*, s. 477-479; M. Sakowska-Baryła, *Komentarz do art. 28, uwaga 28*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 330.

podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Przy czym w myśl art. 28 ust. 4 RODO jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym. W ten sposób RODO określa zarówno podstawę podpowierzenia, jak i relacje pomiędzy administratorem, procesorem i subprocesorem. Szczególnie warte odnotowania, że biorąc pod uwagę te przepisy, obecnie nie wchodzi w rachubę sytuacja, w której administrator nie wie o podpowierzeniu przetwarzania danych osobowych, których przetwarzanie zlecił procesorowi. Jednocześnie zgoda na podpowierzenie musi być uprzednia w stosunku do jego wykonania. W rzeczonym stanie prawnym samorządowy administrator musi przeanalizować, jaką strukturę powierzenia w danym przypadku dopuszcza – czy powierzenie przetwarzania może być realizowane wyłącznie przez procesora, czy też dopuszcza zaistnienie relacji o charakterze kaskadowym, gdzie podmiot przetwarzający korzysta z podwykonawców. Nie zawsze zasadne jest obserwowane często w praktyce czynienie umownych zastrzeżeń o niedopuszczalności dalszego powierzania przetwarzania danych osobowych. Nadto nie wydaje się, by takie rozwiązanie za każdym razem

było korzystne dla samorządowego administratora i bezrefleksyjnie mogło być uzasadniane względami ochrony danych osobowych. Biorąc bowiem pod uwagę uwarunkowania rynkowe, niekiedy okazać się może, że np. dobrej jakości usługi IT oparte są właśnie na umiejętnie dobieranym przez procesora zespole dalszych podmiotów przetwarzających, które zmieniają się w czasie i według potrzeb realizacji konkretnych zadań. Dlatego też nie jest zasadne rekomendowanie wyłączania podpowierzeń z procesów przetwarzania danych osobowych w samorządzie, ale opowiadać się za każdorazowym ustalaniem, na jakich zasadach możliwe jest korzystanie z subprocesora.

Rozdział V

Wdrożenie procedur informacyjnych i komunikacyjnych

(prof. dr hab. Mariusz Jabłoński)

1. Zakres i charakter regulacji w obszarze realizacji obowiązku przejrzystego informowania i przejrzystej komunikacji

Postanowienia 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[111]; RODO) precyzują nowe gwarancje systemowe, redefiniując dotychczasowe procedury oraz mechanizmy ochrony i przetwarzania danych osobowych (sposoby działania zobowiązanych do ochrony)[112]. Ważne znaczenie ma fakt sprecyzowania w RODO konkretnych uprawnień jednostki, które w istotny sposób wzmacniają jej status podmiotu prawnie chronionego. Chodzi tu przede wszystkim o zdefiniowanie treści roszczeń umożliwiających wystąpienie przez osobę fizyczną z żądaniem uzyskania informacji o tym, czy jej dane są przetwarzane (art. 13 i 14 RODO), a ponadto prawa:

[111] Dz. U. UE z 4 maja 2016, L119.

[112] Na temat relacji istniejącego systemu i nowych obowiązków zob.: T. Cygan, *Zabezpieczenie danych według RODO*, „ABI Expert" 2017, nr 3(4), s. 30-32.

– dostępu do informacji, w tym prawa do kopii danych (art. 15 RODO);
– sprostowania danych (art. 16 RODO);
– usunięcia danych osobowych (tzw. prawo do bycia zapomnianym – art. 17 RODO)[113];
– ograniczenia przetwarzania (art. 18 RODO);
– przenoszenia danych (art. 20 RODO);
– sprzeciwu (art. 21 RODO)[114];
– niepodlegania zautomatyzowanym rozstrzygnięciom indywidualnym[115] (z zastrzeżeniem art. 22 ust. 2 RODO)[116];

[113] Warto w tym zakresie wskazać na wyrok TS w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González* C-131/12, w którym Trybunał stwierdził m.in.: „art. 12 lit. b) i art. 14 akapit pierwszy lit. a) dyrektywy 95/46 należy interpretować w taki sposób, iż w ramach oceny tego, czy spełnione zostały warunki zastosowania tych przepisów, należy w szczególności przeanalizować kwestię, czy osoba, której dotyczą dane, ma prawo do tego, aby dana dotycząca jej informacja nie była już, w aktualnym stanie rzeczy, powiązana z jej imieniem i nazwiskiem poprzez listę wyświetlającą wyniki wyszukiwania mającego za punkt wyjścia to imię i nazwisko, przy czym stwierdzenie, iż takie prawo przysługuje, pozostaje bez związku z tym, czy zawarcie na tej liście wyników wyszukiwania danej informacji wyrządza szkodę tej osobie. Ponieważ osoba ta może, ze względu na przysługujące jej i przewidziane w art. 7 i 8 karty prawa podstawowe, zażądać, aby dana informacja nie była już podawana do wiadomości szerokiego kręgu odbiorców poprzez zawarcie jej na takiej liście wyników wyszukiwania, prawa te są co do zasady nadrzędne nie tylko wobec interesu gospodarczego operatora wyszukiwarki internetowej, lecz również wobec interesu, jaki ten krąg odbiorców może mieć w znalezieniu rzeczonej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby. Taka sytuacja nie ma jednak miejsca, jeśli ze szczególnych powodów, takich jak rola odgrywana przez tę osobę w życiu publicznym, należałoby uznać, że ingerencja w prawa podstawowe tej osoby jest uzasadniona nadrzędnym interesem tego kręgu odbiorców, polegającym na posiadaniu, dzięki temu zawarciu na liście, dostępu do danej informacji". Zob. też: Wytyczne Grupy Roboczej Art. 29 dotyczące wykonania wyroku Trybunały Sprawiedliwości Unii Europejskiej w sprawie *Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mario Consteja González* C-131/12, https://giodo.gov.pl/pl/1520203/8648 [dostęp: 10.11.2018].

[114] Zob. szerzej: Ł. Zięba, *Budowanie profili osobowych a wymogi wynikające z nowych przepisów o ochronie danych osobowych*, [w:] M. Kawecki, T. Osiej (red.), *op. cit.,* s. 136 i n.

[115] Zob.: M. Czerniawski, *Nowe procedury ochrony*, „ABI Expert" 2016, nr 1, s. 12-14.

[116] Może to mieć jednak miejsce, jeśli decyzja ta: „...a) jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

– uzyskania informacji o naruszeniu ochrony danych i jego konsekwencjach w sferze gwarantowanych wolności i praw (wskazanych wyżej – art. 15-22 i 34 RODO)[117].

Jednocześnie trzeba podkreślić, że „W przypadku informowania mamy do czynienia z przekazywaniem przez administratora informacji podmiotowi danych, a więc z działaniem jednostronnym, natomiast w przypadku komunikacji działanie to ma wymiar obustronny – powinna następować interakcja między administratorem a podmiotem danych"[118]. W jednym i drugim przypadku działanie administratora przyjmować będzie postać czynności materialno-technicznej, czyli normatywnie regulowanej formy działania administracji, która wywołuje skutki prawne poprzez działanie o charakterze faktycznym[119].

Jak wskazuje się w treści RODO, celem uchwalenia tego aktu jest wzmocnienie i zharmonizowanie ochrony podstawowych wolności i praw osób fizycznych w związku z czynnościami przetwarzania oraz

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą".

[117] Zob. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, s. 6 i n.; K. Szymielewicz, *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony?*, [w:] G. Sibiga (red.), *op. cit.*, s. 11-15; w odniesieniu do prawa do bycia zapomnianym zob.: wyrok TSUE z dnia 13 maja 2014 roku, C-131/12. Szerzej o koncepcji prawa do bycia zapomnianym J. Żak, *Koncepcja „prawa do bycia zapomnianym"*, [w:] M. Jabłoński, S. Jarosz-Żukowska (red.), *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi*, Wrocław 2014, s. 142-155.

[118] P. Fajgielski, *Komentarz do art. 12 RODO*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 227.

[119] Jak wskazuje się w orzecznictwie NSA, czynności takie „Muszą należeć do zakresu administracji publicznej, czyli całokształtu materii w aspekcie podmiotowym (właściwych organów) i przedmiotowym (prawa administracyjnego), w ramach którego realizowane są funkcje i zadania państwa zmierzające do zaspokojenia potrzeb jego obywateli" – uchwała NSA z dnia 26 czerwca 2014 r., I OPS 14/13. Istotne w tym zakresie może być uwzględnienie szerszego znaczenia „sprawy publicznej" zdefiniowane w orzecznictwie Trybunału Konstytucyjnego – zob. uchwała z dnia 27 września 1994 r., W 10/93.

zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi (motyw 3 preambuły). Ochrona ta w istocie nie ogranicza się wyłącznie do stworzenia gwarancji służących zdefiniowaniu prawidłowości procesów przetwarzania i przepływu danych osobowych. Musi być rozumiana o wiele szerzej – pośrednio jako ochrona wszystkich wolności i praw definiujących szeroko rozumianą autonomię informacyjną jednostki. Autonomia ta w najprostszym ujęciu identyfikowana jest ze swobodą jednostki w zakresie samodzielnego decydowania o ujawnianiu innym organom, instytucjom czy podmiotom (np. przedsiębiorcom, organizacjom społecznych, a także różnego rodzaju jednostkom organizacyjnym) informacji o sobie i własnym życiu, a także realnym prawem do sprawowania kontroli nad procesami przetwarzania takich danych, jeśli znajdują się w posiadaniu innych podmiotów, w szczególności tymi, których obowiązek udostępnienia wynika z przepisów prawa powszechnie obowiązującego[120].

Mając na względzie wprowadzenie zasady domyślnej ochrony prywatności (por. art. 25 RODO), w istotny sposób rozwiązania te muszą zmodyfikować dotychczasową praktykę funkcjonowania szeregu organów (instytucji) i podmiotów przetwarzających dane osobowe (w tym także tych tworzących w szerokim znaczeniu administrację publiczną na poziomie samorządu terytorialnego)[121]. Jest to szczególnie istotne, jeżeli weźmiemy pod uwagę, że ani RODO, ani przepisy regulacji krajowych (przynajmniej w Polsce) nie definiują normatywnych wzorców wniosków w zakresie dochodzenia przez osobę, której dane dotyczą, gwarantowanych praw. Nie oznacza to jednak możliwości uchylenia się przez

[120] Szerzej na temat współpracy: M. Kawecki, *Reforma danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych*, Warszawa 2017, s. 260 i n.

[121] K. Szymielewicz, *op. cit.,* s. 12; która definiuje również uwagi dotyczące tych rozwiązań RODO, w istotny sposób osłabiających dotychczasowe standardy ochrony danych osobowych, s. 12-15.

administratorów od obowiązku ich przestrzegania i swobody w ocenie zasadności ich merytorycznego rozpatrzenia.

Warto jednocześnie podkreślić, że stosowanie RODO nie wymaga uprzedniej implementacji jego treści do porządku normatywnego państwa członkowskiego UE[122]. Mamy tu bowiem do czynienia z rozporządzeniem unijnym, które, jak stwierdził Trybunał Konstytucyjny, jest aktem normatywnym, którego „pozycja w polskim systemie konstytucyjnym została wyznaczona w art. 91 ust. 3 Konstytucji"[123], dotyczącym wprost prawa stanowionego przez organizację międzynarodową. Prawo takie stosowane jest bezpośrednio, a ponadto ma pierwszeństwo w przypadku kolizji z ustawami stanowionymi przez polski parlament. Oznacza to, że każdy organ stosujący postanowienia RODO będzie miał obowiązek traktowania go jako części krajowego porządku prawnego, a w razie kolizji z ustawą obowiązek zastosowania tych norm ze skutkiem uchylającym stosowanie norm ustawowych[124]. W tym zakresie warto jedynie

[122] W odróżnieniu od postanowień Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW Dz. U. UE z 4.5.2016, L119. Warto jednocześnie zauważyć, że zgodnie z treścią art. 2 ust. 2 pkt d RODO postanowienia tego aktu nie mają 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.

[123] Wyrok TK z dnia 16 listopada 2011 r. SK 45/09.

[124] Jak podkreśla się: „W zakresie objętym stosowaniem rozporządzenia [RODO – przyp. M.J.] państwa członkowskie nie mają więc, jak przy dyrektywie, marginesu swobody wyboru ani formy, ani środków mających służyć osiągnięciu wyznaczonego w akcie normatywnym rezultatu. Dzięki temu możliwa jest realizacja celu w postaci zapewnienia całkowitego podejścia i jednolitego stosowania prawa UE we wszystkich państwach członkowskich. W tym przypadku jest to całościowa i spójna polityka w zakresie podstawowego prawa do ochrony danych osobowych, a nie, jak dotąd, dostosowanie w minimalnym zakresie wskazanym w dyrektywie. Po drugie, rozporządzenie – w odróżnieniu od dyrektywy – może być bezpośrednio stosowane i wywołuje pełny skutek bezpośredni wobec jednostek, co stanowi immanentną cechę przypisaną temu aktowi prawa na mocy

przypomnieć, że z punktu widzenia standardów unijnych prawo pochodne jest tworzone poza parlamentami państw członkowskich i charakteryzuje się następującymi zasadami: pierwszeństwa wobec porządków prawnych państw członkowskich; bezpośredniego stosowania i skuteczności[125]; jednolitości; solidarności; proporcjonalności; subsydiarności; równowagi kompetencyjnej[126]. Respektowanie tych zasad jest obowiązkiem wszystkich organów państwa członkowskiego. Dotyczy więc władzy ustawodawczej wykonawczej i sądowniczej.

Mając na uwadze miejsce postanowień RODO w systemie prawa, konieczne staje się jednocześnie podkreślenie, że akt ten nie jest aktem kompletnym. W wielu aspektach, w tym także w zakresie procedur, jedynie kierunkowo definiuje się w nim określonego rodzaju mechanizmy, które wdrożyć musi administrator (zobowiązany)[127]. W istotnym zakresie to nawet nie ustawodawca krajowy i krajowy organ nadzoru muszą uszczegółowić konkretne standardy i procedury, ile sam administrator. On bowiem będzie musiał wykazać, że podjął wszystkie niezbędne działania w zakresie wywiązania się z obowiązków wynikających bezpośrednio z treści RODO.

art. 288 TFUE", D. Kornobis-Romanowska, [w:] M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda, *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017, s. 22.

[125] Na temat tych dwóch pierwszych zasad i ich znaczenia w systemie unijnym, zob. C. Mik, *Zasady ustrojowe prawa wspólnotowego a polski porządek konstytucyjny*, „Państwo i Prawo" 1998, nr 1, s. 12-33; K. Wójtowicz, *Istota i źródła prawa wspólnotowego konsekwencje dla prawa krajowego*, [w:] M. Kruk (red.), *Prawo międzynarodowe i wspólnotowe w wewnętrznym porządku prawnym*, Warszawa 1997, s. 145-148.

[126] Szerzej na temat tych zasad zob.: Z. Witkowski, J. Galster, *Kompendium wiedzy o Unii Europejskiej z uwzględnieniem Traktatu Amsterdamskiego i Traktatu z Nicei,* Toruń 2002.

[127] Trzeba w tym miejscu podkreślić, że RODO nie jest aktem tak szerokim w rozumieniu zakresu regulacji, jak stara dyrektywa 95/46/WE – wyłączenie wynika choćby z wydanej dyrektywy „penalnej" – Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

W procesie przygotowania przez administratora mechanizmów realizacji praw przez uprawnionego w zakresie przejrzystego informowania i przejrzystej komunikacji konieczne staje się prowadzenie przez niego odpowiednich wykazów (rejestrów) otrzymanych wniosków (żądań) i prowadzonej w związku z nimi korespondencji. Jest to niezbędne dla celów dowodowych w razie ewentualnych sporów prowadzonych nie tylko z osobami, których dane dotyczą[128], ale również innymi, którzy, nie będąc uprawnionymi, żądania takie będą do administratora kierowali[129]. Dokumentacja taka jest niezbędna nie tylko z punktu widzenia wykazania przez administratora, że wywiązał się z nałożonych na niego obowiązków w postępowaniu przed krajowym organem nadzorczym (Prezesa Urzędu Ochrony Danych[130]), ale również w ramach ewentualnych postępowań sądowych[131].

[128] J. Łuczak, *Komentarz do art. 12 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *op. cit.,* s. 471.

[129] Każdy administrator musi więc stworzyć rejestr wniosków (żądań) składanych na podstawie RODO. Jednocześnie konieczne staje się zdefiniowanie, kto jest odpowiedzialny za przyjmowanie i koordynowanie procesem ich rozpatrywania. W przedmiotowym rejestrze powinno dojść do wyszczególnienia: 1. daty wpływu wniosku, 2. danych nadawcy, 3. adresu nadawcy, 4. przedmiotu sprawy, 5. sposobu załatwienia wniosku, 6. daty załatwienia wniosku, 7. ewentualnych uwag. Administrator musi też wdrożyć zasady i procedurę służące przechowywaniu oryginałów wniosków oraz wydruków wniosków przesłanych drogą elektroniczną, a także kopie udzielonych odpowiedzi.

[130] Zgodnie z treścią art. 7 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. 2018, poz. 1000 ze zm. – w sprawach nieuregulowanych w ustawie do postępowań administracyjnych przed Prezesem Urzędu Ochrony Danych Osobowych, zwanym dalej „Prezesem Urzędu", o których mowa w rozdziałach 4-7 i 11, stosuje się ustawę z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego. Postępowanie takie jest postępowaniem jednoinstancyjnym, a do postanowień wydanych w tych postępowaniach, na które zgodnie z ustawą z dnia 14 czerwca 1960 r. − Kodeks postępowania administracyjnego służy zażalenie, przepisów o zażaleniu nie stosuje się. Na takie postanowienia służy skarga do sądu administracyjnego. Wywiązanie się z obowiązków, o których mowa w art. 12, jest istotne już choćby z punktu widzenia sankcji związanych z możliwością ukarania administratora administracyjnymi karami pieniężnymi.

[131] Trzeba tu jednocześnie podkreślić, że zgodnie z treścią art. 97 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych ustalenia prawomocnej decyzji Prezesa Urzędu o stwierdzeniu naruszenia przepisów o ochronie danych osobowych lub prawomocnego wyroku wydanego w wyniku wniesienia skargi, o której mowa w art. 145a § 3 ustawy z dnia

2. Modelowe podejście administratora do realizacji obowiązków wskazanych w art. 12 RODO

Z punktu widzenia każdego administratora[132] konieczne staje się przygotowanie odpowiednich rozwiązań kształtujących zasady i procedurę (procedury) obsługi wniosków i realizacji praw przez osoby, których dane są przetwarzane. Pożądane w tym zakresie wydaje się najpierw przygotowanie przez administratora odpowiedniej polityki, precyzującej cele i mechanizmy, których wdrożenie zapewni odpowiednie wywiązywanie się niego z obowiązków sprecyzowanych w treści RODO. Jednocześnie polityka taka, stanowiąca składową całości dokumentacji rodowskiej, będzie służyła podnoszeniu świadomości wszystkich tych, którzy w imieniu administratora uczestniczą lub będą uczestniczyć w procesach przetwarzania danych osobowych[133].

Głównym założeniem uzasadniającym przygotowanie tego dokumentu jest więc czytelne określenie wartości i reguł, mających charakteryzować odejście administratora do kwestii realizacji praw osób, których dane dotyczą określonych w RODO oraz w aktach prawa krajowego, w szczególności definiujących ograniczenia takich praw.

---

30 sierpnia 2002 r. – Prawo o postępowaniu przed sądami administracyjnymi, wiążą sąd w postępowaniu o naprawienie szkody wyrządzonej przez naruszenie przepisów o ochronie danych osobowych co do stwierdzenia naruszenia tych przepisów, a także art. 99, w którym stwierdza się, że: Prezes Urzędu, jeżeli uzna, że przemawia za tym interes publiczny, przedstawia sądowi istotny dla sprawy pogląd w sprawie o roszczenie z tytułu naruszenia przepisów o ochronie danych osobowych, co będzie miało na pewno istotny wpływ na wydanie konkretnego rozstrzygnięcia.

[132] Administracja samorządowa działająca na podstawie i w graniach prawa, a więc zgodnie z zasadą legalizmu musi być odpowiednio przygotowana do wyzwań związanych z bezpośrednim stosowaniem RODO. Na temat związania prawem organów administracji publicznej zob. K. Kiczka, *Krajowy organ administracji publicznej w prawie unijnym*, Wrocław 2013, s. 203 i n.

[133] Warto w tym zakresie wskazać, że nie dotyczy to wyłącznie pracowników w klasycznym tego słowa rozumieniu. Na poziomie samorządu terytorialnego kwestie zdefiniowania obowiązków już na płaszczyźnie wójt (burmistrz, prezydent), rada, radni pojawia się wiele problemów interpretacyjnych.

Nie budzi wątpliwości, że RODO definiuje obowiązki administratora, mając na względzie ochronę interesu publicznego[134]. Każdy z administratorów w zakresie realizacji obowiązków informacyjnych na podstawie RODO kierować się musi zasadą przejrzystości. W tym zakresie informacje o przetwarzaniu danych osobowych dotyczących osoby, której dane dotyczą, należy przekazać tej osobie w momencie zbierania danych, a jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła – w rozsądnym terminie, zależnie od okoliczności. Jeżeli dane osobowe można zgodnie z prawem ujawnić innemu odbiorcy, należy poinformować o tym osobę, której dane dotyczą, w momencie pierwszorazowego ujawnienia danych temu odbiorcy. Jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o tym innym celu oraz dostarczyć jej innych niezbędnych informacji. Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny.

Jednocześnie w polityce konieczne staje się wyraźne podkreślenie niezbędności wdrożenia procedur służących osobie, której dane dotyczą, wykonywaniu praw przysługujących jej na mocy RODO, 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.

Na poziomie samorządu terytorialnego ważne staje się zidentyfikowanie skonkretyzowanych wprost w RODO wyłączeń możliwości realizacji określonych praw. Jednym nich są np. te dotyczące ograniczenia

[134] Jak wskazuje J. Blicharz, „Podstawowym celem działania administracji jest dobro jednostki (obywatela). Na drodze prowadzącej do tego celu interes publiczny można widzieć jako narzędzie do kształtowania sytuacji jednostki" – J. Blicharz, *Kategoria interesu publicznego jako przedmiot działania administracji*, Acta Universitatis Wratislaviensis no 2642, „Przegląd Prawa i Administracji" 2004, nr LX, s. 42.

prawa do bycia zapomnianym (art. 17 ust. 3 RODO). Zgodnie z jego treścią prawo do bycia zapomnianym, o którym mowa w ust. 1 i 2, nie ma zastosowania w zakresie, w jakim przetwarzanie jest niezbędne:

a) do korzystania z prawa do wolności wypowiedzi i informacji;
b) do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
c) z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) i art. 9 ust. 3;
d) do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych, lub do celów statystycznych zgodnie z art. 89 ust. 1, o ile prawdopodobne jest, że prawo, o którym mowa w ust. 1, uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
e) do ustalenia, dochodzenia lub obrony roszczeń.

Pomijając w tym miejscu kwestię merytorycznego omówienia tych przesłanek, nie budzi wątpliwości, że administrator będzie musiał w następstwie wpłynięcia konkretnego żądania, w sytuacji, gdy ziszcza się choćby jedna ze wskazanych wcześniej przesłanek, podjąć stosowne działania – na podstawie i w granicach wskazanych w RODO. Problematyczne staje się w tym zakresie wskazanie, czy jego działanie ma przybrać postać wyłącznie pisma informacyjnego, czy też musi wiązać się z wydaniem merytorycznego rozstrzygnięcia (decyzji) odmawiającego występującemu realizacji jego prawa. Gdyby przyjąć, że administrator, odwołując się do obowiązujących przepisów, stwierdza jedynie pewien fakt, tzn. (być może ponownie po wcześniejszym wskazaniu w klauzuli informacyjnej) istnienie prawnego obowiązku wymagającego przetwarzania czy zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej jemu powierzonej, to nie jest wykluczone przyjęcie modelu

odformalizowanego, w tym przypadku opierającego się na przesłaniu wnioskodawcy (żądającemu) pisma informacyjnego, a więc realizacji przez administratora klasycznej czynności materialno-technicznej[135].

Co do zasady czynność materialno-techniczna jako forma działania zobowiązanego może mieć miejsce wtedy, gdy obowiązujące przepisy prawa nie tworzą podstawy dla wydania decyzji[136]. Brak wyraźnych przepisów konkretyzujących te sytuacje, których decyzja taka powinna być wydana, przy jednoczesnym braku wskazania innej postaci rozstrzygnięcia (postanowienie), nie pozostawia administratorowi możliwości domniemywania legitymizacji do innego załatwienia wniosku niż za pomocą czynności materialno-technicznej. Przyjmuję, iż przesłanie zawiadomienia (powiadomienia), które ma postać czynności materialno-technicznej, powinno nastąpić w terminie analogicznym do tego, który został określony w art. 12 ust. 3 RODO. Termin ten nie może być jednak dłuższy niż miesiąc od dnia otrzymania wniosku. W przeciwnym razie zasadne stanie się postawienie administratorowi zarzutu bezczynności i przedstawienie go w drodze skargi skierowanej do Prezesa Urzędu Ochrony Danych Osobowych.

Z bezczynnością administratora będziemy mieli do czynienia wówczas, gdy w terminie ustalonym przez przepisy prawa organ ten nie podjął żadnych czynności w sprawie lub nie zakończył postępowania

[135] Wyrok NSA z 5 dnia lutego 2008 r., I OSK 581/07, w którym podkreślono, iż „Zarówno w doktrynie, jak i orzecznictwie dominujące jest stanowisko, że przez pojęcie aktu lub czynności organu administracji, o jakich mowa w art. 16 ust. 1 pkt 4 powołanej ustawy o NSA, należy rozumieć głównie działania materialno-techniczne, wywołujące określone skutki drogą faktów. Podzielić należy stanowisko, że działania te mogą mieć również charakter władczy, z tym że nie są to rozstrzygnięcia władcze, gdyż wówczas mamy do czynienia z decyzją administracyjną".

[136] Na temat aktów indywidualnych zob.: A. Błaś, *Działania administracji publicznej*, [w:] J. Boć (red.), *Administracja publiczna*, Wrocław 2003, s. 214 i n.; M. Masternak, *Kontrola czynności materialno-technicznych administracji publicznej przez sąd administracyjny*, [w:] Z. Niewiadomski, Z. Cieślak (red.), *Prawo do dobrej administracji. Materiały ze Zjazdu Katedr Prawa i Postępowania Administracyjnego. Warszawa-Dębe 23-25 września 2002 r.*, Warszawa 2003, s. 126 i n.

wydaniem decyzji, postanowienia lub też innego aktu lub nie podjął czynności, do której był prawnie zobowiązany[137]. Akceptując takie założenie, możemy wskazać na tzw. modelowy przykład bezczynności. Będzie ona miała miejsce wtedy, gdy administrator po wpłynięciu do niego żądania nie podejmuje działań mających na celu jego rozpatrzenie w terminach wskazanych w RODO i w konsekwencji uchybia terminowi wskazanemu w art. 12 ust. 3 rozporządzenia ogólnego[138].

Pismo informacyjne administratora ma charakter w pewnym sensie rozstrzygający. W praktyce bowiem stwierdza, że konkretna osoba nie jest uprawniona do realizacji prawa. Należy w tym zakresie przyjąć, iż jedynym możliwym rozwiązaniem jest zakwalifikowanie działań (czynności) administratora jako czynności materialno-technicznych podlegających następnie weryfikacji przez krajowy organ nadzorczy. Kwalifikacja taka zapewni wnioskodawcy możliwość wystąpienia ze skargą Prezesa Urzędu Ochrony Danych Osobowych, który jest właściwy dla oceny, czy ta mimo wszystko czynna, a nie bierna postać zachowania się (kwalifikacja żądania) administratora nie jest w istocie bezczynnością wynikającą z tego, iż nie przeprowadził należytego postępowania wyjaśniającego, którego ustalenia stają się podstawą skierowania do wnioskodawcy odpowiedniego pisma lub/i wadliwie dokonał kwalifikacji z punktu widzenia przepisów definiujących podstawy ograniczenia konkretnych praw.

[137] Odróżnia się również bezczynność od milczenia. Wskazuje się, iż z bezczynność „dotyczy niewykonywania kompetencji w zakresie zadań administracji publicznej, milczenie zaś występuje przy załatwianiu konkretnej sprawy z zakresu administracji publicznej" – P. Sitniewski, *Zasady nieudzielania informacji publicznych*, „Zeszyty Naukowe Wyższej Szkoły Administracji Publicznej w Białymstoku. Administracja Publiczna – Studia krajowe i międzynarodowe" 2006, nr 1/7, s. 73-74 z powołaniem się na prace J. Jendroński, *Milczenie administracji w postępowaniu administracyjnym*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio G. Ius" 1993, vol. XL oraz G. Łaszczycy, *Milczenie organu w świetle kodeksu postępowania administracyjnego*, „Państwo i Prawo" 1999, nr 1.

[138] W odniesieniu do działań podejmowanych przez administratora z bezczynnością będziemy mieli do czynienia również wtedy, gdy po powiadomieniu osoby (w terminie miesiąca) nie podejmuje kolejnych działań.

3. Procedury przejrzystego informowania i przejrzystej komunikacji

3.1. Respektowanie zasady przejrzystości w kontekście informowania i komunikacji

W Motywach RODO podkreśla się bardzo mocno konieczność zagwarantowania i powszechnego respektowania zasady przejrzystości, która wymaga, „by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem”[139]. W wielu opracowaniach podkreśla się jednocześnie, że wobec administratorów naruszających podstawowe zasady przetwarzania, a zatem także zasadę przejrzystości oraz prawa podmiotu danych

[139] „W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe. Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu” (Motyw 39). Konieczne staje się ponadto uwzględnienie treści Motywów: 58; 60; 71; 78; 100.

zagwarantowane treścią art. 12 RODO […] może być zastosowana sankcja w postaci administracyjnej kary pieniężnej w maksymalnej określonej przepisami rozporządzenia"[140].

Mając na względzie treść Motywów, jak również wskazany wyżej art. 12 RODO, administrator zobowiązany jest do odpowiedniego przygotowania procedur informacyjnych i komunikacyjnych służących:

- zwięzłemu, przejrzystemu, zrozumiałemu i w łatwo dostępnej formie, jasnym i prostym językiem udzielaniu informacji, o których mowa w art. 13 i 14 RODO (klauzule informacyjne);
- zwięzłemu, przejrzystemu, zrozumiałemu i w łatwo dostępnej formie, jasnym i prostym językiem prowadzeniu komunikacji na mocy art. 15-22 i 34 RODO w sprawie przetwarzania danych osobowych[141].

Informacje powyższe mają być udzielane na piśmie, jak również w inny sposób, także (w stosownych przypadkach) elektronicznie oraz ustnie. Pomimo że w treści art. 12 ust. 1 RODO podkreśla się, że ustne udzielenie informacji ma miejsce wtedy, gdy „innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą", to nie budzi wątpliwości, że udostępnienie informacji w każdym przypadku musi wiązać się z koniecznością zweryfikowania, że jest ona udostępniana osobie właściwej[142]

[140] J. Łuczak, *op. cit.*, s. 476.

[141] Chodzi tu o realizację: prawa dostępu do informacji, w tym prawa do kopii danych (art. 15 RODO); prawa do sprostowania danych (art. 16 RODO); prawa do usunięcia danych osobowych (art. 17 RODO); prawa do ograniczenia przetwarzania (art.18 RODO); prawa do przenoszenia danych (art. 20 RODO); prawa do sprzeciwu (art. 21 RODO); prawa do niepodlegania automatycznym rozstrzygnięciom indywidualnym (art. 22 RODO); prawa do uzyskania informacji o naruszeniu ochrony danych osobowych (art. 34 RODO).

[142] „Nakaz potwierdzania tożsamości wnioskodawcy w sposób niebudzący wątpliwości, zwłaszcza tam, gdzie na skutek zgłoszonego roszczenia mogłoby dojść do udostępnienia danych lub wprowadzenia innego ryzyka dla bezpieczeństwa danych. Administrator powinien wdrożyć rozwiązania mające na celu przeciwdziałanie ujawnieniu danych w wyniku złożenia żądania przez osobę nieuprawnioną. Dlatego też w przypadku przetwarzania niewymagającego identyfikacji, tam gdzie administrator nie jest w stanie zidentyfikować podmiotu danych i okoliczność tę wykaże, może nawet odmówić podjęcia działań" – J. Łuczak, *op. cit.*, s. 471.

(tzn. takiej, której dane są przetwarzane)[143]. Przy czym można zgodzić się z twierdzeniem, że „[…] wymóg potwierdzenia tożsamości osoby, której dane dotyczą, pozwala na przyjęcie, że ograniczenie możliwości korzystania z formy ustnej dotyczy tylko tych informacji, które odnoszą się do konkretnej osoby fizycznej, którą wcześniej należało zidentyfikować – stąd wydaje się, że ograniczenie posługiwania się formą ustną nie powinno dotyczyć wykonania obowiązków informacyjnych z art. 13 i 14 RODO, choć czysto językowa wykładnia komentowanego przepisu zdaje się temu przeczyć"[144].

Warto jednocześnie podkreślić, że nałożenie obowiązku udzielenia informacji przez administratora nie jest konieczne, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami, jeżeli utrwalenie lub ujawnienie danych są wyraźnie przewidziane prawem, lub jeżeli poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności w przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, prowadzeniu badań naukowych lub historycznych lub celom statystycznym. W tym zakresie realizacja żądania następuje po uwzględnieniu liczby osób, których dane dotyczą, okresu przechowywania danych oraz wszelkich przyjętych odpowiednich zabezpieczeń,

[143] W tym zakresie konieczne jest wprowadzenie równoległych procedur weryfikujących dotyczących złożenia wniosku w kancelarii, drogą elektroniczną lub ustnie. Procedury te będą charakteryzowały się różnym stopniem złożoności od najprostszej dotyczącej klasycznej postaci weryfikacji tożsamości w sytuacji osobistego składania żądania, przez wykorzystanie podpisu kwalifikowanego lub profilu zaufanego czy wreszcie poprzez weryfikację tożsamości polegającą na przesłaniu zwrotnej wiadomości e-maila z linkiem zawierającym prośbę o potwierdzenie złożenia wniosku. Droga telefoniczna musi wiązać się nie tylko z możliwością skutecznego przyjęcia wniosku przez administratora, ale też z możliwością weryfikacji tożsamości. Nie jest to zadanie niemożliwe do wykonania, ale wymaga wprowadzenia dodatkowych elementów techniczno-organizacyjnych, które pozwalają na weryfikację zgodności posiadanych danych. Procedury takie z powodzeniem stosowane są np. przez operatorów telekomunikacyjnych i innych usługodawców.

[144] P. Litwiński (red.), *op. cit.*, s. 356-357.

w tym ochrony tajemnic ustawowych, a w szczególnych przypadkach również umownych.

3.2. Weryfikacja tożsamości występującego

W zakresie prawidłowej identyfikacji tożsamości występującego z osobą, której dane dotyczą, każdy administrator musi wprowadzić stosowną procedurę weryfikacyjną[145]. Oczywiście jej zakres musi uwzględniać specyfikę sytuacji i formy występującego z żądaniem. Należy przy tym zwrócić uwagę na konieczność ograniczenia zakresu podawanych danych, gdyż ich nadmierna ilość i rodzaj prowadzić będą do złamania zasady minimalizmu przetwarzania (art. 25 RODO).

Mając powyższe na uwadze, konieczne staje się rozróżnienie na:

– żądania składane ustnie do protokołu w siedzibie oraz wnioski pisemne dostarczane osobiście przez uprawnionego[146];
– żądania przesyłane drogą pocztową;
– żądania przekazywane drogą telefoniczną.

W przypadku wniosków składanych w wersji papierowej przesłanych drogą pocztową przez wnioskodawcę konieczne staje się wdrożenie procedury, w ramach której administrator przesyła do żądającego bez zbędnej zwłoki zapytania z prośbą o potwierdzenie złożenia wniosku na posiadany adres e-mail (ewentualny link zwrotny) lub przeprowadzenie rozmowy telefonicznej, w ramach której wnioskodawca zostanie poproszony o podanie danych w celu ich weryfikacji z danymi znajdującymi się w posiadaniu administratora.

[145] Jak wskazuje na to J. Łuczak, „nakaz potwierdzania tożsamości wnioskodawcy w sposób niebudzący wątpliwości, zwłaszcza tam, gdzie na skutek zgłoszonego roszczenia mogłoby dojść do udostępnienia danych lub wprowadzenia innego ryzyka dla bezpieczeństwa danych", *op. cit*. s. 471.

[146] Przyjmuję, że w takim przypadku wystarczy sprawdzenie (potwierdzenie) przez uprawnionego pracownika administratora tożsamości uprawnionego (wnoszącego) za pomocą dokumentu tożsamości wnioskodawcy: dowodu osobistego lub paszportu (karty pobytu).

Możliwość skutecznej weryfikacji wiązać się również może z wykorzystaniem drogi elektronicznej – przez stwierdzenie tego, czy wniosek został opatrzony kwalifikowanym podpisem elektronicznym albo podpisem potwierdzonym profilem zaufanym ePUAP, ewentualnie poprzez weryfikację tożsamości polegającą na przesłaniu zwrotnej wiadomości e-mail z linkiem zawierającym prośbę o potwierdzenie złożenia wniosku.

Brak możliwości dokonania weryfikacji lub jedynie częściowe uzyskanie potwierdzenia skutkuje zawiadomieniem wnioskodawcy o braku możliwości rozpatrzenia wniosku z tego powodu wraz z informacją, w jaki sposób można ponownie złożyć wniosek i potwierdzić swoją tożsamość.

W sytuacji, gdy podane we wniosku dane nie umożliwiają identyfikacji wnioskodawcy, administrator powinien zwrócić się do wnioskodawcy o uzupełnienie wniosku tą samą drogą, którą wpłynął wniosek.

W sytuacji, w której nie ma możliwości wystąpienia do wnioskodawcy (np. wniosek przesłany drogą pocztową nie zawiera adresu nadawcy), wniosek należy pozostawić bez rozpoznania. W takim przypadku konieczne staje się sporządzenie odpowiedniej adnotacji na wniosku lub dołączenia doń stosownej notatki.

3.3. Zdefiniowanie wzorca odbiorcy informacji

W RODO podkreśla się znaczenie definiowania tzw. wzorca odbiorcy informacji. Zasadniczo należy uznać, że nie ma jednego stałego wzorca odbiorcy. Inaczej bowiem trzeba podejść do konsumenta i działalności np. przedsiębiorcy świadczącego usługi hotelarskie, inaczej do osoby dorosłej czy dziecka (o czym wprost wskazuje się w treści art. 12 ust. 1 RODO). Zgodzić się należy z założeniem, zgodnie z którym treść tego przepisu kreuje po stronie administratorów „zobowiązanie do należytego działania, a nie zobowiązanie rezultatu”[147]. W praktyce – przynajmniej

[147] J. Łuczak, *op. cit.*, s. 469.

na początku bezpośredniego stosowania RODO – widać pewne różnice w zakresie stosowania spersonalizowanych wzorców klauzul informacyjnych. Zasadniczo można odnieść wrażenie, że zazwyczaj administratorzy przygotowali jeden ogólny wzorzec klauzuli, który stosowany jest wobec każdej osoby.

Być może jest to wynikiem trudności w zakresie ustalenia, jak miałoby wyglądać zwięzłe, przejrzyste, zrozumiałe i w łatwo dostępnej formie, jasnym i prostym językiem prowadzenia komunikacji na mocy art. 15-22 i 34 RODO w sprawie przetwarzania danych osobowych. *De facto* musi to być bowiem komunikat na tyle treściwy, aby uprawniony dowiedział się, o jakie prawa w tym przypadku chodzi[148].

Zazwyczaj stosowane klauzule nie są nadmiernie rozbudowane, znaczna ich część posługuje się prostym i zrozumiałym językiem. Oczywiście istotne w tym zakresie jest zweryfikowanie tego, czy administratorzy prawidłowo skonkretyzowali wszystkie elementy składowe takich klauzul. Pewna część klauzul dotknięta jest błędami, najczęściej charakteryzującymi się jedynie częściowo wskazanymi podstawami w art. 6 i art. 9 RODO: brakiem należytego sprecyzowania, jaki (ewentualnie jakie) akt prawny definiuje szczegółowy zakres obowiązków administratora, komu administrator będzie przekazywał dane osobowe, jak również skonkretyzowanie okresu przechowywania danych.

Różnego rodzaju uchybienia (mniejsze lub większe) nie wywołują obecnie istotnych problemów.

3.4. Zdefiniowanie i wdrożenie procedur. Terminy rozpatrzenia żądań

Administrator zobowiązany jest do ułatwienia osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy art. 15-22

[148] Szerzej na temat przejrzystego informowania zob. K. Wygoda, *Komentarz do art. 12*, [w:] M. Sakowska-Baryła (red.), *op. cit.*, s. 202.

RODO[149], co oznacza, że każdy z administratorów musi mieć na uwadze konieczność wprowadzenia szeregu procedur, które wiązać się będą z realizacją uprawnień przez osoby, których dane przetwarzają[150]. W zasadzie zakres żądań, które mogą być kierowane do administratora, jest jeszcze szerszy. Dotyczyć on bowiem może również tych osób, które będą chciały jedynie zweryfikować, czy konkretny administrator przetwarza ich dane. Co więcej, nie można wykluczyć, że do administratora będą wpływać żądania o różnej treści i charakterze.

Cechą specyficzną jest to, że żądający w zasadzie nie musi znać przepisów RODO, aby skuteczne egzekwować gwarantowane prawa. W praktyce okazać się bowiem może, że w zasadzie każde jego wystąpienie, choćby nawet minimalnie skonkretyzowane, w sytuacji, w której dojdzie do zobowiązanego, musi zostać podjęte i prowadzone w taki sposób, aby nie można temu drugiemu zarzucić bezczynności albo, co więcej naruszenia praw wnioskodawcy. W każdym bowiem przypadku bezczynności żądający będzie uprawniony do wystąpienia do krajowego organu nadzorczego.

Dlatego pierwszym istotnym problemem będzie w wielu przypadkach prawidłowa identyfikacja treści żądania przez administratora. Biorąc pod uwagę wielość procedur dostępowych może – szczególnie w sytuacji, w której żądanie jest ogólnikowe – budzić wątpliwości, czy żądający chce realizować swoje prawa na podstawie RODO, czy też np. na podstawie ustawy o dostępie do informacji publicznej[151] (ewentualnie ustawy o ponownym wykorzystywaniu informacji sektora publicznego[152];

[149] W przypadkach, o których mowa w art. 11 ust. 2, administrator nie odmawia podjęcia działań na żądanie osoby, której dane dotyczą, pragnącej wykonać prawa przysługujące jej na mocy art. 15-22, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.

[150] O ograniczeniach zob. art. 3-5 u.o.d.o.

[151] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, t. j. Dz. U. z 2018 r. poz. 1330.

[152] Ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego, t. j. Dz. U. z 2018 r. poz. 1243.

kodeksu postępowania administracyjnego[153] – skargi lub wniosku, a nawet ustawy o petycjach[154]). Postanowienia RODO, jak również ustawy o ochronie danych osobowych, nie zawierają wzorców wniosków, które miałyby zastosowanie w zakresie realizacji praw przez uprawnionego (w tym potencjalnego uprawnionego).

Bardzo często na skrzynkę podawczą trafiają maile, z których treści wynika ogólne niezadowolenie piszącego odnoszące się do sposobu funkcjonowania adresata tego „pisma", łączące się z żądaniem „udzielenia informacji", np. o tym, co w kwestionowanym zakresie zostało przedsięwzięte w celu poprawy istniejącej sytuacji, w tym jego osoby (np. w następstwie złożenia skargi lub wystąpienia z wnioskiem). Wtedy też pojawia się konieczność ustalenia, czy wnioskodawca wystąpił z wnioskiem lub skargą w rozumieniu postanowień k.p.a., czy też chodzi mu o udostępnienie informacji publicznej, a może właśnie realizuje prawa, o których mowa w RODO.

Istotne w tym miejscu wydaje się podkreślenie, że w orzecznictwie za najczęstszy z błędów uznaje się arbitralne i samodzielne dokonanie kwalifikacji takiego pisma przez adresata (np. jako skargi rozpatrywanej w trybie k.p.a.). Zauważa się bowiem, że w takiej sytuacji konieczne jest wystąpienie przez zobowiązanego do wnioskodawcy o sprecyzowanie tego, czy jego pismo jest wnioskiem/skargą, czy też np. wnioskiem o udostępnienie informacji publicznej itd. Dopiero takie sprecyzowanie może być podstawą do dalszego procedowania. Należy przyjąć, że mechanizm ten będzie musiał dotyczyć również procedury kształtującej realizację praw na podstawie RODO, w sytuacji, w której z pierwotnej treści żądania nie można jednoznacznie ustalić, iż o taką realizację praw chodzi. Co nie mniej istotne, dopiero takie jednoznaczne sprecyzowanie

[153] Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, t. j. Dz. U. z 2017 r. poz. 1257 ze zm. (dalej: k.p.a.).

[154] Ustawa z dnia 11 lipca 2014, t. j. Dz. U. 2018 poz. 870.

może stać się wyznacznikiem rozpoczęcia biegu terminu do ewentualnego udostępnienia danych lub stosownej informacji[155].

Okazuje się przy tym, że informacją, która będzie musiała być identyfikowana jako przejrzysta, będzie informacją o braku posiadania informacji przez adresata (administratora), o którą występuje wnioskodawca. Zobowiązany nie może bowiem – nawet jeżeli żądanej informacji nie posiada – zachować milczenia i w żaden sposób nie zareagować na wniosek, który został do niego skierowany. Informując wnioskodawcę o tym, że żądanej informacji nie posiada, zawsze bowiem udziela określonej informacji, która z istoty swej jest informacją co do pewnego faktu. Co więcej, informacja taka może się różnić ze względu na okoliczności, w których jest wnioskodawcy przekazywana. W sytuacji, w której do zobowiązanego kierowane jest żądanie w oczywisty sposób niewłaściwe, wystarczy, że poinformuje on wnioskodawcę, iż informacji takiej nie posiada.

Jeżeli jednak zobowiązany nie posiada żądanej informacji, ale informację taką powinien posiadać, to sposób jego postępowania musi być już inny. W takiej bowiem sytuacji samo zawiadomienie o tym, że nie posiada żądanej informacji, nie jest wystarczające. Konieczne staje się wskazanie, z jakiego powodu (przyczyn) informacji (danych), które

[155] Zob. wyrok NSA z 17 lipca 2013 r., I OSK 642/13 – „konieczne może być wezwanie wnioskodawcy do uściślenia wniosku o udostępnienie informacji publicznej, tj. jakich konkretnie dokumentów żąda, gdyż może to mieć istotne znaczenie dla ustalenia zakresu przedmiotowego stosowania ustawy o dostępie do informacji publicznej"; podobnie: „Arbitralne zakwalifikowanie przez Ministra Transportu, Budownictwa i Gospodarki Morskiej […] pisma jako skargi w trybie przepisów rozdziału VIII K.p.a., bez uprzedniego wyjaśnienia powyższego zagadnienia (np. w drodze zapytania skarżącego, czy intencją jego pisma jest tryb skargowy przewidziany w rozdziale VIII K.p.a., czy informacja publiczna w rozumieniu ustawy o dostępie do informacji publicznej), było przedwczesne i nieprawidłowe. Błąd ten spowodował nieprawidłowy sposób załatwiania niniejszej sprawy, jednakże nie wpłynął ostatecznie na jej ostateczny wynik – fakt udzielenia przez organ odpowiedzi na pytanie, zadane w trybie ustawy o dostępie do informacji publicznej", wyrok WSA w Warszawie z dnia 25 stycznia 2013 r. II SAB/Wa 459/12; wyrok WSA w Białymstoku z dnia 23 października 2014 r., II SAB/Bk 55/14.

w związku z realizacją ustawowych zadań i kompetencji oraz prowadzonych spraw powinien posiadać (dysponować), nie posiada. Może się przy tym okazać, że brak takiego posiadania jest następstwem niewywiązania się z nałożonych na zobowiązanego przez ustawę obowiązków bądź ich nieterminowego wypełniania, bądź też innych zaniechań, które skutkować będą takim stanem rzeczy. Wtedy też najpełniej ujawniać się będzie funkcja kontrolna RODO i gwarantowanych w tym akcie praw, której celem jest nie tylko doprowadzenie do weryfikacji źródeł informacji, ale również do stwierdzenia tego, czy określona informacja (w tym przypadku dane osobowe) nie została utracona (np. zagubiono dokumenty, utracono bazy danych itd.).

Punktem wyjścia jest więc każdorazowo ustalenie przez adresata żądania tego, czy posiada wnioskowane dane osobowe (lub w określonych sytuacjach dlaczego ich nie posiada). Oczywiście w sytuacji, w której zobowiązany stwierdza, że ich nie posiada, powinien zawiadomić o tym wnioskodawcę w postaci pisma informacyjnego (czynność materialno-techniczna). Co do zasady weryfikacja stanu posiadania powinna nastąpić bez zbędnej zwłoki, co w tym przypadku powinno zasadniczo nastąpić jak najwcześniej. Wydaje się przy tym, że administratorowi trudno będzie uzasadnić każdy przypadek weryfikacji stanu posiadania jako wymagający podejmowania czynności przez okres miesiąca[156]. Oczywiście nie można wykluczyć, że adresat żądania będzie musiał dokonać weryfikacji wielu zbiorów (w tym dokumentacji papierowej). Jeżeli jednak jego działania ograniczać się będą do wykorzystania systemów teleinformatycznych i danych w nich zgromadzonych, nie można

[156] W terminie tym administrator powinien wywiązać się z obowiązku notyfikacyjnego, tzn. „[…] musi poinformować osobę, której dane dotyczą, najpóźniej w ciągu miesiąca od otrzymania żądania o:
1) powodach niepodjęcia działań;
2) prawie podmiotu danych do wniesienia skargi do organu nadzorczego;
3) możliwości skorzystania przez ten podmiot ze środków ochrony prawnej przed sądem", J. Łuczak, *op. cit.,* s. 473.

wykluczyć sytuacji, w których wnioskodawcy będą kwestionować działanie „bez zbędnej" zwłoki, w sytuacji, w której po miesiącu dowiedzą się, że zbiorach elektronicznych nie stwierdzono przetwarzania ich danych osobowych (lub potwierdzi się przetwarzanie w wąskim zakresie).

Termin miesięczny wydaje się być racjonalny w odniesieniu do sytuacji, w której do administratora będą wpływać tzw. kompleksowe żądania, tzn. obejmujące jednocześnie dostęp do informacji o przetwarzaniu; przekazanie kopii danych; ograniczenia przetwarzania; przeniesienie danych; sprzeciwu wobec przetwarzania; niepodleganie automatycznym rozstrzygnięciom indywidualny, jak również sprostowanie i usunięcia danych osobowych. Zakres i charakter czynności będzie w takim przypadku uzasadniał pełne wykorzystanie terminu 30 dni, a nawet jego przedłużenie o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. Przedłużenie terminu wymaga od administratora co najmniej uprawdopodobnienia skomplikowanego charakteru żądania oraz wykazania, że mamy do czynienia z taką liczbą żądań, która odbiega od standardu. Wtedy też uzasadnione staje się – w terminie miesiąca od otrzymania żądania – poinformowanie osoby, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy. Jeżeli administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Warto jedynie zauważyć, że do administratora będą wpływać wnioski niekompletne. Wnioskodawca może bowiem pominąć konkretyzację zakresu danych do skopiowania lub przeniesienia, nie sprecyzować

formatu danych lub technologii; pominąć nazwę i adres innego administratora; podać błędny adres lub nazwę administratora, od którego zażądał przeniesienia danych, czy wreszcie podać niekompletne dane go identyfikujące. Co więcej, w jednym żądaniu może połączyć wnioski składane na podstawie RODO, ustawy o dostępie do informacji publicznej, k.p.a. itd. Konieczne więc staje się ustalenie, czy żądanie wnioskodawcy nie podlega rozpatrzeniu na podstawie odrębnych regulacji prawnych, które kształtują odmienne zasady i tryb udostępnienia informacji – np. informacji publicznej[157] lub innych ustaw szczególnych**.** Jak wskazuje się w orzecznictwie ukształtowanym już na tle odrębnych procedur dostępowych, „Wymaga to skrupulatnego badania przedmiotu wniosku. Odrębna regulacja dotyczy bowiem tylko tego, co wyraźnie wynika z ustawy szczególnej"[158]. Każdy z tych przypadków wymaga przygotowania odpowiedniej procedury, która będzie precyzowała sposób zachowania się administratora (osób upoważnionych).

Mając powyższe na uwadze, należy dążyć do konkretyzacji wymogów, jakimi powinien legitymować się wniosek kierowany przez uprawnionego na podstawie RODO. Jeżeli przyjmiemy koncepcję daleko idącego odformalizowania, możemy doprowadzić do ukształtowania się praktyki tożsamej z tą, która do niedawna charakteryzowała realizację prawa dostępu do informacji publicznej. Stan taki był wynikiem braku normatywnie określonego wzorca (treści) wniosku o udostępnienie informacji publicznej, co doprowadziło do przyjęcia i zaakceptowania

[157] „[...] ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej […] nie jest jedynym aktem normatywnym zapewniającym realizację prawa do informacji. Pewne informacje, będące informacjami publicznymi, mogą być przedmiotem innych, szczególnych uregulowań prawnych i dlatego sposób dostępu do takich informacji będą regulować również i te inne szczególne ustawy. Taki zbieg różnych uregulowań przewidział ustawodawca w przepisie art. 1 ust. 2 tej ustawy, stanowiącym normę rozwiązującą problemy kolizyjne uregulowań zawartych w innych ustawach z omawianą ustawą" – wyrok WSA w Warszawie z dnia 19 czerwca 2007 r., II SAB/Wa 18/07.

[158] Zob. uchwałę NSA z dnia 9 grudnia 2013, I OPS 8/13, w której nastąpiło zebranie orzecznictwa w tym zakresie.

w praktyce udostępniania informacji publicznej koncepcji tzw. odformalizowanej postaci wniosku. Jej zasadniczą cechą było przyjęcie założenia, zgodnie z którym wniosek o udostępnienie informacji publicznej nie musi charakteryzować się wymogami przewidzianymi dla pism składanych na podstawie kodeksu postępowania administracyjnego. Pozwalało to na przyjęcie, że skutecznie obliguje do podjęcia działań każda postać żądania nakierowanego na uzyskania takiej informacji, w tym również wniosek elektroniczny nie opatrzony bezpiecznym podpisem. Podobne rozwiązanie w kontekście RODO nie może mieć miejsca, a więc musi wiązać się z wprowadzeniem procedury:

- identyfikacji i weryfikacji przedmiotu żądania;
- weryfikacji podmiotu występującego z punktu widzenia uznania go za podmiot legitymowany do realizacji praw, o których mowa w art. 15-22 RODO;
- odpowiedniego sprecyzowania etapów postępowania nakierowanego na merytoryczne stwierdzenie zasadności (bądź braku) realizacji uprawnień przez występującego.

Nie można przy tym wykluczyć szerszego sposobu klasyfikacji wniosków i w konsekwencji wyodrębnienie:

- wniosku konkretnego, tzn. takiego, w treści którego sprecyzowane jest żądanie, w którym wnioskodawca definiuje w sposób czytelny realizację jednego wskazanego w RODO uprawnienia. W przypadku tego wniosku z jego treści wynikać musi wprost, czego żąda uprawniony i co do zasady żądanie to ogranicza się maksymalnie do realizacji dwóch uprawnień;
- wniosku złożonego, tzn. takiego, z którego treści wynika, że żądający występuje o realizację wszystkich przysługujących mu uprawnień wskazanych w RODO. W takim przypadku dopiero merytoryczna kwalifikacja żądań poprzedza przygotowanie odpowiedzi. Wniosek podlega realizacji w zakresie dopuszczalnym ze względu na istniejące ograniczenia;

– wniosku uporczywego, tzn. wniosku pochodzącego od tej samej osoby, która w sposób powtarzalny ponawia żądania tożsame przedmiotowo ze wcześniejszymi;
– wniosku niepoważnego lub/i obraźliwego – tzn. wniosku zawierającego wyrazy lub zwroty powszechnie uznawane za wulgarne lub obelżywe albo niepoważne.

Procedura RODO-wska musi więc łączyć się z czytelnym zdefiniowaniem działań podejmowanych przez zobowiązanego (administratora), obejmując nie tylko kwestie identyfikacji odpowiedniej procedury innej niż ta związana z realizacją praw osób, których dane dotyczą, ale równolegle definiujących kolejność poszczególnych działań podejmowanych przez odpowiednio umocowane osoby, działające w imieniu administratora. Musi też łączyć się z wcześniejszym opracowaniem wzorców dokumentów, w tym wezwań do: sprecyzowania treści wniosku i wskazania właściwej procedury; wykazania, że z wnioskiem występuje osoba uprawniona (weryfikacja tożsamości wnioskodawcy); wyeliminowania braków formalnych wniosku (odpowiedniego uzupełnienia treści wniosku) – wraz ze zdefiniowaniem terminów oraz skutków niewywiązania się z nich przez wnioskodawcę (*de facto* rozstrzygnięć)[159], całego obszaru merytorycznego rozpatrzenia prawidłowo wniesionych wniosków (w odniesieniu do konkretnych i sprecyzowanych żądań – np. prawa do sprostowania danych – art. 16 RODO, jak i wniosków złożonych, tzn. obejmujących kilka lub sumę gwarantowanych uprawnień), jak również odmowy podjęcia działań, o której mowa w art. 12 ust. 5 RODO[160].

[159] Z formalnego punktu widzenia nie będzie miało więc znaczenie, czy nazwiemy je powiadomieniami, czy też decyzjami. Wnioskodawca będzie też uprawniony do kwestionowania zasadności takich wezwań.

[160] Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15-22 i 34 są wolne od opłat. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może: a) pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo

Nie budzi też wątpliwości, że zwroty, którymi w treści art. 12 RODO posłużył się ustawodawca unijny (w szczególności: skomplikowany charakter żądania; liczba żądań – ust. 3; żądanie ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter – ust. 5) muszą zostać doprecyzowywane w praktyce stosowania prawa.

4. Pobranie opłaty lub odmowa podjęcia działania przez administratora

4.1. Fakultatywny charakter opłaty

W treści RODO, jak również ustawy o ochronie danych osobowych[161] brak jest szczegółowych wskazówek, które w istotny sposób konkretyzowałyby zasady i mechanizmy kształtowania oraz pobierania opłaty, o której mowa w art. 12 ust. 5 rozporządzenia ogólnego[162].

Zasadniczo w przepisie tym wskazuje się na dwa przedmiotowe elementy składowe, które wiążąc się z działaniami administratora, mogą być brane pod uwagę z punktu widzenia pobrania opłaty, tj.:

- przekazywanie informacji, o których mowa w art. 13 i 14 RODO;
- komunikacja i działania podejmowane na podstawie art. 15-22 i 34 RODO[163].

b) odmówić podjęcia działań w związku z żądaniem. Obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

[161] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz. U. z 2018 r. poz. 1000 ze zm.

[162] Podobna sytuacja ma miejsce w odniesieniu do realizacji zadań przez krajowy organ nadzorczego, który na podstawie art. 57 ust. 4 RODO może pobrać opłatę – „Jeżeli żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, w szczególności ze względu na swą powtarzalność, organ nadzorczy może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych lub może odmówić podjęcia żądanych działań. Obowiązek wykazania, że żądanie jest w sposób oczywisty nieuzasadnione lub nadmierne, spoczywa na organie nadzorczym".

[163] Jednocześnie w pełni zgodzić należy się ze stanowiskiem, zgodnie z którym „Przekazaniu przez administratora podmiotowi danych niezbędnych informacji w przypadku bezpośredniego lub pośredniego pozyskiwania danych czy skierowaniu do niego

Modelowo potwierdza się, że zarówno przekazywanie informacji, jak i komunikacja oraz działania w zakresie wskazanym są wolne od opłat. Nie oznacza to jednak, że opłata taka nie może zostać pobrana, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter.

W praktyce więc dopiero w sytuacji, w której administrator wykaże, że konkretne żądanie jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, może, choć w dalszym ciągu nie musi, zdecydować się na pobranie stosownej opłaty. Opłata nie ma więc charakteru obligatoryjnego nawet wtedy, gdy administrator będzie w stanie wykazać, że ziszczają się przesłanki wskazane w art. 12 ust. 5 RODO. Dopuszczalność jej pobrania szczególnie w odniesieniu do administratorów w obszarze samorządu terytorialnego (a w szerszym znaczeniu do jednostek sektora finansów publicznych)[164] musi się

zawiadomienia o naruszeniu bezpieczeństwa danych nie może towarzyszyć nałożenie opłaty. Rozporządzenie nakłada w tych przypadkach na administratora powinność podejmowania określonej aktywności bez jakichkolwiek działań ze strony podmiotu danych. Może się jednak zdarzyć, że w następstwie wykonania przez administratora obowiązków o charakterze informacyjnym między nim a osobą, której dane dotyczą, dochodzi do systematycznej wymiany korespondencji, w której osoba fizyczna domaga się np. sprostowania dotyczących jej danych, mimo że taka korekta została już dokonana. Wówczas administrator może pobrać rozsądną opłatę, która uwzględnia koszty udzielania odpowiedzi na kolejne nieuzasadnione żądania podmiotu danych" – J. Łuczak, *op. cit.*, s. 474.

[164] Istotne w tym zakresie staje się odróżnienia pojęć jednostki sektora finansów publicznych od jednostki sektora finansów publicznych w rozumieniu art. 9 pkt 1-14 ustawy o finansach publicznych. Odwołując się do wypowiedzi Ministra Cyfryzacji Marka Zagórskiego: „chcę powiedzieć, że w przypadku spółek, których właścicielami są jednostki samorządu terytorialnego, one nie wchodzą w zakres ustawy o finansach publicznych, art. 9 ustawy o finansach publicznych, który jest podstawą do wyłączenia [chodzi o obowiązek powołania IOD – przyp. M.J.]. Musieliśmy przyjąć jakąś normę. Chcę powiedzieć, że to było podnoszone wielokrotnie jako pewien argument, dlaczego np. jest to rozróżnienie: szpital prywatny a szpital publiczny" – 62. posiedzenie Sejmu w dniu 9 maja 2018 r. Projekt ustawy o ochronie danych osobowych, s. 287, http://orka2.sejm.gov.pl/StenoInter8.nsf/0/21200BC57892378CC1258289000B4032/%24File/62_b_ksiazka_bis.pdf [dostęp: 10.11.2018] – można jedynie przypuszczać, że doszło do celowego – węższego zdefiniowania wyłączeń podmiotowych i konkretyzacji tej grupy jednostek sektora finansów publicznych, które mogą być ukarane karami pieniężnymi do 100 tys. złotych.

jednak wiązać ze zracjonalizowaniem ponoszonych kosztów, także w kontekście respektowania zasad dyscypliny budżetowej[165]. Między innymi choćby już z tego powodu każdy administrator (np. kierownik jednostki sektora finansów publicznych[166]) powinien być odpowiednio merytorycznie i proceduralnie przygotowany, tzn. powinien wdrożyć odpowiednie zasady i procedury, które służyć będą identyfikacji żądania jako:

- ewidentnie nieuzasadnionego i/lub nadmiernego;
- ewidentnie nieuzasadnionego i/lub nadmiernego, dla którego istotne stanie się ustalenie wielokrotnego formułowania żądań przez tego samego wnioskodawcę (zweryfikowanie ustawicznego charakteru żądań);
- ewidentnie nieuzasadnionego i/lub nadmiernego z punktu widzenia przesłanki innej niż „ustawiczny charakter".

Kolejnym krokiem jest zdefiniowanie zasad oraz mechanizmów ustalania ewentualnej i zawsze rozsądnej opłaty, i równolegle – ustalenie procedury jej pobierania w kontekście realizacji żądań pochodzących od zainteresowanego. Niezależnie od powyższego administrator powinien również przygotować się do podjęcia i uzasadnienia decyzji o odmowie podjęcia działań w związku z żądaniem.

[165] Ustawa z dnia 17 grudnia 2004 r. o odpowiedzialności za naruszenie dyscypliny finansów publicznych t. j. Dz. U. z 2017 r. poz. 1311, ze zm.

[166] Chodzi tu o: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; 2) jednostki samorządu terytorialnego oraz ich związki; 2a) związki metropolitalne; 3) jednostki budżetowe; 4) samorządowe zakłady budżetowe; 5) agencje wykonawcze; 6) instytucje gospodarki budżetowej; 7) państwowe fundusze celowe; 8) Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; 9) Narodowy Fundusz Zdrowia; 10) samodzielne publiczne zakłady opieki zdrowotnej; 11) uczelnie publiczne; 12) Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne; 13) państwowe i samorządowe instytucje kultury; 14) inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego – art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, t. j. Dz. U. z 2017 r. poz. 2077 ze zm.

Na pewno pierwszorzędnym celem analizy – istotnej z punktu widzenia zbudowania konkretnych rozwiązań szczegółowych – jest kwestia identyfikacji zwrotów niedookreślonych, którymi posłużył się ustawodawca unijny, tj. treści pojęć: „żądania ewidentnie nieuzasadnionego" oraz „żądania nadmiernego" również z punktu widzenia ich „ustawicznego charakteru", a także rozumienia tego, co znaczy „rozsądna opłata"[167]. W treści RODO, jak również w ustawie o ochronie danych osobowych nie doszło do jakiegokolwiek sprecyzowania tych zwrotów, co w konsekwencji grozi tym, że dopiero przyszła praktyka (i to z pewnością rozbudowana praktyka sądowa) doprowadzi do ukształtowania się trwałych i jednolitych rozwiązań. Nie oznacza to jednak, że już dzisiaj nie istnieje potrzeba wdrożenia odpowiednich procedur, które z punktu widzenia administratora zapewnią mu należyte przygotowanie do ustalania, a następnie pobierania opłaty lub odmowy podjęcia działań w związku z żądaniem w każdym przypadku, w którym okaże się to uzasadnione. W tym zakresie jeszcze raz podkreślić trzeba, że administrator będzie zobligowany do prawidłowej kwalifikacji samego żądania, jak i wykazania tego, że opłata przez niego ustalona jest opłatą „rozsądną". Ten ostatni wymóg oznacza, że elementy składowe pobieranej opłaty trzeba będzie sprecyzować w sposób obiektywny – różny jednak w zależności od zakresu i charakteru żądania i konkretnych okoliczności towarzyszących jego realizacji – mając na względzie, iż stanie się to prawdopodobnie przedmiotem analizy krajowego organu nadzoru, jak i w okresie późniejszym – sądów administracyjnych.

Wstępnie należy przyjąć, że każdy administrator jest uprawniony, jak i zobowiązany do dokonania oceny kierowanych do niego żądań pod kątem tego, czy w ogóle dotyczą one realizacji uprawnień wskazanych

[167] Jak się wskazuje, nie jest celem opłaty „[…] zniechęcenie osoby, której dane dotyczą, do korzystania z jej praw, ale zrekompensowanie kosztów powstałych po stronie administratora danych" – P. Litwiński, P. Barta, M. Kawecki, *Komentarz do art. 12*, [w:] P. Litwiński (red.), *op. cit.*, s. 359.

w RODO[168]. Niedookreślone, ocenne pojęcia użyte w art. 12 ust. 5 RODO niejako przekazują więc każdemu administratorowi szeroki zakres władzy dyskrecjonalnej. Nie można przy tym twierdzić, że choć administratorzy dysponują pełną swobodą decyzyjną, to muszą jednocześnie pamiętać o tym, że każde ich rozstrzygnięcie będzie musiało zostać odpowiednio uzasadnione[169], a następnie będzie najczęściej podlegało weryfikacji w ramach określonych przez przepisy prawa procedur odwoławczych, jak również sądowych[170].

[168] „Dzięki uzasadnieniu sądy powinny niejako udostępniać informację o tym, jak ujmują sens niedookreślonego pojęcia. Trybunał […], stwierdza, że ze swobodą oceny, jaką zyskuje sąd na skutek posługiwania się przez ustawodawcę zwrotami niedookreślonymi, ocennymi, powinna być związana odpowiedzialność sądu za prawidłowe stosowanie przepisu. Rzecz jasna, prawidłowość stosowania można ocenić wyłącznie na podstawie uzasadnienia, w którym powinno być przedstawione rozumowanie sądu. Uzasadnienie to powinno być weryfikowalne. Nie chodzi przy tym […] o obszerne wywody sądu stosującego przepis, lecz o zwięzłą wypowiedź" – wyrok TK z 2 października 2006 r., SK 34/06.

[169] Jak podkreśla Trybunał Konstytucyjny, „Posługiwanie się przez ustawodawcę przepisami zawierającymi zwroty niedookreślone, pojęcia generalne, wymagające wykładni, oddala normowanie prawne od standardu claritas w dwóch płaszczyznach […]. Z jednej bowiem strony oceny wymaga wymóg jasności i pewności prawa, prowadzący do określenia granic normowania in abstracto. I to jest kwestia, której ocena należy do Trybunału Konstytucyjnego. […] Z drugiej jednak strony przepisy posługujące się techniką odesłań i zwrotami ocennymi są trudniejsze do stosowania in concreto, do wyinterpretowania z ich treści normy jednostkowego zastosowania. Może zatem dojść do naruszenia chronionych konstytucyjnie dóbr (wolności, prawa) jednostki ze względu na błędy powstałe w sferze stosowania prawa, tj. odczytanie przez organ stosujący prawo przepisów, korzystających wprawdzie ze zwrotów generalnych i odesłań, jednak samych w sobie konstytucyjnych, lecz źle odczytanych, zinterpretowanych. Wszakże w tym ostatnim wypadku brak jest podstaw do wykonywania przez Trybunał Konstytucyjny funkcji kontrolnych w ramach skargi konstytucyjnej. Gdyby bowiem Trybunał, dostrzegając naruszenie konstytucyjnych praw jednostki przez błędy w stosowaniu przepisów niedookreślonych i zawierających odesłanie, zdyskwalifikował ich konstytucyjność, tylko z uwagi na sam fakt ich błędnego zastosowania – mielibyśmy do czynienia ze zbędną destrukcją systemu prawnego. Byłoby tak zwłaszcza wtedy, gdy praktyka sądowa – ujednolicana w trybie kontroli instancyjnej i nadzoru judykacyjnego – mogłaby (wykorzystana do wypracowania właściwej interpretacji) samodzielnie zagwarantować konstytucyjny standard bezpieczeństwa prawnego i zaufania do państwa i prawa." – wyrok TK z dnia 12 września 2005 r., SK 13/05.

[170] „[…] w świetle ustalonego dorobku sądów administracyjnych, wydawanie decyzji w oparciu o zwroty niedookreślone, a nawet mającej pewne cechy uznaniowości nie oznacza, po pierwsze, «dowolności» oceny. Nawet bowiem w takich warunkach na organie

4.2. Zasady i mechanizmy kształtowania opłat w ustawodawstwie unijnym i krajowym

Na charakter opłaty, o której mowa w art. 12 ust. 5 RODO, musimy spojrzeć z punktu widzenia administratora, a więc tego, kto będzie zobowiązany do podejmowania komunikacji i działań tam wskazanych. Z punktu widzenia RODO o byciu administratorem danych rozstrzyga nie forma organizacyjna podmiotu, a samodzielnie lub wspólnie z innymi ustalanie celów i sposobów 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 – art. 4 pkt 7 RODO). Oczywiste jest zatem, że administratorem w myśl RODO nie będzie wyłącznie podmiot prawa publicznego, ale również wiele innych podmiotów prawa prywatnego, w tym oczywiście przedsiębiorców, prowadzących klasyczną działalność gospodarczą. W praktyce więc bardzo trudne staje się takie skonstruowanie mechanizmu pobierania opłaty, który byłby w każdym przypadku podobny. Wręcz przeciwnie, konieczne jest uwzględnienie charakteru i specyfiki działalności podmiotu prawa (z uwzględnieniem tego, czy jest to podmiot publiczny, czy prywatny) będącego jednocześnie administratorem w rozumieniu RODO.

Niezależnie od podniesionej wyżej specyfiki działalności administratora w pełni zgodzić się trzeba ze stanowiskiem, w myśl którego „W sytuacji wystąpienia pierwotnego lub wtórnego obowiązku informacyjnego

wydającym decyzje ciąży obowiązek wskazania kryteriów, jakimi się kierował i przedstawienia swego sposobu rozumowania, co umożliwia weryfikację decyzji oraz jej ocenę na tle innych decyzji dotyczących zbliżonych kwestii; po drugie, sądy administracyjne dysponują efektywnymi instrumentami kontroli nawet uznania administracyjnego, nie wspominając o decyzjach wprawdzie formalnie nieuznaniowych, lecz zawierających szerokie marginesy ocenne; po trzecie, nawet wówczas, gdy […] pomija się uzasadnienie w decyzji doręczanej stronie, sądy administracyjne dysponują wysoce wysublimowanymi instrumentami kontroli decyzji." – wyrok TK z dnia 25 listopada 2008 r., K 5/08.

oraz prowadzenia korespondencji technicznej (formalnej) mającej na celu ustalenie tożsamości wnioskodawcy, doprecyzowanie zakresu wniosku, ustalenie realnej formy przekazania informacji itd. administrator nie dysponuje możliwością pobierania opłat”[171].

Jednocześnie warto podkreślić, że zagadnienie ustalania opłat w ustawodawstwie unijnym nie ma charakteru incydentalnego. Na przykład w treści dyrektywy w sprawie publicznego dostępu do informacji dotyczących środowiska, w motywie 18 wskazuje się na możliwość pobrania opłaty przez organy władzy publicznej za dostarczenie żądającemu informacji (informacji o środowisku). Opłata ta ma charakter fakultatywny, jeżeli jednak organ zdecyduje się ją pobrać, to „opłata taka nie powinna być wygórowana, co oznacza, że nie może ona przekraczać rzeczywistych kosztów omawianych materiałów”. Opłata taka musi więc być ustalona w oparciu o realne ceny rynkowe funkcjonujące w czasie realizacji żądania (uwzględniając ponadto: przedmiot, techniki, formaty, materiał, charakter realizującego obowiązek). Organ może pobrać też zaliczkę, „jeśli jest to konieczne, by zagwarantować ciągłość gromadzenia i publikowania takich informacji”. Jednocześnie w akcie tym wskazuje się, że „wykaz opłat powinien zostać opublikowany i udostępniony wnioskodawcom łącznie z informacjami dotyczącymi okoliczności pobierania i uchylania opłat”[172].

W art. 5 tej dyrektywy używa się już nie pojęcia „opłaty wygórowanej”, lecz „opłaty nie przekraczającej uzasadnionej kwoty” (art. 5 ust. 2 dyrektywy). Pomimo różnej treści wydaje się, że w jednym i drugim przypadku chodzi o opłatę będącą sumą realnych kosztów, które w związku z przygotowaniem i przekazaniem informacji musiał ponieść zobowiązany.

[171] K. Wygoda, *Komentarz do art. 12...*, s. 205.

[172] Dyrektywa 2003/4/WE Parlamenty Europejskiego i Rady z dnia 28 stycznia 2003 r. w sprawie publicznego dostępu do informacji dotyczących środowiska i uchylająca dyrektywę Rady 90/313/EWG.

Wiemy, że w polskim porządku prawnym implementacja tej dyrektywy ma miejsce w ustawie z dnia 3 października 2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko[173]. Jej przepisy (art. 26-28)[174], jak również postanowienia w rozporządzeniu Ministra Środowiska z dnia 12 listopada 2010 r. w sprawie opłat za udostępnianie informacji o środowisku zawierają odpowiednie normatywne regulacje prawa krajowego. Rozwiązania te definiują zarówno zasady, jak i tryb (stawki, współczynniki, sposób naliczania, terminy i sposób uiszczania) pobierania opłaty, mają więc kompletny charakter, eliminując jakiekolwiek wątpliwości dotyczące tego, kiedy i jak może taka opłata zostać pobrana i czy jej wpłacenie warunkuje udostępnienie żądanej informacji[175].

[173] T. j. Dz. U. 2018 poz. 2081.

[174] Art. 27. 1. Górne jednostkowe stawki opłat, o których mowa w art. 26 ust. 2, wynoszą: 1) za wyszukiwanie informacji – 10 zł, jeżeli wymaga wyszukiwania do dziesięciu dokumentów; opłata ulega zwiększeniu o nie więcej niż 1 zł za każdy kolejny dokument, jeżeli informacja wymaga wyszukiwania więcej niż dziesięciu dokumentów; 2) za przekształcanie informacji w formę wskazaną we wniosku – 3 zł za każdy informatyczny nośnik danych; 3) za sporządzanie kopii dokumentów lub danych w formacie 210 mm × 297 mm (A4): a) za stronę kopii czarno-białej – 0,60 zł, b) za stronę kopii kolorowej – 6 zł. 2. Za przesłanie kopii dokumentów lub danych drogą pocztową pobiera się opłatę za przesyłkę danego rodzaju i danej kategorii wagowej w wysokości podanej w obowiązującym cenniku usług powszechnych operatora wyznaczonego w rozumieniu ustawy z dnia 23 listopada 2012 r. – Prawo pocztowe (Dz. U. z 2017 r. poz. 1481 oraz z 2018 r. poz. 106, 138, 650, 1118 i 1629), zwiększoną o: 1) nie więcej niż 4 zł – za kopię dokumentów lub danych w formie wydruku lub kserokopii; 2) nie więcej niż 10 zł – za kopię dokumentów lub danych na informatycznym nośniku danych dostarczonym przez podmiot żądający informacji.

[175] Warto szczególnie zwrócić uwagę na treść „§ 5. Za przesłanie kopii dokumentów lub danych drogą pocztową pobiera się opłatę w wysokości podanej w obowiązującym cenniku usług pocztowych lub kurierskich operatora, który obsługuje władze publiczne, za przesyłkę danego rodzaju i danej kategorii wagowej, § 6. Opłaty, o których mowa w § 2-5, uiszcza się w terminie 14 dni od dnia zawiadomienia o wysokości opłaty, przez wpłatę do kasy, na rachunek bankowy właściwych władz publicznych lub przy odbiorze przesyłki. Dodatkową opłatę przy odbiorze przesyłki uiszcza również wnioskujący." nadaną rozporządzeniem Ministra Środowiska z dnia 12 grudnia 2016 r., zmieniającym rozporządzenie w sprawie opłat za udostępnianie informacji o środowisku, Dz. U. 2016, Poz. 2089; Rozporządzenie Ministra Środowiska z 12 listopada 2010 r., Dz. U. Nr 215, poz. 1415 w sprawie opłat za udostępnianie informacji o środowisku.

Nieco inaczej kwestia opłaty uregulowana zostaje na poziomie unijnym w treści dyrektywy w sprawie ponownego wykorzystywania informacji sektora publicznego. Różnica ta – przynajmniej po części – jest wynikiem szerzej określonego zobowiązanego. Jest nim bowiem „podmiot prawa publicznego", tzn. jakikolwiek organ:

„a) ustanowiony w szczególnym celu zaspokajania potrzeb w interesie ogólnym, który nie ma charakteru przemysłowego lub handlowego;
b) posiadający osobowość prawną; oraz
c) finansowany w przeważającej części przez państwo, władze regionalne lub lokalne czy też inne podmioty prawa publicznego; lub jeżeli jego zarząd podlega nadzorowi ze strony tych podmiotów; lub jeżeli ponad połowę składu jego organu administracji, zarządu lub nadzoru stanowią osoby mianowane przez państwo, władze regionalne lub lokalne lub inne podmioty prawa publicznego" (art. 2 ust. 2 dyrektywy).

Takie rozumienie zobowiązanego obejmuje więc nie tylko organy władzy publicznej *sensu stricto*, ale w szerszym zakresie podmioty administrujące, w tym oczywiście np. spółki skarbu państwa czy komunalne.

„Podmiot prawa publicznego" w rozumieniu dyrektywy (zdefiniowany wyżej jako a i b) może obliczyć i pobrać stosowną opłatę na podstawie obiektywnych, przejrzystych i sprawdzalnych kryteriów. Kryteria te mają być określone przez państwo członkowskie. Jednocześnie całkowity dochód tych organów z wydawania dokumentów i zezwalania na ich ponowne wykorzystywanie we właściwym okresie obrachunkowym nie może przekraczać kosztów gromadzenia, produkowania, reprodukowania i rozpowszechniania wraz z rozsądnym zwrotem z inwestycji. Opłaty są obliczane zgodnie z zasadami rachunkowości

obowiązującymi wobec danego organu sektora publicznego (art. 7 ust. 3 dyrektywy)[176].

Implementacja tej dyrektywy ma miejsce w treści ustawy o ponownym wykorzystywaniu informacji sektora publicznego[177].

Istota prawa do ponownego wykorzystania informacji publicznej sprowadza się do tego, że każdy zainteresowany po otrzymaniu informacji może, wykorzystując ją na dowolnym polu (polach) eksploatacji, czerpać z tego tytułu różnego rodzaju korzyści. Jak zauważa A. Piskorz-Ryń, prawo do ponownego wykorzystania informacji publicznej to „prawo do domagania się od władzy publicznej informacji publicznej w celu jej wykorzystania na różnych polach aktywności człowieka, dla wytworzenia dóbr, usług oraz produktów o charakterze komercyjnym lub niekomercyjnym"[178].

Celem ponownego wykorzystania informacji publicznej jest więc stworzenie możliwości swoistego – ponownego, innego niż pierwotny cel wytworzenia – „zagospodarowania" (komercyjnego lub niekomercyjnego albo inaczej ekonomicznego i pozaekonomicznego) informacji publicznej przez jednostkę, wspólnotę, osobę prawną lub inny podmiot (jednostkę organizacyjną). Jak podkreśla się w literaturze, „do ekonomicznych celów należy zaliczyć przede wszystkim zapewnienie wzrostu gospodarczego. […]", natomiast do pozaekonomicznych „[…] rozwój społeczeństwa informacyjnego i naukowego"[179].

[176] Wskazany w punkcie c – opłata może objąć koszty ochrony i ustalania praw.

[177] Pierwotnie miało to miejsce w drodze nowelizacji ustawy o dostępie do informacji publicznej – Ustawa z dnia 16 września 2011 r. o dostępie do informacji publicznej oraz niektórych innych ustaw, Dz. U. Nr 204, poz. 1195.

[178] A. Piskorz-Ryń, *Niewzorowy wniosek od ministra*, „IT w Administracji" 2012, nr 10(59), s. 47.

[179] B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz, *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Wrocław 2017, s. 17; por.: Ł. Cieślak, *Wspólnotowa regulacja ponownego wykorzystania informacji sektora publicznego w świetle zasady dostępu do informacji publicznej*, „CBKE e-Biuletyn" 2009, nr 2.

Obecnie obowiązująca ustawa o ponownym wykorzystywania informacji sektora publicznego[180], w art. 16-20 jedynie kierunkowo definiuje zasady i tryb pobierania opłaty, która może, ale oczywiście nie musi zostać przez zobowiązanego pobierana. Ustawodawca polski wskazuje jednocześnie, że opłata taka może zostać nałożona za ponowne wykorzystywanie, jeżeli przygotowanie lub przekazanie informacji w sposób lub w formie wskazanych we wniosku o ponowne wykorzystywanie wymaga poniesienia dodatkowych kosztów. W zakresie dodatkowych kosztów uwzględnia się koszty przygotowania lub przekazania informacji sektora publicznego w określony sposób i w określonej formie oraz inne czynniki, które będą brane pod uwagę przy rozpatrywaniu nietypowych wniosków o ponowne wykorzystywanie, mogące mieć wpływ w szczególności na koszt lub czas przygotowania lub przekazania informacji. Łączna wysokość opłaty nie może przekroczyć sumy kosztów poniesionych bezpośrednio w celu przygotowania lub przekazania informacji sektora publicznego w celu ponownego wykorzystywania w określony sposób i w określonej formie.

Formuła ta uszczegółowiana jest jedynie w odniesieniu do pobierania opłaty przez muzea państwowe i samorządowe. W rozporządzeniu w sprawie maksymalnych stawek opłat za ponowne wykorzystywanie informacji sektora publicznego nakładanych przez muzea państwowe i muzea samorządowe dochodzi bowiem do jasnego i kompletnego zdefiniowania stawek opłat nie tylko w odniesieniu do sporządzania kopii, przesyłania, ale również wyceny pracy pracownika[181].

[180] Ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego, t. j. Dz. U. z 2018 r. poz. 1243 ze zm.

[181] Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z 5 lipca 20116 r., Dz. U. 2016 r., poz. 1011. Zgodnie z treścią § 2. Maksymalne stawki opłat wynoszą w przypadku udostępniania lub przekazywania informacji:

1) za pośrednictwem systemu teleinformatycznego – 118 zł za jednorazowe udostępnienie;
2) w postaci kopii (reprodukcji) cyfrowej – 172 zł za jeden skan lub fotografię cyfrową zapisane na nośniku cyfrowym;

Analiza rozwiązań dotyczących opłat w obszarze udostępniania informacji o środowisku czy ponownego wykorzystywania informacji sektora publicznego pozwala na stwierdzenie kilku faktów istotnych z punktu widzenia kwalifikowania charakteru i składowych opłaty w rozumieniu RODO:

– nawet jeżeli zobowiązanym jest klasyczny organ prawa publicznego, opłata może być pobierana, musi mieć jednak rzeczywisty charakter, co oznacza, że konieczne staje się wykazanie, co stanowi jej element składowy;
– opłata może uwzględniać nie tylko koszt materiałów czy amortyzacji urządzeń, ale również koszt pracy pracownika niezbędnej do przygotowania i przekazania informacji, a ponadto koszt jej przesłania;
– opłata taka może być pobrana przed udostępnieniem informacji (danych).

Rozwiązań podobnych do wskazanych wyżej nie odnajdujemy ani w RODO, ani w ustawie o ochronie danych osobowych. Jak wskazywałem na to wcześniej, pominięcie to wydaje się celowe – zarówno w odniesieniu do prawodawcy unijnego, jak i krajowego. Przyjmując, że opłata ma charakter fakultatywny, w zasadzie będący wyjątkiem od zasady bezpłatności, ani na poziomie unijnym, ani krajowym nie

3) w postaci fotografii:
   a) za sztukę w formacie nie większym niż 50 x 60 cm – 168 zł,
   b) za 1 m^2 w formacie większym niż określony w lit. a – 513 zł;
4) w postaci papierowej:
   a) za jedną stronę odbitki lub wydruku kolorowego: w formacie A4 – 33 zł, w formacie A3 – 61 zł,
   b) za jedną stronę odbitki lub wydruku czarno-białego: w formacie A4 – 25 zł, w formacie A3 – 45 zł;
5) w postaci nagrania dźwięku lub obrazu na nośnik cyfrowy – 63 zł za każdą rozpoczętą godzinę nagrania;
6) w sposób lub w postaci innych niż określone w pkt 1-5 – 86 zł za każdą rozpoczętą godzinę koniecznej pracy pracownika muzeum.

podejmowano szczególnych kroków w celu zdefiniowania zasad, jak i trybu jej ustalania i pobierania. Przyjąć można, że dodatkowym argumentem wprowadzenia jedynie ogólnej formuły pozwalającej na pobranie opłaty było uwzględnienie wielości potencjalnych administratorów należących z jednej strony do kategorii podmiotów publicznych, z drugiej zaś do klasycznie prywatnych. Administratorów tych będzie – w sensie organizacyjnym, majątkowych czy każdym innym – różnić w zasadzie wszystko poza oczywiście tym, że będą jednakowo zobowiązani do poszanowania postanowień RODO. Tym ważniejsze wydaje się więc podjęcie analizy, która doprowadzi do ukształtowania – choćby pewnego rodzaju – kierunkowych przesłanek pozwalających na zdefiniowanie zasadności obliczenia i pobrania opłaty na podstawie art. 12 ust. 5 RODO.

4.3. Żądanie ewidentnie nieuzasadnione

Nie da się ukryć, że w zakresie zdefiniowania pojęcia „żądania ewidentnie nieuzasadnionego" pojawiają się istotne problemy interpretacyjne. Posługując się wykładnią językową, jesteśmy w stanie stwierdzić, że identyfikacja żądania „ewidentnie nieuzasadnionego" będzie miała miejsce wtedy, gdy jest ono w sposób oczywisty, tj. nie budzący wątpliwości (bezsprzeczny, czytelny, klarowny, obiektywnie weryfikowalny) niezasadne. Teoretycznie mogłoby to oznaczać, że żądaniem takim m.in. byłoby to, w którym na podstawie RODO (np. art. 15-22 i 34) konkretna osoba chce realizować uprawnienia zdefiniowane na gruncie odrębnych ustaw (np. realizacja prawa dostępu do informacji publicznej, petycja, ponowne wykorzystanie informacji sektora publicznego, skarga itd.). W takim jednak przypadku wadliwe wydaje się podejmowanie działań przez administratora, których efektem miałoby być pobranie opłaty na podstawie art. 12 ust. 5 RODO. Mając bowiem na względzie fakt, że administrator jest podmiotem publicznym (a szerzej jednostką sektora finansów publicznych), konieczne staje się podkreślenie, iż ani RODO, ani ustawa o ochronie danych osobowych nie zawierają w swej treści

wskazania elementów wzorcowych żądania, z którym występowałby uprawniony (bądź szerzej każdy z potencjalnie uprawnionych, co przecież podlegać będzie musiało każdorazowo weryfikacji przez administratora). Z tego też powodu jakiekolwiek działania przyjmujące postać definiowania przez administratora opłaty przed ustaleniem istoty treści żądania byłoby przedwczesne, podobnie jak działanie przybierające postać zwrotu pisma w związku z tym, iż nie spełnia ono „wymogów normatywnych"[182]. Jednocześnie można przyjąć, że przez długi czas pojawiać się będą żądania, w treści których żądający w ogóle nie będzie odwoływać się do postanowień RODO, ograniczając się do wskazania mniej lub bardziej konkretnych żądań o charakterze informacyjnym. W sytuacji, w której administrator nie jest w stanie dokonać kwalifikacji żądania (jednego lub wielu) lub powstają uzasadnione wątpliwości co do ich specyfiki, administrator nie może zastanawiać się nad pobraniem opłaty na podstawie RODO, tylko nad odpowiednim (uwalniającym od ewentualnego zarzutu arbitralności) zidentyfikowaniem trybu rozpatrzenia żądania (wniosku). Dlatego też będzie musiał przeprowadzić postępowanie wyjaśniające w zakresie, w którym każdorazowo charakter (treść) pisma wnoszonego przez konkretną osobę budzi uzasadnione wątpliwości[183]. Konsekwencją następczego zobiektywizowania przez żądającego istoty

[182] Wymogów takich po prostu nie wprowadzono. Nie ma jakiegokolwiek wzorca normatywnego żądania (wniosku) składanego na podstawie art. 12 RODO.

[183] „Organ administracji ma obowiązek prowadzenia postępowania wyjaśniającego w tym zakresie, co dotyczy takich sytuacji, w których charakter pisma wnoszonego przez strony budzi wątpliwości" – wyrok NSA z dnia 1 czerwca 2007 r., I OSK 1121/06. Podobna praktyka charakteryzuje analizę wniosku o udostępnienie informacji publicznej. Jak wskazywało się w orzecznictwie „Arbitralne zakwalifikowanie przez Ministra Transportu, Budownictwa i Gospodarki Morskiej […] pisma jako skargi w trybie przepisów rozdziału VIII K.p.a., bez uprzedniego wyjaśnienia powyższego zagadnienia (np. w drodze zapytania skarżącego, czy intencją jego pisma jest tryb skargowy przewidziany w rozdziale VIII K.p.a., czy informacja publiczna w rozumieniu ustawy o dostępie do informacji publicznej), było przedwczesne i nieprawidłowe. Błąd ten spowodował nieprawidłowy sposób załatwiania niniejszej sprawy, jednakże nie wpłynął ostatecznie na jej ostateczny wynik – fakt udzielenia przez organ odpowiedzi na pytanie, zadane w trybie ustawy o dostępie do informacji publicznej" – wyrok WSA w Warszawie z dnia 25 stycznia 2013 r., II SAB/Wa 459/12.

żądania jest więc albo stwierdzenie przez administratora, że żądanie podlega rozpatrzeniu na podstawie odrębnych przepisów (np. ustawy o dostępie do informacji publicznej itd.), albo że są to jednak odpowiednie przepisy RODO. Wniosek taki nie będzie mógł jednak w takim przypadku zostać uznany za ewidentnie nieuzasadniony. Nawet bowiem w przypadku, gdy następstwem wezwania przez administratora do sprecyzowania żądania jest milczenie żądającego, konieczne stanie się pozostawienie wniosku bez rozpoznania, a nie pobranie opłaty.

W tym zakresie widoczna stanie się specyfika tzw. administratorów publicznych, tj. jednostek sektora finansów publicznych, które zobowiązane są nie tylko do ewentualnego stwierdzenia oczywistej bezzasadności żądania, ale przede wszystkim do ustalenia istoty tego żądania i podjęcia stosownych działań, których efektem stanie się wyeliminowanie możliwości zarzucenia im arbitralności lub/i bezczynności. W tym też zakresie będą oni musieli podejmować działania zgodnie z regułą koniecznego współdziałania organu czy szerzej instytucji publicznej i osoby ubiegającej się o załatwienie określonej sprawy konkretny sposób[184]. Nie oznacza to jednak, że przesłanka żądania ewidentnie nieuzasadnionego znajdzie szersze zastosowanie w odniesieniu do administratorów niepublicznych (przedsiębiorców), bo przecież również jak w odniesieniu do podmiotów publicznych nie będą oni mogli pozostawić wpływającego do nich wniosku bez jakiejkolwiek reakcji. W przypadku żądań kierowanych do przedsiębiorców o wiele częściej konsekwencją jego merytorycznego rozpatrzenia będzie jedynie poinformowanie (pismem informacyjnym), że nie podlegają oni określonej regulacji (np. nie są zobowiązani do udostępniania informacji publicznej, rozpatrzenia petycji itd.).

[184] Por. wyrok WSA w Warszawie z dnia 14 maja 2007 r., II SAB/Wa 170/06, dotyczący uwolnienia się od zarzutu bezczynności w kontekście udostępniania informacji publicznej przez podmiot zobowiązany.

Mając na względzie powyższe, należy podjąć próbę wskazania, na czym w istocie polegać będzie prawidłowa weryfikacja żądania ewidentnie nieuzasadnionego.

W najbardziej prawdopodobnym ujęciu chodziłoby tu o sytuację, w której ta sama osoba w krótkich odstępach czasu chce realizować te same uprawnienia[185]. Jednak w takim zakresie będziemy mówili jednak o żądaniu nadmiernym, w szczególności ze względu na swój ustawiczny charakter, a nie ewidentnie nieuzasadnionym.

Inna postać żądania ewidentnie nieuzasadnionego dotyczyć będzie sytuacji, w której z treści żądania wynika, że dotyczy takiego sposobu i/lub formy realizacji prawa, wykraczającego poza klasyczne powszechnie stosowane i normatywnie zdefiniowane rozwiązania (w szczególności chodzi o formaty i nośniki).

Wreszcie, co chyba będzie najczęstszym przypadkiem, chodzić tu będzie o formułowanie żądań pozornych, tzn. takich, w których żądający, wskazując na konkretne uprawnienie (czyli powołując się na art. 15, 16, 17 itd. RODO), w rzeczywistości chce otrzymać informacje wykraczające poza ramy uprawnień wskazanych w RODO bądź formułuje takie kryteria lub sposoby generowania informacji lub formy ich przekazania, które nie są niezbędne lub możliwe do realizacji z punktu widzenia wywiązania przez administratora z obowiązków informacyjnych lub komunikacyjnych. W szczególności chodzi tu o sytuacje, w których istnieją przesłanki negatywne realizacji żądania zawarte bezpośrednio w przepisach RODO (np. art. 17 ust. 3 RODO).

[185] Jak w przeszłości stwierdził to NSA – w odniesieniu do praktyki realizacji prawa dostępu do informacji publicznej – duża liczba spraw pochodzących od jednej osoby może świadczyć o nadużyciu tego prawa, zob. wyrok NSA z dnia 13 stycznia 2016 r., I OSK 285/15. W orzecznictwie sądów administracyjnych podkreśla się, że z nadużyciem prawa mamy miejsce wtedy, gdy jego realizacja w praktyce byłaby nakierowana na realizację „celów, które są trudne do pogodzenia z założeniami całego systemu prawa, składającego się z leżących u jego fundamentów wartości i zasad aksjologicznych" – wyrok WSA we Wrocławiu z dnia 11 października 2015 r., IV SAB/Wr 295/15.

4.4. Żądanie nadmierne

Jednoznaczne zdefiniowanie przykładów żądań, które będą nadmierne, również może sprawiać pewne problemy. Pojęcie „żądania nadmiernego" jest zwrotem niedookreślonym, a jednocześnie ustawodawca unijny nie definiuje jednoznacznych kryteriów rozstrzygających o tym, jakie i ewentualnie kiedy (w jakim przedziale czasu) żądanie będzie mogło być uznane przez administratora za nadmierne. Z jednej strony świadczy to na pewno o swoistym uelastycznieniu przyszłej praktyki oceny żądań, także z punktu widzenia działań krajowego organu nadzorczego, a w późniejszym okresie sądów administracyjnych. Z drugiej jednak będzie prowadzić do powstawiania różnego rodzaju sporów interpretacyjnych.

W najprostszym ujęciu „żądanie nadmierne" to takie, które przekracza granice wynikające z uprawnień zagwarantowanych osobie w treści RODO. Wydaje się, że właśnie na płaszczyźnie identyfikacji zakresu uprawnień i sposobu ich realizacji przez osobę, której dane dotyczą, mogą w przyszłości nastręczać najwięcej problemów interpretacyjnych. Administrator będzie bowiem zmuszony do każdorazowej oceny okoliczności faktycznych i wcześniej (lub równolegle) realizowanych żądań kierowanych do niego przez tego samego uprawnionego. Dokonując oceny, administrator musi więc wziąć pod uwagę takie elementy, jak zakres i czas oddzielający kolejne wystąpienia, ich tożsamość przedmiotową oraz fakt, czy i jakie zmiany dotyczą przetwarzanych danych, a także zasadność ponownego powoływania się na te same prawa przez występującego (w odniesieniu do zmiany stan faktycznego, które zaistniały od czasu poprzedniego żądania).

Warto jednak zaznaczyć, że żądaniem nadmiernym może być oczywiście to samo żądanie powtarzane cyklicznie przez tego samego uprawnionego. Konieczne przy tym będzie wykazanie przez administratora, że wcześniejsze jego działania dotyczyły przekazania informacji tożsamych

z tymi, które otrzyma występujący. Jednak w tym przypadku będziemy mieli do czynienia z żądaniem nadmiernym ze względu na swój ustawiczny charakter[186].

4.5. Żądanie nieuzasadnione i/lub nadmierne ze względu na swój ustawiczny charakter

Łatwiejsze – przynajmniej *prima facie* – wydaje się sprecyzowanie pojęcia żądań nieuzasadnionych i nadmiernych ze względu na swój ustawiczny charakter. Ustawodawca unijny wskazał, że chodzi tu o żądania nadmierne ze względu na swój ustawiczny charakter. W praktyce więc nie będzie można mówić o żądaniu nadmiernym w przypadku pierwszej realizacji uprawnień w zakresie komunikacji i to w pełnym obszarze gwarantowanych przez RODO. Z tego też powodu dopiero kolejne wystąpienie może być kwalifikowane jako nadmierne, choć i w tym zakresie pojawia się wątpliwość dotycząca upływu czasu od realizacji poprzedniego żądania, pozwalającego administratorowi na jego identyfikację jako żądania nadmiernego.

Żądanie nadmierne będzie identyfikowane z takim, które spełniać będzie równocześnie co najmniej dwie przesłanki:

- będzie można stwierdzić, że mamy do czynienia z występowaniem tego samego uprawnionego, czyli cały czas tej samej osoby, której dane dotyczą (tożsamość podmiotowa);
- ten sam uprawniony w sposób ciągły, powtarzalny będzie występował o to samo, co uzyskał już wcześniej od administratora (tożsamość przedmiotowa).

W praktyce „żądanie nadmierne ze względu na swój ustawiczny charakter" będzie mogło być identyfikowane z pewnego rodzaju stałym

[186] Problematyczne byłoby jednak stwierdzenie, że o nadmierności żądania można mówić w sytuacji, w której z żądaniem takim występuje jednocześnie wielu uprawnionych. Niewątpliwie jednak sytuacja taka będzie miała istotny wpływ na możliwość realizacji żądań przez administratora.

i powtarzalnym procesem realizacji uprawnień na podstawie RODO przez tego samego uprawnionego.

Nie budzi jednak wątpliwości, że pewnego rodzaju problemem jest zdefiniowanie „ustawicznego" charakteru żądań. Po pierwsze, upływ określonego czasu musi być równoznaczny z brakiem możliwości identyfikacji przez administratora kolejnego wystąpienia tego samego uprawnionego z żądaniem na podstawie RODO. W tym zakresie wydaje się, że nawiązanie do wcześniejszych rozwiązań ustawy o ochronie danych osobowych z 1997 roku wydają się być zasadne w celu wskazania, że okres taki powinien być identyfikowany z upływem 6 miesięcy[187]. Z drugiej jednak strony przyszła praktyka sądowa będzie musiała znaleźć odpowiedź na pytanie, czy jednak taka kwalifikacja nie jest pod rządami RODO wadliwa w każdej sytuacji, w której ze względu na zmiany w zakresie przetwarzanych przez administratora danych nie będzie uzasadnione twierdzenie o konieczności zweryfikowania dotychczasowej wiedzy o zakresie danych przez niego przetwarzanych.

Po drugie, istotne stanie się wykazanie, że żądanie kierowane przez tego samego uprawnionego (bądź szerzej przez tą samą osobę) jest tożsame przedmiotowo. Nie można bowiem wykluczyć, że upływ nawet krótkiego czasu będzie miał wpływ na zasadność ponownego realizowania gwarantowanego przez RODO prawa. Z punktu widzenia żądającego istotne będzie bowiem uzyskanie przez niego aktualnych informacji w zakresie żądań kierowanych na podstawie RODO.

[187] Art. 32 ust. 5. Osoba zainteresowana może skorzystać z prawa do informacji, o których mowa w ust. 1 pkt 1-5 nie częściej niż raz na 6 miesięcy, Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t. j. Dz. U. z 2016 r. poz. 922 ze zm.

4.6. Żądanie ewidentnie nieuzasadnione i/lub nadmierne z punktu widzenia przesłanki innej niż „ustawiczny charakter" – koncepcja nadużycia praw

W tym właśnie obszarze konieczne staje się zwrócenie uwagi na definiowanie żądań (wniosków) jako mających na celu tzw.: „zakłócenie normalnej pracy urzędu", wniosków niepoważnych bądź obraźliwych czy też w ogóle niezgodnych z celem konkretnej regulacji. Rozwiązania takie, w szczególności w zakresie dostępu do informacji publicznej znane są ustawodawstwu Unii Europejskiej[188], jak i poszczególnych państw europejskich[189]. Choć zarówno w przypadku RODO, jak i polskiej ustawy o ochronie danych osobowych nie definiuje się wprost żądania ewidentnie nieuzasadnione lub nadmiernego, w szczególności ze względu na swój ustawiczny charakter z zakazem nadużywania praw[190], to jednak należy przyjąć, że poglądy wyrażone w literaturze przedmiotu są w tym zakresie zasadne[191]. Nie można w związku z tym wykluczyć, że konieczne będzie każdorazowe identyfikowanie treści żądania nie tylko z punktu widzenia konkretnych postanowień art. 15-22 i 34 RODO, ale również identyfikacji zakresu obowiązku informacyjnego towarzyszącego realizacji tych uprawnień oraz celu, któremu obowiązek ten służy[192]. W tym obszarze konieczne stanie się też przyjęcie i stosowanie klasycznego

[188] D. Adamski, *Prawo do informacji o działaniach władz publicznych Unii Europejskiej*, Warszawa 2011, s. 199-298 i szerokie omówienie fakultatywnych wyjątków od zasady jawności.

[189] A. Piskorz-Ryń, *Nadużywanie prawa do informacji publicznej – uwagi de lege lata i de lege ferenda*, „Kontrola Państwowa" 2008 nr 6, s. 41 i n.; M. Bernaczyk, M. Jabłoński, *Wnioskowy tryb udostępniania informacji*, „Wspólnota" – Wydanie Monografie 2007, nr 12/810, s. 16 i n. oraz wskazana tam literatura i orzecznictwo.

[190] Zob. szerzej na temat koncepcji nadużycia prawa: A. Knopkiewicz*, O nadużyciu prawa do informacji publicznej*, „Państwo i Prawo" 2004 nr 10, s. 70 i n.

[191] Zob. P. Litwiński, P. Barta, M. Kawecki, *op. cit.*, s. 358.

[192] Jak wskazywał NSA, do nadużycia prawa „dochodzi jednak w sytuacjach, gdy strona podejmuje działania prawnie dozwolone dla celów innych niż przewidziane przez ustawodawcę", wyrok NSA z dnia 31 lipca 2014 r., I OSK 9/14.; zob. też: wyrok NSA z dnia 14 lutego 2017 r., I OSK 2642/16; wyrok NSA z dnia 23 listopada 2016 r., I OSK 1601/15.

testu wartościowania, w ramach którego niezbędne będzie wykazanie przez administratora, że realizacja żądania np. zaburzy (lub może zaburzyć) równowagę między korzyściami wynikającymi z zapewnienia należytej komunikacji i realizacji uprawnień, a szeroko rozumianymi kosztami, jakie musi w tym zakresie ponieść. Ustalenia te będą podstawą do określenia takich kosztów, a w konsekwencji ustalenia wysokości należnej opłaty właśnie w sytuacji wniesienia żądania ewidentnie nieuzasadnionego lub po dodatkowej analizie odmowy podjęcia działania[193].

5. Znaczenie zwrotów niedookreślonych w praktyce definiowania przez administratora zasadności pobierania opłaty lub odmowy podjęcia działań w związku z żądaniem

Odwołanie się przez prawodawcę unijnego do pojęć „żądania ewidentnie nieuzasadnionego" oraz „żądania nadmiernego", w „szczególności ze względu na swój ustawiczny charakter", czy „rozsądnej opłaty" jest przykładem wykorzystania tzw. zwrotów niedookreślonych[194]. W literaturze przedmiotu zauważa się, że „O klauzulach generalnych w klasycznym rozumieniu tego terminu mówi się bowiem właśnie wtedy, gdy niespornie choćby zinterpretowany przepis prawny głosi, że sposób stosowania prawa w określonych wypadkach ma być uzależniony od oceny organu co do słuszności takiego czy innego rozstrzygnięcia w danej konkretnej sytuacji, czy też od odniesienia do jakiegoś zespołu

[193] W literaturze komentarzowej ma miejsce identyfikacja żądań nadmiernych z nadużyciem praw. K. Wygoda stwierdza, że „Żądania nadmierne mogą wynikać z sytuacji, w której administrator zauważy, że nie ma możliwości jego zaspokojenia bez jednoczesnego dezorganizowania funkcjonowania danego podmiotu, lub nie będą istniały przesłanki stwierdzenia, że wnioskodawca zamierza posłużyć się RODO czysto instrumentalnie, de facto nie realizując swego prawa do ochrony danych osobowych", *op. cit*., s. 206.

[194] Na temat terminologii, odróżnienie zwrotów nieostrych, nieokreślonych, klauzul generalnych zob. Z. Tobor, *W poszukiwaniu intencji prawodawcy*, Warszawa 2014, s. 189 i n.

wartości bezpośrednio niewyznaczonych w samym tekście prawnym, wartości pozaprawnych, albo szerzej – obejmuje się tym mianem również wypadki, gdy przepisy zawierają zwroty niedookreślone znaczeniowo, które w funkcjonowaniu systemu prawnego mają rolę analogiczną do roli klauzul klasycznych"[195], z jednoczesnym podniesieniem, że zwroty takie (pojęcie nieostre) powinny być, rozpatrywane, „gdy tylko jest to możliwe, z punktu widzenia praw obywatela"[196].

Odwoływanie się przez prawodawcę do zwrotów niedookreślonych nie jest zjawiskiem rzadkim. Wręcz przeciwnie, praktyka taka także na poziomie krajowym jest dość częsta. W znacznej części przypadków stosowanie tego rodzaju zwrotów znajduje uzasadnienie w złożoności sytuacji faktycznych, które objęte mają zostać wprowadzaną regulacją prawną (na gruncie prawa krajowego chodzi oczywiście o regulację ustawową). Ich różnorodność, a często specyfika uzasadnia posługiwanie się zwrotami, które pozostawią organowi (podmiotowi, w tym także przedsiębiorcy, a w omawianym zakresie – administratorowi) stosującemu prawo możliwość obiektywnego zidentyfikowania konkretnego żądania z punktu widzenia jego przedmiotu, okoliczności mu towarzyszących, jak również konsekwencji wynikających z podejmowanych działań.

Trybunał Konstytucyjny wielokrotnie podkreślał, że „[...] sfera pojęć niedookreślonych, bez względu na to, czy chodzi o niedookreślone zwroty opisowe, czy też ocenne, jest nieodłącznym elementem każdego systemu prawnego. Czyni ona system prawa bardziej elastycznym i wrażliwym na rzeczywistość. Stanowi też istotne otwarcie prawno-pozytywnych rozwiązań na poszukiwanie pełnej treści prawa. Z pojęcia niedookreślonego (nieostrego) nie wynika swoboda wykładni prawa, lecz kompetencja posługiwania się w jego stosowaniu zasadami prawa oraz ocenami pozaprawnymi. Proces interpretacji pojęć nieostrych jest elementem wykładni prawa. Zadaniem organu administracji publicznej jest

[195] W. Jakimowicz, *Publiczne prawa podmiotowe*, Kraków 2002, s. 114 i n.
[196] *Ibidem*.

w tego rodzaju sytuacjach nie tyle tworzenie prawa, co odtwarzanie treści tychże pojęć na podstawie obowiązującego prawa i z uwzględnieniem różnego rodzaju metod wykładni, zasad wnioskowania i reguł inferencyjnych”[197]. W innych wskazywał ponadto, że „Posługiwanie się przez ustawodawcę pojęciami ogólnymi – oznaczające konieczność nadawania im konkretnej treści przez organ stosujący prawo – jest nieodzowne w wypadkach, gdy stosowanie określonej instytucji prawnej oparte jest na kryteriach ocennych. Brak definicji takich pojęć spowodowany jest zazwyczaj tym, że dla dokonania konkretnych ocen brane jest pod uwagę wiele okoliczności, które różnią się w zależności od sprawy, a ujęcie ich w sposób ogólny i wyczerpujący w jednym katalogu byłoby niemożliwe. Wszelkie zaś próby w tym zakresie musiałyby prowadzić do nadmiernej kazuistyki przepisów prawa, co w istocie zaprzeczałoby ich abstrakcyjnemu charakterowi”[198].

Użycie zwrotów niedookreślonych w tekście aktu prawnego rodzi istotne konsekwencje z punktu widzenia stosowania takich postanowień. Ich dookreślenie musi bowiem nastąpić w treści uzasadnień[199] konkretnych

[197] Orzeczenie TK z dnia 8 kwietnia 1997 r., K. 14/96.

[198] Wyrok TK z dnia 16 stycznia 2006 r., SK 30/05.

[199] „Nośnikiem takiej informacji jest uzasadnienie rozstrzygnięcia (także wpadkowego), dokonane wobec osoby zainteresowanej, czy to ustnie, czy pisemnie. Sam fakt istnienia zróżnicowanej praktyki sądowej na tle zwrotu niedookreślonego nie jest świadectwem wadliwości takiego przepisu. Istnienie takiej praktyki jest bowiem wyrazem wykorzystania potencjału, jaki zawiera taki przepis, i nie jest tożsame z istnieniem jego konstytucyjnie nagannej niejasności. Nie w każdym zatem wypadku nieprecyzyjne brzmienie lub niejednoznaczna treść przepisu uzasadniają tak daleko idącą ingerencję w system prawny, jaką jest wyeliminowanie z niego tego przepisu w wyniku orzeczenia Trybunału Konstytucyjnego. Do wyjątków należą sytuacje, gdy dany przepis, zawierający zwrot niedookreślony będzie sam w sobie w takim stopniu wadliwy, że w żaden sposób, przy przyjęciu różnych metod wykładni, nie daje się interpretować w sposób racjonalny i zgodny z Konstytucją. Zdaniem Trybunału Konstytucyjnego, niejasność przepisu może uzasadniać stwierdzenie jego niezgodności z Konstytucją, o ile jest tak daleko posunięta, iż wynikających z niej rozbieżności nie da się usunąć za pomocą zwyczajnych środków mających na celu wyeliminowanie niejednolitości stosowania prawa. Pozbawienie mocy obowiązującej przepisu z powodu jego niejasności jest więc środkiem ostatecznym, stosowanym dopiero wtedy, gdy inne metody usuwania skutków niejasności treści przepisu, w szczególności przez jego

rozstrzygnięć[200]. Jak wskazuje Trybunał Konstytucyjny, „Wymaganie prawidłowego uzasadnienia rozstrzygnięcia jest niewątpliwie jednym z elementów składających się na sprawiedliwość proceduralną. […] uzasadnienie pozwala kontrolować orzeczenia, zwłaszcza wtedy gdy ich podstawą były pojęcia ocenne. Zapobiega to dowolności i arbitralności. Uzasadnienie pełni ważną rolę nawet wówczas, gdy orzeczenie nie podlega kontroli. Dzięki informacjom zawartym w uzasadnieniu uczestnicy postępowania, a także potencjalne strony przyszłych postępowań, mogą uzyskać obraz funkcjonowania pewnych mechanizmów procesowych i ocenić szanse powodzenia w konkretnej sprawie. W ten sposób realizuje się kolejny wymóg sprawiedliwości proceduralnej, a mianowicie – przewidywalność rozstrzygnięć sądowych”[201]. Co więcej, Trybunał Konstytucyjny podkreślał, że prawo do sprawiedliwej procedury sądowej „jest konstrukcyjnym elementem prawa do sądu wyrażonego przede wszystkim w art. 45 i art. 77 ust. 2 Konstytucji”[202], które łączy się z poszanowaniem zasady państwa prawnego, co konsekwencji – dla jednostki – oznacza, że ma ona prawo „[…] oczekiwać od władzy, której zachowanie się ocenia (ustawodawca, sąd), czytelności, przejrzystości, poszanowania zasad systemowych gwarantujących ochronę praw człowieka”[203]. Nie budzi przy tym wątpliwości, że zwroty niedookreślone

interpretację w orzecznictwie sądowym, okażą się niewystarczające (zob. wyrok TK z dnia 9 października 2007 r., SK 70/06, OTK ZU nr 9/A/2007, poz. 103). Sam zaś fakt praktyki zróżnicowanej na tle zwrotu niedookreślonego nie może być utożsamiany z jego „niejasnością” – wyrok TK z dnia 16 czerwca 2008 r., P 37/07.

[200] „W świetle dotychczasowego orzecznictwa Trybunału Konstytucyjnego nie ulega wątpliwości, że status ustrojowy podmiotu stosującego klauzule generalne lub zwroty niedookreślone ma kluczowe znaczenie dla oceny konstytucyjności przepisu, który ten podmiot upoważnia do ingerencji w prawa obywatelskie; por. wyrok z dnia 16 stycznia 2006 r., SK 30/05.

[201] Wyrok TK z dnia 2 października 2006 r., SK 34/06.

[202] Zob. postanowienie TK z dnia 11 kwietnia 2005 r., SK 48/04 oraz wyroki: z dnia 31 marca 2005 r., SK 26/02; z dnia 7 września 2004 r., P 4/04; z dnia 10 maja 2000 r., K 21/99.

[203] Wyrok TK z dnia 16 stycznia 2006 r., SK 30/05.

muszą być doprecyzowywane w praktyce stosowania prawa sądów[204], a wcześniej wszystkich organów i instytucji administracyjnych stosujących to prawo (rozstrzygających).

Mając powyższe na uwadze, z punktu widzenia stosowania postanowień art. 12 ust. 5 RODO oznacza to, że konkretyzacja zwrotów niedookreślonych musi nastąpić na etapie analizy konkretnego żądania, a w przypadku jego odmowy – w treści i uzasadnieniu rozstrzygnięcia. Obowiązek ten dotyczy oczywiście rozstrzygnięć podejmowanych przez administratora. Oznacza to też, że uzasadnienia takich rozstrzygnięć, które będą opierają się na identyfikacji zwrotów niedookreślonych w odniesieniu do indywidualnej sprawy (żądania), muszą zawierać stosowne zobiektywizowanie, jak również skonkretyzowanie takiego zwrotu w odniesieniu do indywidualnego żądania i sytuacji faktycznej, w ramach której nastąpić miałaby stosowna odmowa.

Nie budzi wątpliwości, że opłata ta może, ale nie musi być pobierana, a więc ma charakter fakultatywny, nawet w sytuacji wielokrotnego występowania przez tego samego uprawnionego w zakresie realizacji praw

[204] „Zasada określoności wywodzona z zasady demokratycznego państwa prawnego nie wyklucza zatem posługiwania się przez ustawodawcę zwrotami niedookreślonymi, m.in. takimi jak «oczywista bezzasadność», jeśli ich desygnaty można ustalić (zob. wyrok z 12 września 2005 r., sygn. SK 13/05, a także wyrok z 28 stycznia 2003 r., sygn. K 2/02, OTK ZU nr 1/A/2003, poz. 4). Znaczenie zwrotów niedookreślonych w konkretnej sytuacji nie może być jednak – jak to podkreśla TK – ustalane arbitralnie. Dlatego użycie zwrotu nieostrego wymaga istnienia szczególnych gwarancji proceduralnych, zapewniających przejrzystość i ocenność praktyki wypełniania nieostrego zwrotu konkretną treścią przez organ, decydujący o tym wypełnieniu. Inaczej mówiąc – jeśli odrzucić pogląd, że samo posłużenie się przez legislatora zwrotem nieostrym jest już naruszeniem wymagania jasności, ostrości i przewidywalności treści przepisów prawnych (czego wymaga art. 2 Konstytucji) – należy jednak zaaprobować argument, iż wykorzystanie przez ustawodawcę tej właśnie techniki legislacyjnej z punktu widzenia oceny konstytucyjności będzie wymagało zaostrzonych kryteriów dotyczących procedury posługiwania się zwrotami niedookreślonymi, jak np. dostępność przeprowadzonego rozumowania dla zainteresowanych dzięki jawności postępowania lub ujawnianiu motywów rozstrzygnięcia. Z tego więc punktu widzenia, skoro ustalanie treści zwrotu niedookreślonego następuje w procesie stosowania prawa, procedurze tego stosowania należy stawiać jakieś wymogi" – wyrok TK z dnia 16 stycznia 2006 r., SK 30/05.

wskazanych w RODO. W praktyce jednak brak określenia zasad obliczania oraz pobierania takiej opłaty może być dla zobowiązanego bardzo dotkliwy, w szczególności gdy chodzi o szeroko rozumianą sferę jednostek sektora finansów publicznych. Wydatkowanie środków publicznych musi się bowiem wiązać z zachowaniem dyscypliny budżetowej, a w sytuacji powtarzającej się „dużej" liczby żądań wydatki w zakresie procedur przejrzystego komunikowania się mogą przybrać spore rozmiary.

W odniesieniu do jednostek sektora finansów publicznych należy przyjąć, że opłata ta powinna być traktowana jako inna czynność z zakresu administracji publicznej. Nie można jednocześnie przyjąć modelu jak najdalej odformalizowanej postaci aktu, który definiowałby elementy i ostatecznie wysokość takiej opłaty. Mając na uwadze fakt, iż każdorazowe ustalenie i pobór opłaty wiążą się z definiowaniem przez administratora zwrotów niedookreślonych, konieczne wydaje się wydawanie rozstrzygnięcia (decyzji) ustalającego zasadność jej obliczenia oraz pobrania. Administrator musi bowiem wykazać, dlaczego opłatę taką pobiera, musi ponadto zdefiniować składowe takiej opłaty. Z tego też powodu przyszła praktyka nie może – jak ma to miejsce w przypadku opłaty pobieranej na podstawie przepisów ustawy o dostępie do informacji publicznej – przybrać postaci powiadomienia, będącego *de facto* pismem informacyjnym, a nie decyzją lub postanowieniem[205]. W treści decyzji konieczne byłoby:

[205] „Ustalenie wysokości opłaty za dostęp do informacji publicznej nie następuje w drodze postanowienia, od którego przysługuje zażalenie, lecz w drodze aktu, stwierdzającego obowiązek poniesienia opłaty oraz ustalającego jej wysokość, który kreuje zobowiązanie o charakterze finansowym. Akt ten może być określony przykładowo jako: «zarządzenie», «zawiadomienie», «wezwanie» czy «informacja», jak również może nie zawierać określenia formy i stanowić pismo skierowane do wnioskodawcy. Samo zawarcie w treści pisma informacji o wysokości opłaty za udostępnienie informacji publicznej wypełnia dyspozycję normy z art. 15 ust. 2 u.d.i.p. Przyjęta nazwa pisma nie ma jednak znaczenia, gdyż nie jest to decyzja czy postanowienie, lecz akt z zakresu administracji publicznej, o którym mowa w art. 3 § 2 pkt 4 p.p.s.a. 2. Od takich aktów nie przysługuje zażalenie, lecz wezwanie do usunięcia naruszenia prawa. Po dokonaniu takiego wezwania i bezskutecznym upływie terminu, przewidzianego do zajęcia stanowiska przez organ, bądź też po odmowie

– potwierdzenie istnienia obowiązku poniesienia przez występującego opłaty, co byłoby równoznaczne z potwierdzeniem realizacji przez zobowiązanego uprawnienia, które mu na gruncie RODO zapewniono;
– ustalenie wysokości opłaty, które zindywidualizowane stosowanie do charakteru i zakresu żądania, potwierdzałoby po stronie żądającego obowiązek jej uiszczenia;
– wskazanie terminu uiszczenia opłaty oraz skutki braku tego działania.

6. Elementy składowe opłaty

Będzie to oczywiście opłata wyrażona kwotą pieniężną o zmiennej wysokości, adekwatnej i obiektywizowanej pod kątem zakresu i charakteru żądania, a także ustalenia, w jakim stopniu żądanie jest ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, a w konsekwencji zobiektywizowania przez administratora zakresu czynności (działań) osobowych, rzeczowych i finansowych, które dodatkowo musi podjąć w celu jego realizacji[206].

Ustawodawca unijny odwołuje się do pojęcia rozsądnej opłaty. Oczywiście znowu mamy w tym przypadku do czynienia ze zwrotem niedookreślonym. Ustawodawca krajowy również nie definiuje pojęcia tzw. „rozsądnej opłaty". Nie budzi przy tym wątpliwości, że identyfikacja rozsądnej opłaty w odniesieniu do jej wysokości będzie różnorodna w zależności od tego, kto jest administratorem i czego dotyczy żądanie. Inaczej będzie ta kwestia identyfikowana w odniesieniu do jednostek sektora publicznego, inaczej w stosunku do przedsiębiorców (choćby

uwzględnienia wystosowanego wezwania, przysługuje skarga do właściwego sądu administracyjnego" – postanowienie NSA z dnia 25 października 2012 r., OSK 2359/12.

[206] Opłata ta będzie opłatą wyrażoną wielkością o wartości określonej w sposób arytmetyczny, a więc za pomocą liczb, a niekiedy także działań na liczbach.

w kontekście ustalenia równowartości kosztów osobowych). Oczywiste staje się jednak, że administrator musi wykazać w każdym przypadku, iż ustalona przez niego opłata ma charakter rozsądny z punktu widzenia kosztów, które musi ponieść w związku z realizacją żądania. Problematyczne stać się może jedynie ustalenie, co w ocenie krajowego organu nadzorczego, a potem – z całą pewnością – sądów administracyjnych zostanie uznane za rozsądną opłatę. Przyjmuję, że administrator będzie uprawniony do definiowania elementów składowych opłaty w pełnym zakresie, tzn. takim, który uwzględnia rzeczywiste koszty administracyjne przyszłej komunikacji i/lub działań. W sytuacji, w której sam ustawodawca unijny odwołuje się do pojęcia „kosztów administracyjnych". oznacza to uprawnienie administratora do uwzględnienia rzeczywistych kosztów ogólnozakładowych, tzn. również kosztów osobowych (tu pracowniczych) i rzeczowych (dodatkowo do kosztów tych zalicza się również inne składniki np. amortyzację czy podatki i opłaty)[207], których ogólna suma składać się będzie na opłatę. Uwzględnienie w ramach kosztów administracyjnych kosztów osobowych w odniesieniu do jednostek sektora finansów publicznych wymagać będzie przyjęcia określonego rodzaju kryteriów obiektywizujących. Wydaje się, że wobec braku stosownych aktów prawa krajowego definiujących zasady i procedurę ich pobierania konieczne będzie ich definiowanie w oparciu o składniki wynagrodzenia pracownika, który jest merytorycznie wyznaczony do realizacji żądań na podstawie RODO, a więc nie abstrakcyjnie ustalonych kwot, które nie będą mogły być w żadnym razie uznane za obiektywne, a tym samym rozsądne[208]. Jednocześnie, nawiązując do ustaleń dotyczących opłaty na gruncie ustawy o ponownym wykorzystywaniu

[207] Praktyka ustalania tych kosztów w odniesieniu do administratorów będących przedsiębiorcami będzie bardzo ciekawa. Analiza wysokości „rozsądnej opłaty" przez krajowy organ nadzorczy i sądy będzie niewątpliwie *pro futuro* istotnym zagadnieniem badawczym.

[208] Jak wskazuje się w literaturze komentarzowej, „W większości przypadków to właśnie ten element, a nie wartość zużytych materiałów, będzie stanowił najistotniejszy składnik opłaty" – J. Łuczak, *op. cit*., s. 475.

informacji sektora publicznego, zgodzić się trzeba, że również w tym przypadku opłata „nie może obejmować kosztów, które podmiot zobowiązany zwykle ponosi w ramach swej działalności, niezależnie od wniosku konkretnego użytkownika. Wystąpienie kosztów dodatkowych uwarunkowane jest zaistnieniem bezpośredniego związku między żądaniem wniosku a kosztem stanowiącym element opłaty, przy czym koszt ten musi być rzeczywiście poniesiony przez podmiot zobowiązany w związku z przygotowaniem lub przekazaniem informacji w sposób wskazany we wniosku”[209].

Rozsądny koszt wcale nie musi oznaczać jednak kosztu rzeczywistego. Gdyby tak miało być, ustawodawca unijny posłużyłby się pojęciem „opłaty odpowiadającej realnym, «rzeczywistym kosztom» poniesionym przez administratora w zakresie realizacji konkretnego żądania”[210]. Mając to na względzie, nie można wykluczać możliwości tworzenia przez administratora stałych mechanizmów wykorzystywanych w zakresie definiowania kosztów opłat związanych z realizacją żądań ewidentnie nieuzasadnionych lub nadmiernych, szczególnie ze względu na ustawiczny ich charakter, które będą opierać się o pewną średnią kosztów ważonych uwzględniających koszty osobowe (pracownicze), rzeczowe i finansowe (a więc koszty administracyjne). Owe „średnie ważenie” będzie wymagało od administratora ustalenie miernika opłaty w taki sposób, aby obiektywizować – w szczególności koszt pracy osoby (osób) – koszt jej poszczególnych elementów składowych, w zakresie niezbędnym do spełnienia żądania.

[209] B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz, *op. cit.*, s. 274.

[210] Jak zauważa P. Fajgielski, „Prawodawca unijny wskazuje, że wysokość opłaty powinna uwzględniać administracyjne koszty podejmowanych działań (udzielenia informacji, prowadzenia komunikacji lub podjęcia innych żądanych działań), przy czym opłata ta nie powinna być wygórowana, aby nie zniechęcała (nie uniemożliwiała) korzystania z przysługujących podmiotowi danych uprawnień, a jedynie ograniczała żądania nieuzasadnione i nadmierne”, *Komentarz do art. 12*…, s. 230. Opłata nie będzie wygórowana w sytuacji, gdy racjonalnie będzie możliwe stosowania konkretnych mierników będących jej składowymi.

7. Pobranie opłaty

W mojej ocenie administrator skutecznie może uzależnić podjęcie działań od wcześniejszego uiszczenia opłaty przez żądającego, tzn. osoby, której dane dotyczą. Przy przyjęciu takiego założenia administrator po otrzymaniu żądania powinien w terminie miesiąca rozstrzygnąć o zasadności pobrania opłaty i w terminie tym wezwać żądającego do jej uiszczenia, wskazując jednocześnie, do kiedy i w jaki sposób opłata ta ma zostać uiszczona. Po uzyskaniu potwierdzenia jej wpłaty administrator bez zbędnej zwłoki, co również oznacza, że nie później niż w terminie miesiąca od tej daty wywiązuje się z obowiązku podjęcia stosownych działań.

Założenie takie uzasadniam przez odwołanie się do prostego faktu – tzn. jeżeli administrator może odmówić podjęcia działań w związku z żądaniem, to tak samo może – oczywiście o ile jest to obiektywnie zasadne – uzależnić podjęcie takiego działania od wcześniejszego uzyskania odpowiednich środków zapewniających pokrycie kosztów związanych z jego realizacją. Co więcej, żądający po uzyskaniu rozstrzygnięcia administratora (*de facto* decyzji ustalającej wysokość opłaty) będzie mógł się skutecznie skarżyć do Prezesa Urzędu Ochrony Danych Osobowych. W skardze będzie mógł kwestionować zarówno dokonaną przez administratora identyfikację żądania z żądaniem ewidentnie nieuzasadnionym lub nadmiernym, jak również będzie mógł negować wysokość opłaty, w szczególności wskazując, że przekracza ona granice „opłaty rozsądnej". Do kompetencji krajowego organu nadzoru będzie należało zweryfikowanie zasadności działań administratora tak w odniesieniu do kwalifikacji merytorycznej żądania, jak i do ustalonej wysokości opłaty.

8. Odmowa podjęcia działania w związku z żądaniem i jej relacja z ustaleniem opłaty

W treści art. 12 ust. 5 pkt b RODO wskazuje się na uprawnienie administratora, który może odmówić podjęcia działania w związku z żądaniem, jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. W praktyce możliwe są więc trzy warianty zachowania się administratora w sytuacji, w której po weryfikacji definiuje konkretne żądanie jako ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Może on bowiem:

- pomimo stwierdzenia takiego faktu przekazywać informacje na mocy art. 13 i 14, a także prowadzić komunikację i podejmować działania na podstawie art. 15-22 i 34 RODO bez pobierania opłat lub odmowy podjęcia działania w związku z żądaniem;
- stwierdzić, że podejmie działania po wcześniejszym pobraniu odpowiedniej opłaty;
- odmówić podjęcia działań w związku z żądaniem[211].

Nie budzi wątpliwości, że w przypadku jednostek sektora publicznego (w tym oczywiście wszystkich funkcjonujących w ramach samorządu terytorialnego) odmowa podjęcia takich działań będzie musiała nastąpić w drodze merytorycznego rozstrzygnięcia (decyzji). W jej uzasadnieniu administrator musi wykazać, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, w szczególności ze względu na swój ustawiczny charakter. Tylko decyzja i jej uzasadnienie zapewnia bowiem możliwość oceny prawidłowości kwalifikacji konkretnej sytuacji faktycznej pod kątem prawidłowości działania administratora.

Podobnie jak w przypadku ustalenia zasadności pobrania opłaty administrator musi w tym zakresie wykazać, że albo żądania konkretnej osoby nie znajdują umocowania w obowiązujących przepisach

[211] Por. J. Łuczak, *op. cit*., s. 475.

(wykraczają poza zakres uprawnień), albo są nadmierne, co – gdyby przyjąć, że administrator musiałby je realizować – w praktyce mogłoby prowadzić do zakłócenia normalnego toku funkcjonowania zobowiązanego[212] czy też do ograniczenia lub uniemożliwienia prawidłowego funkcjonowania w celu wykonywania przypisanych mu zadań i kompetencji[213].

Oznacza to, że administrator będzie w ramach procesu analizy konkretnego żądania decydował o konieczności wydania jednego z dwóch odmiennych przedmiotowo rozstrzygnięć. Pierwsze z nich dotyczyć będzie ziszczenia się przesłanki pozwalającej zakwalifikować żądanie jako ewidentnie nieuzasadnione i/lub nadmierne ze względu na „ustawiczny charakter", jak również inny (np. kwalifikowane jako nadużycie prawa). Administrator mimo stwierdzenia, iż konkretna sytuacja i towarzyszące jej żądanie obiektywizuje istnienie takiej nadmierności bądź ewidentnie nieuzasadnionego żądania, musi wykazać ich istnienie i w konsekwencji stwierdzić, że podejmie stosowane działania, ale dopiero po dokonaniu przez występującego stosowanej opłaty. W praktyce administrator będzie zobowiązany do wydania rozstrzygnięcia, które w swej treści będzie zawierało trzy elementy składowe. Po pierwsze będzie musiał wykazać, że żądanie jest ewidentnie nieuzasadnione i/lub nadmierne, po drugie będzie musiał wskazać, jaką opłatę będzie w związku z tym chciał pobrać, a więc musi wskazać elementy składowe takiej opłaty, które uzasadnią przysługujące mu prawa do jej pobrania. Wreszcie po trzecie będzie musiał wskazać występującemu, w jakiej wysokości (jakie są elementy składowe pod kątem oceny, czy ustalona opłata jest rozsądna) i w jakim terminie (wskazując jednocześnie sposób) opłata ta ma zostać uiszczona. Pierwsza część takiego rozstrzygnięcia będzie *de facto* rozstrzygnięciem odmownym, w tej części, identyfikując żądanie

[212] Kwalifikacja taka dotyczyła praktyki udostępnienia informacji publicznej, zob.: wyrok NSA z dnia 12 czerwca 2014 r., I OSK 2721/13.

[213] Kwalifikacja taka dotyczyła praktyki udostępnienia informacji publicznej zob.: wyrok NSA z dnia 27 lutego 2014 r., I OSK 1769/13.

jako ewidentnie nieuzasadnione i/lub nadmierne, administrator musi wykazać, że działając na podstawie przepisów prawa, jest uprawniony do ustalenia, a następnie uzależnienia podjęcia działania od wcześniejszego uiszczenia opłaty przez żądającego[214].

O wiele prostsza jest w związku z tym sytuacja, w której administrator ogranicza się do odmowy podjęcia żądanych działań.

W takim bowiem przypadku będziemy mieli do czynienia z rozstrzygnięciem (decyzją), w którym wykazać będzie musiał jedynie, że konkretne żądanie jest ewidentnie nieuzasadnione i/lub nadmierne. Odmawiając tylko z tego powodu, nie musi odnosić się do kwestii definiowania wysokości opłaty, o której mowa w art. 12 ust. 5 RODO[215].

Różnica ta staje się jednak widoczna w dalszym etapie postępowania. Mając na względzie rozwiązania RODO, trzeba przyjąć, że żądający będzie (często) w takim przypadku odwoływał się do krajowego organu nadzoru, czyli Prezesa Urzędu Ochrony Danych Osobowych. Należy też przypuszczać, że kierując się wyłącznie przesłanką swoistej racjonalności w zakresie konieczności merytorycznego uzasadnienia decyzji, administratorowi nie będzie zależeć na dodatkowym uzasadnianiu, dlaczego chce pobrać opłatę w sytuacji, w której wystarczy, że uzasadni podstawy odmowy podjęcia działania.

9. Opłata za kopię danych jako opłata odrębna

Błędem byłaby identyfikacja opłaty pobieranej na podstawie art. 12 ust. 5 RODO z opłatą wskazaną w art. 15 ust. 3 RODO. Zgodnie z jego

[214] Brak klarownego i kompletnego uzasadnienia w sytuacji stosowania prawa w granicach zwrotów niedookreślonych będzie przesłanką wskazującą na wadliwość takiego aktu stosowania prawa.

[215] Warto w tym zakresie przypomnieć, że każde uzasadnienie decyzji o odmowie powinno być jak „[…] garnitur uszyty na miarę, a nie jak garnitur pierwszy lepszy zdjęty w sklepie z wieszaka, który może kupić każdy klient i będzie jakoś pasował" – wyrok NSA z dnia 28 kwietnia 2005 r., I OSK 1468/04.

treścią za drugą i (ewentualnie) kolejne kopie danych dostarczone osobie, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

Również i ta opłata ma charakter fakultatywny, co oznacza, że administrator – nawet, gdy żądanie jest powtarzane przez tę samą osobę – opłaty tej nie musi pobierać. W razie jej pobierania musi znowu dojść do zdefiniowania zasad i procedury jej pobierania. Administrator będzie w tym zakresie zobowiązany do wykazania, że opłata ta ma charakter „rozsądny" w takim samym znaczeniu jak przy okazji obliczania opłaty na podstawie art. 12 ust. 5 lit. b RODO. Zasadność opłaty, jak również jej wysokość może być kwestionowana przez żądającego przez wystąpienie ze skargą do Prezesa Urzędu Ochrony Danych Osobowych.

10. Problemy interpretacyjne

Brak jakichkolwiek konkretyzacji ustawowych może w przyszłości rodzić różnego rodzaju problemy.

Po pierwsze, mogą pojawiać się zarzuty, w których kwestionować się będzie zasadność pobierania opłaty, powołując na zasadę legalizmu, zasadę wyłączności ustawowej, jak również na sprzeczność treścią art. 217 Konstytucji RP, szczególnie wtedy, gdy administratorzy należący do jednostek sektora finansów publicznych tworzyć będą stałe cenniki konkretyzujące wysokość opłat. Argumentacja opierać się będzie również na podkreśleniu, iż taka opłata nie będzie miała charakteru opłaty incydentalnej, ale stałej wynikającej z ustalenia kosztów ryczałtowych.

Po drugie, RODO ani ustawa o ochronie danych osobowych nie uwzględnia konsekwencji zmiany żądania lub jego wycofania przez

osobę, której dane dotyczą po wytworzeniu informacji i/lub podjęciu działań przez administratora.

Po trzecie brak jest czytelnego rozwiązania w zakresie zdefiniowania procedury towarzyszącej pobieraniu opłaty z jednoczesnym określeniem zależności terminów determinujących działania administratora i żądającego. Jednocześnie to właśnie praktyka będzie musiała udzielić odpowiedzi na pytanie, czy administrator może uzależnić podjęcie stosownych działań od wcześniejszego uiszczenia opłaty przez żądającego, działającego na podstawie RODO.

Mając na względzie charakter działań, które musi podjąć administrator w celu realizacji żądań osoby, której dane dotyczą, milczenie ustawodawcy w zakresie ukształtowania zasad i trybu pobierania opłaty za wytworzenie takiej informacji jest więc istotnym mankamentem, prowadzącym do powstawania różnego rodzaju sporów interpretacyjnych.

Bibliografia

Adamski D., *Prawo do informacji o działaniach władz publicznych Unii Europejskiej*, Warszawa 2011

Anisimowicz J., *Akredytacja dla podmiotów certyfikujących oraz przebieg procesu certyfikacji*, „ABI Expert" 2017, nr 4

Barta P., *Prawnie uzasadniony interes w działalności marketingowej*, „ABI Expert" 2018, nr 3

Barta P., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, wyd. 4, Warszawa 2007

Barta P, Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, wyd. 4, Warszawa 2016

Bernaczyk M., Jabłoński M., *Wnioskowy tryb udostępniania informacji*, „Wspólnota" – Wydanie Monografie 2017, nr 12/810

Bielak-Jomaa E., *Komentarz do art. 38*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, Lex

Blicharz J., *Kategoria interesu publicznego jako przedmiot działania administracji*, Acta Universitatis Wratislaviensis no 2642, „Przegląd Prawa i Administracji" 2004, nr LX

Błaś A., *Działania administracji publicznej*, [w:] J. Boć (red.), *Administracja publiczna*, Wrocław 2003

Bury B., *Podporządkowanie pracownika pracodawcy*, „Państwo i Prawo" 2006, nr 9

Byrski J., *Umowne powierzenie do przetwarzania danych osobowych w ustawie o ochronie danych osobowych, dyrektywie 95/46/WE i w ogólnym rozporządzeniu o ochronie danych*, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016

Cieślak Ł., *Wspólnotowa regulacja ponownego wykorzystania informacji sektora publicznego w świetle zasady dostępu do informacji publicznej*, „CBKE e-Biuletyn" 2009, nr 2

Cygan T., *Zabezpieczenie danych według RODO*, „ABI Expert" 2017, nr 3(4)

Czachórski W., *Zobowiązania. Zarys wykładu*, Warszawa 1999

Czerniawski M., *Nowe procedury ochrony*, „ABI Expert" 2016, nr 1

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*. Warszawa 2005

Drozd A., *Zabezpieczenie danych osobowych,* Wrocław 2008

Fajgielski P., *Komentarz do art. 4 uwaga 31*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Fajgielski P., *Komentarz do art. 12 RODO*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Fajgielski P., *Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018

Fischer B., Piskorz-Ryń A. (red.), Sakowska-Baryła M., Wyporska-Frankiewicz J., *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Wrocław 2017

Gawroński M. (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018

Gumularz M, *Ochrona danych osobowych w sektorze publicznym,* Warszawa 2018

Gumularz M., *Uzasadniony interes w sektorze publicznym – na przykładzie monitoringu*, „ABI Expert" 2018, nr 2

Gumularz M., Kozieł K., Kozik P. (red.), *Ustawa o ochronie danych osobowych. Przepisy wdrażające Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). Komentarz*, Warszawa 2018

Izydorczyk T., *Działania organizacyjne*, „ABI Expert" 2017, nr 4

Jabłoński M., Flaga-Gieruszyńska K., Wygoda K. (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017

Jabłoński M., Kronobis-Romanowska D., Wygoda K., *Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym*, Wrocław 2017

Jabłoński M., Węgrzyn J., *Zmiana modelu ochrony danych osobowych – podejście oparte na ryzyku, privacy by design i privacy by default,* [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017

Jakimowicz W., *Publiczne prawa podmiotowe*, Kraków 2002

Jakimowicz W., *Wykładnia w prawie administracyjnym*, Kraków 2006

Jendrośka J., *Milczenie administracji w postępowaniu administracyjnym*, „Annales Universitatis Mariae Curie-Skłodowska. Sectio G. Ius" 1993, vol. XL

Kaczmarek-Templin B., *Podstawy legalizacyjne przetwarzania danych osobowych w ogólnym rozporządzeniu o ochronie danych – wybrane zagadnienia*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *Polska i europejska reforma ochrony danych osobowych,* Warszawa 2016

Kawecki K., *Reforma danych osobowych. Współpraca administracyjna w świetle ogólnego rozporządzenia o ochronie danych osobowych*, Warszawa 2017

Kiczka K., *Krajowy organ administracji publicznej w prawie unijnym*, Wrocław 2013

Klimas D., Wróbel P., *Cywilnoprawna odpowiedzialność za naruszenie ochrony danych osobowych na gruncie RODO – wstęp do zagadnienia*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017

Knopkiewicz A*., O nadużyciu prawa do informacji publicznej*, „Państwo i Prawo" 2004, nr 10

Krasuski A., *Ochrona danych osobowych na podstawie RODO*, Warszawa 2018

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014

Krzysztofek M., *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016

Krzysztofek M., *Warunki dopuszczalności powierzenia – lista kontrolna*, „ABI Expert" 2017, nr 4

Litwiński P., *Wyznaczenie jednego IOD przez grupę podmiotów,* „ABI EXPERT" 2017, nr 2

Litwiński P. (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018

Litwiński P. (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018

Litwiński P., Barta P., Kawecki M., *Komentarz do art. 4 pkt 7, uwaga 92*, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018

Litwiński P., Barta P., Kawecki M., *Komentarz do art. 4 pkt 7, uwaga 96*, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018

Litwiński P., Barta P., Kawecki M., *Komentarz do art. 12*, [w:] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, Warszawa 2018

Łaszczyca G., *Milczenie organu w świetle kodeksu postępowania administracyjnego*, „Państwo i Prawo" 1999, nr 1

Łuczak J., *Komentarz do art. 12 RODO,* [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018

Masternak M., *Kontrola czynności materialno-technicznych administracji publicznej przez sąd administracyjny*, [w:] Z. Niewiadomski, Z. Cieślak (red.), *Prawo do dobrej administracji. Materiały ze Zjazdu Katedr Prawa i Postępowania Administracyjnego. Warszawa-Dębe 23-25 września 2002 r.*, Warszawa 2003

Mik C., *Zasady ustrojowe prawa wspólnotowego a polski porządek konstytucyjny*, „Państwo i Prawo" 1998, nr 1

Ministerstwo Cyfryzacji, *RODO. Poradnik dla sektora Fintech*, Warszawa 2018

Nerka A., *Komentarz do art. 37*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych*, Warszawa 2018

Nerka A., Sakowska-Baryła M., *Komentarz do art. 6*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Osiej T., *Mechanizmy certyfikacji, znaki jakości i oznaczenia w zakresie ochrony danych w świetle przepisów ogólnego rozporządzenia o ochronie danych,* [w:] M. Kawecki, T. Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017

Piskorz-Ryń A., *Nadużywanie prawa do informacji publicznej – uwagi de lege lata i de lege ferenda*, „Kontrola Państwowa" 2008, nr 6

Piskorz-Ryń A., *Niewzorowy wniosek od ministra*, „IT w Administracji" 2012, nr 10(59)

Radwański Z., *Prawo cywilne – część ogólna*, Warszawa 2007

Sakowska-Baryła M., *Dostęp do informacji publicznej a ochrona danych osobowych,* Wrocław 2014

Sakowska-Baryła M., *Komentarz do art. 4 pkt 7 i 8, art. 26 i art. 28*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Komentarz do art. 4 pkt 8*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Komentarz do art. 4 pkt 8, uwaga 86 i 87*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Komentarz do art. 28, uwaga 2*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Komentarz do art. 28, uwaga 11*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Komentarz do art. 28, uwaga 28*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Komentarz do art. 38*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Komentarz do art. 39*, [w:] M. Sakowska-Baryła (red.),*Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Sakowska-Baryła M., *Obowiązek wyznaczenia IOD w podmiotach publicznych*, „ABI Expert" 2017, nr 2

Sakowska-Baryła M., *Organizacja ochrony danych osobowych w ramach wspólnej obsługi w centrum usług wspólnych,* [w:] M. Sakowska-Baryła, M. Górski (red.), *Samorządowe centra usług wspólnych*, Warszawa 2017

Sakowska-Baryła M., *Powierzenie przetwarzania danych osobowych w sektorze publicznym*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław, 2017

Sakowska-Baryła M., *Prawo do ochrony danych osobowych,* Wrocław 2015

Sitniewski P., *Zasady nieudzielania informacji publicznych*, „Zeszyty Naukowe Wyższej Szkoły Administracji Publicznej w Białymstoku, Administracja Publiczna. Studia krajowe i międzynarodowe" 2006, t. 1/7

Szymielewicz K., *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony*?, [w:] G. Sibiga (red.), *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, Warszawa 2016

Tobor Z., *W poszukiwaniu intencji prawodawcy*, Warszawa 2014

Więckowska M., *Prawnie uzasadniony interes – test badania równowagi*, „ABI Expert" 2018, nr 3

Więckowska M., *Przetwarzanie danych na podstawie prawnie uzasadnionego interesu*, „ABI Expert" 2018, nr 3

Witkowska-Nowakowska K., *Komentarz do art. 28, uwaga 16*, [w:] E. Bielak-Jomaa, D. Lubasz (red. nauk.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018

Witkowski Z., Galster J., *Kompendium wiedzy o Unii Europejskiej z uwzględnieniem Traktatu Amsterdamskiego i Traktatu z Nicei,* Toruń 2002

Wójcik-Prządka K., *Sądy Powszechne a rodo*, „ABI Expert" 2018, nr 2

Wójtowicz K., *Istota i źródła prawa wspólnotowego konsekwencje dla prawa krajowego*, [w:] M. Kruk (red.), *Prawo międzynarodowe i wspólnotowe w wewnętrznym porządku prawnym*, Warszawa 1997

Wygoda K.*, Czy potrzebne są umowy powierzenia przetwarzania?*, „ABI Expert" 2018, nr 3

Wygoda K., *Komentarz do art. 4 pkt 2*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Wygoda K., *Komentarz do art. 12*, [w:] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018

Wygoda K., *Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych w oparciu o art. 6 RODO a działania podmiotów sektora publicznego*, [w:] M. Jabłoński, K. Flaga-Gieruszyńska, Wygoda K. (red.), *Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej – aspekty proceduralne*, Wrocław 2017

Zięba Ł., *Budowanie profili osobowych a wymogi wynikające z nowych przepisów o ochronie danych osobowych*, [w:] M. Kawecki, T. Osiej (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, Warszawa 2017

Żak J., *Koncepcja „prawa do bycia zapomnianym"*, [w:] M. Jabłoński, S. Jarosz-Żukowska (red.), *Aktualne wyzwania ochrony wolności i praw jednostki. Prace uczniów i współpracowników dedykowane Profesorowi Bogusławowi Banaszakowi*, Wrocław 2014.

„Monografia zawiera propozycje wstępnych rozwiązań, zwłaszcza istotnych w systemie przejściowym, przy nie zawsze do końca skonkretyzowanych elementach składowych systemu. Uwzględnia ona rozwiązania praktyczne i racjonalne, tak z punktu widzenia administratora, jak i osoby, której dane dotyczą. Monografia obejmuje więc istotne problemy związane z tematyką ochrony danych osobowych. Zawiera określone propozycje co do interpretacji postanowień RODO i ustawy o ochronie danych osobowych, co pozwoli uniknąć pojawiających się w praktyce rozbieżności w tym zakresie. Ułatwi też rozwiązywanie problemów organizacyjnych i proceduralnych w systemie ochrony danych osobowych".

Z recenzji wydawniczej prof. zw. dr. hab. Andrzeja Szmyta

ISBN 978-83-65653-41-3 (druk)
ISBN 978-83-65653-42-0 (online)