Uniwersytet w Białymstoku

Wydział Prawa

Marta Czech

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH JAKO INSTRUMENT ICH OCHRONY

Rozprawa doktorska
napisana pod kierunkiem
Prof. dr hab. Teresy Mróz

Białystok 2019

SPIS TREŚCI

WYKAZ SKRÓTÓW

Akty prawne:

RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych, Dz. Urz. UE.L 2016 Nr 119, str. 1 ze zm.;

Dyrektywa 95/46/WE - Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz.UE.L 2000 Nr 178, str. 1 ze zm.;

Dyrektywa 2000/31/WE - Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz.Urz.UE.L 2000 Nr 178, str. 1 ze zm.;

Konwencja 108 - Konwencja Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r., Dz.U. 2003 Nr 3, poz. 25 ze zm.;

Karta - Karta Praw Podstawowych Unii Europejskiej, Dz.Urz.UE.C 2010 Nr 83, str. 389;

Konstytucja RP - Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U. 1997 Nr 78, poz. 483);

UODO z 1997 r. - ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2016 r. poz. 922 ze zm.);

UODO z 2018 r.- ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2018 r. poz. 1000 ze zm.);

KC - ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz.U. z 2018 r. poz. 1025, ze zm.);

DziałUbezpReasU - Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (t.j. Dz.U. z 2018 r. poz. 999 ze zm.);

UsługiElektrU - Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2019 r. poz. 123 ze zm.)

Rozporządzenie ZTP - Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 roku w sprawie „Zasad techniki prawodawczej", (t.j. Dz. U. 2016, poz. 283 ze zm.),

Rozporządzenie PKD - Rozporządzenie Rady Ministrów w sprawie Polskiej Klasyfikacji Działalności z dnia 24 grudnia 2007 r. (Dz.U. 2007, Nr 251, poz. 1885 ze zm.);

Czasopisma:

OSNC – Orzecznictwo Sądu Najwyższego Izba Cywilna

OTK – Orzecznictwo Trybunału Konstytucyjnego

Organy:

SN – Sąd Najwyższy

TK – Trybunał Konstytucyjny

NSA – Naczelny Sąd Administracyjny

SA – Sąd Apelacyjny

WSA – Wojewódzki Sąd Administracyjny

GIODO – Generalny Inspektor Ochrony Danych Osobowych

PUODO – Prezes Urzędu Ochrony Danych Osobowych

UKNF – Urząd Komisji Nadzoru Finansowego

Grupa Robocza - Grupa Robocza ds. ochrony danych powołana na mocy art. 29 Dyrektywy 95/46/WE (niezależny europejski organ doradczy w zakresie ochrony danych i prywatności), zastąpiona Europejską Radą Ochrony Danych

Inne:

LEX – System Informacji Prawnej LEX

Legalis – System Informacji Prawnej Legalis

WSTĘP

Umowa powierzenia przetwarzania danych osobowych jest instrumentem prawa prywatnego, wyraźnie powiązanym z prawem publicznym, służącym ochronie szczególnego dobra, jakim są informacje dotyczące osób fizycznych, kwalifikowane jako dane osobowe. Ma ona już swoją historię w obrocie prawnym, jednakże dopiero z chwilą rozpoczęcia bezpośredniego stosowania przepisów 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[1], wyraźnie zaczęła nabierać doniosłości praktycznej. W dużej mierze stało się tak dzięki uszczegółowieniu jej regulacji oraz określeniu zasad ponoszenia odpowiedzialności na gruncie prawa prywatnego i publicznego. Umowa powierzenia przetwarzania danych osobowych kształtuje relacje między uczestnikami procesów przetwarzania danych osobowych (administratorem, podmiotem przetwarzającym i podmiotem podprzetwarzającym), mając jednocześnie wpływ na sferę praw[2] osób, których dane dotyczą (podmiotów danych).

Należy podkreślić, że umowa powierzenia nie ma charakteru samodzielnego – jest związana z innym stosunkiem prawnym (umowa zasadnicza), w ramach którego dochodzi do sytuacji, gdy administrator danych powierza zewnętrznemu podmiotowi przetwarzanie danych osobowych w jego imieniu i na jego polecenie. Umowa powierzenia przetwarzania danych osobowych ma zatem charakter akcesoryjny wobec zasadniczej (podstawowej) umowy łączącej oba wskazane podmioty. Dodatkowo może powstać tzw. „łańcuch powierzeń", w sytuacji, gdy podmiot przetwarzający korzysta z usług „podwykonawców" (podmioty podprzetwarzające) przy przetwarzaniu danych powierzonych przez administratora. Wykorzystywanie tego instrumentu prawnego wynika z obowiązku nałożonego przepisami RODO zarówno na podmioty sektora prywatnego, jak i publicznego, których działalność obejmuje przetwarzanie danych osobowych. Umowa powierzenia przetwarzania danych osobowych dotyczy zarówno interesu prywatnego, którym jest zapewnienie gwarancji prawa do ochrony danych osobowych jako sfery prawa do prywatności, jak również interesu publicznego, jakim jest zagwarantowanie szeroko rozumianego bezpieczeństwa informacji oraz pewności obrotu.

[1] Ogólne rozporządzenie o ochronie danych, Dz. Urz. UE.L 2016 Nr 119, str. 1 ze zm.; dalej powoływane jako RODO).

[2] Sformułowanie "prawa osoby, której dane dotyczą" wynika z RODO - tak jest zatytułowany rozdział III RODO (w polskiej wersji językowej).

W dotychczasowym dorobku nauki prawa nie ma kompleksowego opracowania o charakterze monografii, dotyczącego umowy powierzenia przetwarzania danych osobowych. W publikacjach naukowych z zakresu ochrony danych osobowych jest ona uwzględniana jedynie jako jedno z wielu zagadnień szczegółowych. Autorzy poprzestają zwykle na generalnym omówieniu istotnych elementów tej umowy, oznaczeniu stron oraz wymienieniu ich obowiązków. Warto podkreślić, że nikt do tej pory nie zajął się kompleksową analizą umowy powierzenia przetwarzania danych osobowych na gruncie nauki prawa. Kwestia umowy powierzenia, jako jednego z narzędzi ochrony danych osobowych, dostrzegana jest obecnie przede wszystkim w kontekście rozwoju nowoczesnych technologii, intensyfikacji prawnej ochrony danych osobowych oraz wzrostu świadomości co do doniosłości danych osobowych.

Do wyboru tematu rozprawy skłoniła przede wszystkim zapowiedziana w 2016 roku znacząca zmiana w prawie, związana z przyjęciem przez Unię Europejską nowych przepisów RODO, co do których bezpośrednie stosowanie ustanowiono na dzień 25 maja 2018 roku[3]. W tym dwuletnim okresie na gruncie praktyki coraz wyraźniej kształtowały się potrzeby podmiotów sektora prywatnego i publicznego związane z dostosowywaniem ich działań, wewnętrznych procedur, relacji z innymi podmiotami, do wymogów RODO. Okazało się, że zawieranie lub aneksowanie umów powierzenia przetwarzania danych osobowych jest jednym z najczęstszych problemów zgłaszanych przede wszystkim przez przedsiębiorców, ale też inne podmioty prawa. Dlatego należy uznać, że istnieje uzasadniona potrzeba zbadania zagadnienia objętego tematem dysertacji. Ponadto można wyrazić przekonanie, że poczynione tu ustalenia dotyczące umowy powierzenia przetwarzania danych osobowych mogą stać się inspiracją do dalszych badań naukowych, a także posiadają walory praktyczne, są więc potrzebne i ważne z perspektywy nauki i praktyki.

Badania zostały ograniczone do prawa Unii Europejskiej. Poza obszarem badawczym pozostała problematyka międzynarodowych transferów danych (tzn. przepływów danych do państw trzecich, czyli krajów nienależących do Unii Europejskiej i Europejskiego Obszaru Gospodarczego), związanych z działalnością nieobjętą zakresem

[3] Od 2012 roku trwały prace legislacyjne nad nowym aktem prawnym i w 2016 roku uchwalono Rozporządzenie 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. RODO weszło w życie w dniu 25 maja 2016 roku, jednakże rozpoczęło bezpośrednie stosowanie dopiero od 25 maja 2018 roku.

prawa Unii, gdzie przepisy RODO nie mają zastosowania. Z obszaru rozważań należało również wyłączyć zagadnienie tzw. standardowych klauzul umownych (art. 28 ust. 7-8 RODO), które nie zostały określone przez Komisję Europejską do dnia zakończenia prac nad rozprawą.

Podstawową hipotezę badawczą można zawrzeć w twierdzeniu, że umowa powierzenia przetwarzania danych osobowych jest ważnym i adekwatnym do współczesnych potrzeb instrumentem ochrony danych osobowych, który ma gwarantować ochronę interesów zarówno podmiotów, które uczestniczą w procesie przetwarzania danych, jak i osób, których dane dotyczą. Jednocześnie sformułować można kilka hipotez pomocniczych, które stanowią przedmiot rozważań poszczególnych rozdziałów dysertacji. Dane osobowe, jako kategoria informacji, są szczególnym rodzajem dóbr chronionych prawnie, wobec których niekiedy trudno jest nadążyć z gwarantowaniem skutecznej ich ochrony. Należy przyjąć, że obecnie w praktyce prywatnoprawna ochrona danych osobowych ma znaczenie kluczowe, a na tym obszarze umowa powierzenia przetwarzania danych osobowych jest istotnym instrumentem i gwarantem tej ochrony.

Przepisy prawa regulujące umowę powierzenia przetwarzania danych osobowych są skonstruowane tak, aby przetwarzanie danych uwzględniało ustanowione przez prawodawcę zasady przetwarzania danych osobowych, ale regulacje umowne pełnią rolę doprecyzowującą przepisy. Specyfika umowy powierzenia przetwarzania danych osobowych, w tym jej akcesoryjny charakter, nie pozwalają na jednoznaczne umiejscowienie jej w klasycznych systematyzacjach umów, co może wskazywać na niejednolity charakter prawny umów tego typu. Ponadto jej znaczenie prawne, ekonomiczne i społeczne jest szczególne z uwagi na wielość i różnorodność funkcji, jakie może pełnić ta umowa.

Pierwszy rozdział dysertacji dotyczy kwestii terminologicznych o znaczeniu priorytetowym dla ochrony danych osobowych. Punktem wyjścia jest pojęcie informacji. Informacja w ujęciu ogólnym nie została w prawie zdefiniowana, dlatego wymaga analizy już na samym wstępie rozprawy. Staje się ona coraz bardziej wartościowym dobrem, a głównie z uwagi na tempo postępu technologicznego, jest ona dobrem coraz bardziej zagrożonym i wymagającym ochrony. Można powiedzieć, że aktualnie informacja jest przedmiotem ochrony prawa prywatnego i publicznego, jednakże nie jest wskazywana pośród tradycyjnie wymienianych przedmiotów stosunku cywilnoprawnego – rzeczy, praw

i gospodarstwa rolnego. Należy ocenić, czy sformułowanie definicji legalnej informacji ma rację bytu na gruncie prawa. Bez wątpienia potrzeba skonstruowania ogólnej definicji pojęcia informacji jest dostrzegalna, szczególnie w sytuacji, gdy prawo go używa i przyznaje ochronę wielu jej rodzajom. Należy też ustalić, czy brak w prawie legalnej definicji pojęcia informacja, oddziałuje negatywnie na funkcjonowanie przepisów w praktyce. Problemem pojawiającym się bardzo często w praktyce (a który ma charakter zasadniczy dla dalszych rozstrzygnięć), jest kwalifikacja określonej informacji do kategorii danych osobowych. Rozważenia wymaga, czy istnieje możliwość sformułowania katalogu informacji, które w każdych okolicznościach będą stanowiły dane osobowe oraz katalogu kryteriów jednoznacznie kwalifikujących informację do kategorii danych osobowych. Jednym z celów rozważań będzie także przedstawienie zmian, jakie RODO wprowadziło do rozumienia pojęcia danych osobowych oraz próba ich oceny.

W drugim rozdziale dysertacji ważne miejsce zajmuje problematyka przetwarzania danych osobowych. Trzeba tu jednoznacznie wskazać, że powierzenie danych osobowych do przetwarzania stanowi przetwarzanie danych, choć prawodawca nie wymienia powierzenia w treści legalnej definicji przetwarzania. Warto dodać, że aktualnie termin „powierzenie" istnieje w praktycznym użyciu, choć nie funkcjonuje na gruncie obowiązujących przepisów o ochronie danych osobowych. Pojęcie to występowało w treści art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[4], zgodnie z którym administrator danych mógł powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Treść art. 28 ust. 3 RODO[5] stanowiącego fundamentalny przepis dla powierzenia przetwarzania danych osobowych, nie jest jednoznaczna. Trudno na podstawie tego przepisu ustalić w jaki sposób należy rozumieć elementy umowy powierzenia, co rodzi wiele problemów interpretacyjnych. Można również stanąć na stanowisku, że uregulowanie powierzenia przetwarzania danych oraz konstruowana na tej podstawie modelowa umowa powierzenia przetwarzania jest instrumentem, który w założeniach ma gwarantować realizację zasad ochrony danych osobowych wymienionych w treści art. 5 RODO. Dopełnieniem tej problematyki jest zagadnienie zasad ochrony danych osobowych i próba ich uporządkowania. W związku

[4] T. j. Dz. U. z 2016 r., poz. 922 ze zm., dalej powoływana jako UODO z 1997 r.

[5] Przede wszystkim chodzi o treść: 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, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

z tym można sformułować pytanie, w jaki sposób uregulowanie powierzenia przetwarzania danych oraz konstruowana na tej podstawie modelowa umowa powierzenia przetwarzania danych osobowych realizuje poszczególne zasady.

W trzecim rozdziale centralne miejsce zajmuje charakterystyka prawna umowy powierzenia przetwarzania danych osobowych i próba umiejscowienia umowy powierzenia przetwarzania danych osobowych w systematyce umów. Z uwagi na doniosłe miejsce zasady swobody umów w prawie obligacyjnym, warto odnieść tę zasadę do umowy powierzenia przetwarzania danych osobowych. Wydaje się, że zasada swobody umów ma wyraźnie ograniczoną moc w tym przypadku, przede wszystkim z uwagi na imperatywny charakter przepisów RODO. Ponadto szczególnej uwagi wymaga charakterystyka stron umowy powierzenia przetwarzania danych osobowych. Można stwierdzić, że kluczowym podmiotem w procesie przetwarzania danych jest administrator, od którego zależy byt prawny innych uczestników procesu przetwarzania danych – podmiotu przetwarzającego i podprzetwarzającego. O ile z przepisów RODO jasno wynika rozróżnienie między administratorem (jako stroną decyzyjną) oraz podmiotem przetwarzającym (jako podmiotem działającym w imieniu administratora i wykonującym jego decyzje), to w praktyce okazuje się, że stosunki prawne są na tyle złożone i skomplikowane, że jest wiele trudności z właściwym przypisaniem ról uczestnikom procesów przetwarzania danych osobowych. Umowa powierzenia może być traktowana jako instrument obligujący podmiot przetwarzający do stosowania odpowiedniego poziomu zabezpieczeń danych oraz wymuszający stosowanie przepisów RODO, przez co dane są bardziej bezpieczne, niż w przypadku gdy nie zawiera się takiej umowy (co stanowi naruszenie prawa).

Czwarty rozdział jest poświęcony zastosowaniu umów powierzenia przetwarzania danych osobowych w praktyce oraz analizie funkcji, jakie pełni ta umowa. Można generalnie powiedzieć, że z usług podmiotów przetwarzających korzysta praktycznie każdy podmiot obrotu gospodarczego- zarówno przedsiębiorcy, jak i podmioty sektora publicznego Zarysowane zostały trzy obszary działalności podmiotów prawa, w których najczęściej stosowany jest (lub powinien być) ten instrument prawny. Po pierwsze, analizowane jest zastosowanie umów powierzenia w kontekście outsourcingu usług. Zauważa się, że powierzenie przetwarzania danych osobowych jest najczęściej integralną częścią procesów polegających na outsourcowaniu usług przez jeden podmiot innym podmiotom, o ile do świadczenia tych usług niezbędne jest przetwarzanie danych

osobowych. Chodzi tu o szerokie spektrum usług, m. in. prawne, księgowe, kadrowo-płacowe, informatyczne, archiwizacyjne itp. Sama umowa outsourcingu nie jest w takich przypadkach wystarczająca, aby stanowić podstawę zgodnego z wymogami prawnymi „zlecenia" czynności podmiotowi zewnętrznemu, wymagana jest również umowa powierzenia przetwarzania danych osobowych. Drugi obszar zastosowania umów powierzenia to usługi hostingu, który jest związany z powierzaniem przetwarzania danych osobowych ze względu na to, że polega na przechowywaniu danych. Jeśli wśród danych przechowywanych na „wynajętym" serwerze są również dane osobowe, umowa hostingu musi uwzględniać regulacje dotyczące powierzania danych osobowych przez administratora podmiotowi zewnętrznemu. Trzeci z wskazanych obszarów zastosowania umów powierzenia to nowy i szybko rozwijający się sektor usług chmurowych. Z uwagi na to, że *cloud computing* to obszar powodujący wiele zagrożeń prywatności (ze względu na przypisywane mu cechy zautomatyzowania, nieograniczoności, braku transparentności czy też rozmycia odpowiedzialności), umowa powierzenia przetwarzania jest bardzo istotnym instrumentem ochrony zarówno dla użytkowników chmury, jak i dostawców tej usługi, ale i podmiotów przetwarzanych w niej danych osobowych. W odniesieniu do trzech analizowanych obszarów ważne jest to, by treść umów powierzenia przetwarzania danych osobowych realnie chroniła dane osobowe, a nie jedynie stanowiła narzucone sztampowe konstrukcje, zdejmujące obowiązki i odpowiedzialność z dostawcy hostingu, usług chmurowych czy też podmiotu wykonującego usługi outsourcingowe. Na podstawie zarówno rozważań teoretycznych, jak i analiz konkretnych umów powierzenia przetwarzania danych osobowych, należało ustalić, jakie funkcje realizuje ten instrument prawny. Chodzi tu o wskazanie najistotniejszych ról, jakie umowa pełni wobec stron umowy, osób, których dane dotyczą, jak i wobec organu nadzoru nad przetwarzaniem danych osobowych.

Rozważania prowadzone w piątym rozdziale rozprawy można uznać za klamrę wcześniejszych ustaleń, ponieważ dotyczą kwestii odpowiedzialności na gruncie prawa prywatnego i publicznego, związanej ze stosunkiem powierzania przetwarzania danych w drodze umowy. Instrumenty prawne z zakresu odpowiedzialności mogą być wykorzystywane jako narzędzie do osiągania założonych celów obowiązujących przepisów prawa, jednakże tak, by nie dochodziło do instrumentalizacji prawa, które wówczas przestaje być gwarantem sprawiedliwości, bezpieczeństwa czy też pewności w obrocie. Ze względu na charakter przedmiotowego instrumentu ochrony danych

osobowych będącego stosunkiem umownym, najczęściej zastosowanie ma odpowiedzialność prywatnoprawna. Jednakże można powiedzieć, że sankcje administracyjne w praktyce powodują największą motywację podmiotów do działania zgodnie z przepisami o ochronie danych osobowych. Określone w treści przepisów (wychodzących poza regulację powierzania przetwarzania danych osobowych) reguły ponoszenia odpowiedzialności przez uczestników procesów przetwarzania danych osobowych, stanowią gwarancję ochrony interesów podmiotów danych oraz podmiotów dokonujących przetwarzania, wzmacnianej przez umowę powierzenia przetwarzania danych osobowych, wtedy gdy okaże się, że postanowienia umowy nie są realizowane w sposób zakładany przez jej strony oraz prawodawcę.

Przy przedstawianiu w kolejnych rozdziałach poszczególnych zagadnień, ujętych co do zasady według klasycznego podziału materii przyjmowanego w analizie umów, wykorzystana została przede wszystkim metoda dogmatycznej wykładni tekstów normatywnych, jednak z uwzględnieniem praktycznego aspektu stosowanych przepisów. Przydatne okazało się także komparatystyczne spojrzenie na regulacje unijne i polskie (obowiązujące przed 25 maja 2018 roku). Z uwagi na niedawne rozpoczęcie bezpośredniego stosowania RODO, jak również praktycznie niezmienione podejście prawodawcy unijnego do pojęcia danych osobowych, w dużej mierze aktualne pozostają rozważania prowadzone na gruncie Dyrektywy 95/46/WE[6] i UODO z 1997 roku, jak też poglądy judykatury, decyzje Generalnego Inspektora Ochrony Danych Osobowych (GIODO)[7] oraz dorobek przedstawicieli nauki prawa dotyczący poprzedniego stanu prawnego. W dysertacji zostały wykorzystane także badania własne i doświadczenie zawodowe. Rozprawa powstała więc na podstawie analizy przepisów prawa i literatury przedmiotu (w tym publikacje naukowe z zakresu prawa cywilnego, administracyjnego, karnego czy konstytucyjnego), ale również wykorzystano w niej wiele innych źródeł informacji i doświadczenie zawodowe. Należy podkreślić, że cenne okazały się tu także publikacje z obszaru pozaprawnego, takich jak np. artykuły publikowane w czasopismach Computerworld, IT w Administracji, ABI Expert, co pozwoliło uchwycić funkcjonalne, praktyczne postrzeganie rozważanych problemów, m.in. w sferze usług IT, takich jak hosting czy przetwarzanie chmurowe. Bazę do prowadzonych badań własnych stanowiły

[6] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, (Dz.Urz.UE.L 2000 Nr 178, str. 1 ze zm.), dalej jako Dyrektywa 95/46/WE.
[7] Aktualnie Prezes Urzędu Ochrony Danych Osobowych.

także umowy powierzenia przetwarzania danych osobowych, pojawiające się w praktyce zawodowej autorki, jak również dostępne w Internecie umowy outsourcingowe, umowy o hosting, czy też umowy o świadczenie usług w chmurze. Korzystano również ze źródeł oraz tekstów umów w języku angielskim.

Ważnym celem prowadzonych tu rozważań jest sformułowanie wniosków potwierdzających lub modyfikujących wskazane hipotezy badawcze, jak również zaproponowanie wniosków *de lege ferenda*. Konsekwencją tych celów jest zarówno konstrukcja rozprawy, jak i metodologia badań.

W dysertacji uwzględniono stan normatywny na dzień 1.02.2019 r.

ROZDZIAŁ I

Dane osobowe jako przedmiot ochrony prawnej

1. Interdyscyplinarny charakter pojęcia informacja a przedmiot ochrony prawnej

1.1. Pojęcie informacji – uwagi ogólne

Rozważania nad istotą danych osobowych należy rozpocząć od ustalenia, czym jest informacja. Stanowi ona istotny element, na którym opiera się definicja danych osobowych (dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej). Chodzi bowiem o odpowiedź na pytanie w jakiej wzajemnej relacji znajdują się informacje oraz dane (w ogólnym ujęciu). Wywody nad pojęciem informacji wymagają analizy poglądów wypracowanych przez przedstawicieli różnych dziedzin nauki, zwłaszcza prawa, informatyki, ekonomii i zarządzania, nauk społecznych. Należy przyjąć, że informacja, jak i dane osobowe są pojęciami interdyscyplinarnymi i wieloaspektowymi.

Termin „informacja" funkcjonuje w powszechnym użyciu, jednakże można odnieść wrażenie, że jest używany i stosowany bardziej w oparciu o intuicję, wyczucie i doświadczenie, niż naukowe uzasadnienie. W literaturze przedmiotu spotyka się poglądy wskazujące na to, że część teoretyków uznaje informację za pojęcie pierwotne i w konsekwencji niedefiniowalne[8]. Informacji można przypisać charakter abstrakcyjny i niematerialny.

Informacja jest terminem zarówno języka prawnego, jak i prawniczego. Analizując to zagadnienie można odnaleźć obrazowe statystyki, pokazujące, że słowo informacja, pojawia się w „(...) polskich dziennikach ustaw ponad 5 tysięcy razy, i w monitorach polskich ponad 21 tysięcy"[9]. Zaznaczyć przy tym należy, że o ile prawo posługuje się pojęciem informacji stosunkowo często (np. informacja publiczna, informacja gospodarcza, informacje niejawne, informacja o środowisku), to dorobek nauki prawa w zakresie wypracowania definicji informacji jest znikomy. W konsekwencji tego niezbędne jest odwołanie się do obszarów innych nauk, przede wszystkim nauk

[8] B. Nadolna, *Informacja i komunikacja jako element kontroli zarządczej w jednostkach sektora finansów publicznych*, Zeszyty Naukowe Uniwersytetu Szczecińskiego 2011 nr 669, Finanse, Rynki Finansowe, Ubezpieczenia nr 42, s. 85, dostępne na: http://www.wneiz.pl/nauka_wneiz/frfu/42-2011/FRFU-42-81.pdf, dostęp: 2.08.2016 r.

[9] G. Szpor, *Jawność i jej ograniczenia. Tom I, Idee i pojęcia*, 2016, Legalis.

społecznych, w tym filozofii, socjologii i socjotechniki, jak również informatyki, ekonomii czy cybernetyki. W ten sposób może okazać się możliwym działanie polegające na przeniesieniu, przynajmniej w pewnym stopniu, do nauk prawnych osiągnięć w zakresie wyznaczenia ram definicyjnych pojęcia informacji wypracowanych na gruncie innych nauk. Pojawiają się jednak obawy, że działanie to będzie powodowało wiele problemów interpretacyjnych[10].

Na wstępie postawić można tezę, że w dostępnych źródłach nie dostrzega się jednolitej i uniwersalnej definicji informacji. Problem z definiowaniem informacji na gruncie nauki trafnie zobrazował M. Mazur[11], wskazując, że niektórzy autorzy posługują się terminem informacja bez żadnych dodatkowych wyjaśnień, co należałoby przez to rozumieć. Wychodzą więc oni z założenia, że znaczenie tego pojęcia nie budzi wątpliwości. Inni autorzy zagłębiają się w szczegółowych dociekaniach w celu wyjaśnienia pojęcia informacji.

Ogólnie rzecz ujmując, słowo „informacja" pochodzi od łacińskiego *informatio,* czyli wyobrażenie, wyjaśnienie, zawiadomienie, formowanie, nadawanie kształtu[12]. Według wyjaśnienia zawartego w słowniku języka polskiego, informacja to „wiadomość o czymś lub zakomunikowanie czegoś", a w znaczeniu informatycznym „dane przetwarzane przez komputer"[13], albo też „coś, co zostało powiedziane lub napisane o czymś", zaś w znaczeniu informatycznym „treść wprowadzana do komputera i w odpowiedni sposób przetwarzana w nim" [14]. Jeśli chodzi o synonimy słowa informacja, w słownikach najczęściej spotyka się m.in. wiadomość, wieść, notyfikacja, nowina, relacja, komunikat, ogłoszenie, zawiadomienie, powiadomienie, oznajmienie, obwieszczenie, oświadczenie, deklaracja, wypowiedź, wzmianka, ciekawostka, przekaz, wskazówka, pouczenie, instrukcja, sygnał, namiar[15].

Wielu przedstawicieli nauki zajmujących się problematyką informacji, z biegiem lat dochodziło do sformułowania bardziej konkretnych poglądów zawierających elementy

[10] M. Kłodawski, *Pojęcie informacji w naukach teoretyczno prawnych*, s. 1, dostępne na: http://depot.ceon.pl/bitstream/handle/123456789/316/Maciej_Klodawski_-_Pojecie_informacji_w_naukach_teoretycznoprawnych.pdf.

[11] M. Mazur, *Jakościowa teoria informac*ji, dostępne na http://www.autonom.edu.pl/publikacje/mazur_marian/jakosciowa_teoria_informacji-tiff.pdf .

[12] https://encyklopedia.pwn.pl/haslo/informacja;3914686.html.

[13] http://sjp.pwn.pl/szukaj/informacja.html

[14] http://www.wsjp.pl/index.php?id_hasla=22125&id_znaczenia=3976450&l=10&ind=0

[15] https://www.synonimy.pl/synonim/informacja/.

wyjaśnienia rozważanego pojęcia. Przykładem jest amerykański matematyk i twórca cybernetyki N. Wiener. Początkowo w jego pracach odnajduje się jedynie generalne wypowiedzi na ten temat: „Informacja jest informacją, nie materią, nie energią, nie różnorodnością, ani niczym innym”[16]. Dopiero parę lat później N. Wiener zaproponował bardziej rozbudowaną definicję: „Informacja jest nazwą treści zaczerpniętej ze świata zewnętrznego, w miarę jak się do niego dostosowujemy i jak przystosowujemy doń swoje zmysły"[17]. O ile jej przydatność można oceniać nisko z uwagi na zawarty w niej inny problematyczny i niewyjaśniony termin „treść”, to należy przyznać, że element czerpania informacji z zewnątrz za pomocą zmysłów, mógł dawać badaczom kierunek dalszych dywagacji. W związku z powyższym, warte uwagi jest dokonanie przeglądu sposobów rozumienia pojęcia informacja na gruncie różnych nauk, zarówno ścisłych, jak i humanistycznych.

Wśród poglądów teoretyków wyraźnie dostrzegalne jest bardzo ścisłe powiązanie nauki i informacji. Zdobywanie informacji jest jednym z celów nauki. Co więcej, podkreśla się, że informacja jest elementem nieodzownym w próbach zdefiniowania pojęcia nauki: „nauka jako czynność dostarczająca informacji”, „nauka jako proces polegający na zdobywaniu informacji”[18]. Informacja jest konieczną bazą dla ogólnie pojmowanej nauki, elementem, bez którego nauka nie istnieje, wokół którego się rozwija i w którym jest ustanowiony jej cel. Wśród sposobów rozumienia pojęcia informacji o generalnym charakterze wyróżnić można m.in. pogląd H Greniewskiego, dla którego informacja to „wiadomość uzyskiwana przez człowieka poprzez obserwację lub czynność umysłową, podlegającą przekazowi w układzie nadawca-odbiorca”[19], czy też T. Wierzbickiego, który stwierdził, że informacją jest „treść zaczerpnięta ze świata zewnętrznego, która zwiększa wiedzę lub zmniejsza niewiedzę decydującego, niepewność i nieokreśloność sytuacji decyzyjnej”[20]. Definicje te zwracają uwagę na następujące elementy pojęcia informacja: źródło - świat zewnętrzny, nadawcę i odbiorcę, treść zmniejszającą niepewność, operacje myślowe. Nie są to elementy, które są

[16] N. Wiener, *Cybernetics or Control and Communication and the Animal and the Machine*, Nowy Jork 1948, cyt. za: M Mazur, *Jakościowa…, op. ci*t, s. 19.
[17] N. Wiener, cyt. za A. Piotrowska, *Wiedza jawna i niejawna jako zasób decyzyjny w zarządzaniu personelem* [w:] A. Grzegorczyk (red.) *Procesy decyzyjne w warunkach niepewności*, Warszawa 2012.
[18] P. Iwański [w:] A. Maryniarczyk (red.), *Powszechna Encyklopedia Filozofii*, dostępna na: www.ptta.pl/pef.
[19] H. Greniewski, *Cybernetyka niema tematyczna*, Warszawa 1982, s.6.
[20] T. Wierzbicki, *System informacji gospodarczej*, Warszawa 1981, s.11.

charakterystyczne dla języka prawnego i prawniczego, co potwierdza tezę o interdyscyplinarnej naturze pojęcia informacji.

W literaturze przedmiotu stosunkowo często wyróżnia się cybernetyczne rozumienie informacji[21]. Definicje informacji na gruncie cybernetyki zebrał i szczegółowo omówił M. Kłodawski[22]. Zdaniem tego Autora informacja to zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne. W kolejnej definicji zawarto stwierdzenie, że informacja to każdy czynnik, który ludzie, organizmy żywe lub urządzenia mogą wykorzystywać dla bardziej sprecyzowanego celowego działania. Ponadto informacja to bodziec, który oddziałuje na układ recepcyjny człowieka i powoduje wytwarzanie w jego wyobraźni przedmiotu myślowego, odzwierciedlającego obraz rzeczy materialnej lub abstrakcyjnej, który w jego świadomości kojarzy się z tym bodźcem. Oznacza to, że informacje to te doznania, które inspirują umysł ludzki do wyobraźni, której istnienie jest relatywnie związane z istnieniem człowieka i jego umysłem. Należy podkreślić, że w ujęciu M. Kłodawskiego informację stanowi nie tylko wszelki opis, lecz także nakazy, zakazy, polecenia, dyrektywy działania. Autor wskazuje, że informacja może być wyrażona nie tylko w dowolnym języku, lecz także za pomocą dowolnego kodu, np. kodu genetycznego, kodu impulsów elektronicznych, kodu impulsów nerwowych, kodu hormonów itd. „To ujęcie informacji umożliwia potraktowanie jako jej nadawcy i odbiorcy zarówno człowieka, jak i organizmów żywych, ich organów, a także maszyn i organizacji”[23]. Formułując wspólny wniosek dla przytoczonych wyżej definicji cybernetycznych, można stwierdzić, że cechuje je znaczny stopień ogólności i pojemności, co dotyczy tak treści informacji, jak i jej formy. W większości definicje informacji skupiają się wokół człowieka i jego umysłu, ale nie ograniczają się do niego, dopuszczając również m.in. urządzenia automatyczne. Ponadto odnosi się wrażenie, że w definicjach tych większą wagę przywiązuje się do odbiorcy informacji (przede wszystkim człowieka), niż do nadawcy, który nie jest określony, ale intuicyjnie wyczuwa się, że może nim być świat zewnętrzny, otoczenie.

[21] Zgodnie ze znaczeniem encyklopedycznym, cybernetyka to [gr. kybernḗtes ‘sternik’, ‘zarządca’, kybernáō ‘steruję’], nauka o sterowaniu oraz przesyłaniu i przetwarzaniu informacji w systemach technicznych, biologicznych i społecznych, http://encyklopedia.pwn.pl/szukaj/cybernetyka.html
[22] M. Kłodawski, *Pojęcie…, op. cit.*, s. 4-5 oraz cytowane tam źródła.
[23] *Ibidem*.

W naukach informatycznych i w rozumieniu systemów informatycznych, informacja to dane, tworzące zrozumiałą i poddającą się interpretacji użytkownika systemu treść[24]. Najważniejsze w tej definicji są trzy elementy: zespół danych, użytkownik systemu, zachodzący pomiędzy dwoma powyższymi proces interpretacji i zrozumienia. Według innych źródeł informacją jest zbiór danych zebranych w celu ich przetwarzania i otrzymania wyników (nowych danych)[25]. Na gruncie nauk informatycznych wskazuje się również infologiczne i datalogiczne podejście do zagadnienia informacji. Zgodnie z pierwszym informacja to subiektywne znaczenie, jakie treści komunikatu nadaje jego odbiorca, natomiast w aspekcie datalogicznym będzie to treść komunikatu niezależna od odbiorcy komunikatu[26].

Warto też przytoczyć techniczną definicję informacji zawartą w istotnych dla obszaru informatyki oraz zarządzania Polskich Normach. Zgodnie z treścią Normy PN-ISO/IEC 27000:2014-11, informacje to aktywa niezbędne dla organizacji biznesu i wymagające odpowiedniej ochrony niezależnie od tego, jaką formę posiadają, ani od tego, jaki jest środek ich przesyłania[27]. Pojęcie informacji prezentowane w treści powołanej normy jest zróżnicowane pod kątem formy ich przechowywania (postać cyfrowa – pliki danych przechowywane na mediach elektronicznych i optycznych, postać materialna – na papierze, postać niematerialna – wiedza posiadana przez pracowników), jak też pod kątem środków ich przesyłania (komunikacja elektroniczna, komunikacja werbalna, komunikacja za pośrednictwem kuriera). Zwraca się też uwagę na zależność informacji od technologii informacyjnych i telekomunikacyjnych, które umożliwiają w organizacji tworzenie, przetwarzanie, przechowywanie, przesyłanie, ochronę i niszczenie informacji[28].

Informacja może być postrzegana jako kategoria filozoficzna, o czym świadczy już sam fakt trudności z wyznaczeniem jej ram definicyjnych, a także ogólny i stosunkowo uniwersalny charakter. Jak wynika z dostępnych źródeł, termin *informatio* używany był w filozofii scholastycznej i oznaczał zdeterminowanie, ukonstytuowanie materii przez

[24] A. Rydz w: D. Jemielniak, A.K. Koźmiński, *Zarządzanie wiedzą*, Warszawa 2012, s. 303.
[25] M. Kuraś, *System informacyjny - system informatyczny. Co poza nazwą różni te dwa obiekty?*, dostępne na: uci.agh.edu.pl/uczelnia/tad/PSI9/3.rtf oraz powołana tam literatura.
[26] M Szmit, *Wybrane zagadnienia opiniowania sądowo-informatycznego*, Warszawa 2014, s. 125 i powołana tam literatura.
[27] Polska Norma PN-ISO/IEC 27000:2014-11: Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia, PKN, Warszawa 2014, s. 20.
[28] *Ibidem*.

formę[29]. Aktualnie informacja traktowana jest niejednokrotnie jako odpowiednik terminu „poznanie" i służy do definiowania czym jest poznanie[30]. Aby traktować informację jako kategorię filozoficzną, należy mówić w największej ogólności o jej istocie, aspektach, przejawach i faktycznych zastosowaniach[31].

Należy także uwzględnić pojęcie informacji w ujęciu współczesnej ekonomii. Na tym gruncie informacja jest postrzegana obok pracy, kapitału i ziemi jako jeden z podstawowych zasobów warunkujący potencjał ekonomiczny oraz możliwości rozwojowe gospodarki[32]. Znaczenie informacji jako zasobu stale rośnie, staje się ona coraz bardziej wartościowym towarem. W konsekwencji takie tendencje mogą z czasem doprowadzić do wyodrębnienia się w gospodarce obok sektora rolniczego, przemysłowego i usługowego, nowego sektora informacyjnego obejmującego działalność związaną z wytwarzaniem, gromadzeniem, przetwarzaniem, ochroną i transferem informacji[33]. Wydaje się, że informacja jest niezwykle istotnym elementem dla wszystkich wymienionych sektorach, co może utrudniać wyodrębnienie sektora informacyjnego jako równorzędnej części gospodarki.

Reasumując problematykę definicji pojęcia informacji na gruncie pozaprawnym, można sformułować wniosek, że jest to pojęcie o charakterze interdyscyplinarnym i wieloaspektowym, ogólnym i nieostrym, a w konsekwencji – skomplikowanym. Informacja to termin o ogromnej pojemności treściowej. Co więcej, pojemność ta z biegiem czasu stale zmienia się i rośnie. Nie jest odkryciem stwierdzenie, że ilość informacji w każdej dziedzinie nauki, techniki, a nawet życia codziennego jest niewyobrażalnie większa niż kilkadziesiąt lat temu. Ponadto można zaryzykować stwierdzenie, że człowiek w sposób intuicyjny rozpoznaje co jest informacją, a docierają do niego z zewnątrz poprzez różne środki przekazu ciągle nowe bodźce, których jest i będzie coraz więcej. Dlatego też uzasadnionym wydaje się wniosek, że trudno dostrzec możliwość skonstruowania uniwersalnej dla wszystkich nauk definicji informacji. Co więcej, wydaje się to bezprzedmiotowe, gdyż każda z nauk obiera sobie inny aspekt informacji jako punkt zainteresowania. Potwierdzają to również słowa J. Janowskiego, według którego próbom zdefiniowania informacji towarzyszy zawsze pewna

[29] P. Iwański, *Powszechna…, op. cit.*
[30] M. Lubański, *Filozoficzne zagadnienia teorii informacji*, Warszawa 1975.
[31] W. Wawszczak, *Wprowadzenie do filozofii informacji*, dostępne na: chfpn.pl/files/?id_plik=413.
[32] P. Iwański, *Powszechna…, op. cit*.
[33] *Ibidem*.

niedookreśloność, uzupełniana opisem akcentującym aspekty ważne dla danej dziedziny wiedzy[34]. Należy zatem traktować to pojęcie jako abstrakcyjne, zaś jego konkretyzacja powinna następować w odniesieniu do odpowiedniego kontekstu i w oparciu o stosowne kryteria. Wydaje się, że prawo i nauka prawa najbardziej skorzystać mogą z definicji cybernetycznych. Analizując je, można bowiem dojść do wniosku, że mają one wiele cech wspólnych ze sposobami rozumienia pojęcia normy prawnej. Definicje cybernetyczne informacji, podobnie jak normy prawne, obejmują nakazy, zakazy, polecenia, dyrektywy działania. Ponadto oddziałują i w znacznym stopniu determinują działanie człowieka, dzięki nim człowiek podejmuje działania.

1.2. Pojęcie informacji w wybranych polskich regulacjach prawnych

Termin informacja występuje w aktach prawnych, jednakże przeważnie niesamodzielnie, ponieważ opatrzony jest konkretyzującym go przymiotnikiem (jak np. informacje niejawne, informacja publiczna).

Warto zauważyć, że na gruncie obowiązujących regulacji prawnych brak jest ogólnie obowiązującej definicji legalnej informacji, mimo że prawo niejednokrotnie posługuje się tym terminem. Dla dalszych rozważań przyjęte zostaje założenie, że informacja stanowi określone dobro (często majątkowe), chronione prawem. Należy zastanowić się, w jaki sposób ustawodawca reguluje dobro jakim jest informacja w konkretnych aktach prawnych. Ponadto rozważyć trzeba, czy w ogóle istnieje potrzeba oraz możliwość sformułowania definicji legalnej informacji.

Warto odwołać się w tym momencie do przesłanek wprowadzenia sformułowań definicyjnych do tekstu aktu prawnego, które określone zostały w treści rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 roku w sprawie „Zasad techniki prawodawczej”[35]. Z treści § 146 ust. 1 rozporządzenia wynika, że w ustawie lub innym akcie normatywnym formułuje się definicję danego określenia, jeżeli: dane określenie jest wieloznaczne lub dane określenie jest nieostre, a jest pożądane ograniczenie jego nieostrości. Ponadto definicja jest niezbędna, gdy znaczenie danego określenia nie jest powszechnie zrozumiałe lub ze względu na dziedzinę regulowanych spraw istnieje potrzeba ustalenia nowego znaczenia danego określenia. W odniesieniu do wymienionych

[34] J. Janowski, *Informatyka prawnicza*, Warszawa 2011, s. 20.
[35] t.j. Dz. U. 2016, poz. 283, dalej jako rozporządzenie ZTP.

przesłanek można powiedzieć, że samo pojęcie informacja nie jest raczej pojęciem wieloznacznym, większość powyższych prób zdefiniowania go oscyluje wokół procesu przekazywania treści uzewnętrznianych przez nadawcę i odbieranych czy interpretowanych przez odbiorcę[36]. Natomiast można zająć stanowisko, że pojęcie informacji charakteryzuje się nieostrością i jest ona niepożądana, ponieważ może powodować wątpliwości interpretacyjne i problemy w sferze stosowania prawa.

Warto rozważyć w kontekście zasad dotyczących techniki tworzenia przepisów prawnych kilka przykładów regulowania dobra prawnego, jakim jest informacja. W treści ustawy z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej[37] ustawodawca umieszcza pojęcie informacji wśród definicji pojęć w art. 3. ustawy Trudno uznać powołany przepis za pomocny w zrozumieniu pojęcia informacji używanego na gruncie tego aktu prawnego, skoro z brzmienia art. 3 powołanej ustawy wynika, że ilekroć w ustawie jest mowa o informacji - rozumie się przez to informacje. Wydaje się, że mamy tu przykład błędu w definiowaniu *idem per idem* (łac. to samo przez to samo), w konsekwencji czego trudno uznać zacytowane sformułowanie za skuteczne i zrozumiałe wyjaśnienie pojęcia informacja.

W świetle przepisów rozporządzenia ZTP wątpliwości budzi sformułowanie definicji informacji publicznej, zawarte w treści art.1 ustawy o dostępie do informacji publicznej[38], zgodnie z którym każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu na zasadach i w trybie określonych w niniejszej ustawie. Parafrazując można powiedzieć, że informację publiczną w rozumieniu ustawy stanowi każda informacja o sprawach publicznych. W przepisie ustawowym pojawia się błąd *ignotum per ignotum*, polegający na wyjaśnieniu nieznanego - pojęcia informacja publiczna za pomocą innego pojęcia również nieznanego - informacja o sprawach publicznych. Nie można zatem stwierdzić, że pojęcie informacji publicznej w tym obszarze prawa ma sformułowaną definicję legalną[39].

---

[36] Tak również M. Szmit, *Wybrane zagadnienia opiniowania sądowo-informatycznego*, Warszawa 2014, s. 125.

[37] Dz. U. z 2018 r. poz. 484. Zgodnie z art. 3 powołanej ustawy: *Ilekroć w ustawie jest mowa o informacji: rozumie się przez to informacje, w tym dane osobowe, do których pobierania, uzyskiwania, przekazywania, gromadzenia, wykorzystywania i przetwarzania, w celu realizacji swoich zadań ustawowych są uprawnione, na podstawie przepisów odrębnych, podmioty uprawnione.*

[38] t.j. Dz.U. z 2018 r. poz. 1330.

[39] Inaczej wygląda podejście prawodawcy do wyjaśnienia terminu informacji geologicznej. Jej definicja ustawowa została zawarta w treści art. 6 ust. 1 pkt 2 ustawy z dnia 9 czerwca 2011 roku Prawo geologiczne i górnicze (t.j. Dz. U. z 2017r. poz. 2126). Zgodnie z treścią przepisu *informacją geologiczną są dane i próbki*

Kolejnym przykładem uregulowania kategorii informacji w akcie prawnym i podjęcia próby zdefiniowania pojęcia informacja na gruncie prawa, jest przyznanie ochrony prawnej informacjom niejawnym, co uczynił ustawodawca w treści ustawy z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych[40]. Wyjaśnienia terminu informacji niejawnych ustawodawca spróbował dokonać w treści art. 1 ustawy, z którego wynika, że chodzi tu o informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania. Należy zastanowić się, czy powyższe wyjaśnienie pojęcia informacji niejawnych można traktować jako ich definicję legalną. W kontekście przesłanek uzasadniających wprowadzenie definicji legalnej do aktu prawnego sformułowanych w § 146 rozporządzenia ZTP, można postawić tezę, że w przypadku informacji niejawnych, zachodzi przesłanka związana z potrzebą ustalenia nowego znaczenia danego określenia ze względu na dziedzinę regulowanych spraw. Wynika to z faktu, że w potocznym rozumieniu słowo „niejawne" oznacza najczęściej „dokonywany albo odbywający się w tajemnicy"[41] czy też „tajny, sekretny, konspiracyjny, poufny, nieoficjalny, pozostający w ukryciu"[42]. Znaczenie potoczne wydaje się zatem szersze niż znaczenie nadane przez ustawodawcę. Założeniem jest więc objęcie ochroną informacji, które są niejawne tylko w zakresie dotyczącym Rzeczpospolitej Polskiej, a nie np. informacje niejawne dotyczące kwestii pozapaństwowych. Dlatego też należało ustalić tu nowe znaczenie dla przedmiotu ochrony. Jednakże odnosi się wrażenie, że rozważana definicja ustawowa skupia się tylko na części omawianego pojęcia. Nacisk położony tu zostaje na przymiotnik niejawne, bardziej niż na całość terminu informacji niejawnych,

---

geologiczne wraz z wynikami ich przetworzenia i interpretacji, w szczególności przedstawione w dokumentacjach geologicznych oraz zapisane na informatycznych nośnikach danych. W definicji tej warto podkreślić następujące elementy: dane i próbki (jako nośniki informacji) oraz wyniki ich przetworzenia i interpretacji (jako przejawy procesu poznania i zrozumienia). W ocenie autorki należy tu wysoko ocenić starania ustawodawcy podjęte w celu wyjaśnienia i skonkretyzowania niełatwego do zdefiniowania pojęcia. Wprowadzenie definicji legalnej uzasadnione jest tu przede wszystkim przesłanką określoną w § 146 ust. 1 pkt 3 rozporządzenia ZTP (*znaczenie danego określenia nie jest powszechnie zrozumiałe*). Wydaje się, obiektywnie oceniając, że termin informacja geologiczna wykracza poza zasób wiedzy przeciętnego człowieka, przede wszystkim z uwagi na specyfikę dziedziny nauki, jaką jest geologia, jak również wąską i specjalistyczną dziedzinę prawa, jakim jest prawo geologiczne i górnicze. Ponadto definicja legalna informacji geologicznej zdecydowanie bardziej respektuje przepis § 151 ust. 1 rozporządzenia ZTP niż definicja informacji publicznej. W przeciwieństwie do tej drugiej, nie dostrzega się tu podobnego błędu polegającego na wyjaśnianiu nieznanego pojęcia za pomocą innego pojęcia o charakterze niejasnym bądź też za pomocą tego samego pojęcia w innym układzie.

[40] t.j. Dz.U. z 2018 r. poz. 412.

[41] http://sjp.pwn.pl/szukaj/niejawny.html.

[42] https://www.synonimy.pl/synonim/niejawny/.

skoro pojęcie informacji wyjaśniane jest przez pojęcie informacji. Podobnie jak w przypadku zdefiniowania informacji publicznej, mamy tu do czynienia z niepełną zgodnością z treścią przepisu zawartego w § 151 ust. 1 rozporządzenia ZTP[43]. Dodatkowo można stwierdzić, że przepis art. 1 ustawy o ochronie informacji niejawnych nie prezentuje definicji legalnej wprost, w sposób tradycyjny, a raczej wymaga wyinterpretowania definicji. Niemniej jednak jego treść należy ocenić jako potrzebną i spełniającą funkcję wyjaśnienia nowego znaczenia przedmiotowego określenia.

Zupełnie inaczej do kwestii uregulowania zagadnienia informacji podchodzi ustawodawca na gruncie ustawy z dnia 3 października 2008 roku o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko[44]. W przeciwieństwie do wcześniej powołanych regulacji, w przepisach tej ustawy nie zawarto żadnego wyjaśnienia, jak należy rozumieć pojęcie informacji o środowisku. Takie działanie ustawodawcy można próbować wytłumaczyć tym, że uznał on, iż kluczowe dla tej ustawy pojęcie nie budzi wątpliwości. Sam termin informacja pozostawiony jest wykładni językowej. Do takiego wniosku skłania sposób, w jaki definiowane są inne pojęcia z art. 3 ustawy, zawierające ten termin. Wyjaśniając, co oznacza informacja przeznaczona dla organu, ustawodawca wskazuje, że rozumie się przez to informację, którą w imieniu organu administracji dysponują osoby trzecie, w tym też informację, której organ ten ma prawo żądać od osób trzecich. Przez informację znajdującą się w posiadaniu organu administracji rozumie się informację znajdującą się w posiadaniu organu administracji, wytworzoną przez ten organ lub otrzymaną przez organ od osoby trzeciej. Po pierwsze, trudno przyznać tym próbom wyjaśnień walor definicyjny, skoro informacja definiowana jest jako informacja. Takie działania zakwalifikować można do kategorii błędu *idem per idem*, a ponadto, mogą one w konsekwencji skłaniać do czerpania znaczenia z języka potocznego

Warto zastanowić się, czy drogą do rozwiązania problemu ze zdefiniowaniem informacji na gruncie prawa nie mogłaby być próba sformułowania definicji zakresowej, zgodnie z treścią § 153 rozporządzenia ZTP[45]. Niezbędnym do tego jest konkretne nazwanie elementów składowych tego zakresu, przynajmniej kilku, by zbudować definicję

[43] Definicję formułuje się tak, aby wskazywała w sposób niebudzący wątpliwości, że odnosi się do znaczenia określeń, w szczególności nadaje się jej postać: „Określenie „a" oznacza b." albo „Określenie „a" znaczy tyle co wyrażenie „b".".
[44] t.j. Dz.U. z 2017 r. poz. 1405.
[45] Definicję zakresową (wyliczającą elementy składowe zakresu) formułuje się w jednym przepisie prawnym i obejmuje się nią cały zakres definiowanego pojęcia.

niepełną (ust. 3). Można podjąć próbę sformułowania zakresowej definicji informacji, czerpiąc inspirację z różnych dziedzin nauki, choć jak wskazano, na grunt prawa najłatwiej będzie przenieść osiągnięcia z zakresu cybernetyki. Z wyżej poczynionych ustaleń wynika, że informacja oznacza dobro niematerialne, które stanowi rezultat procesu myślowego nad wszelkimi bodźcami ze świata zewnętrznego, przekazywanymi między nadawcą a odbiorcą, wyrażanymi w formie językowej, jak i za pomocą znaków, liczb, sygnałów, obrazów, dźwięków, kodów, którego celem jest zmniejszenie niepewności i zwiększenie wiedzy, w szczególności: zinterpretowane dane, wiadomości, komunikaty, opisy, polecenia, nakazy, zakazy, opinie, wnioski, wyniki. Pojawia się jednak pytanie, na ile taka propozycja zdefiniowania informacji będzie użyteczna z punktu widzenia prawa. Należy przyjąć, że wyjaśnianie pojęcia nieostrego za pomocą innych pojęć nieostrych i niezdefiniowanych w prawie, nie jest celowe z uwagi na jego nieużyteczność praktyczną.

Wydaje się, że stworzenie definicji legalnej informacji nie rozwiąże problemów prawnych związanych z tym pojęciem. Sformułowanie takiej definicji z użyciem słów typu „dobro niematerialne", „treść", „wiadomość", „dane", „interpretacja", „niepewność", spowoduje jedynie to, że pojawi się jeszcze więcej pojęć niedefiniowanych w prawie. Podmioty stosujące prawo wcale nie otrzymałyby narzędzia stanowiącego wskazówkę, która pozwalałaby jednoznacznie stwierdzić, czy rzeczywiście w danej sytuacji przedmiotem ochrony jest informacja. Można odnieść wrażenie, że język prawny i język prawniczy są zbyt ubogie, by zwerbalizować wyjaśnienie pojęcia informacji w sposób konkretny i precyzyjny. Co więcej, w języku potocznym również trudno jest zakreślić granice tego słowa, zdecydować, co jest informacją, a co nią nie jest. W takim przypadku pewności nie da nawet rozwiązanie polegające na odwołaniu się do wykładni językowej. W procesie stosowania prawa najczęściej stosuje się zasadę pierwszeństwa wykładni językowej, zgodnie z którą w przypadku, gdy brakuje ustawowej definicji danego określenia, organy stosujące prawo powinny przyjąć, że prawodawca posługuje się danym określeniem zgodnie z jego poprawnym, podstawowym i powszechnie przyjętym znaczeniem. Fakt, że dotąd nie wypracowano jednolitego i spójnego sposobu rozumienia pojęcia informacja, pozwala uniknąć zarzutu, że w dobie intensywnego postępu szybko zdezaktualizuje się definicja tego bardzo prężnie rozwijającego się pojęcia. Taki stan rzeczy nie przeszkadza jednak traktować informację w kategoriach dobra chronionego prawnie, również jako przedmiot obrotu (jak np. bazy danych klientów, know-how). Z drugiej jednak strony, brak ustalenia, co należy rozumieć pod pojęciem informacji, jako

elementu, na którym opiera się definicja danych osobowych (dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej), może powodować problemy w zakresie rozstrzygania, czy w określonej sytuacji mamy do czynienia z naruszeniem godzącym w dane osobowe.

2. Relacja między pojęciami informacja a dane osobowe

Kolejnym zagadnieniem, które wymaga uwagi w kontekście problematyki danych osobowych, jest pojęcie danych w ujęciu ogólnym. Podobnie jak w przypadku informacji, dane również są pojęciem trudno definiowalnym. Zauważa się, że dane w ujęciu ogólnym rzadziej stanowią przedmiot badań naukowych niż informacje, o czym świadczy chociażby dużo mniejsza liczba dostępnych źródeł na ich temat. Należy podkreślić, że analiza znaczenia pojęcia dane wymaga odniesienia go do pojęcia informacji, co pozwoli następnie na określenie relacji zachodzącej między dwoma terminami.

W literaturze przedmiotu z zakresu nauk prawnych odnajduje się bardzo zwięzłe i powściągliwe wypowiedzi na temat tego, jak należy rozumieć dane w aspekcie generalnym. Traktowane są one jako nośniki informacji, zapis określonej informacji w różnej postaci: literowej, cyfrowej, dźwiękowej, rysunkowej[46]. W podobny, pozbawiony wnikliwych analiz sposób definiuje dane J. Błachut. Autor traktuje dane jako proste jednostki informacyjne, znaki, liczby, litery o neutralnym charakterze[47]. P. Fajgielski rozbudowuje nieco definicję danych, twierdząc, że przez dane rozumie się przedstawienie faktów, pojęć, poleceń, w sposób sformalizowany oraz umożliwiający ich komunikowanie, interpretację lub przetwarzanie przez ludzi i urządzenia[48]. Najbardziej szczegółowa wydaje się definicja danych opracowana przez G. Szpor. Autorka stwierdza, że są to znaki nadające się do przetworzenia na nośnikach fizycznych (litery, cyfry, impulsy elektryczne), które mogą mieć zerową (gdy nie redukują niepewności) lub dodatnią wartość informacyjną (jeśli redukują niepewność), ponadto postać danych nie ma

[46] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 38-39.
[47] J. Błachut, *Dokument jako przedmiot ochrony prawno karnej*, Warszawa 2011, s. 34-35.
[48] P. Fajgielski, *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007, s. 15.

większego znaczenia, natomiast nośniki, na których są one zapisane, powinny być nośnikami fizycznymi[49].

Z punktu widzenia nauk informatycznych, dane postrzegać można jako fizyczną reprezentację elementarnej porcji informacji, w postaci której jest ona rejestrowana lub przesyłana. Innymi słowy, dane są wykorzystywane do rejestrowania informacji i jej przekazu[50]. Warto dodać, że J. Janowski proponuje sposób rozumienia danych jako wyodrębnionych jednostek znaczeniowych, wyrażonych przez zespoły nieprzypadkowo dobranych znaków, składających się na proste charakterystyki obiektów stanów i zdarzeń[51]. Dane rozumiane są również jako wartości, które przechowywane są w bazie, jako zawartości pól danych[52].

Definicja legalna danych została sformułowana w przepisach prawa rangi ustawowej, a dokładnie w ustawie z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia[53]. Z treści art. 2 pkt 4 wynika, że termin dane oznacza litery, wyrazy, cyfry, teksty, liczby, znaki, symbole, obrazy, kombinacje liter, cyfr, liczb, symboli i znaków, zebrane w zbiory o określonej strukturze, dostępne według określonych kryteriów, w tym dane osobowe. W kontekście naukowych definicji danych, można zaryzykować stwierdzenie, że zacytowana definicja legalna pojęcia danych jest niepełna, potrzebuje odpowiedniego dokończenia. Odnosi się wrażenie, że brakuje w niej odniesienia do pojęcia informacji. Trudno bez zastrzeżeń przyjąć, iż o tym, czy coś stanowi dane decyduje to, czy jest zebrane w zbiór o określonej strukturze i czy jest dostępne według określonych kryteriów. Alternatywę dla powyższej definicji legalnej mogłaby potencjalnie stanowić definicja zakresowa o charakterze niepełnym. Wydaje się, że w ujęciu zakresowym poprawne byłoby uznanie, że dane rozumieć należy jako podstawową jednostkę stanowiącą zapis informacji w każdej formie możliwej do odczytania, zinterpretowania, komunikowania lub przetwarzania przez ludzi i urządzenia, w szczególności słowo, znak, liczba, sygnał, obraz, dźwięk, kod.

Ponadto ustawodawca posługuje się terminem danych w tekstach aktów prawnych, konkretyzując ich rodzaj, np. dane statystyczne, dane geologiczne, dane osobowe, bazy

[49] G. Szpor, *Pojęcie informacji a zakres ochrony danych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008, s. 18 i n.
[50] M. Kuraś, *System..., op. cit.,* dostępne na: uci.agh.edu.pl/uczelnia/tad/PSI9/3.rtf.
[51] J. Janowski, *Technologia informacyjna dla prawników i administratywistów*, Warszawa 2009, s. 114-115.
[52] *Ibidem*, s. 118.
[53] T.j. Dz.U. z 2017 r. poz. 1845.

danych. Warto sprawdzić, czy przytoczone powyżej definicje pojęcia dane funkcjonujące na gruncie nauki są w jakikolwiek sposób użyteczne dla polskiego ustawodawcy, przy regulowaniu konkretnych ich rodzajów, jak również, czy ustawodawca traktuje terminy dane i informacje synonimicznie, czy jako odrębne pojęcia.

W treści art. 2 pkt 1a ustawy z dnia z dnia 29 czerwca 1995 r. o statystyce publicznej[54] ustawodawca zdefiniował dane statystyczne. Zgodnie z treścią przepisu, należy je rozumieć jako dane dotyczące zjawisk, zdarzeń, obiektów i działalności podmiotów gospodarki narodowej oraz życia i sytuacji osób fizycznych, w tym dane osobowe, pozyskane bezpośrednio od respondentów albo z systemów informacyjnych administracji publicznej i rejestrów urzędowych, od momentu ich zebrania na potrzeby wykonywania zadań statystyki publicznej. Ze sposobu sformułowania powyższej definicji można wywnioskować, że ustawodawca potraktował (podobnie jak wykazano wcześniej w przypadku definiowania pojęcia informacji), że dane stanowią termin, którego nie ma potrzeby wyjaśniać. Analizując treść tego przepisu, można zauważyć tu błąd *idem per idem*. Ustawodawca skupił się tu nie na istocie danych statystycznych, a na tym czego dotyczą i skąd pochodzą.

Drugi przykład polega na użyciu terminu danych w nieco innym kontekście. W treści art. 2 ust. 1 pkt 1 ustawy z dnia 27 lipca 2001 r. o ochronie baz danych[55] sformułowano definicję bazy danych. Nie chodzi tu o same dane lub ich konkretny rodzaj, ale o całą ich bazę. Zgodnie z treścią przepisu, baza danych oznacza zbiór danych lub jakichkolwiek innych materiałów i elementów zgromadzonych według określonej systematyki lub metody, indywidualnie dostępnych w jakikolwiek sposób, w tym środkami elektronicznymi, wymagający istotnego, co do jakości lub ilości, nakładu inwestycyjnego w celu sporządzenia, weryfikacji lub prezentacji jego zawartości. W tym przypadku również należy stwierdzić, że sposoby rozumienia pojęcia danych wypracowane na gruncie doktryny, nie mają przełożenia na formułowanie przepisów prawa. W powyższej definicji uznającej bazę danych za zbiór danych, zauważalny jest tym razem błąd *ignotum per ignotus* (łac. nieznane przez nieznane).

W szczególności trzeba przyjrzeć się definicji ustawowej danych osobowych, zawartej w treści art. 6 ust. 1 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych

[54] T.j. Dz. U. z 2018 r., poz. 997.
[55] Dz.U. 2001 Nr 128, poz. 1402.

osobowych[56]. Ustawodawca przyjął rozumienie danych osobowych jako wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Definicja ta będzie analizowana szczegółowo w dalszych rozważaniach, jednakże w tym momencie należy zauważyć, że jest ona obarczona błędem definicyjnym *ignotum per ignotus,* ponieważ prawu nie jest znane ani pojęcie danych ani pojęcie informacji. Bez głębszej refleksji można wywnioskować, że w sformułowaniu, iż za dane uważa się informacje, ustawodawca traktuje pojęcie danych i pojęcie informacji na zasadzie synonimów.

Podobnie jak w przypadku poczynionych uwag dotyczących informacji, w porównaniu z powyższymi przykładami, wysoko ocenić należy starania ustawodawcy co do zdefiniowania pojęcia dane geologiczne w treści art. 6 ust. 1 pkt 1 ustawy Prawo geologiczne i górnicze. Warto przypomnieć, że w treści tego aktu prawnego ustawodawca posługuje się zarówno pojęciem danych geologicznych, jak i informacji geologicznej. Dla dostrzeżenia różnicy należy zestawić obie definicje legalne: zgodnie z treścią art. 6 ust. 1 pkt 1 danymi geologicznymi są wyniki bezpośrednich obserwacji i pomiarów uzyskanych w toku prowadzenia prac geologicznych. Natomiast definicję informacji geologicznej ustawodawca zawarł w art. 6 ust. 1 pkt 1 powołanej ustawy, stanowiąc, że informacją geologiczną są dane i próbki geologiczne wraz z wynikami ich przetworzenia i interpretacji, w szczególności przedstawione w dokumentacjach geologicznych oraz zapisane na informatycznych nośnikach danych. Wykładnia językowa obu pojęć sugeruje, że w przypadku danych chodzi tu o czysty zapis wyników, zaś w przypadku informacji istotny jest zapis oraz przetworzenie i interpretacja (proces myślowy). Zatem relacja danych i informacji jest tu jasna, nie polega na zamiennym stosowaniu tych terminów, a na rozróżnieniu ich.

Wydaje się, że podobnie jak w przypadku kwestii definicji informacji, trudno jest poszukiwać formułowania definicji legalnych danych o skonkretyzowanym rodzaju, przy jednoczesnym braku narzędzi umożliwiających skonstruowanie kompleksowej definicji o charakterze ogólnym. Przede wszystkim definicja nie rozwiałaby wszelkich wątpliwości i nie stanowiłaby rozwiązania problemów prawnych.

[56] T.j. Dz. U. z 2016 poz. 922 ze zm., ustawa aktualnie już nie obowiązuje, ale na jej gruncie kształtowała się definicja danych osobowych w polskim porządku prawnym. Dalej jako UODO z 1997 roku.

Podkreślenia w odniesieniu do zagadnienia danych w ogólnym ujęciu wymaga wynikający z analizowanych definicji (przede wszystkim proponowanej przez G. Szpor), ale raczej nie wskazywany bezpośrednio w przepisach prawa wymóg, by dane były utrwalone na fizycznym nośniku. Nie ma przy tym znaczenia jego forma (papierowa, wizyjna, głosowa, elektroniczna). Jest to bardzo istotne dla dalszych rozważań, ponieważ przepisy prawa nie odnoszą się do danych nieutrwalonych np. do nienagrywanych rozmów telefonicznych, tylko do zarejestrowanego głosu na nośniku. Wynika to również z definicji przetwarzania danych osobowych. Każda z otwartego katalogu operacji na danych osobowych może być wykonywana na danych utrwalonych. Należy przy tym pamiętać, że ochronie podlegać będzie nie nośnik danych, a dane utrwalone na nośniku.

Z analizy treści przytoczonych prób definicyjnych pojęcia dane, tak na gruncie aktów obowiązującego prawa jak i na gruncie nauki, wyciągnąć można wniosek, że znaczeniowo jest ono bardzo zbliżone do pojęcia informacji. Cecha bliskoznaczności jest na tyle wyraźna, że bardzo często niełatwo jest określić, co jest daną a co informacją. Problem ten doprowadził do pojawienia się w nauce dwóch koncepcji co do relacji danych i informacji. Pierwsze stanowisko polega na utożsamianiu pojęcia danych z pojęciem informacji[57]. Niejednokrotnie są one używane w sposób zamienny, bez precyzyjnego rozróżnienia[58]. Druga koncepcja polega na rozgraniczaniu obu pojęć i nietraktowaniu ich w sposób synonimiczny. Informacja jest wtedy postrzegana jako proces zachodzący pomiędzy umysłem człowieka, a oddziałującym na niego bodźcem, natomiast dane –jako ten bodziec w różnej postaci[59]. W obrazowym ujęciu można powiedzieć, że dane stanowią niejako surowiec poddawany procesom myślowym, zaś informacja to efekt powstały w wyniku tych procesów, który może stanowić albo efekt finalny, albo może zostać poddany dalszym procesom przetwarzania.

Na podstawie analiz definicji danych i informacji, jak i relacji między tymi pojęciami, można sformułować kilka wniosków. Po pierwsze, nie wszystkie dane stanowią informację. Za informację nie można bowiem uznać takich danych, które nie będą powodowały zmniejszenia niepewności, jak też danych, które nie będą mogły zostać zinterpretowane w oparciu o określony kontekst. Ograniczenia działają również a drugim

[57] Co czyni m.in. K. Napierała, *Prawne aspekty ochrony danych osobowych, przetwarzanych w systemach informatycznych*, Warszawa 1997, s. 13.
[58] M. Grabowski, A. Zając, *Dane, informacja, wiedza – próba definicji*, dostępne na www.uci.agh.edu.pl.
[59] J. Gołaczyński, *Informacja jako przedmiot ochrony*, Prawo Mediów Elektronicznych 1/2004, Legalis 2004.

kierunku, jako że nie każda informacja będzie miała postać danych, które chronione są przez prawo. Wśród poglądów przedstawicieli nauki prawa odnajduje się również stanowiska, że dane powinny mieć charakter informacji, aby były przedmiotem ochrony prawnej, a te same dane niejednokrotnie mogą być źródłem różnych informacji[60], co wydaje się jeszcze bardziej komplikować omawiane zagadnienie, jak również, że posiadanie dostępu do danych nie będzie oznaczało każdorazowo możliwości zapoznania się z treścią zawartych w nich informacji[61].

Zasadnym wydaje się zaaprobowanie koncepcji drugiej, zakładającej rozróżnienie pojęcia danych i informacji. Można powiedzieć, że jest to pogląd większościowy i preferowany przez naukowców reprezentujących różne dyscypliny naukowe, co znalazło wyraz w wypracowaniu koncepcji tzw. hierarchii pojęć poznawczych[62]. Tworzy ją piramida składająca się z czterech poziomów, dla której bazą są dane, następne poziomy to kolejno informacja i wiedza, zaś na szczycie umieszczono mądrość[63].

3. Dane osobowe oraz prawo do ochrony danych osobowych w ujęciu prawa międzynarodowego, prawa Unii Europejskiej i prawa krajowego

3.1. Dane osobowe i prawo do ochrony danych osobowych w świetle aktów prawnych Rady Europy

Ochrona danych osobowych jest przedmiotem regulacji prawnych w dwóch odrębnych europejskich systemach prawnych: Rady Europy oraz Unii Europejskiej. Unia Europejska liczy obecnie 28 państw członkowskich, zaś każde z tych państw jednocześnie jest członkiem Rady Europy. Relacje między obydwoma systemami należy zatem określić jako wzajemne przenikanie się i uzupełnianie regulacji prawnych.

W ramach funkcjonowania Rady Europy, jako sztandarowy akt prawny o kluczowym znaczeniu wymienia się Europejską Konwencję Praw Człowieka

[60] A. Walaszek-Pyzioł, *Regulacja – innowacja w sektorze energetycznym*, Legalis 2013, tak również G. Szpor, G. Sibiga.
[61] J. Gołaczyński, *Informacja..., op. cit*., Legalis 2004.
[62] M. Grabowski, A. Zając, *Dane ..., op. cit.,* s. 5.
[63] Wśród twórców hierarchii pojęć poznawczych wymienia się: T.S. Eliota, H. Clevelanda, M. Cooleya czy M. Zelenego.

i Podstawowych Wolności[64]. W postanowieniach konwencyjnych nie sformułowano definicji danych osobowych, ani nie ukonstytuowano w sposób bezpośredni prawa do ochrony danych osobowych. Jednakże na gruncie porządku prawnego Rady Europy, w orzecznictwie oraz poglądach przedstawicieli nauki prawa powoływana jest treść art. 8 Europejskiej Konwencji Praw Człowieka, zgodnie z którym każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności osób. Na podstawie tego przepisu wywodzi się, że prawo do ochrony przed gromadzeniem i wykorzystywaniem danych osobowych jest częścią prawa do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji[65]. Treść tej regulacji stanowiła fundament do przyjęcia przez Komitet Ministrów Rady Europy szeregu rezolucji dotyczących ochrony danych osobowych, jak również opracowania postanowień Konwencji Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 28 stycznia 1981 roku[66].

Wskazuje się, że chronologicznie pierwszym[67], a także jedynym wiążącym prawnie[68] międzynarodowym aktem prawnym dotyczącym bezpośrednio ochrony danych osobowych jest Konwencja Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 28 stycznia 1981 roku. Należy jednak zauważyć, że o ile Konwencja 108 generalnie weszła w życie w 1985 roku, to z perspektywy Polski, która stała się jej stroną po jej podpisaniu w 1999 roku, datą ratyfikacji i wejścia w życie był dopiero rok 2002. Ten odstęp czasowy uzasadniony jest faktem, że w treści art. 4 Konwencji 108 zastrzeżono obowiązek stron umowy osiągnięcia zgodności prawa wewnętrznego z zasadami ochrony danych wynikającymi z treści Konwencji 108, a osiągnięcie tego celu ma nastąpić do dnia wejścia Konwencji 108 w życie w odniesieniu do danej strony. Konwencyjna definicja danych osobowych

[64] RE, Europejska Konwencja Praw Człowieka, CETS nr 005, 1950. Rzeczpospolita Polska przystąpiła do umowy w 1993 roku.
[65] P. Boillat, M. Kjaerum, *Podręcznik europejskiego prawa o ochronie danych osobowych*, Luksemburg 2014, s. 14.
[66] Dz. U. z 2003 r., nr 3, poz. 25, dalej jako Konwencja 108.
[67] P. Barta, P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2016, s. 4.
[68] P. Boillat, M. Kjaerum, *Podręcznik…, op. cit*., s. 16.

wskazuje, że jest to każda informacja dotycząca osoby fizycznej o określonej tożsamości lub dającej się zidentyfikować. Podejmując próbę analizy tak sformułowanej definicji, można w niej wyróżnić następujące elementy: każda informacja, osoba fizyczna, określona tożsamość, możliwość zidentyfikowania. Pojęcie „każdej informacji" jest niezwykle pojemne treściowo i odnoszą się do niego prowadzone wcześniej rozważania dotyczące informacji. Nie została sprecyzowana forma informacji, źródło jej pozyskania, ani też cel jej przetwarzania. Zakres treściowy zostaje zawężony poprzez kolejne elementy definicji. Każda informacja może oznaczać dane osobowe tylko wtedy, gdy będzie dotyczyła osoby fizycznej. Sprecyzowanie pojęcia każdej informacji ma w takim razie charakter podmiotowy. W konsekwencji tego wywnioskować należy, że ochroną przepisów Konwencji 108 nie będą objęte informacje dotyczące osoby prawnej, osoby zmarłej, czy też informacje o osobie do momentu jej narodzin. Dokonując dalszej analizy, zauważa się kolejne zawężenie poprzez następny element, jakim jest określona tożsamość osoby fizycznej. Można zatem wyciągnąć wniosek, że danymi osobowymi w rozumieniu Konwencji 108 będą takie informacje o osobie fizycznej, które w sposób stosunkowo pewny i jednoznaczny wskazują konkretną osobę, pozwalają wyróżnić ją spośród innych osób. Innymi słowy, informacja ta przypisana jest jednej osobie i na nią nakierowuje, a więc posiadając taką informację, jesteśmy w stanie ustalić kogo ona dotyczy. Jednakże wydaje się, że sformułowanie osoba fizyczna dająca się zidentyfikować, w odróżnieniu od osoby fizycznej o określonej tożsamości, rozumiane może być jako mniej precyzyjne, dające mniej pewności. Informacja dotycząca osoby o określonej tożsamości będzie bezpośrednio i jednoznacznie wskazywać określoną osobę, której tożsamość jest znana uprzednio. Przykładem może być przede wszystkim numer PESEL, który jest numerem niepowtarzalnym i przypisanym każdej jednostce. Natomiast informacja dotycząca osoby dającej się zidentyfikować, będzie informacją o osobie, której tożsamości jeszcze nie znamy oraz która nie samodzielnie i bezpośrednio, ale dopiero po wykonaniu dodatkowych działań, operacji myślowych lub w powiązaniu z innymi informacjami pozwoli na wskazanie, że mowa o jednej konkretnej osobie, tej a nie żadnej innej. Przykładem może być np. adres zameldowania, który stanowi informację w danych okolicznościach umożliwiającą zidentyfikowanie osoby.

Pomimo tego, że celem Konwencji 108 było zapewnienie, aby każdy na obszarze państw członkowskich Rady Europy, bez względu na narodowość, obywatelstwo i miejsce zamieszkania, objęty został jednakową ochroną sfery osobistej, w związku

z przetwarzaniem automatycznym jego danych osobowych[69], to zakres obowiązywania Konwencji jest zróżnicowany. Przewiduje ona minimalny, standardowy poziom ochrony, który może być modyfikowany poprzez jego rozszerzenie przez strony umowy (państwa członkowskie Rady Europy będące jej sygnatariuszami). Zgodnie z treścią art. 3 ust. 1 strony zobowiązały się do jej stosowania do zautomatyzowanych zbiorów danych oraz do automatycznego przetwarzania danych osobowych, zarówno w sektorze publicznym, jak i sektorze prywatnym. Kluczowe znaczenie dla rozważań na gruncie przepisów Konwencji 108 ma sformułowanie „automatycznego przetwarzania danych osobowych". Wyjaśnione zostało ono w treści art. 2 Konwencji jako operacje na danych wykonane w całości lub częściowo za pomocą procedur zautomatyzowanych, takie jak gromadzenie danych, stosowanie do nich operacji logicznych i/lub arytmetycznych, modyfikowanie, usuwanie, wybieranie lub rozpowszechnianie. Ponadto wspomnianym przy regulacji zakresu stosowania Konwencji zbiorem zautomatyzowanym jest każdy zbiór danych będących przedmiotem automatycznego przetwarzania. W treści przepisów nie odnajduje się natomiast wyjaśnienia pojęć „automatyczny" czy „zautomatyzowany". Odwołując się do słownikowego wyjaśnienia tych terminów, można je rozumieć jako „działający samoczynnie, za pomocą odpowiedniego urządzenia"[70]. Wnioskować więc można, że chodzi tu o przetwarzanie za pomocą urządzeń i programów komputerowych, sieci teleinformatycznych, systemów operacyjnych, szeroko rozumianych rozwiązań technologicznych zastępujących pracę fizyczną i intelektualną człowieka.

Konwencja 108, postrzegana jako najwcześniejszy międzynarodowy akt prawny dotyczący ochrony danych osobowych, ma istotne znaczenie dla kształtu systemu prawnej ochrony danych osobowych na gruncie prawa krajowego. Celem przepisów było przede wszystkim skłonienie państw-stron do wdrożenia w ich prawie wewnętrznym środków ochrony o charakterze co najmniej niezbędnym[71]. W tym celu Konwencja 108 ustanowiła podwaliny pod funkcjonujące do chwili obecnej zasady zgodnego z prawem przetwarzania danych osobowych. Wśród zasad tych przedstawiciele nauki prawa wymieniają wyznaczenie zakresu danych szczegółowych, tzw. wrażliwych, wdrożenie odpowiednich środków bezpieczeństwa danych w zautomatyzowanych zbiorach zapobiegających utracie,

[69] J. Sobczak, *Ochrona danych osobowych - standardy unijne i rzeczywistość polska* [w:] J. Jaskiernia (red.), *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka*, Warszawa 2013, s. 485.
[70] www.sjp.pwn.pl
[71] J. Sobczak [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2013, s. 267 i n.

zniszczeniu, udostępnieniu bez podstawy, wprowadzenie systemu sankcji i odszkodowań za naruszenie przepisów dotyczących ochrony danych osobowych, a także zasady: rzetelności, poprawności, odpowiedniej jakości, adekwatności, celowości i ograniczonego czasu przetwarzania danych osobowych[72]. Jednakże z treści art. 9 wynika, że zasady te doznają wyjątków, jeżeli przewiduje to prawo wewnętrzne. Zgodnie z treścią Konwencji odstępstwo od zasady musi stanowić środek konieczny w społeczeństwie demokratycznym oraz opierać się na co najmniej jednej z wymienionych w treści art. 9 podstaw, które podzielić można na podstawy uzasadniające odstępstwo ze względu na dobro publiczne: ochrona państwa, ochrona interesów finansowych państwa, utrzymanie porządku i bezpieczeństwa publicznego, zwalczanie przestępczości; oraz podstawy uzasadniające odstępstwo ze względu na dobro prywatne, jednostkowe: ochrona osoby której dane dotyczą, albo ochrona praw i wolności innych osób. Zauważyć należy, że obie grupy są równoważne, nie przyznano priorytetu żadnej z nich.

W kontekście dotychczasowych rozważań, niezbędnym jest dokonanie analizy zobowiązań umownych stron Konwencji. Można zaproponować ich podział na trzy grupy. Kryterium podziału stanowiłby podmiot bądź obszar, w stosunku do którego dane zobowiązanie się odnosi.

Do pierwszej grupy zaliczyć można zobowiązania państw względem osób, których dane dotyczą. Znalazłby się tu przede wszystkim wywiedziony z treści art. 8 Konwencji 108 obowiązek państwa do zapewnienia każdej osobie prawa do uzyskania informacji o tym, czy jej dane znajdują się w zautomatyzowanym zbiorze danych osobowych, jak również uzyskania informacji o celach utworzenia takiego zbioru. Następnie wskazać można obowiązek uzyskania informacji o tożsamości, miejscu zamieszkania lub siedziby administratora takiego zbioru, obowiązek sprostowania lub usunięcia danych dotyczących tej osoby przetwarzanych z naruszeniem przepisów prawa wewnętrznego, a ponadto obowiązek złożenia skargi w przypadku nieuwzględnienia żądań dotyczących wymienionych praw, w myśl określonych w Konwencji zasad i z uwzględnieniem określonych wyjątków. Ponadto w tej grupie umieścić można by również zobowiązanie państwa wynikające z treści art. 14 dotyczące udzielenia pomocy osobie mieszkającej za granicą w korzystaniu z praw przewidzianych w prawie wewnętrznym, z poszanowaniem postanowień art. 8 Konwencji.

[72] *Ibidem*.

Druga grupa obowiązków dotyczy współpracy między stronami Konwencji, należy zaliczyć do niej następujące zobowiązania: umożliwiania przepływu danych osobowych przez granice (art. 12), czy też udzielania sobie wzajemnej pomocy w celu wprowadzenia w życie Konwencji (art. 13).

W ostatniej grupie umieścić można zobowiązania państwa w zakresie ukształtowania regulacji prawa wewnętrznego dotyczących ochrony danych osobowych. Wśród nich wyróżnić można obowiązek: podjęcia kroków w celu osiągnięcia zgodności przepisów prawa wewnętrznego z przepisami Konwencji (art. 4), obowiązek podjęcia odpowiednich środków bezpieczeństwa w odniesieniu do danych osobowych zgromadzonych w zbiorach zautomatyzowanych (art. 7), jak również wprowadzenia sankcji karnych i odszkodowania za naruszenie prawa wewnętrznego (art. 10).

Postanowienia Konwencji 108 przyznają stosunkowo sporą samodzielność prawu wewnętrznemu każdego z państw będących stronami Konwencji. Przewidują one wiele wyjątków od przyjętych w jej treści zasad (art. 9). Odstąpienie od postanowień umownych dopuszczalne jest jako środek konieczny w społeczeństwie demokratycznym dla ochrony państwa, interesów finansowych, utrzymania porządku i bezpieczeństwa publicznego, zwalczania przestępczości oraz ochrony osoby, której dane dotyczą, praw lub wolności innych osób. Warto również podkreślić, że postanowienia tego aktu prawnego mają odniesienie tylko do sfery publicznoprawnej. Obywatele państw, które ratyfikowały Konwencję 108 nie wywodzą z jej przepisów praw ani obowiązków, gdyż bezpośrednie skutki prawne wywoływane są jedynie po stronie państw[73]. Wspomnieć należy, że zasięg obowiązywania postanowień Konwencji 108 wykracza poza Unię Europejską, przy czym 45 z 46 stron to państwa należące do Rady Europy. W 2013 roku do Konwencji przystąpił Urugwaj, zaś zaproszenie do przystąpienia otrzymało Maroko[74]. Tekst Konwencji z biegiem czasu uzupełniany był szeregiem protokołów dodatkowych.

3.2. Dane osobowe i prawo do ochrony danych osobowych na tle prawa Unii Europejskiej

Przenosząc rozważania na grunt prawa Unii Europejskiej, analizie pod kątem regulacji dotyczących danych osobowych należy poddać zarówno prawo pierwotne, jak

[73] Tak również M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 55.
[74] P. Boillat, M. Kjaerum, *Podręcznik..., op. cit*., s. 17.

i prawo wtórne UE. Trzeba zdawać sobie sprawę z wpływu, jaki na kształt przedmiotowych regulacji, w szczególności prawa wtórnego, wywierały postanowienia Konwencji 108. Na podstawie analizy poglądów przedstawicieli nauki prawa można interpretować, że system prawny Rady Europy był asumptem do zainteresowania Unii Europejskiej problematyką danych osobowych. Podnosi się, że początkowo w systemie prawnym Unii Europejskiej nie dostrzegano problemu ochrony danych, Komisja Europejska zalecała państwom członkowskim ratyfikację Konwencji 108, zaś w prawie Unii Europejskiej regulacje pojawiły się dopiero w latach dziewięćdziesiątych. Mając na uwadze fakt, że Konwencję ratyfikowały wszystkie państwa członkowskie Unii Europejskiej, a ona sama również stała się stroną tej umowy, prawo Unii Europejskiej nie mogło być sprzeczne z postanowieniami Konwencji 108[75]. Dlatego też, w związku z unijną reformą prawa w zakresie ochrony danych osobowych, która nastąpiła w 2018 roku wraz z wejściem 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)[76], treść Konwencji 108 jest aktualnie modernizowana. Celem zmian jej przepisów jest z jednej strony dostosowanie ich treści do wyzwań technologicznych XXI wieku, a z drugiej strony zapewnienie spójności dwóch systemów prawa ochrony danych osobowych w Europie[77]. Z powyższych uwag wywnioskować można wzajemne przenikanie się systemu Rady Europy i systemu Unii Europejskiej w obszarze ochrony danych osobowych, jak również dbałość o wzajemną zgodność i aktualność regulacji obu europejskich systemów prawnych.

W odniesieniu do prawa Unii Europejskiej przede wszystkim należy wskazać że kwestia danych osobowych ujęta została w treści art. 16 Traktatu o Funkcjonowaniu Unii Europejskiej[78], który stanowi, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących. Ponadto zgodnie z treścią tego przepisu prawodawca zobowiązał Parlament Europejski i Radę do określenia w drodze zwykłej procedury prawodawczej stosownych zasad dotyczących ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez Państwa Członkowskie

[75] *Ibidem*, s. 19.
[76] Dz. Urz. UE.L 2016 Nr 119, str. 1 ze zm., dalej powoływane będzie jako RODO.
[77] http://www.giodo.gov.pl/pl/1520286/9964.
[78] Traktat o Funkcjonowaniu Unii Europejskiej z 26 października 2012 roku, Dz. Urz. UE C nr 326, s. 47 (TFUE)

w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Z literalnego brzmienia art. 16 Traktatu wynika przede wszystkim pojawienie się w prawie Unii Europejskiej prawa do ochrony danych osobowych, przysługującego każdej osobie. Regulacja ta ma charakter generalny, prawodawca nie sformułował żadnych gwarancji tego prawa ani jego ograniczeń. Ponadto z treści tej wynika przekazanie ogólnej kompetencji do uregulowania problematyki ochrony danych osobowych Parlamentowi Europejskiemu i Radzie w drodze ustanowienia aktu prawa wtórnego. Prawodawca unijny w treści art. 39 Traktatu o Unii Europejskiej[79] nadał generalny kierunek regulacji i zapowiedział dalsze kroki legislacyjne, które powierzył wskazanym organom Unii Europejskiej[80].

W 2009 roku na mocy Traktatu z Lizbony, do prawa pierwotnego została włączona Karta Praw Podstawowych Unii Europejskiej[81], co oznaczało, że waga tego aktu została zrównana z wagą traktatów. W treści art. 8 Karty zapisano, że każdy ma prawo do ochrony danych osobowych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Przestrzeganie tych zasad podlega kontroli niezależnego organu. Z powyższej regulacji wynika, że w treści Karty Praw Podstawowych sformułowane zostały najistotniejsze regulacje dotyczące ochrony danych osobowych. Mianowicie dane osobowe i ich ochrona zostały zaliczone do kategorii podstawowych praw człowieka. Takim prawem jest też dostęp do zebranych danych i dokonywanie ich sprostowania, przez osobę, której te dane dotyczą. Ponadto sformułowano tu wymogi dotyczące przetwarzania danych osobowych w sposób legalny. Wśród nich wskazać należy rzetelność przetwarzania, przetwarzanie w określonych celach, przetwarzanie danych za zgodą osoby zainteresowanej bądź na innej podstawie, która musi być uzasadniona i przewidziana ustawą.

Analizując prawo do ochrony danych osobowych na gruncie Karty Praw Podstawowych Unii Europejskiej, błędem byłoby niezwrócenie uwagi na fakt,

[79] Traktat o Unii Europejskiej, Dz. Urz. UE.C 2012 Nr 326, str. 13 (TUE).
[80] Art. 39 TUE: Zgodnie z artykułem 16 Traktatu o funkcjonowaniu Unii Europejskiej i na zasadzie odstępstwa od jego ustępu 2, Rada przyjmuje decyzję określającą zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania niniejszego rozdziału oraz zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów.
[81] Karta Praw Podstawowych Unii Europejskiej (Dz. Urz. UE C 326 z 26.10.2012, s. 391), dalej jako Karta.

że gwarantowane na mocy jej przepisów prawa nie mają charakteru absolutnego. Wniosek taki wypływa z treści art. 52 Karty, dotyczącego zakresu i wykładni praw i zasad, a konkretniej z treści ustępu 1, gdzie ujęto kwestię ograniczeń w korzystaniu z praw i wolności uznanych w Karcie. Odnosząc ten przepis do prawa do ochrony danych osobowych, prawodawca unijny dopuszcza możliwość ograniczenia tego prawa, o ile ograniczenie to będzie spełniało określone warunki: przewidziane zostanie ustawą, będzie szanowało istotę tego prawa, może być wprowadzone jedynie w takich sytuacjach, gdy będzie to konieczne oraz uzasadnione celami interesu ogólnego uznawanymi przez Unię lub potrzebami ochrony i wolności innych osób. Przepis art. 52 ust. 1 Karty w zestawieniu z przepisem art. 8 Karty interpretować można w ten sposób, że Karta Praw Podstawowych Unii Europejskiej gwarantuje każdemu prawo do ochrony danych osobowych, co stanowi zasadę, natomiast w wyjątkowych przypadkach dopuszczalne jest ograniczenie tego prawa, przy czym przypadki te są enumeratywnie wymienione w treści Karty (art. 52).

Pojawia się tu potrzeba skonfrontowania sposobu uregulowania prawa do ochrony danych osobowych w Karcie Praw Podstawowych Unii Europejskiej i w Europejskiej Konwencji Praw Człowieka. Wyraźnego podkreślenia wymaga fakt, że Europejska Konwencja weszła w życie w 1953 roku, zaś Karta w 2009 roku, a 56 lat w kontekście danych osobowych stanowi niemałą różnicę. O ile w Konwencji nie odnajdujemy bezpośredniego ukonstytuowania prawa do ochrony danych osobowych, a wywodzimy je z prawa do poszanowania życia prywatnego i rodzinnego (art. 8), to w treści Karty mamy już do czynienia z osobnym prawem, wyodrębnionym z prawa do prywatności (art. 7), uregulowanym w osobnym artykule (art. 8). Z perspektywy powyższych rozważań istotna wydaje się treść art. 52 ust. 3 Karty, który ustanawia wzajemną relację pomiędzy obydwoma omawianymi aktami prawnymi w zakresie regulacji gwarantowanych w nich praw człowieka. Zgodnie z nim, w zakresie, w jakim Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności, ich znaczenie i zakres są takie same jak praw przyznanych przez tę Konwencję. Niniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę. Rodzi się przy tym pytanie o to, czy prawo Unii przyznaje prawu do ochrony danych osobowych takie samo znaczenie i zakres jak Konwencja, czy jednak przyznaje większą ochronę. Bardziej przekonujący okazuje się drugi wariant. Argumentem przemawiającym za takim poglądem jest już sam fakt, że w treści Konwencji nie ma bezpośrednich regulacji dotyczących danych osobowych, zaś

prawo do ich ochrony należy wyinterpretować z szerszego zakresowo prawa do prywatności, co czyni przede wszystkim Europejski Trybunał Praw Człowieka na gruncie orzecznictwa[82]. W Karcie Praw Podstawowych Unii Europejskiej zagadnieniu danych osobowych, a dokładnie prawu do ich ochrony, poświęcono osobny artykuł, *de facto* konstytuując to podstawowe prawo człowieka na gruncie prawodawstwa Unii Europejskiej. Zgodnie z literalnym brzmieniem przepisu, obejmuje ono ochronę danych osobowych, dostęp do zebranych danych i dokonywanie ich sprostowania. Ponadto, ochrona tego prawa została zapewniona poprzez wyraźnie wskazane warunki i zasady, przy spełnieniu których dane mogą być przetwarzane (rzetelność przetwarzania, określenie celu przetwarzania, uzyskanie zgody na przetwarzanie od osoby zainteresowanej, zaistnienie innej uzasadnionej podstawy przewidzianej w przepisach prawa). Po trzecie, o większej ochronie świadczy również przepis przewidujący kontrolę przestrzegania zasad przetwarzania danych sprawowaną przez niezależny organ. W kontekście regulacji zawartych w obu wymienionych aktach prawnych można potwierdzić współdziałanie systemu prawnego Rady Europy i Unii Europejskiej.

Podsumowując, w konstrukcji uregulowania w Karcie Praw Podstawowych Unii Europejskiej prawa do ochrony danych osobowych jako odrębnego prawa, wyróżnić można następujące elementy: normy materialne, prawa osoby fizycznej oraz niezależny nadzór nad przestrzeganiem zasad przetwarzania danych osobowych[83]. Z ogólnych zasad wykładni określonych w treści Karty wywnioskować należy brak absolutnego charakteru tego prawa (może ono doznawać ograniczeń ze względu na inne wartości) oraz przypadki, w których może ono być ograniczane. Taki kształt regulacji można ocenić jako szeroki i nadający ogólny kierunek, ale jednocześnie wyczerpujący w stosunku do rangi aktu. Dzięki temu prawodawca unijny pozostawia szerokie pole do działania legislacyjnego na poziomie państw członkowskich, orzecznictwu i praktyce (w tym działalności organów państwowych), jak również nauce prawa.

Na gruncie prawa wtórnego Unii Europejskiej kwestię ochrony danych osobowych reguluje szereg dyrektyw. Najważniejsze z nich są wymienione na liście źródeł prawa Unii Europejskiej na stronie internetowej Generalnego Inspektora Danych Osobowych (od 25

[82] Np. Wyrok Europejskiego Trybunału Praw Człowieka z dnia 4 grudnia 2008 r. 30562/04, Legalis nr 114022.
[83] M. Sakowska-Baryła, *Prawo..., op. cit.*, s. 60.

maja 2018 roku Prezesa Urzędu Ochrony Danych Osobowych)[84]. W prowadzonych badaniach koniecznym jest odniesienie się do przepisów, które już nie obowiązują, ale przez wiele lat stanowiły fundament ochrony danych osobowych i bazę dla nowych regulacji prawnych. Przedmiotem prowadzonych analiz będzie więc obowiązująca do dnia 25 maja 2018 roku Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[85], z uwagi na fakt, że ma ona ogólny i ramowy charakter w porównaniu z pozostałymi dyrektywami, dotyczącymi konkretnych zagadnień, takich jak usługi łączności elektronicznej, ochrona prywatności i komunikacji elektronicznej czy też zapobieganie przestępczości. Przepisy Dyrektywy 95/46/WE były implementowane do polskiego porządku prawnego za pomocą przepisów ustawy o ochronie danych osobowych z 1997 roku. Akt ten zawierał najważniejsze kwestie, jak definicje podstawowych terminów odnoszących się do dziedziny danych osobowych, ustalał zasady przetwarzania danych osobowych, a także warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą[86].

Prawodawca unijny zawarł definicję danych osobowych w treści art. 2 lit. a Dyrektywy 95/46/WE. Zgodnie z nią termin dane osobowe oznaczał wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"); osoba możliwa do identyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. To kluczowe pojęcie z Dyrektywy 95/46/WE zostało odwzorowane na gruncie polskich przepisów prawa w treści art. 6 UODO z 1997 roku[87].

[84] http://www.giodo.gov.pl/568/j/pl/, wypunktowano następujące akty: Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady WE, Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady, Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady WE, Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady WE, Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady WE oraz Dyrektywa 2016/680 (UE) Parlamentu Europejskiego i Rady.

[85] Dz.Urz.UE.L 1995 Nr 281, str. 31, dalej jako Dyrektywa 95/46/WE.

[86] http://www.giodo.gov.pl/568/id_art/603/j/pl/.

[87] Dlatego też dla porządku w układzie treści niniejszej dysertacji, rozważania nad definicją danych osobowych będą odnosiły się jednocześnie do obu powołanych aktów prawa, jednakże w pierwszej kolejności do regulacji prawnych powiązanych z zagadnieniem danych osobowych i prawa do ich ochrony, które zostały zawarte w Konstytucji Rzeczpospolitej Polskiej z 2 kwietnia 1997 roku.

3.3. Dane osobowe i prawo do ochrony danych osobowych w świetle Konstytucji Rzeczypospolitej Polskiej z 1997 roku oraz orzeczeń Trybunału Konstytucyjnego

Już na wstępie podkreślenia wymaga fakt, że ustawodawca nie posługuje się w treści Ustawy Zasadniczej pojęciem danych osobowych, nie tylko go nie definiuje, ale w ogóle go nie używa. Nie istnieje na gruncie Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku[88] przepis, który stanowiłby odpowiednik treści art. 8 Karty Praw Podstawowych Unii Europejskiej, nie mamy bowiem wśród przepisów rozdziału II Ustawy Zasadniczej wyraźnej konstytucyjnej regulacji mówiącej, że każdy ma prawo do ochrony danych osobowych, które go dotyczą. Nie oznacza to jednak, że Konstytucja RP nie obejmuje danych osobowych ochroną prawną, czy też nie gwarantuje prawa do ochrony danych osobowych. Przeciwnie, co potwierdzone zostało w literaturze przedmiotu[89], ochrona danych osobowych stanowi wartość konstytucyjną.

Mając na uwadze fakt, że bezspornym w nauce prawa i orzecznictwie jest to, że prawo do ochrony danych osobowych jest jednym z aspektów prawa do prywatności[90], należy zauważyć, że w przepisach konstytucyjnych prawo do ochrony danych osobowych nie zostało przez ustawodawcę sformułowane wprost, a wywodzone jest z zasady autonomii informacyjnej jednostki. Zgodnie z treścią art. 51 ust. 1 Konstytucji RP nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby. Nie wolno przy tym zapomnieć o tym, że źródłem zarówno prawa do prywatności jak i prawa do ochrony danych osobowych jest, zgodnie z art. 30 Konstytucji RP, przyrodzona i niezbywalna godność człowieka, jako źródło wszystkich praw i wolności człowieka i obywatela[91]. W kontekście tego przepisu warto odnieść się do orzecznictwa Trybunału Konstytucyjnego. W uzasadnieniu do wyroku z dnia 12 grudnia 2005 roku[92] Trybunał podkreślił związek prawa do prywatności i prawa do ochrony danych osobowych z godnością człowieka, jako wartości współistotnych. W innym

[88] Dz.U. 1997 Nr 78, poz. 483, dalej jako Konstytucja RP.
[89] Tak R. Piotrowski, [w:] A. Mednis (red.), *Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016, Legalis.
[90] Dla przykładu: M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Legalis; K. Motyka, *Prawo do prywatności*, Zeszyty Naukowe Akademii Podlaskiej w Siedlcach 2010, Nr 85, s. 25–35; M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 23–24.
[91] L. Bosek stoi na stanowisku, że godność ludzka obok wolności, równości i państwa prawnego jest jednym z najbardziej abstrakcyjnych pojęć prawnych. Autor rozpatruje ją w kategorii zasady prawnej, wartości konstytucyjnej, prawo podmiotowe, zasady porządku publicznego, konstytucyjnej klauzuli generalnej. Zob. szerzej: L. Bosek, *Gwarancje godności ludzkiej*, Warszawa 2012, s. 144 i n.
[92] K 32/04, Legalis nr 71527.

wyroku Trybunał wskazał rodowód prawa do ochrony danych osobowych wynikający z godności człowieka, stwierdzając jednoznacznie, że ochrona prywatności i autonomii informacyjnej jest konsekwencją ochrony przyrodzonej i niezbywalnej godności człowieka (art. 30 Konstytucji)[93].

Zakres treściowy artykułu 47 Konstytucji RP przyjmuje, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Formułuje on zasadę poszanowania życia prywatnego jednostki, zasadę samostanowienia i autonomii jednostki, ma charakter bez wątpienia ogólny i jest bardzo pojemny. Wskazuje to, że przepis ten powinien być traktowany jako punkt wyjścia dla wielu gwarancji konstytucyjnych, takich jak: ochrona przed niedobrowolnymi eksperymentami medycznymi, gwarancja wolności i nietykalności osobistej, gwarancja miru domowego, gwarancja autonomii informacyjnej, gwarancja swobody poruszania, czy gwarancja wolności religijnej[94]. Innymi słowy, można traktować art. 47 Konstytucji jako uregulowanie prawa do prywatności w szerokim znaczeniu, zaś pozostałe wymienione przepisy jako elementy tego prawa, jego emanacje. Wśród przedstawicieli nauki prawa panuje zasadniczo zgoda co do traktowania tego przepisu jako *lex generalis* w odniesieniu do innych regulacji konstytucyjnych gwarantujących ochronę aspektów prywatności[95]. Nietrudno zauważyć, że treść art. 47 Konstytucji RP wyraźnie koresponduje z przepisami aktów prawnych międzynarodowych oraz aktów prawnych Unii Europejskiej, m.in.: art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych[96] art. 8 Europejskiej Konwencji Praw Człowieka i Podstawowych Wolności, art. 7 Karty Praw Podstawowych Unii Europejskiej. Wymienione akty miały znaczący wpływ na kształt regulacji odnoszącej się do szeroko rozumianego prawa do prywatności w Konstytucji RP, stanowiły inspirację i kierunek do aktualnego sformułowania przepisu w art. 47.

Treść art. 47 Konstytucji RP ma bardzo istotne funkcje. Przede wszystkim ma on na celu zapewnienie jak najwyższego standardu ochrony prywatności (życia prywatnego,

[93] Uzasadnienie do wyroku TK z dnia 30 lipca 2014 roku, K 23/11, (Dz.U. z 2014 r. poz. 1055).
[94] M. Wild, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016, Legalis.
[95] Potwierdza to B. Banaszak, *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012, Legalis.
[96] Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (Dz. U. z 1977 r. nr 38 poz. 167).

rodzinnego, czci i dobrego imienia oraz decydowania o swoim życiu osobistym)[97]. Ponadto buduje kontekst dla regulacji dotyczących szczegółowych gwarancji konstytucyjnych, takich jak wymienione powyżej. Stanowi kierunek interpretacji regulacji zarówno konstytucyjnych, jak i zawartych w innych przepisach, które dotyczą sfery życia prywatnego jednostki, jest wskazówką przy wykładni tych przepisów[98]. Warto dodać, że w sferze prawa prywatnego duże znaczenie ma regulacja prawna zawarta w treści art. 23 Kodeksu cywilnego[99] dotycząca dóbr osobistych.

Z tej perspektywy należy rozważyć zagadnienie zakresu podmiotowego art. 47 Konstytucji RP. Jeśli chodzi o stronę uprawnioną, literalne brzmienie przepisu wskazuje, że podmiotem wymienionym w nich praw jest każdy. Z analizy literatury przedmiotu wynika stanowisko, że z uwagi na fakt, że do posiadania życia prywatnego, rodzinnego, czci i dobrego imienia zdolne są jedynie osoby fizyczne, przyjąć należy, że jest to prawo dotyczące wszystkich osób fizycznych[100]. Natomiast alternatywny pogląd poddaje powyższe pod wątpliwość, sugerując, że stosowane jest tu uproszczenie, a prawo do prywatności może być również rozciągane na jednostki organizacyjne[101]. Jako argument przemawiający za takim podejściem wskazywany jest wyrok Trybunału Konstytucyjnego z 24 czerwca 1997 roku[102] (opierającego swoje stanowisko na stanie prawnym na chwilę przed wejściem w życie Konstytucji RP z 1997 roku), gdzie przyznano podatnikowi, którym może być nie tylko osoba fizyczna, prawo do prywatności określonej działalności. Trudno znaleźć racjonalne podstawy do ograniczenia zakresu podmiotowego art. 47 Konstytucji RP jedynie do osób fizycznych. Jednak należy wziąć pod uwagę, że o ile cześć i dobre imię może odnosić się do pełnego spektrum podmiotów – osób fizycznych, prawnych oraz jednostek organizacyjnych nieposiadających osobowości prawnej, jak np. do fundacji czy stowarzyszeń, to życie prywatne, rodzinne i osobiste jest na tyle ściśle związane z człowiekiem, że rzeczywiście trudno byłoby rozciągnąć prawo do ich ochrony również na inne podmioty.

---

[97] Szersze uwagi na temat prawa do prywatności odnaleźć można w poglądach wyrażonych przez J. Sieńczyło-Chlabicz. Jednym z analizowanych przez tę autorkę aspektów prywatności jest prywatność jako prawo do kontroli nad ujawnianiem informacji o charakterze osobistym. Prywatny charakter informacji warunkowany jest tym, że musi ona dotyczyć konkretnej osoby i odnosić się do spraw objętych sferą prywatności. Zob. szerzej: J. Sieńczyło-Chlabicz, *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Zakamycze 2006, s. 87.
[98] M. Wild, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP*..., op. cit, Legalis.
[99] t.j. Dz.U. z 2018 r. poz. 1025 ze zm.
[100] B. Banaszak, *Konstytucja*..., op. cit., Legalis.
[101] M. Wild, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP*..., op. cit, Legalis.
[102] K 21/96, OTK 1997, Nr 2, poz. 23.

Funkcjonują też podmioty zobowiązane powołaną regulacją prawną do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o życiu osobistym. W kontekście przepisu w art. 51 Konstytucji bardzo duże znaczenie ma fakt, iż obowiązek respektowania prawa do ochrony informacji dotyczących osoby, które skorelowane jest z prawem do prywatności, nie jest skierowany do bliżej określonego podmiotu czy też grupy podmiotów, np. do organów władzy publicznej. Oznacza to, że w sposób bierny do ochrony zobowiązany jest *de facto* każdy podmiot prawa. Od władzy publicznej natomiast oczekuje się ochrony w sposób aktywny. Stanowisko to znajduje potwierdzenie wśród poglądów przedstawicieli nauki prawa, którzy zgodnie twierdzą, że jednostka może domagać się od władzy publicznej, by zapewniono jej efektywną ochronę wartości określonych treści art. 47 Konstytucji RP[103].

Przenosząc punkt rozważań z przepisu ogólnego (art. 47 Konstytucji RP) na przepis szczegółowy (art. 51 Konstytucji RP), w pierwszej kolejności zauważyć trzeba, że w doktrynie i w dorobku judykatury przyjęto, że treść tego przepisu ma dwa główne zadania. Po pierwsze, ma gwarantować prawo do prywatności w aspekcie ochrony danych osobowych, a po drugie, konkretyzować prawo do prywatności w aspektach proceduralnych[104]. Można w poglądach reprezentantów nauki prawa znaleźć również odmienne stanowisko, zgodnie z którym prawo do prywatności i prawo do ochrony danych osobowych podlegają reżimom wzajemnie niezależnym, a między regulacjami tymi zachodzi stosunek krzyżowania[105]. Takie rozumowanie prowadziłoby jednak do osłabienia prawa do ochrony danych osobowych poprzez nadanie mu odrębnego statusu[106], a poza tym jest to odmienne stanowisko w stosunku do wyrażanego niejednokrotnie przez Trybunał Konstytucyjny. W związku z tym należy zgodzić się z poglądem, że treść art. 51 Konstytucji RP uzupełnia regulację zawartą w treści art. 47 i ustanawia jego gwarancje w aspekcie ochrony danych osobowych, co potwierdza Trybunał Konstytucyjny, wskazując, że prawo do prywatności, statuowane w art. 47,

[103] M. Wild, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP*..., op. cit, Legalis, B. Banaszak, *Konstytucja*..., *op. cit*., Legalis.
[104] Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r., U 5/97, Legalis nr 10436.
[105] W ten sposób autorzy Komentarza: J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 151.
[106] J. Rzucidło, *Prawo do prywatności i ochrona danych osobowych*, tekst dostępny na http://www.repozytorium.uni.wroc.pl/Content/52920/09_Jakub_Rzucidlo.pdf.

zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51[107].

W powołanym wyroku Trybunału wyjaśniono, że zasadę autonomii informacyjnej należy rozumieć jako prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów. Pojęcie autonomii informacyjnej obejmuje swoim zakresem zarówno dane o charakterze personalnym, jak również te, które dotyczą majątku i sfery ekonomicznej jednostki[108]. Przedstawiciele doktryny upatrują istoty autonomii informacyjnej w prawie do decydowania o ujawnianiu informacji dotyczących swojej osoby innym podmiotom, prawie do sprawowania kontroli nad takimi informacjami[109], albo też w stwierdzeniu, że jednostka powinna posiadać uprawnienie do kontrolowania treści i obiegu dotyczących jej informacji, anonimowości, poprawiania swoich danych i aktualizowania ich[110], jak również w „pozostawieniu każdej osobie swobody w określeniu sfery dostępności dla innych wiedzy o sobie", jako że jest to „dopełnienie, a zarazem najistotniejszy przejaw prawa do prywatności" [111].

Na konstrukcję art. 51 Konstytucji RP składa się pięć gwarancji w formie nakazów, uprawnień i zakazów. Każda z nich ma charakter samodzielny i odrębny, o czym świadczy przede wszystkim zróżnicowany zakres podmiotowy i przedmiotowy regulacji. Co istotne, dokonując szerszej analizy rozdziału II Konstytucji RP, można dojść do wniosku, że regulacja art. 51 nie wypełnia całkowicie zakresu autonomii informacyjnej jednostki, innymi słowy, nie tylko treść art. 51 odnosi się do tego prawa. Prawo do autonomii informacyjnej konstytuuje również wolność i ochrona tajemnicy komunikowania się (art. 49), wolność sumienia i religii w aspekcie ujawniania światopoglądu, przekonań religijnych lub wyznania (art. 53 ust. 7).

W kontekście treści wyżej wskazanych przepisów Konstytucji, pojawia się potrzeba uporządkowania terminologicznego w zakresie pojęć prawo do ochrony danych osobowych i prawa do autonomii informacyjnej. Analizując poglądy przedstawicieli nauki prawa i judykatury można odnieść wrażenie, że traktowane są one niejednokrotnie jako

[107] Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r., U 5/97, Legalis nr 10436.
[108] Wyrok z dnia 17 czerwca 2008, K 8/04, http://trybunal.gov.pl/fileadmin/content/omowienia/K_8_04_PL.pdf
[109] M. Wild, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP..., op. cit*, Legalis.
[110] M. Sakowska-Baryła, *Prawo…, op. cit.,* s. 31.
[111] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 127.

synonimy. Można tu jednak mieć wątpliwości, czy poprawne jest zamienne stosowanie tych terminów. Z uwagi na fakt, iż w dostępnych źródłach nie pojawiają się poglądy wskazujące na konieczność rozgraniczania wskazanych pojęć, można przyjąć za poprawne posługiwanie się pojęciem prawa do autonomii informacyjnej i prawa do ochrony danych osobowych na zasadzie synonimów. Warto jednak dla większej ścisłości posługiwać się tym terminem, który bliżej związany jest z danym aktem prawnym. Skoro ustawodawca w treści Konstytucji RP nie używa sformułowania danych osobowych, a informacji dotyczących osoby, wydaje się właściwszym stosowanie w odniesieniu do rozważań nad regulacjami konstytucyjnymi pojęcia autonomii informacyjnej. Natomiast jeśli chodzi o analizy przepisów prawa rangi ustawowej (ustawy o ochronie danych osobowych), odpowiedniejszym terminem wydaje się być prawo do ochrony danych osobowych, jako zgodne z przyjętą konwencją terminologii ustawowej. Ustawodawca nie posługiwał się w treści ustawy o ochronie danych osobowych pojęciem informacji poza użyciem go w celu wyjaśnienia definicji danych osobowych w art. 6 UODO z 1997 r.

Jak zauważono już wcześniej, regulacja z art. 51 Konstytucji RP nie zawiera pojęcia danych osobowych. Ustawodawca posłużył się tu terminem informacji dotyczących osoby. W oparciu o prowadzone wcześniej rozważania na temat relacji pojęć danych i informacji, na gruncie Konstytucji RP należy traktować dane osobowe jako informacje dotyczące osoby. W konsekwencji pozwala to chronić dane osobowe zarówno za pomocą przepisów rangi ustawowej, jak i konstytucyjnej. Wydaje się, że sformułowanie konstytucyjne jest szersze niż treść definicji legalnej danych osobowych wynikającej z treści art. 6 UODO z 1997 r. Wskazuje na to chociażby zawarte w ustawie podmiotowe ograniczenie odnoszenia terminu danych osobowych jedynie do osób fizycznych. Trudno byłoby bowiem uzasadnić, że gwarancje z art. 51 Konstytucji RP nie będą odnosiły się do dóbr osób zmarłych, co *de facto* dawałoby możliwość władzom publicznym np. nieskrępowanego gromadzenia i udostępniania informacji o osobie już nieżyjącej, pomimo iż nie jest to niezbędne w demokratycznym państwie prawnym (art. 51 ust. 2 Konstytucji RP). Mogłoby to stać w sprzeczności z ochroną dóbr osób zmarłych, prawem do kultu pamięci o osobie zmarłej, którego elementem byłaby ochrona czci i prywatności osoby zmarłej. Relację między pojęciami dane osobowe i informacje o osobie można uporządkować w ten sposób, iż informacje o osobie mają szerszy zakres treściowy, zaś dane osobowe to termin o węższym zakresie. Innymi słowy, dane osobowe zawsze będą

informacją dotyczącą osoby w ujęciu konstytucyjnym, natomiast nie wszystkie informacje o osobie będą stanowiły dane osobowe.

Istotne z punktu widzenia prowadzonych tu rozważań jest ustalenie relacji pomiędzy przepisami art. 47 i 51 Konstytucji RP. W konsekwencji tego, że przyjęty został pogląd o ogólnym charakterze normy zawartej w treści art. 47 Konstytucji RP (ochrona prawa do prywatności), należy również przychylić się do stanowisk powszechnie reprezentowanych w nauce prawa, iż prawo do autonomii informacyjnej stanowiące przedmiot regulacji art. 51 Konstytucji RP jest jednym z aspektów prawa do prywatności[112]. Pogląd, iż prawo do prywatności obejmuje swoim zakresem prawo do ochrony danych dotyczących jednostki, został wyrażony również w orzecznictwie Trybunału Konstytucyjnego[113]. Relację obu artykułów można zatem uznać jako funkcjonowanie przepisu ogólnego (art. 47) i przepisu szczególnego (art. 51). Uzasadnia to wniosek, iż jeśli regulacje szczególne nie gwarantują w pełnym zakresie ochrony prywatności, z pomocą przyjść może *lex generalis*. Jeśli chodzi o prawo do prywatności w aspekcie ochrony danych osobowych, to jest ono gwarantowane w treści art. 51 Konstytucji RP. Niemniej jednak dany stan faktyczny dotyczyć może np. banku, który w swoich procedurach uzależnia zrealizowanie określonej transakcji od uzyskania od klienta (osoby fizycznej) informacji dotyczących jego osoby, bez podstawy prawnej rangi ustawowej. Należy przy tym zauważyć, że zastosowania w tej sytuacji nie znajdzie art. 51 Konstytucji RP, ze względu na fakt, że autonomia informacyjna gwarantowana przez ten przepis odnosi się wyłącznie do obowiązków obciążających organy władzy publicznej. Zgodzić się należy ze stanowiskiem, iż ograniczenie to nie oznacza, że w stosunkach horyzontalnych wskutek wnioskowania *a contrario* z art. 51 Konstytucji RP, jednostka będzie pozbawiona ochrony[114]. W takich sytuacjach, gdy stan faktyczny nie spełnia przesłanek określonych w treści art. 51 Konstytucji RP, ochrona powinna być konstruowana na podstawie art. 47 Konstytucji RP. Świadczy o tym fakt, że z uwagi na szerszy zakres (w powyższym przypadku – podmiotowy), wynikające z niego gwarancje przyznają jednostkom ochronę w zakresie nieobjętym innymi przepisami[115]. Ponadto, zestawiając oba artykuły, już na pierwszy rzut oka dostrzega się, iż treść art. 47 ma

[112] D. Ossowska-Salamonowicz, *Ochrona danych osobowych w działalności dziennikarskiej*, Olsztyn 2015, s. 78.
[113] Orzeczenie Trybunału Konstytucyjnego z dnia 24 czerwca 1997 r., K 21/96, Legalis nr 10365.
[114] M. Wild, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP..., op. cit*., Legalis.
[115] *Ibidem*.

charakter ogólnego uprawnienia, natomiast treść art. 51 skupia uwagę na bardziej szczegółowych i precyzyjnych zakazach (ust. 1 i 2) oraz uprawnieniach (ust. 3 i 4).

Kluczowym jest tu pytanie, czy można powiedzieć, że powołany przepis ustanawia konstytucyjne prawo do ochrony danych osobowych. Przepis art. 51 Konstytucji RP został umiejscowiony w jej II rozdziale o nazwie „Wolności, prawa i obowiązki człowieka i obywatela". Jest on, jak już wcześniej wskazano, bardzo ściśle związany z konstytucyjnym prawem do prywatności sformułowanym literalnie w treści art. 47 Konstytucji RP. Jednakże bardziej właściwym byłoby stwierdzenie, że w treści art. 51 Ustawy zasadniczej ustawodawca statuuje na gruncie prawa krajowego zasadę autonomii informacyjnej i formułuje jej gwarancje. Z zasady tej wynika prawo do ochrony danych osobowych, które wprost wyrażone zostało w przepisie rangi ustawowej (art. 1 ust.1 UODO z 1997 r.). Uzasadnia to odmienna redakcja przepisu art. 51 wyrażającego zespół pięciu różnych gwarancji autonomii informacyjnej jednostki, od sformułowania innych praw konstytucyjnych w treści rozdziału II Konstytucji RP, np. art. 45 ust.1, zgodnie z którym każdy ma prawo do sprawiedliwego i jawnego rozpatrzenia sprawy, czy art. 53 ust. 1: zgodnie z którym każdemu zapewnia się wolność sumienia i religii. Nie mamy tu zatem wyraźnie przyznanego prawa do ochrony danych osobowych (na gruncie Konstytucji RP nie pada sformułowanie dane osobowe), jak uczynił to prawodawca unijny w treści art. 8 Karty Praw Podstawowych Unii Europejskiej. Ustawodawca krajowy zdecydował się ustanowić generalną zasadę autonomii informacyjnej jednostki oraz szereg jej gwarancji, zaś faktyczne prawo do ochrony danych osobowych i instrumenty tej ochrony pozostawiono do skonkretyzowania ustawodawstwu zwykłemu. Należy przy tym pamiętać o szerokim zakresie treściowym prawa do prywatności wynikającego na gruncie prawa krajowego z treści art. 47 Konstytucji RP, którego jednym z aspektów jest prawo do ochrony danych osobowych, jak również o przyjęciu w orzecznictwie Trybunału Konstytucyjnego, że prawo do prywatności w aspekcie ochrony danych osobowych jest gwarantowane przez art. 51 Konstytucji RP, konkretyzujący aspekty proceduralne[116].

[116]Wyrok Trybunału Konstytucyjnego z dnia 24 czerwca 1997, K 21/96, Legalis nr 10365, wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998, U 5/97, Legalis nr 10436.

3.4. Definicja danych osobowych w podstawowych aktach prawnych regulujących ich ochronę

W praktyce często niełatwe jest rozróżnianie czy określona informacja o charakterze osobowym odpowiada, czy nie odpowiada kryteriom definicji legalnej danych osobowych. Niejednokrotnie zdarza się, że określoną informację traktuje się jako pozbawioną cech danych osobowych i nie przyznaje się jej ochrony należnej danym osobowym, albo z drugiej strony, przyznaje się jej status danych osobowych pomimo tego, że *de facto* nie odpowiada ona ustawowym kryteriom danych osobowych.

Rozważania nad aktualnym rozumieniem pojęcia danych osobowych rozpocząć trzeba od wyjaśnienia, że definicja danych osobowych w Rozporządzeniu Parlamentu Europejskiego i Rady EU 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46/WE[117], konstruowana była na bazie definicji zawartej w Dyrektywie 95/46/WE i w ogólnym kształcie pokrywa się z nią, a tym samym z definicją danych osobowych zawartą w treści art. 6 UODO z 1997 r. Przywołać i poddać weryfikacji należy stanowisko wyrażone w literaturze, zgodnie z którym „RODO nie zrywa ze szkieletem pojęciowym prawa ochrony danych osobowych, jaki ukształtował się na gruncie Dyrektywy 95/46/WE i ustawy o ochronie danych osobowych z 29 sierpnia 1997 r.[118]. Wręcz przeciwnie, podstawowe definicje nie ulegają zmianie – oczywiście rozwój technologiczny i potrzeba stałego nadążania prawa za technologią sprawiają, że tych definicji w RODO znajdziemy znacznie więcej, niż mieliśmy dotychczas w polskim systemie prawnym na gruncie ustawy o ochronie danych osobowych. Nie oznacza to jednak istotnej jakościowo rewolucji”[119]. Zgodnie z powyższym szczegółowej analizie należy w pierwszej kolejności poddać przepisy obowiązujące do 25 maja 2018 roku[120].

[117] Dz. Urz. UE. L Nr 119, str. 1 ze zm., dalej RODO.
[118] T.j. Dz.U. z 2016 r. poz. 922 ze zm.
[119] P. Litwiński [w:] D. Szostek (red.) *Bezpieczeństwo danych i IT w kancelarii prawnej radcowskiej/adwokackiej/notarialnej/komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej*, Warszawa 2018, LEGALIS.
[120] Należy pamiętać, że RODO uchyliło Dyrektywę 95/46/WE. Natomiast polska ustawa o ochronie danych osobowych utraciła moc z dniem 25.05.2018 r. z wyjątkiem art. 1, art. 2, art. 3 ust. 1, art. 4–7, art. 14–22, art. 23–28, art. 31 oraz rozdziałów 4, 5 i 7, które zachowują moc w odniesieniu do przetwarzania danych osobowych w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, prowadzenia postępowań w sprawach dotyczących tych czynów oraz wykonywania orzeczeń w nich wydanych, kar porządkowych i środków przymusu w zakresie określonym w przepisach stanowiących podstawę działania służb i organów uprawnionych do realizacji zadań w tym zakresie, w terminie do dnia wejścia w życie przepisów wdrażających dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez

Przepisy ustawy o ochronie danych osobowych implementowały do polskiego porządku prawnego Dyrektywę 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. W związku z tym powołać należy definicję, którą prawodawca unijny sformułował w treści art. 2 Dyrektywy 95/46/WE, zgodnie z którym termin dane osobowe oznaczał wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą"); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość. Na podstawie tej definicji zbudowano legalną definicję danych osobowych na gruncie polskiego porządku prawnego. Ustawodawca sformułował ją w treści art. 6 UODO z 1997 r. W rozumieniu tego przepisu za dane osobowe uważa się wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Z uwagi na fakt, że definicja wynikająca z Dyrektywy 95/46/WE literalnie pokrywa się z brzmieniem definicji danych osobowych w polskiej ustawie, dalsze analizy pojęcia danych osobowych będą odnosiły się jednocześnie do obu wskazanych aktów prawnych.

Należy zwrócić uwagę, że brzmienie definicji danych osobowych w UODO z 1997 r. przed jej nowelizacją w 2001 roku[121], różniło się od treści art. 2 Dyrektywy 95/46/WE. Za dane osobowe uznawano każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby. Ponadto warto zauważyć, że definicja, która została przyjęta przez ustawodawcę, różniła się od treści art. 5 rządowego projektu ustawy

właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119 z 04.05.2016, str. 89). Do dnia zakończenia prac nad rozprawą przepisy wdrażające dyrektywę nie weszły w życie, ale trwają prace legislacyjne nad nową ustawą.

[121] Dz. U. Nr 133, poz. 883.

o ochronie danych osobowych[122]. Proponowana regulacja była bardziej zbliżona do sformułowania zawartego w Dyrektywie 95/46/WE[123]. Zestawiając definicję danych osobowych wynikającą z Dyrektywy 95/46/WE z definicją ujętą w brzmieniu polskiej ustawy, która w tej wersji obowiązywała od 1998 roku do 2001 roku, można odnieść wrażenie, że ich zakresy nie pokrywały się. Definicja ustawowa była węższa od tej, którą zamieszczono w przepisie Dyrektywy 95/46/WE. Wynikało z niej, że status danych osobowych należało przyznawać jedynie informacjom dotyczącym osoby fizycznej, pozwalającym na określenie tożsamości tej osoby. Poza zakresem ochrony pozostawały zatem informacje dotyczące już zidentyfikowanej osoby, jak również informacje, które bezpośrednio lub pośrednio pozwalały ustalić tożsamość osoby. Innymi słowy, gdy Dyrektywa 95/46/WE za dane osobowe uznawała wszelkie informacje na temat osoby fizycznej, polska ustawa przyznawała to miano jedynie informacjom umożliwiającym ustalenie tożsamości osoby fizycznej[124]. W konsekwencji tego, że ustawa nie może zawężać ochrony gwarantowanej przepisami Dyrektywy 95/46/WE, podjęte zostały działania w celu zmiany przepisów ustawowych. W uzasadnieniu do projektu z dnia 6 lipca 2001 roku[125] przekonywano, że w celu dostosowania polskich przepisów o ochronie danych osobowych do Dyrektywy95/46/WE, ochroną wynikającą z przepisów ustawy należy objąć nie tylko każdą informację dotyczącą osoby fizycznej, pozwalającą na określenie tożsamości tej osoby, ale również wszelkie informacje dotyczące osoby fizycznej lub pozwalające na identyfikację jej tożsamości bezpośrednio lub pośrednio. Z dniem 3 października 2001 roku weszła w życie ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych[126]. Rozszerzono zakres ochrony prawnej na wszelkie informacje dotyczące osoby fizycznej lub pozwalające na identyfikację jej tożsamości bezpośrednio lub pośrednio. Zrównano zakresy definicji danych osobowych w Dyrektywie 95/46/WE i polskiej ustawie[127]. Na marginesie można

[122] Rządowy projekt ustawy o ochronie danych osobowych (druk nr 1928 z dn. 1996-10-03), źródło: http://orka.sejm.gov.pl/proc2.nsf/projekty/1928_p.htm
[123] W rozumieniu niniejszej ustawy za dane osobowe uważa się każdą informację dotyczącą osoby fizycznej, której tożsamość jest określona lub daje się określić bezpośrednio lub pośrednio, zwłaszcza na podstawie numeru ewidencyjnego, numeru identyfikacji podatkowej, jednej lub więcej cech szczególnych tej osoby, takich jak: cechy fizyczne, fizjologiczne, psychiczne, umysłowe, kulturowe, społeczne lub majątkowe.
[124] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona..., op. cit.,* s. 59, 94 i n.
[125] Druk nr 3171, http://orka.sejm.gov.pl/Rejestrd.nsf/wgdruku/3171/$file/3171.pdf.
[126] Dz. U. nr 100 poz. 1087.
[127] Wprowadzono definicję legalną pojęcia danych osobowych funkcjonującą niezmiennie przez kolejne 17 lat (do momentu wejścia w życie Rozporządzenia 2016/679).

dodać, że okazuje się, że w ustawodawstwie funkcjonują też inne definicje danych osobowych, są one jednak przyjmowane na potrzeby tylko konkretnych ustaw[128].

Analizując konstrukcję definicji danych osobowych, która obowiązywała po nowelizacji ustawy, czyli od 2001 roku, zaakcentowania wymaga to, że ustawodawca wskazuje na *wszelkie* informacje (w pierwotnym brzmieniu ustawy z 1997 toku – *każda* informacja). Świadczyć to może o tym, że ustawodawca miał w swych intencjach ustanowienie szerokiego zakresu pojęcia danych osobowych, które wymaga szerokiej interpretacji[129]. Autorzy jednego z komentarzy do ustawy o ochronie danych osobowych prezentują pogląd, że zwrot „wszelkie informacje" służy pokazaniu, że chodzi o informacje odnoszące się do każdego aspektu osoby, w tym stosunków osobistych, rzeczowych, życia zawodowego, prywatnego, wykształcenia, wiedzy, cech charakteru[130]. Określenie „wszelkie" może być odnoszone zarówno do treści informacji, jak i jej formy.

W odniesieniu do treści informacji, trzeba stwierdzić, że o tym, czy należy przyznać jej status danych osobowych i w konsekwencji tego odpowiednią ochronę, nie decydują inne czynniki poza spełnieniem przesłanek wynikających z przepisu prawa. Zgodnie z nimi informacja dotyczy osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania. Innymi słowy, bez znaczenia dla takiej kwalifikacji pozostaje to, czy informacja jest prawdziwa czy nieprawdziwa, czy dotyczy kwestii zaistniałych, aktualnie istniejących lub mających zaistnieć dopiero w przyszłości, czy jest ona zrozumiała ogólnie czy tylko w ograniczonym zakresie podmiotowym (dla niektórych) i przedmiotowym (np.

[128] Definicja danych osobowych funkcjonuje również na gruncie ustawy z dnia 27 maja 2004 roku o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (t.j. Dz. U. z 2016 r. poz. 1896), gdzie w treści art. 2 pkt 33, gdzie przez dane osobowe rozumie się imiona i nazwisko, datę i miejsce urodzenia, adres zamieszkania, a w przypadku obywateli Rzeczypospolitej Polskiej także numer PESEL. Ponadto, z treści ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz.U. z 2016 r. poz. 1068) również wynika wskazówka do interpretacji przedmiotowego pojęcia. W treści art. 35 b znajduje się katalog danych danych osobowych, do których przetwarzania dla celów statystycznych upoważnione się służby statystyki publicznej: imiona i nazwisko; data i miejsce urodzenia; płeć; numer PESEL; obywatelstwo; narodowość, pochodzenie etniczne; pochodzenie rasowe; wyznanie, przynależność do kościoła lub związku wyznaniowego; stan cywilny; data zawarcia małżeństwa; data ustania małżeństwa; wykształcenie; zawód; rodzaj miejsca pracy lub nauki; numer identyfikacji podatkowej; stan zdrowia; stopień niezdolności do pracy, posiadanie orzeczenia o niepełnosprawności, stopień niepełnosprawności; tytuł ubezpieczenia z wyłączeniem części kodu objętej tajemnicą; adres zamieszkania lub adres miejsca pobytu; adres do korespondencji; adres poczty elektronicznej; numer telefonu.

[129] Tak w swojej opinii wypowiedziała się Grupa Robocza ds. ochrony danych powołana na mocy art. 29 Dyrektywy 95/46/WE (niezależny europejski organ doradczy w zakresie ochrony danych i prywatności) – Opinia 4/2007 w sprawie pojęcia danych osobowych WP 136, dalej jako: Opinia 4/2007. Zgodnie z treścią art. 94 RODO odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy 95/46/WE, należy traktować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej rozporządzeniem.

[130] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…*, *op. cit.*, s. 304.

po wykonaniu określonych działań, w zestawieniu z innymi informacjami, wynikająca z przetwarzania innych informacji). Ponadto nie jest istotne to, czy jest ona powszechnie znana, opublikowana, ogólnie dostępna, czy ujawniona tylko w ograniczonym zakresie lub w ogóle nie ujawniona[131]. Jeśli chodzi o formę informacji (sposób jej wyrażenia, nośnik), sytuacja kształtuje się podobnie. Dla ustalenia, że mamy do czynienia z danymi osobowymi nie ma znaczenia forma przedmiotowej informacji. Może być to informacja alfabetyczna, liczbowa, szyfrowa, graficzna, fotograficzna, dźwiękowa, obraz ruchomy. Istotne jest, by informacja była zapisana na nośniku, np. papierze, na nośniku informatycznym (pendrive, płyta, kaseta wideo, taśma nagraniowa), w pamięci komputera, może być też częścią dokumentu elektronicznego, zorganizowanej bazy danych albo też cechą zachowania czy organizmu człowieka (biometria)[132]. Można na tej podstawie powiedzieć, że brak ustalonego w prawie znaczenia pojęcia informacja nie oddziałuje negatywnie na rozstrzyganie, czym coś stanowi dane osobowe czy nie, ponieważ przy tak szerokiej interpretacji „wszelkich informacji" można przewidywać, że w kategorii tej może mieścić się praktycznie wszystko.

Kolejnym punktem poddanym analizie jest sformułowanie „dotyczące osoby fizycznej". Rozumieć to można jako relację zachodzącą pomiędzy informacją a osobą fizyczną[133], polegającą na powiązaniu określonej informacji z osobą, przypisaniu jej do osoby[134]. O ile ustalenie istnienia takiej relacji wydaje się nieskomplikowanym zabiegiem, to zdarzają się sytuacje budzące wątpliwości, czy dana informacja dotyczy osoby, czy tylko przedmiotu. Przykładem ilustrującym ten problem może być przedstawiona w Opinii 4/2007 wątpliwość co do charakteru informacji, jaką jest wartość nieruchomości[135]. Na początku nasuwa się wniosek, że jest to informacja dotycząca przedmiotu a nie osoby, w konsekwencji czego przepisy o ochronie danych osobowych nie znajdą tu zastosowania. Jednakże rozważyć trzeba by to, w jakim celu informacja ta będzie wykorzystana. Jeśli tylko np. dla zobrazowania kształtowania się cen nieruchomości na określonym obszarze, to powyższy wniosek jest prawidłowy. Jeśli natomiast będzie to informacja zawarta

[131] W ten sposób wypowiadają się również J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona..., op. cit.,* s. 304.
[132] Opinia Grupy Roboczej art. 29, 4/2007 s. 7-8.
[133] W Opinii Grupy Roboczej art. 29, 4/2007 stwierdzono, że informacja dotyczy osoby, jeżeli jest ona na temat tej osoby.
[134] Podobne stwierdzenie zawiera *Dokument roboczy na temat kwestii z zakresu ochrony danych związanych z technologią RFID*, tekst w języku angielskim dostępny na: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm: Dane dotyczą osoby, jeżeli odnoszą się do tożsamości, cech lub zachowania danej osoby lub też jeśli informacje te determinują lub też wpływają na sposób traktowania lub ocenę danej osoby.
[135] Opinia 4/2007, s. 9.

w oświadczeniu majątkowym osoby czy też będzie uwzględniana np. do ustalenia jej zobowiązań podatkowych, to należy uznać, że informacja ta dotyczy właściciela nieruchomości i może spełniać ustawowe kryteria danych osobowych. Na podstawie tych spostrzeżeń można wywnioskować, że dla oceny, czy dana informacja dotyczy osoby fizycznej, należy rozpatrzeć nie tylko samą treść informacji, ale również cały kontekst jej przetwarzania, np. jaki jest jej cel czy też jaki skutek ma odnieść. W związku z tym kwalifikacja powinna następować każdorazowo w danym stanie faktycznym, z uwzględnieniem okoliczności konkretnego przypadku, w tym możliwości administratora danych[136].

Z literalnego brzmienia przepisów (zarówno UODO z 1997 r., jak i Dyrektywy 95/46/WE) wynikało, że informacja, aby mogła zyskać status danej osobowej, musi dotyczyć osoby fizycznej. To osoba fizyczna jest podmiotem danych osobowych i ich ochrony. Pozostawiając poza zakresem rozważań szczegółowe analizy pojęcia osoby fizycznej prowadzone na gruncie prawa cywilnego[137], należy przyjąć pogląd powszechnie wyrażany w nauce prawa, że przepisy dotyczące ochrony danych osobowych dotyczą wyłącznie osób żyjących. Taka teza argumentowana jest tym, że w prawie przyjęta została konstrukcja aktywnej realizacji praw przez osobę, której dane dotyczą, co *de facto* może być dokonywane jedynie przez osobę żyjącą[138]. W konsekwencji takiego przyjęcia poza regulacją przepisów o ochronie danych osobowych pozostał szeroki krąg podmiotów (w tym osoby prawne, spółki, fundacje, stowarzyszenia).

Wśród poglądów przedstawicieli nauki prawa panuje zgoda co do poglądu, że informacje, które dotyczą dziecka poczętego (np. zdjęcia USG) aż do momentu jego urodzenia będą podlegały ochronie gwarantowanej ustawą o ochronie danych osobowych, ale tylko jako dane osobowe jego matki (wyjątkowo ojca), a nie samego dziecka[139].

Z zakresu pojęcia danych osobowych wyłączone są informacje dotyczące osób zmarłych. Wynika to w naturalny sposób z faktu, że nie są one osobami fizycznymi,

---

[136] A. Drozd, *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2008, s. 54.

[137] Szerzej zob. A. Stelmachowski, *Zarys teorii prawa cywilnego*, Warszawa 1998, s. 156 i n., oraz komentarze do art. 8 i następnych Kodeksu Cywilnego (np. Komentarze pod redakcją E. Gniewka, M. Frasa, K. Pietrzykowskiego, K. Osajdy), jak również *System Prawa Prywatnego tom I* pod red. M. Safjana.

[138] P. Barta, P. Litwiński, *Ustawa..., op. cit.*, s.77.

[139] A. Drozd, *Ustawa…*, *op. cit.*, s. 50. Poza zakresem rozważań pozostawić należy, czy w przypadku nienarodzonego dziecka chodzi tylko o okres ciąży, czy też o długotrwałe procesy związane z kwestią zamrożonych embrionów, ponieważ jest to przedmiot szczegółowych uregulowań dotyczących technik prokreacji.

w związku z tym przepisy o ochronie danych osobowych nie będą miały do nich zastosowania. Na interesującą kwestię zwróciła uwagę Grupa Robocza art. 29[140]. Według jej stanowiska informacje dotyczące osób zmarłych niejednokrotnie korzystają z ochrony, jaką przyznaje się danym osobowym z tego względu, że w trakcie przetwarzania danych po prostu nie wiadomo, że dotyczą one osoby już nieżyjącej (dla przykładu – administrator nie aktualizuje wystarczająco często przetwarzanych danych i np. wysyła korespondencję na adres osoby, która już nie żyje). Jeśli administrator danych spełnia nałożone na niego obowiązki związane z zabezpieczaniem danych, to zdarza się, że nie ma świadomości, że określona osoba nie żyje i jej dane będące elementem większego zbioru (np. baza klientów) nadal faktycznie podlegają ochronie na mocy przepisów o ochronie danych osobowych, pomimo że utraciły ten status[141]. Na marginesie warto dodać, że poza śmiercią byt prawny osoby fizycznej może zostać zakończony również w drodze uznania za zmarłego (art. 29 i n. Kodeksu cywilnego, a także Kodeksu postępowania cywilnego[142]).

Podsumowując, należy stwierdzić, że z zakresu podmiotowego definicji danych osobowych wyłączone są osoby nieżyjące, o których informacje co do zasady nie są chronione przepisami o ochronie danych osobowych. Jednakże należy mieć na uwadze, że sytuacje z życia codziennego mogą kreować pewne wyjątki od tej zasady. W nauce prawa bardzo wyraźnie wskazuje się, że od zasady, że danymi osobowymi mogą być tylko dane osoby żyjącej, wyjątkiem są takie dane, które choć dotyczą osób zmarłych, to jednocześnie mogą być odniesione do osób żyjących[143]. Taka sytuacja dotyczy np. informacji o chorobie genetycznej czy cechach dziedzicznych.

Językowa wykładnia definicji legalnej danych osobowych pozwala wywnioskować, że informacje dotyczące osób prawnych (oraz jednostek organizacyjnych nieposiadających osobowości prawnej) nie wypełniają przesłanek ustawowych, które umożliwiłyby ich zakwalifikowanie do kategorii danych osobowych. Wątpliwości co do

[140] Opinia 4/2007, s. 22.
[141] *Ibidem*, s. 23. W treści Opinii 4/2007 zwrócono także uwagę na możliwość, jaką posiadają ustawodawcy krajowi państw członkowskich, co do rozszerzenia zasięgu regulacji krajowych w stosunku do Dyrektywy 95/46/WE. O ile istnieje uzasadniony interes i nie wyklucza tego przepis prawa Unii Europejskiej, można objąć regulacją przepisów o ochronie danych osobowych również informacje dotyczące osób zmarłych.
[142] T.j. Dz.U. z 2018 r. poz. 1360 ze zm. Analizując treść art. 516 Kodeksu postępowania cywilnego, należy wywnioskować, że z chwilą uprawomocnienia się postanowienia sądu w przedmiocie uznania za zmarłego lub też stwierdzenia zgonu, informacje o osobie, której orzeczenie dotyczy, nie stanowią już danych osobowych. Tak m.in. T. Szewc [w:] S. Hoc, T. Szewc, *Ochrona danych osobowych i informacji niejawnych*, Warszawa 2014, s. 4.
[143] K. Kaźmierczak, P. Litwiński [w:] D. Dörre-Kolasa (red.), *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2017, Legalis.

przyjęcia modelu ochrony danych osobowych wyłączającego poza jej zakres informacje dotyczące osób prawnych, nie pozostawiało również sformułowanie art. 2 Dyrektywy 95/46/WE. Definicja legalna danych osobowych nie obejmuje informacji dotyczących takich podmiotów jak stowarzyszenia, fundacje, spółki handlowe, korporacje, organizacje stanowiące ugrupowania osób fizycznych[144]. W konsekwencji tego nie istnieją podstawy do uznawania za dane osobowe i co za tym idzie - do stosowania przepisów o ochronie danych osobowych, w stosunku do tych jednostek, nawet w drodze wnioskowania *per analogiam*. Takie rozwiązanie jest uzasadnione dostatecznie, przede wszystkim z tego względu, że prawo do ochrony danych osobowych jest emanacją prawa do prywatności jako prawa człowieka. Jednakże wyłączając z zakresu podmiotowego definicji danych osobowych inne podmioty prawa niż osoby fizyczne, nie można pominąć bardzo istotnej uwagi. Informacje o innych podmiotach, bez względu na formę prawną w jakiej występują, będą podlegać ochronie „wynikającej z sektorowych tajemnic profesjonalnych, np. tajemnicy bankowej, ubezpieczeniowej, adwokackiej, skarbowej, przedsiębiorstwa"[145].

Aspekt podmiotowy definicji danych osobowych wymaga również poświęcenia uwagi osobom fizycznym prowadzącym działalność gospodarczą. W tym przypadku założenia polskiego ustawodawcy, jak i poglądy wyrażane w orzecznictwie i nauce prawa, nie były od początku ukształtowane w sposób jednolity i wciąż budzą kontrowersje. Faktem jest, że definicja danych osobowych obejmuje swoim zakresem informacje dotyczące osób fizycznych, ale okazuje się, że ta zasada nie jest pozbawiona wyjątków. Sytuacja osób fizycznych prowadzących działalność gospodarczą na przestrzeni lat funkcjonowania ustawy o ochronie danych osobowych zmieniała się, w związku z czym warto prześledzić chronologicznie proces kształtowania się obowiązujących regulacji w odniesieniu do tych podmiotów. Do dnia 30 grudnia 2011 roku obowiązywała ustawa z dnia 19 listopada 1999 roku Prawo działalności gospodarczej[146]. W art. 7a ust. 2 zawarto przepis, zgodnie z którym ewidencja działalności gospodarczej jest jawna i dane osobowe w niej zawarte nie podlegają przepisom ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. Przepis ten został zastosowany m.in. przez Naczelny Sąd Administracyjny w wyroku z dnia 28 listopada 2002 roku[147], gdzie postanowiono, że w przypadku gdy przedsiębiorca objął zakresem danych indywidualnych dotyczących

[144] M. Sakowska-Baryła, *Prawo…, op. cit.*, s. 115.
[145] M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej po reformie. Komentarz do Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2016, s. 40.
[146] Dz.U. 1999 Nr 101, poz. 1178.
[147] II SA 3389/01, Legalis nr 99136.

działalności gospodarczej swoje dane osobowe, w sytuacji gdy dane te pokrywają się, nie może on jako osoba fizyczna domagać się ochrony swoich danych osobowych, bo wtedy są one wykorzystywane nie jako dane osobowe, lecz jako dane działalności gospodarczej. W związku z decyzją o utożsamieniu tych danych, przedsiębiorca godzi się na szersze ich ujawnianie i słabszą ochronę. W 2004 roku uchwalono ustawę z dnia 2 lipca 2004 roku o swobodzie działalności gospodarczej[148], która nie regulowała kwestii ochrony danych osobowych osoby fizycznej prowadzącej działalność gospodarczą. Z dniem 19 maja 2016 roku znowelizowano wspomnianą ustawę poprzez dodanie art. 39b, zgodnie z którym do jawnych danych i informacji udostępnianych przez CEIDG co do zasady nie stosuje się przepisów ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[149]. Wydaje się wobec tego, że informacje dotyczące przedsiębiorców mogły stanowić dane osobowe, ale dane ujawnione w Centralnej Ewidencji i Informacji o Działalności Gospodarczej nie korzystały z ochrony gwarantowanej ustawą o ochronie danych osobowych (poza wskazanymi wyjątkami). Natomiast do przetwarzania danych osobowych przedsiębiorców, które nie zostały zawarte w CEIDG (np. nr telefonu, nr rachunku bankowego przedsiębiorcy, jego wynagrodzenie) była stosowana ustawa o ochronie danych osobowych w całości[150]. Przepis art. 39b ustawy o swobodzie działalności gospodarczej należało ocenić jako ułatwienie w aspekcie przetwarzania danych osobowych przedsiębiorców.

Trzeba tu podkreślić, że ustawa o swobodzie działalności gospodarczej utraciła moc z dniem wejścia w życie ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców[151]. Nie dostrzega się w nowych przepisach regulacji, która stanowiłaby kontynuację wyłączenia stosowania przepisów RODO w odniesieniu do przedsiębiorców funkcjonujących w formie jednoosobowej działalności gospodarczej[152]. Ponadto RODO również nie zawiera takiego wyłączenia, jak art. 39a ustawy o swobodzie działalności gospodarczej i aktualnie osoby fizyczne prowadzące działalność gospodarczą traktowane

[148] Dz. U. nr 173, poz. 1807.
[149] Z wyjątkiem przepisów art. 14-19a i art. 21-22a oraz rozdziału 5 tej ustawy (w zakresie zabezpieczenia danych czy też realizowania przez GIODO kontroli w stosunku do tych danych).
[150] P. Kowalik, D. Wociór [w:] D. Wociór (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa 2016, Legalis.
[151] Dz.U. z 2018 r. poz. 646.
[152] Zgodnie ustawą Prawo przedsiębiorców w odniesieniu do przedsiębiorców należy uwzględniać przepisy o ochronie danych osobowych, czego przykładem jest treść art. 43 ust. 4: Rejestry działalności regulowanej są jawne. Dane z rejestrów dotyczące firmy przedsiębiorcy oraz jego numeru identyfikacji podatkowej (NIP) są udostępniane w sieci teleinformatycznej. Organ może udostępnić w sieci teleinformatycznej także inne dane, z uwzględnieniem przepisów o ochronie danych osobowych.

są tak samo jak osoby fizyczne niebędące przedsiębiorcami. Ponadto w literaturze stwierdzono, że według RODO przetwarzanie danych osób ujętych w CEIDG jest objęte takimi samymi wymogami, jak przetwarzanie danych osób fizycznych. RODO nie różnicuje poziomu ochrony danych osób fizycznych wykonujących i niewykonujących działalności gospodarczej[153]. W stosunku do poprzedniego stanu prawnego jest to znacząca zmiana.

Warto zauważyć, że poza wspomnianymi wyłączeniami z zakresu podmiotowego pojęcia danych osobowych, które *de facto* wynikają z ustalonego zakresu pojęcia osoby fizycznej, nie ma innych, dodatkowych wyłączeń. Oznacza to, że dla kwalifikacji informacji jako danej osobowej bez znaczenia pozostają takie aspekty osoby jak status prawny, obywatelstwo i miejsce zamieszkania, posiadanie zdolności do czynności prawnych czy też praw publicznych[154].

Przechodząc do trzeciego elementu konstrukcyjnego definicji danych osobowych, można powiedzieć, że w treści art. 6 UODO z 1997 r. ustawodawca w sposób na pierwszy rzut oka niebudzący wątpliwości wyjaśniał, że osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne. Z powołanego przepisu wynikało, że przez identyfikowanie osoby rozumiane jest określenie tożsamości osoby. Należy przyjąć, że określenie to może być rozumiane jako wskazanie konkretnej osoby na podstawie cech o charakterze unikalnym i odróżniających ją od innych osób. Wywnioskować można, że sposób bezpośredni oznaczać mógłby sposób wskazujący wprost, natomiast pośredni - np. wymagający dokładniejszej analizy, uzupełnienia, połączenia z innymi informacjami. W dalszej kolejności ustawodawca wskazał narzędzia umożliwiające identyfikację osoby. Uczynił to jednakże tylko ogólnie poprzez otwarty katalog sposobów („w szczególności"), wśród których wyróżnił powołanie się na numer identyfikacyjny czy też jeden lub kilka specyficznych czynników. Ustawodawca nie sprecyzował, o jakich czynnikach mowa, nie podał żadnego przykładu takich czynników, jedynie wyjaśnił, że mają one określać cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne osoby. Wydaje

[153] M. Czaplińska, *Informacje z CEIDG jako dane osobowe* [w:] ABI-EXPERT 1/2018, dostępne również na stronie internetowej http://www.abi-expert.pl/wydania/styczen-marzec-2018/art,1969,zasady-informowania.html.
[154] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit,* s. 309.

się, że jako numer indentyfikacyjny rozumieć można np. numer PESEL, serię i numer dowodu tożsamości. Natomiast specyficznymi czynnikami określającymi wymienione cechy osoby mogą być np. imię i nazwisko, kolor skóry, linie papilarne, stanowisko i wynagrodzenie. Motyw 26 preambuły Dyrektywy 95/46/WE stanowił, że w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator danych lub inna osoba w celu zidentyfikowania owej osoby. Należy zatem mieć na uwadze kontekst zmieniającej się rzeczywistości, w tym takie jej aspekty jak postęp cywilizacyjny, nowoczesne technologie, i wiążący się z tym coraz łatwiejszy dostęp do danych osobowych, coraz mniej kontrolowany ich przepływ, a w konsekwencji – zagrożenia dla prywatności.

Warta odnotowania jest jeszcze uwaga, która pozostaje w dalszym ciągu aktualna po rozpoczęciu bezpośredniego stosowania RODO. Ustawodawca w treści ustępu 2 art.6 UODO, ani też prawodawca w treści art. 4 pkt 1 RODO, nie poświęcili uwagi pojęciu osoby zidentyfikowanej, a jedynie osoby możliwej do zidentyfikowania. Trzeba przychylić się do poglądu, zgodnie z którym informacja dotyczy osoby zidentyfikowanej wtedy, gdy istnieje obiektywna możliwość powiązania informacji z osobą bez podjęcia innych działań składających się na proces identyfikacji[155].

Na podstawie powyższych analiz można wyciągnąć wniosek, że informacjom o charakterze osobowym może zostać przyznany status danych osobowych w dwóch momentach w odniesieniu do procesu identyfikacji osoby fizycznej. Po pierwsze, określone informacje mogą stanowić dane osobowe z uwagi na fakt, że wcześniej nastąpiła identyfikacja osoby i w związku z tym informacje te dotyczą już skonkretyzowanej osoby (identyfikacja jako proces uprzedni). Po drugie, informacje mogą być uznane za dane osobowe dlatego, że dzięki nim możliwa jest identyfikacja osoby (identyfikacja jako proces następczy). Innymi słowy, informacja ma charakter osobowy jeśli wiemy, kogo dotyczy bądź jeśli nie wiemy ale możemy to ustalić[156].

Na potrzeby prowadzonych rozważań dodatkowy element konstrukcji legalnej definicji danych osobowych, który choć już nie występuje na gruncie przepisów RODO, to wymaga analizy z uwagi na to, że stanowi znaczącą zmianę w podejściu do definicji danych osobowych, dalej powoływany będzie jako ograniczenie nadmiernych kosztów,

[155] P. Litwiński, *Pojęcie danych osobowych w rozporządzeniu ogólnym o ochronie danych osobowych*, [w:] *Informacja w administracji publicznej* 2017 nr 3, s. 4.
[156] A. Mednis, *Ustawa*…, *op. cit*., s. 21 i n.

czasu lub działań. Według treści art. 6 ust. 3 UODO z 1997 roku, informacji nie uważało się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań. Założenie, na którym opierało się to ograniczenie, uświadamiało, że mogą istnieć takie sytuacje, gdy określenie tożsamości osoby wiąże się z koniecznością podjęcia działań, które będą wymagały dodatkowych nakładów czy kosztów (np. wynajęcie prywatnego detektywa, uzyskanie dostępu do wyspecjalizowanych baz np. PESEL-SAD), a skala tych nakładów lub kosztów może pozbawić informacje statusu danych osobowych[157]. Zwrócić też trzeba uwagę, że ograniczenie nadmiernych kosztów, czasu i działań nie występowało w treści definicji danych osobowych zawartej w treści art. 2 lit. a Dyrektywy 95/46/WE, zatem należy je traktować jako specyficzne dla polskiego ustawodawcy, które ponadto nie było sformułowane w pierwotnym brzmieniu regulacji ustawowej, ale zostało wyrażone w drodze zmiany przepisu art. 6, w ustawie z dnia 25 sierpnia 2001 r.[158].

Z zapisu, z którego zrezygnował prawodawca unijny w nowych przepisach o ochronie danych osobowych, wynikało po pierwsze, że weryfikacja informacji pod kątem tego, czy stanowi czy nie stanowi danych osobowych, musiała następować z uwzględnieniem aspektu finansowego (koszty), aspektu czasowego (czas) oraz aspektu możliwości, sił i zasobów (działania). Ponadto, ze sformułowania, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań, można wyinterpretować, że ograniczenie kosztów, czasu i działań stanowiło istotne ograniczenie w przyznawaniu informacji statusu danych osobowych. Nie miało jedynie uzupełniającego charakteru, ale stanowiło równoważną z pozostałymi przesłankę uznania informacji za dane osobowe. Regulacyjne znaczenie tego ograniczenia zilustrowane zostało w orzecznictwie sądów. Naczelny Sąd Administracyjny w jednym z wyroków wyjaśnił, że chodziło o informacje, które bez nadzwyczajnego wysiłku, bez nieproporcjonalnie dużych nakładów, dają się powiązać z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych[159]. Można więc powiedzieć, że ograniczenie nadmiernych kosztów, czasu i działań z jednej strony miało za zadanie zmniejszać rygoryzm przepisów prawa. Stanowiło ono pewną przeciwwagę dla szerokiego rozumienia definicji danych osobowych jako wszelkich informacji o osobie fizycznej. Tworząc zdroworozsądkowy

[157] T. Szewc, *Ochrona…*, *op. cit.*, s.6.
[158] Dz. U. Nr 100, poz. 1087.
[159] Wyrok NSA z dnia 19 maja 2011r., I OSK 1086/10, Legalis nr 378897.

balans[160], pozwalało unikać niewłaściwego stosowania przepisów z zakresu ochrony danych, co mogłoby doprowadzać do absurdalnych sytuacji w życiu codziennym. Z drugiej strony, ograniczenie to doprecyzowywało legalną definicję danych osobowych. Taki wniosek można wywieść, poprzez odwrócenie jej treści, idąc za przykładem wypracowanym na gruncie orzecznictwa. Stwierdzono, że informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań czyli *a contrario* informacje, które bez nadzwyczajnego wysiłku, bez nieproporcjonalnie dużych nakładów dają się "powiązać" z określoną osobą, zwłaszcza przy wykorzystaniu łatwo osiągalnych źródeł powszechnie dostępnych, również zasługują na zaliczenie ich do kategorii danych osobowych[161].

Dokonując próby oceny przedstawionej zmiany w postrzeganiu danych osobowych na gruncie UODO z 1997 r. i RODO, wydaje się właściwe podzielenie poglądu, że dodatkowy element definicji danych osobowych, jakim było ograniczenie nadmiernych kosztów, czasu i działań nie dawał jednoznacznych rozwiązań, miał charakter niedookreślony, a jego rzeczywiste znaczenie kształtowało się dopiero w drodze rozstrzygnięć w konkretnych stanach faktycznych[162]. Argumentem potwierdzającym powyższe stwierdzenie jest fakt, że nie istnieją z góry ustalone kryteria mierzalności ani skala oceny kosztów, czasu i działań, w związku z czym w praktyce ocena dokonywana była każdorazowo przez podmiot, który przetwarza dane, w oparciu o różne okoliczności tworzące kontekst przetwarzania, np. dostępność podmiotu do baz danych, systemów informatycznych, dokumentacji w formie papierowej.

O ile ograniczenie nadmiernych kosztów, czasu i działań mogło mieć pozytywne znaczenie dla klasyfikacji informacji jako danych osobowych, z uwagi na to, że wprowadzało pewien stopień elastyczności i relatywności przy kwalifikacji, to rezygnacja z niego w treści nowych przepisów RODO nie prognozuje negatywnych skutków, wzmacnia neutralność technologiczną RODO i uwzględnia możliwości zmian, jakie są nieuchronną konsekwencją postępu gospodarczego, naukowego, społecznego i technologicznego. To co dziś stanowiłoby nadmierny koszt, czas i działanie, wcale nie

[160] Na temat „zasady rozsądku" zob. szerzej: K. Malinowska, *Umowa ubezpieczenia w Europie bez granic*, Warszawa 2008, s. 247 i n. Autorka stoi na stanowisku, że zasada rozsądku może stanowić klauzulę generalną do wypełniania luk prawnych, metodę wykładni oświadczeń, jej funkcja zbliża się do zasady dobrej wiary.
[161] Wyrok Naczelnego Sądu Administracyjnego z dnia 19 stycznia 2010 r., I OSK 491/09, Legalis nr 222666.
[162] M. Kluska [w:] M. Kołodziej (red.), *Vademecum administratora bezpieczeństwa informacji*, Warszawa 2016, s. 3.

musi być nim za kilka lub kilkanaście lat. Element ten mógłby być polem do nadużyć np. podczas udostępniania danych osobowych. Dlatego też zmianę można ocenić pozytywnie.

Definicję danych osobowych funkcjonującą przez lata na gruncie UODO z 1997 r. (implementującą Dyrektywę 95/46/WE) należy całościowo zestawić i porównać z definicją tego kluczowego pojęcia wynikającą z nowych przepisów RODO. Wyjaśnienia już na wstępie wymaga, że RODO co do zasady zawiera całość przepisów prawa materialnego o ochronie danych osobowych, poza wyjątkami, co do których państwa członkowskie UE nie doszły do porozumienia, lub celowo pozostawiły regulacji wewnętrznej[163].

Zgodnie z treścią art. 4 pkt 1 RODO dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Łatwo można stwierdzić, że definicja danych osobowych w RODO konstruowana była na bazie definicji zawartej w Dyrektywie 95/46/WE i w ogólnym kształcie pokrywa się z nią. Składa się z dwóch części tj. wskazania trzech kryteriów kwalifikacji (informacja, dotycząca osoby fizycznej, osoba jest zidentyfikowana lub możliwa do zidentyfikowania) a następnie otwartego katalogu przykładowych rodzajów danych osobowych. Dlatego też pomimo nowego stanu prawnego, aktualne pozostają rozważania, w których zaakcentowane zostały zmiany w odniesieniu od dotychczasowych przepisów krajowych (np. rezygnacja z ograniczenia nadmiernego kosztu czasu i działań, czy zaliczenie danych biometrycznych do kategorii nadysz szczególnej kategorii. W związku z tym należy podkreślić, że RODO nie zrywa z dotychczasową siatką pojęć charakterystycznych dla prawa ochrony danych osobowych, jaki ukształtował się na gruncie Dyrektywy 95/46/WE i ustawy o ochronie danych osobowych, ponieważ podstawowe definicje nie ulegają zmianie. Słusznie zauważono, że RODO uwzględnia

[163] K. Kaźmierczak, P. Litwiński, *Ochrona…, op. cit,* Legalis. Poza zakresem regulacji RODO, a więc jako przedmiot regulacji krajowych, znajdują się pozostałe kwestie, przede wszystkim zagadnienia o charakterze ustrojowym (takie jak dotyczące organu ochrony danych osobowych), zagadnienia o charakterze proceduralnym (związane z postępowaniem przed organem ochrony danych osobowych), czy też zagadnienia dotyczące kar.

rozwój technologiczny i potrzebę stałego nadążania prawa za technologią, ale nie oznacza istotnej jakościowo rewolucji[164].

Mimo poczynionych ustaleń wskazać można kilka szczegółowych elementów różniących definicje danych osobowych występujących na gruncie UODO i RODO. Dla przykładu zwrócić uwagę należy na brak w treści definicji RODO określenia „wszelkie" w odniesieniu do informacji, ale za to dodanie nowych podstaw identyfikacji osoby fizycznej (identyfikator taki jak imię i nazwisko, dane o lokalizacji, identyfikator internetowy). Ponadto zauważa się brak w treści definicji RODO użycia pojęcia tożsamość, a zamiast tego wyjaśnienie -możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, jak również dodany w treści definicji RODO nowy rodzaj tożsamości osoby – genetyczna. Zawarte w treści przepisu wyjaśnienie sformułowania -możliwa do zidentyfikowania osoba fizyczna, stanowi błąd w definiowaniu *idem per idem*. Nie uległy natomiast zmianie kwestie, takie jak to, że nadal danymi osobowymi mogą być informacje – nie ma znaczenia ich forma czy źródło. W dalszym ciągu zakres podmiotowy definicji danych osobowych dotyczy jedynie osób fizycznych. Nowa definicja nadal nie umożliwia ustanowienia katalogu danych osobowych, ponadto wciąż jedną z przesłanek nadania informacji statusu danych osobowych jest kwestia identyfikacji/możliwości zidentyfikowania osoby. Prawodawca dalej nie definiuje osoby zidentyfikowanej tylko osobę możliwą do zidentyfikowania[165].

To, co sanowi pewne *novum* w stosunku do dotychczasowych przepisów, to zdefiniowanie przez prawodawcę w treści RODO (poza zakresem definicji danych osobowych, danych genetycznych, danych biometrycznych i danych dotyczących zdrowia. Pojęcie „dane genetyczne" na gruncie RODO oznacza dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej. Dane biometryczne to dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne. Na gruncie RODO dane biometryczne

[164] P. Litwiński [w:] D. Szostek (red.), *Bezpieczeństwo...*, *op. cit*., Legalis.
[165] P. Litwiński, *Pojęcie danych osobowych w rozporządzeniu ogólnym o ochronie danych osobowych*, Informacja w Administracji Publicznej 2016 nr 3, s. 21-22.

zyskują status szczególnej kategorii danych, jako wymienione w treści art. 9 RODO. Natomiast dane dotyczące zdrowia to dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia. Do tej pory Dyrektywa 95/46/WE w ogóle nie odnosiła się do pojęcia danych genetycznych, natomiast UODO z 1997 r. wspominała w treści art. 27 o kodzie genetycznym (jako tzw. danych wrażliwych). Jeśli chodzi o dane dotyczące zdrowia – oba aktualnie obowiązujące akty bez definiowania ich uznają je za dane szczególnej kategorii (art. 27 UODO z 1997 r. i art. 8 Dyrektywy 95/46/WE). Natomiast pojęcie danych biometrycznych w ogóle nie występuje w treści żadnego z tych aktów.

Nowym elementem są też wymienione w definicji danych osobowych zawartej w treści art. 4 RODO, dane o lokalizacji i identyfikator internetowy. Oba wymienione elementy nie zostały przez prawodawcę doprecyzowane. Jako przykład danych lokalizacyjnych można wskazać współrzędne w lokalizatorach GPS, zaś identyfikatora internetowego - *nick* - pseudonim używany w Internecie[166], *nickname,* przezwisko, pseudonim, termin ten często używany jest w polskojęzycznych programach do określenia pseudonimu, loginu, identyfikatora itp.[167]. Wydaje się, że identyfikatorem internetowym może być też adres IP, który był przedmiotem rozważań powyżej.

W niezmienionym kształcie pozostaje wyłączenie z zakresu ochrony danych osobowych danych osób zmarłych. W dalszym ciągu jest to argumentowane zakończeniem bytu osoby fizycznej z chwilą śmierci czy niedziedzicznym charakterem roszczeń o ochronę danych osobowych, natomiast ewentualnie możliwe roszczenie spadkobiercy o usunięcie danych zmarłego nie wynika z prawa do sprzeciwu wobec przetwarzania danych, a z kultu pamięci zmarłych – jako dobra osobistego bliskich[168].

Ponadto, jak podkreślono już wcześniej, RODO nakazuje inaczej niż dotychczas w polskim porządku prawnym traktować dane osobowe osób fizycznych prowadzących jednoosobową działalność gospodarczą. Zakres ochrony danych osób fizycznych prowadzących działalność gospodarczą nie jest jednakże jasny, przepisy RODO wprost tego nie regulują. W konsekwencji należy odwołać się do opinii przedstawicieli nauki prawa. P. Litwiński uważa, że „wyłączenie stosowania przepisów RODO wobec danych

[166] https://sjp.pwn.pl/slowniki/nick.html.
[167] https://pl.wikipedia.org/wiki/Nick.
[168] M. Krzysztofek, *Ochrona*…, *op. cit.*, s. 41.

pochodzących z rejestru publicznego, powinno zostać uznane za sprzeczne z RODO”[169]. Wprowadzony nowymi przepisami kształt regulacji pozostaje spójny z Dyrektywą 95/46/WE, ale jest odmienny od funkcjonującego przez kilka ostatnich lat w polskim porządku prawnym. Rozwiązania w kwestii ochrony danych osobowych osób fizycznych prowadzących jednoosobową działalność gospodarczą mogą ewaluować w przyszłości, ponieważ jak pokazano we wcześniejszych uwagach, sytuacja przedsiębiorców od początku była zmienna.

Ogólnym wnioskiem wynikającym z porównania definicji danych osobowych wynikającej z treści Dyrektywy 95/46/WE i UODO z 1997 r. z definicją wynikającą z przepisów RODO jest to, że nowa definicja jest wzorowana na definicji z Dyrektywy 95/46/WE, a co za tym idzie, ma wiele wspólnego z rozumieniem danych osobowych w polskim porządku prawnym, ale wprowadza jednocześnie klika istotnych zmian. Intencje unijnego prawodawcy wydają się pozostawać w tym samym kształcie co dwadzieścia kilka lat temu, gdy w życie wchodziła Dyrektywa 95/46/WE. Jednakże RODO różni się od niej w kilku szczegółach, które rzucają nowe światło na sposób traktowania niektórych informacji jako danych osobowych, jak również na postrzeganie nowoczesnych technologii przez pryzmat ochrony danych osobowych. Pociąga to za sobą dalsze refleksje i kolejny wniosek, że poprzez zmiany w pojmowaniu danych osobowych prawodawca zrobił krok w kierunku nadążania za zmieniającą się rzeczywistością i postępem technologicznym (mowa tu konkretnie o uzupełnieniu ram definicji o dane o lokalizacji, identyfikator internetowy, a także osobne zdefiniowanie danych biometrycznych i genetycznych). Należy stwierdzić, że definicja danych osobowych ujęta w treści art. 6 ust 1 UODO z 1997 r. była bardziej rozbudowana i rozszerzona na inne jednostki redakcyjne artykułu 6 (ustęp 2 i 3) niż jej kształt funkcjonujący na gruncie Dyrektywy 95/46/WE, a aktualnie RODO. Przede wszystkim definicja z UODO z 1997 r. uzupełniona była poprzez treść innej definicji, która sformułowana została w treści ustępu drugiego art. 6 UODO z 1997 r. i dotyczyła osoby możliwej do zidentyfikowania. Ponadto dane osobowe w sposób negatywny definiowała również treść ustępu trzeciego powołanego artykułu, poprzez ograniczenie nadmiernych kosztów, czasu lub działań.

W literaturze przedmiotu przełożenie normatywnej i doktrynalnej definicji danych osobowych, a w szczególności jej drugiej części zawierającej otwarty katalog rodzajów

[169] P. Litwiński, *Pojęcie…*, *op. cit*., s. 23.

danych osobowych, na przykłady proponuje M. Kluska. Autor wyjaśnia, że numerami identyfikacyjnymi, o których mowa w art. 6 UODO są: numer powszechnego elektronicznego systemu ewidencji ludności (PESEL), numer identyfikacji podatkowej (NIP), numer dokumentu tożsamości (dowodu osobistego, paszportu)[170]. Natomiast jeśli chodzi o przykłady wymienionych przez ustawodawcę cech, autor proponuje następujące: cechy fizyczne – wygląd zewnętrzny, wzór siatkówki oka; cechy fizjologiczne – struktura kodu genetycznego, grupa krwi; cechy ekonomiczne – status majątkowy; cechy umysłowe, kulturowe lub społeczne – pochodzenie, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniowa, partyjna, związkowa (łączne ich potraktowanie wynika z różnych sposobów interpretacji tych pojęć)[171]. Ponadto cenny kontekst dla przykładów danych osobowych tworzy orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, który w swoich orzeczeniach uznał, że danymi osobowymi są m.in.: nazwisko osobowy w połączeniu z jej numerem telefonu lub informacjami dotyczącymi jej warunków pracy czy sposobu spędzania wolnego czasu oraz informacja, że osoba na skutek doznanego urazu stopy korzysta ze zwolnienia lekarskiego, nazwiska osób i ich roczne dochody; dane dotyczące dochodów z działalności zarobkowej i kapitału, a także majątku osoby fizycznej; imię, nazwisko, data i miejsce urodzenia, płeć, narodowość, stan cywilny, historia wjazdów i opuszczania terytorium danego państwa, status pobytu, szczegóły dotyczące kolejnych paszportów, meldunków, oznaczenie urzędów i służb przekazujących dane[172].

Kategoria danych osobowych podlega wielu klasyfikacjom, z których najczęściej obserwowanym jest podział na dane zwykłe i dane wrażliwe (w treści RODO określane jako szczególna kategoria danych, jednakże w praktyce i w literaturze ugruntowało się to pierwsze określenie). Przede wszystkim oba określenia kategorii danych osobowych nie stanowią terminologii, której źródłem byłby akt prawny, są to *de facto* terminy języka prawniczego, wytwór piśmiennictwa. Innymi słowy dostrzega się rozróżnienie danych na zwykłe i wrażliwe w regulacjach prawa krajowego, jak i unijnego czy międzynarodowego, niemniej jednak prawodawcy nie posługują się tą nomenklaturą. Dane wrażliwe stanowią część zbioru, jakim są wszystkie dane osobowe, wymienione są enumeratywnie w treści

[170] M. Kluska [w:] M. Kołodziej (red.), *Vademecum..., op. cit.,* s. 3.
[171] *Ibidem*.
[172] Wyrok Trybunału Sprawiedliwości z dnia 6 listopada 2003 r., C-101/01, Legalis nr 67277; Wyrok Trybunału Sprawiedliwości z dnia 20 maja 2003 r., C-465/00, Legalis nr 154084; Opinia Rzecznika Generalnego z dnia 14 listopada 2002 r., C-139/01, Legalis nr 153553; Wyrok Trybunału Sprawiedliwości z dnia 16 grudnia 2008 r., C-73/07, Legalis nr 114052; Wyrok Trybunału Sprawiedliwości z dnia 16 grudnia 2008 r.,C-524/06, Legalis nr 113034.

art. 9 RODO (wcześniej art. 27 UODO z 1997 r.)[173]. Rozróżnienie niezmiennie opiera się na tym, że dane zwykłe (czyli wszystkie inne poza wrażliwymi) przetwarzane są na ogólnych zasadach, które wynikały z treści art. 6 RODO (wcześniej art. 23 ust. 1 UODO z 1997 r.). Dane te można przetwarzać wyłącznie, jeśli wystąpi jeden z przypadków wymienionych w przepisie prawa. Nie sformułowano tu zakazu przetwarzania tego rodzaju danych. Natomiast w odniesieniu do danych wrażliwych istnieje wyraźnie sformułowany zakaz ich przetwarzania (art. 9 RODO oraz art. 27 ust. 1 UODO z 1997 r.), chyba że spełniona zostaje jedna z przesłanek uchylających ten zakaz, wymienionych w treści przepisu. Regulujący dane wrażliwe art. 27 UODO z 1997 r. był interpretowany jako *lex specialis* w stosunku do art. 23 UODO z 1997 r.[174]. RODO, podobnie jak uchylona Dyrektywa 95/46/WE i UODO z 1997 r., wyróżnia pewne szczególne kategorie danych osobowych, których przetwarzanie co do zasady jest zabronione, a dopuszczalne jedynie na zasadzie wyjątku od ogólnej reguły[175]. Uzasadnienie wyodrębnienia szczególnej kategorii danych w przepisach RODO zawarte zostało w treści motywu 51 preambuły, zgodnie z którym dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności.

Na gruncie nauki prawa spotyka się też inne próby klasyfikacji danych osobowych. J. Barta, P. Fajgielski i R. Markiewicz proponują wyróżnienie sześciu grup informacji mogących stanowić dane osobowe[176]. Do pierwszej grupy autorzy zaliczają „informacje o zasadniczo niezależnych okolicznościach (imię, nazwisko, płeć, wzrost, znaki szczególne, obywatelstwo, linie papilarne, miejsce i data urodzenia, cechy dokumentów tożsamości, numer PESEL)"; drugą grupę stanowią „informacje o cechach nabytych (wykształcenie, znajomość języków, posiadane uprawnienia, charakter pisma, stan cywilny)"; trzecia grupa to „informacje o cechach osobowościowych, psychologicznych, przekonaniach, zainteresowaniach, światopoglądzie, upodobaniach, sposobie spędzania wolnego czasu"; w czwartej grupie znajdują się „informacje o sytuacji majątkowej,

[173]Dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również dane o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz dane dotyczące skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym. RODO dodaje również dane biometryczne.
[174] A. Drozd, *Ustawa..., op. cit.,* s. 172.
[175] P. Litwiński, *Pojęcie ... op. cit.*, s. 23.
[176] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit*, s. 314.

operacjach finansowych"; w piątej grupie znalazły się: „informacje o najróżniejszych przejawach działalności (podróżach, uczestniczeniu w życiu kulturalnym)"; w ostatniej grupie umieszczono *„*informacje dotyczące aktywnego lub biernego uczestnictwa w różnego rodzaju wydarzeniach*"*. Można przyjąć, że jest kilka kryteriów przedstawionego usystematyzowania danych osobowych. Podstawowe znaczenie ma tu kryterium wagi informacji dla zidentyfikowania osoby fizycznej. W pierwszej grupie znalazły się te dane, które są najistotniejsze przy określaniu, że chodzi o konkretną osobę, dające największą pewność co do tożsamości osoby, najczęściej to one wskazywane są jako dane osobowe w różnych sytuacjach życia codziennego. Do ostatniej grupy natomiast zaliczono informacje, które mogą mieć wpływ na identyfikację, ale mają jedynie pomocniczy charakter – w celu wskazania konkretnej osoby wymagają uzupełnienia informacjami zaklasyfikowanymi do poprzednich grup. Ponadto podział ten pozwala dostrzec pewną hierarchię wśród informacji dotyczących osoby fizycznej. Potencjalnie danymi ważniejszymi dla identyfikacji będą np. informacje z dokumentu tożsamości niż np. informacje o uczęszczaniu na wernisaże sztuki.

M. Sakowska-Baryła wyróżnia dwie kategorie informacji kwalifikowanych jako dane osobowe: „informacje identyfikacyjne, które umożliwiają ustalenie tożsamości osoby i informacje osobo poznawcze, umożliwiające dokładniejsze poznanie szczególnych przymiotów osoby, takich jak cechy fizyczne, fizjologiczne, psychiczne, kulturowe, społeczne, stan majątkowy*"*[177]. Podkreślić jednak należy, że próby kształtowania systematyzacji danych osobowych, są bez wątpienia istotne dla nauki jednak nie znajduje to odzwierciedlenia w materii normatywnej. Przepisy UODO z 1997 r. nie wprowadzały różnic w poziomie ochrony danych ze względu na ich rodzaj, żadnemu rodzajowi nie przyznaje priorytetu. Rozróżnieniem mającym znaczenie na gruncie regulacji prawnych jest podział danych osobowych na dane zwykłe i dane wrażliwe (szczególnej kategorii), gdzie różnice są dostrzegalne przede wszystkim w podstawach prawnych ich przetwarzania (art. 6 i 9 RODO).

Praktyka pokazała, że do kręgu informacji o charakterze osobowym, które aktualnie sprawiają problemy co do odpowiedniej kwalifikacji jako dane osobowe, zaliczają się przede wszystkim: numer telefonu, adres poczty elektronicznej, numer karty

[177] M. Sakowska-Baryła, *Prawo*…, *op. cit*., s. 206.

miejskiej, numer VIN pojazdu, czy adres IP komputera. Spory wokół tych informacji nie gasną, w związku z czym warto podjąć próbę uporządkowania tych kwestii.

Z wyszczególnionych informacji budzących wątpliwości w kontekście ochrony danych osobowych, wydaje się, że najbliżej z osobą fizyczną powiązany jest numer telefonu. Wątpliwość polega na tym, czy dysponując samym ciągiem 9 cyfr (numer telefonu komórkowego bądź numer telefonu stacjonarnego wraz z kierunkowym), nie wiedząc do kogo numer należy, mamy do czynienia z daną osobową. Patrząc z perspektywy operatora telefonii komórkowej czy stacjonarnej, należy wziąć pod uwagę to, że aby otrzymać numer telefonu, wymagana jest rejestracja użytkownika numeru. Dochodzi do niej przy zawarciu przez klienta umowy na usługę telekomunikacyjną, kiedy podaje on wymagane dane, w tym m.in. imię, nazwisko, serię i numer dowodu tożsamości czy adres zamieszkania. Od niedawna numer telefonu na kartę (bez umowy abonamentowej) również podlega obowiązkowi rejestracji użytkownika[178], w związku z czym operator ma dostęp do innych informacji dotyczących użytkownika. Mając na uwadze powyższe uwagi, połączenie przez operatora telefonii numeru telefonu z innymi informacjami o użytkowniku umożliwia dokonanie skutecznej identyfikacji osoby, w konsekwencji czego uzasadnione jest przyjęcie, że numer telefonu jest daną osobową dla operatora. Nieoczywiste jest to natomiast z punktu widzenia innej osoby, która dysponuje wyłącznie numerem telefonu, a nie ma dostępu do żadnych dodatkowych informacji na temat użytkownika tego numeru. Problem ten stanowił przedmiot rozstrzygnięcia Generalnego Inspektora Ochrony Danych Osobowych w decyzji z dnia 22 stycznia 2008 roku, w której treści GIODO stwierdził, że informacje obejmujące kod respondenta, numer telefonu i imię respondenta stanowią dane osobowe w rozumieniu UODO z 1997 r. Informacje te rzeczywiście nie określają bezpośrednio tożsamości osoby, ale będą umożliwiały określenie tożsamości tych osób np. poprzez bezpośredni kontakt z respondentem. Wynika więc jednoznacznie, że powyżej wskazane dane dotyczące respondentów stanowią informacje dotyczące możliwej do zidentyfikowania osoby

[178] Zmiana w ustawie Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907) poprzez dodanie art. 60b. o treści: 1. Abonent, z wyłączeniem abonenta korzystającego z publicznie dostępnych usług telefonicznych świadczonych za pomocą aparatu publicznego lub przez wybranie numeru dostępu do sieci dostawcy usług oraz abonenta usług przedpłaconych polegających na rozpowszechnianiu lub rozprowadzaniu programów telewizyjnych drogą naziemną, kablową lub satelitarną, podaje dostawcy usług następujące dane:
1) w przypadku abonenta będącego osobą fizyczną:
a) imię i nazwisko,
b) numer PESEL, jeżeli go posiada, albo nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu.

fizycznej, a samo ustalenie tożsamości nie wymaga nadmiernych kosztów, czasu lub działań. Wobec tego stanowiły one dane osobowe zgodnie z art. 6 UODO z 1997 r.[179]. Przytoczoną argumentację zinterpretować można tak, że numer telefonu stanowi daną osobową, ponieważ umożliwia bezpośredni kontakt z osobą (zadzwonienie do niej) i dzięki temu skuteczne ustalenie jej tożsamości. Co ciekawe, o ile GIODO wypowiedział się w kwestii uznania numeru telefonu za daną osobową stosunkowo jednoznacznie, to uzasadnienie tej decyzji nie znajduje poparcia wśród przedstawicieli nauki prawa. Zdaniem P. Barty i P. Litwińskiego sam numer telefonu nie powinien być traktowany jako dane osobowe (chyba że w powiązaniu z innymi informacjami pozwala zidentyfikować osobę, a przywołane wyżej uzasadnienie GIODO nie znajduje w ich ocenie oparcia w treści przepisu art. 6 ustawy o ochronie danych osobowych[180]. Autorzy tego stanowiska przekonują, że możliwość zidentyfikowania osoby odnosi się do samej informacji, którą się posiada lub którą można zdobyć bez nadmiernych kosztów, czasu i działań, a nie do działań, których dopiero zamiarem jest ustalenie informacji, która może zidentyfikować osobę fizyczną. Ich rację dobrze ukazuje przykład porównujący numer telefonu do nazwy ulicy i numeru: jeśli numer telefonu stanowi daną osobową, bo umożliwia bezpośredni kontakt z jego użytkownikiem i dzięki temu jego identyfikację, to nazwa ulicy z numerem analogicznie też jest daną osobową, bo można przyjść i sprawdzić, kto tam mieszka. Rację należy więc przyznać przedstawicielom nauki prawa, ponieważ proponowane przez GIODO rozwiązanie nie rozwiązuje problemu.

Na temat traktowania adresów poczty elektronicznej jako danych osobowych powiedziano już bardzo wiele, jednakże nie dostrzega się jednoznacznego rozstrzygnięcia, czy adres email może stanowić daną osobową. W pierwszej kolejności warto prześledzić proces powstawania adresów mailowych. Wydaje się, że najlepiej widać istotę zagadnienia na przykładzie popularnej na całym świecie poczty Gmail. Zakładając konto poczty elektronicznej oferowanej przez Google, użytkownik odsyłany jest na stronę internetową[181], gdzie wymagane jest wypełnienie zamieszczonego formularza. W celu utworzenia konta użytkownik proszony jest o podanie danych, w tym: imię, nazwisko, nazwa użytkownika i hasło, data urodzenia, płeć, telefon komórkowy, obecny adres email i lokalizacja. Następnie dowiadujemy się, że dzięki danym konto jest lepiej zabezpieczone,

[179] DIS-DEC-42/1511, 1515, 1520/08/08 dot. GI-DIS-K-411/22/07, dostępna na: http://www.giodo.gov.pl/pl/306/2329

[180] P. Barta, P. Litwiński, *Ustawa…, op. cit.*, s. 82.

[181] https://accounts.google.com/SignUp?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail % 2Fu%2F0%2F&ltmpl=default

a usługi bardziej przydatne, czyli poznajemy cel zbierania danych[182]. Wyjaśnić należy, że nie ulega wątpliwości, że dane zawarte w formularzu rejestracyjnym są przetwarzane przez podmiot administrujący portalem Gmail (Google). W związku z tym, utworzony przez użytkownika adres mailowy stanowi zawsze daną osobową dla dostawcy usługi poczty elektronicznej[183], z uwagi na fakt, że dostawca może powiązać go bez żadnych trudności z innymi informacjami o użytkowniku, będącymi w jego posiadaniu (np. wypełniony formularz rejestracyjny) i w ten sposób zidentyfikować użytkownika. Inaczej jednakże kształtuje się sytuacja, gdy chodzi o każdy inny podmiot mający styczność z adresem mailowym, poza dostawcą usługi poczty elektronicznej, np. podmioty rozsyłające informacje w postaci newslettera[184]. W nauce prawa najczęściej podzielanym jest pogląd, zgodnie z którym to, czy określony adres mailowy może stanowić daną osobową czy nie, zależy od konfiguracji tego adresu. Innymi słowy rozstrzyga o tym budowa adresu, która pozwalałaby wskazać na konkretnego użytkownika. Dotyczy to zarówno loginu jak i domeny. Nie zawsze login składający się z imienia i nazwiska użytkownika będzie pozwalał na jego identyfikację (np. adres marta.czech@gmail.com nie będzie stanowił danej osobowej, ponieważ istnieje więcej niż jedna osoba o takim imieniu i nazwisku, która potencjalnie mogłaby założyć pocztę elektroniczną Gmail). Adres typu imię.nazwisko@gmail.com mógłby hipotetycznie stanowić daną osobową w przypadku, gdy istnieje tylko jedna osoba o takim imieniu i nazwisku. Natomiast adres taki jak marta.czech@...(nazwa przedsiębiorstwa) będzie stanowił daną osobową z uwagi na fakt, że w przedsiębiorstwie o danej nazwie pracuje najprawdopodobniej tylko jedna Marta Czech. Ponadto adres taki jak prezes@...(nazwa spółki) pomimo faktu, że nie zawiera imienia i nazwiska prezesa określonej spółki, będzie stanowił daną osobową, bo nietrudno uzyskać informację, kto jest prezesem tego podmiotu. Adres mailowy taki jak ksiegowosc@...(nazwa przedsiębiorstwa) może budzić wątpliwości co do zakwalifikowania jako dana osobowa bądź też jako informacja pozbawiona takiego statusu. Pomimo braku wskazania użytkownika z imienia i nazwiska może stanowić daną osobową o ile wiemy, że w księgowości tego przedsiębiorstwa pracuje tylko jedna osoba, którą możemy jednoznacznie zidentyfikować. Nasuwa się tu więc wniosek, że przed przyznaniem bądź odmową przyznania statusu danych osobowych, każdy adres mailowy

[182] https://support.google.com/accounts/answer/1733224?hl=pl
[183] Pogląd taki wyrazili również P. Kowalik i B. Nowakowski [w:] A. Gałach, S. Hoc, A. Jędruszczak, K. Kędzierka, P. Kowalik, A. Kuszel, M. Kuźma, R. Marek, B. Nowakowski, *Ochrona danych osobowych i informacji niejawnych w sektorze publicznym,* Warszawa 2015, s. 11.
[184] Newsletter - elektroniczna forma biuletynu – czasopisma rozsyłanego za pomocą poczty elektronicznej do prenumeratorów. Źródło: https://pl.wikipedia.org/wiki/Newsletter.

należałoby poddawać osobnej kwalifikacji, z uwzględnieniem zarówno jego loginu jak i domeny. Podobne analizy prowadzące do powyższego ogólnego wniosku dokonywane były również przez przedstawicieli nauki prawa[185].

Kolejnym z wymienionych rodzajów informacji problematycznych ze względu na ich postrzeganie przez pryzmat definicji danych osobowych, jest adres IP komputera. Poprzez IP rozumiany jest numer (składający się z czterech segmentów oddzielonych kropkami, każdy to liczba w zakresie od 0 do 255), nadany urządzeniu funkcjonującemu w sieci opartej na protokole IP, służący do jednoznacznej identyfikacji urządzenia w sieci wewnętrznej (adres lokalny, wewnętrzny) lub w Internecie (adres publiczny, zewnętrzny)[186]. Jednakże adres IP poza tym, że pozwala na zidentyfikowanie urządzenia, to niejednokrotnie umożliwia też identyfikację użytkownika (osoby fizycznej). Największe trudności sprawia dynamiczny adres IP (zmieniany często np. z każdym uruchomieniem komputera), ponieważ jego zmienność nie pozwala w praktyce na skuteczną identyfikację użytkownika[187]. Natomiast jeśli chodzi o adresy IP statyczne, zostały one co do zasady przyjęte jako dane osobowe[188]. W kwestii uznania przedmiotowej informacji za dane osobowe wypowiedział się również Generalny Inspektor Ochrony Danych Osobowych, stwierdzając, że należy uznać, że adres IP stanowi daną osobową w przypadkach gdy jest na stałe lub na dłuższy okres czasu przypisany do konkretnego urządzenia, które przypisane jest z kolei konkretnemu użytkownikowi[189]. Wydaje się, że aby można było mówić o adresie IP jako danej osobowej, podmiot dysponujący adresem IP określonej osoby powinien mieć jednocześnie dostęp do innych danych identyfikujących określoną osobę (np. do imienia i nazwiska użytkownika urządzenia, do płatności realizowanych za pomocą karty kredytowej). Dopiero połączenie tych informacji mogłoby dać pewność, że można dokonać skutecznej identyfikacji osoby[190]. Posiadając sam numer IP, bez możliwości pozyskania wiedzy kto korzysta z danego urządzenia, trudno jest mówić o spełnieniu przesłanek definiujących pojęcie danych osobowych. IP będzie wtedy informacją o rzeczy a nie o osobie fizycznej. Co wymaga podkreślenia, GIODO (aktualnie

[185] M.in. T. Banyś [w:] T. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków*, Warszawa 2016, s. 63; K. Gałaj-Emiliańczyk, *Tworzenie systemu ochrony danych osobowych krok po kroku*, Warszawa 2016, s. 41-42.
[186] https://slownik.intensys.pl/definicja/adres-ip/.
[187] P. Kowalik, B. Nowakowski, *Ochrona*…, *op. cit.*, s. 12.
[188] Opinia 4/2007, s. 16: Grupa robocza uznała adresy IP za dane dotyczące osoby możliwej do zidentyfikowania.
[189] http://www.giodo.gov.pl/pl/319/2258.
[190] P. Kowalik, B. Nowakowski, *Ochrona*…, *op. cit.*, s. 12.

PUODO) zastrzega, że podmiot powinien zabezpieczać adres IP tak, jakby był on daną osobową, do czasu, gdy nie uzyska pewności, że sam nie jest w stanie łączyć adresu IP z innymi danymi identyfikującymi osobę[191]. Trzeba tu stwierdzić, że z uwagi na możliwości w obecnych czasach wynikające przede wszystkim z zastosowania nowoczesnych technologii, powiązanie adresu IP z innymi informacjami dotyczącymi osoby fizycznej jest stosunkowo łatwe dla podmiotu dysponującego adresem IP użytkownika, dlatego co do zasady należy przyznać mu należną ochronę, chyba że zaistnieje pewność co do braku zaistnienia możliwości połączenia adresu IP z innymi danymi. Nietrudno dostrzec, że w praktyce życia codziennego, aktywność użytkowników Internetu jest badana przez podmioty gromadzące informacje i profilujące ich działania za pomocą różnych metod, łącznie z zastosowaniem tzw. procesów *Business Intelligence*[192]. Grupa Robocza art. 29 wyraziła podobne stanowisko, zgodnie z którym dopóki dostawca usług internetowych może stwierdzić z całkowitą pewnością, że dane dotyczą użytkowników niemożliwych do zidentyfikowania, musi on ze względów bezpieczeństwa traktować wszystkie informacje związane z adresem IP jako dane osobowe[193]. Jednocześnie warto pamiętać, że istnieją szczególne przypadki, kiedy ze względów technicznych i organizacyjnych nie będzie możliwości zidentyfikowania użytkownika, np. korzystanie z komputera w kafejce internetowej.

Podobnie kształtuje się zagadnienie uznania numeru VIN[194] pojazdu jako danej osobowej, co też uznawane jest za problematyczne zarówno na gruncie praktyki życia codziennego, jak i wśród poglądów autorytetów w dziedzinie ochrony danych osobowych. Analogicznie jak adres IP, sam numer VIN jest informacją o rzeczy (pojeździe), a nie o osobie. Jednakże trzeba mieć na uwadze, że prowadzona jest Centralna Ewidencja Pojazdów[195]. Dostęp do danych zawartych w ewidencji mają m.in. policja, prokuratura, sądy, organy rejestrujące pojazdy, organy podatkowe czy skarbowe. Podsumowując

[191] http://www.giodo.gov.pl/pl/319/2258.
[192] https://pl.wikipedia.org/wiki/Business_Intelligence - są to procesy przekształcania danych w informacje, a informacji w wiedzę, która może być wykorzystywana do zwiększenia konkurencyjności przedsiębiorstwa, m.in. z wykorzystaniem hurtowni danych, która pozwala na ujednolicenie i powiązanie danych zgromadzonych z różnorodnych systemów informatycznych w celu dostosowania raportów wynikowych do potrzeb.
[193] Opinia 4/2007, s. 17.
[194] Zgodnie z definicją zawartą w art. 2 pkt 58 ustawy z dnia 24 czerwca 1997 roku Prawo o ruchu drogowym (t.j. Dz. U. z 2017r. poz. 1260), numer VIN to numer identyfikacyjny pojazdu nadany i umieszczony przez producenta.
[195] Zgodnie z treścią art. 80a ust. 2 pkt 1 ustawy Prawo o ruchu drogowym, w Centralnej ewidencji pojazdów gromadzi się dane i informacje o pojazdach zarejestrowanych oraz o ich właścicielach lub niektórych posiadaczach, w tym numer VIN pojazdu oraz dane właściciela pojazdu, m.in. imię, nazwisko, PESEL (art. 80 b powołanej ustawy).

powyższe uwagi, należy przyznać rację stanowisku GIODO, który twierdzi, że co do zasady sam numer VIN nie stanowi informacji, na podstawie której można zidentyfikować konkretną osobę. Zatem nie można uznać go za dane osobowe. Jednak dla administratora danych, jakim w tym przypadku jest minister właściwy do spraw administracji publicznej, powiązanie numeru VIN z innymi informacjami identyfikującymi właściciela pojazdu umożliwia bez nadmiernego kosztu, czasu i działań, zidentyfikować konkretną osobę. Wobec tego dla niego numer VIN stanowi dane osobowe[196]. Należy przyjąć, że krąg podmiotów, dla których numer VIN będzie stanowił dane osobowe należy rozszerzyć o wszystkie podmioty, które mają dostęp do danych zawartych w Centralnej ewidencji pojazdów, ponieważ dzięki połączeniu tych informacji możliwe jest zidentyfikowanie osoby fizycznej. Na marginesie warto dodać, że podobnie jak numer VIN traktowany jest numer rejestracyjny pojazdu. W opinii Wojewódzkiego Sądu Administracyjnego w Warszawie nie można przyjąć, że numer rejestracyjny pojazdu nie może prowadzić do identyfikacji osoby, a zatem, że nie stanowi on danych osobowych w rozumieniu art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych[197].

Niejednokrotnie okazuje się, że wątpliwości w kontekście ochrony danych osobowych budzą przypadki z praktyki życia codziennego. Jeden z nich dotyczy traktowania jako danych osobowych numeru karty miejskiej. Mogą one zawierać zdjęcie posiadacza, jego imię i nazwisko, podpis, ale zawsze podany jest na niej numer generowany w systemie informatycznym przewoźnika. W systemie tym znajdują się również inne dane pasażera (imię, nazwisko, adres, historia użycia karty)[198]. Generalny Inspektor Ochrony Danych Osobowych uznał, że numer karty miejskiej jest daną osobową w rozumieniu UODO z 1997 r., ale tylko dla tych osób, które na jego podstawie mogą ustalić tożsamość jej właściciela. Będą to np. pracownicy przewoźnika upoważnieni do przetwarzania informacji zawartych w systemie informatycznym związanym z funkcjonowaniem karty miejskiej[199]. Sam numer karty (podobnie jak sam adres IP czy numer VIN) nie będzie zatem daną osobową dla osoby, która nie ma dostępu do innych danych pasażera, które znajdują się w systemie przewoźnika obsługującym karty miejskie.

Dla zarysowania pełniejszego kontekstu pojęcia danych osobowych należy jeszcze dodać kilka uwag w kwestii tego, jakie informacje na pewno nie mogą zostać

[196] http://www.giodo.gov.pl/pl/319/2836.
[197] Wyrok z dnia 9 kwietnia 2013 r. II SA/Wa 211/13, Legalis nr 1186854.
[198] http://www.giodo.gov.pl/317/id_art/3512/j/pl.
[199] *Ibidem*.

zakwalifikowane do kategorii danych osobowych. W literaturze przedmiotu wskazuje się, że za dane osobowe nie można uznawać informacji dotyczących osób nierzeczywistych, fikcyjnych (np. występujących w powieściach)[200], informacji zbiorczych bez ograniczeń np. czasu i miejsca (np. osoby bezdomne), danych anonimowych, danych statystycznych. Jako dane o charakterze nieosobowym wskazywane są też rodzaj wykorzystywanej wyszukiwarki, systemu operacyjnego, przeglądane strony, liczba wizyt na stronach i średni czas ich przeglądania[201].

Podsumowując problematykę danych osobowych jako przedmiotu ochrony prawnej, należy poczynić kilka uwag natury ogólniejszej. Zagadnienie danych osobowych (informacji) jako dobra chronionego prawnie nie jest częstym przedmiotem rozważań przedstawicieli nauki prawa. W literaturze został wyrażony pogląd, zgodnie z którym „pod pojęciem dobra prawnie chronione kryją się różnorodne, lecz odrębne wartości o charakterze materialnym lub niematerialnym (intelektualnym), istniejące, odkrywane, służące bezpośrednio lub pośrednio zaspokajaniu potrzeb ludzkich"[202]. Dobra chronione prawnie są bardzo różnorodne, co wpłynęło na dywersyfikację regulacji wyodrębnionych stosunków prawnych (np. rzeczy i formy korzystania z nich regulowane są przez prawo rzeczowe, utwory regulowane są prawem własności intelektualnej a wynalazki prawem własności przemysłowej). W odniesieniu do danych osobowych, można zaryzykować stwierdzenie, że są to dobra niematerialne, zaspokajają prawo do poszanowania godności jednostki[203], poprzez ich ochronę realizowane jest prawo do prywatności. Regulowane są pozakodeksowo poprzez przepisy o ochronie danych osobowych. Regulacje te, z uwagi, że ochrona danych osobowych aktualnie nie jest wyodrębnioną gałęzią prawa, umiejscowić można na styku prawa prywatnego i prawa publicznego.

Klasycznie co do przedmiotów stosunków cywilnoprawnych wymieniane są dwie teorie. Teoria monistyczna wskazuje tylko dozwolone, nakazane lub zakazane zachowania podmiotów, stosownie do wynikających ze stosunku prawnego uprawnień oraz obowiązków. Według teorii pluralistycznej, przedmiotem stosunku cywilnoprawnego nie jest tylko zachowanie podmiotów, lecz również obiekty występujące poza nimi, jak

[200] M. Sakowska-Baryła, *Prawo…*, *op. cit.,* s. 206.
[201] E. Świętochowska, *Dane nieosobowe mogą płynąć ponad granicami UE,* Gazeta Prawna z dnia 19 września 2017 roku, http://prawo.gazetaprawna.pl/artykuly/1071970,transgraniczny-transfer-danych-nieosobowych.html
[202] A. Bierć, *Zarys prawa prywatnego*, Warszawa 2015, s. 352.
[203] Na temat prawnej ochrony godności zob. szerzej: : L. Bosek, *Gwarancje godności ludzkiej*, Warszawa 2012, s. 144 i n.

zwłaszcza rzeczy i dobra niematerialne[204]. Na gruncie nauki prawa w zakresie spornego pojęcia przedmiotu stosunku cywilnoprawnego wyróżnia się najczęściej rzeczy oraz przedmioty inne niż rzeczy, w tym przedmioty materialne niebędące rzeczami (jak kopaliny, zwierzęta w stanie wolnym), przedmioty niematerialne (np. dobra osobiste, papiery wartościowe), przedsiębiorstwo oraz gospodarstwo rolne[205]. Można powiedzieć, że informacjom i danym osobowym najbliżej jest do kategorii przedmiotów niematerialnych.

Istnieje wiele dóbr, które nie są standardowymi przedmiotami w obrocie prawnym z punktu widzenia prawa cywilnego. W literaturze przedmiotu wskazuje się postaci energii, formy elektroniczne, programy i domeny internetowe, przedsiębiorstwo, zwierzęta, wody, usługi[206]. Powyższy zbiór stale ewaluuje, szczególnie z uwagi na nieustannie postępujący rozwój technologii i nauki. Wydaje się, że można do niego zaliczyć również informacje, w tym dane osobowe. Informacja, której wartość ekonomiczna oraz poziom zagrożenia stale rosną, nie stanowi wyraźnie wyodrębnionego przedmiotu ochrony prawa cywilnego. W literaturze wskazano, że we współczesnych czasach kształtuje się społeczeństwo informacyjne i gospodarka oparta na wiedzy, więc coraz większego znaczenia nabierają dobra niematerialne, „jako nieodłączny element egzystencji podmiotów prawa prywatnego i ważny składnik ich majątku”[207]. Ponadto podkreśla się, że nowym zjawiskiem w obrocie są tzw. dobra informacyjne (np. programy komputerowe, bazy danych, domeny internetowe), co rodzi potrzebę poszukiwania nowych środków ochrony prawnej tych dóbr[208]. Wydaje się, że właśnie tak należy postrzegać dane osobowe, które nie stanowią standardowego przedmiotu ochrony prawa cywilnego. Pokazuje to, że przepisy Kodeksu cywilnego nie nadążają za tempem postępu technologicznego i naukowego, a także zmian społecznych.

Nie wymaga argumentacji pogląd, że dane osobowe stanowią przedmiot obrotu, zarówno w odniesieniu do zbiorów danych, jak i do poszczególnych informacji o charakterze danych osobowych[209]. Obrót rozumiany jest tu jako „sytuacje, w których

[204] W J. Katner [w:] M. Safjan (red.) *System Prawa Prywatnego, tom I, Prawo cywilne – część ogólna,* Warszawa 2012, Legalis, s. 1294.
[205] Z. Radwański, A. Olejniczak, *Prawo cywilne – część ogólna*, Warszawa 2015, s 110 i n.
[206] W J. Katner [w:] M. Safjan (red.) *System..., op. cit.,* s. 1295.
[207] A. Bierć, *Zarys...*, op. cit., s. 353.
[208] *Ibidem*.
[209] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona..., op. cit.,* s. 160.

przez umowy cywilnoprawne dochodzi do udostępnienia danych innemu podmiotowi”[210], w drodze różnych konstrukcji prawnych np. umów licencyjnych, w tym umów mających za przedmiot dane osobowe. Jako jedną z nich można rozpatrywać umowę powierzenia przetwarzania danych osobowych. Należy przy tym pamiętać, że informacje, a w tym dane osobowe, stanowią w dzisiejszych czasach coraz większą wartość ekonomiczną[211]. Uznawane są za atrakcyjny „towar”, ważny zwłaszcza dla przedsiębiorcy, będący przedmiotem obrotu samoistnie, bez fizycznych nośników[212].

Z powyższych względów należy wnioskować, że dane osobowe powinny być traktowane jako dobra niematerialne stanowiące przedmiot obrotu i ochrony prawnej. Ponadto powinny stanowić przedmiot ochrony nie tylko prawa publicznego, ale i prywatnego. Dopiero połączenie regulacji z tych dwóch obszarów może gwarantować skuteczną ochronę. Kodeks cywilny, nie uwzględniający ochrony informacji[213], w tym danych osobowych, wymaga przeglądu i aktualizacji, by spełniać swoje funkcje w sposób pełniejszy i dostosowany do obecnych realiów społecznych, gospodarczych i technologicznych.

[210] *Ibidem*.
[211] Według danych szacunkowych do 2020 r. wartość danych osobowych obywateli państw europejskich może sięgnąć 1 biliona euro (Publikacja Narodowego Instytutu Wolności oraz GIODO, *Gotowi na RODO*, s. 5). Ponadto szacuje się, że koszt wycieku danych osobowych w firmie SONY w 2011 roku wynosił ok 170 mln dolarów (https://finanse.wp.pl/sony-stracilo-ponad-170-mln-dolarow-przez-hakerow-6114319048091777a)
[212] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona..., op. cit.,* s. 163.
[213] W odróżnieniu od Kodeksu karnego, gdzie ochronie informacji poświęcono rozdział XXXIII Przestępstwa przeciwko ochronie informacji.

ROZDZIAŁ II

Powierzenie przetwarzania danych osobowych jako czynność przetwarzania w kontekście zasad przetwarzania danych

1. Przetwarzanie danych – analiza definicji. Powierzenie danych osobowych jako czynność przetwarzania

1.1. Zakres normatywnej definicji pojęcia przetwarzania danych osobowych

Pojęcie „przetwarzanie" na gruncie języka prawnego i prawniczego nie pokrywa się ze znaczeniem tego słowa w języku potocznym. Według definicji słownikowej, przetwarzać oznacza „przerabiać, zmieniać coś nadając inny kształt, wygląd, inną postać, formę, przekształcać, przeobrażać"[214]. Pojęcie przetwarzania danych zostało wyjaśnione przez prawodawcę unijnego i polskiego. Jako pierwszą przytoczyć trzeba definicję z Dyrektywy 95/46/WE, zgodnie z którą przez przetwarzanie rozumiano każdą operację lub zestaw operacji dokonywanych na danych osobowych przy pomocy środków zautomatyzowanych lub innych, jak np. gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez transmisję, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie (art. 2 lit. b Dyrektywy 95/46/WE). W przepisach UODO z 1997 r. definicja przetwarzania została sformułowana jako 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 (art. 7 pkt 2 UODO z 1997 r.). Natomiast RODO definiuje przetwarzanie jako 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 (art. 4 pkt 2 RODO). Wszystkie trzy zacytowane definicje zbudowane są w ten sam sposób. Składają się z części ogólnej, która

[214] M. Szymczak (red.), *Słownik języka polskiego*, tom II, Warszawa 1993, s. 1017.

powtarzalnie wskazuje szeroki zakres operacji na danych osobowych, oraz części szczegółowej, wskazującej rodzaje tych operacji. Wyjaśnienie z osobna wymienionych operacji zostało dokonane na gruncie nauki prawa[215]. Przepisy UODO z 1997r. i RODO dodatkowo eksponują sposób przetwarzania, poprzez wskazanie na przetwarzanie w formie zautomatyzowanej lub niezautomatyzowanej.

Czynności przetwarzania zwykle mają charakter aktywnego podejmowania działań, choć są wśród nich również takie, które kojarzą się z zachowaniem biernym jak np. przechowywanie czy gromadzenie. W nauce prawa zwraca się uwagę, że objęcie zakresem pojęcia przetwarzania zarówno tego co wymaga, jak i tego co nie wymaga pracy nad danymi, ma spore znaczenie praktyczne[216]. Warto zwrócić uwagę na specyficzne sytuacje, gdy podmiot zbierał określone dane osobowe do określonych celów działalności, natomiast po pewnym czasie tę działalność zakończył. Jeśli jednakże po zakończeniu działalności podmiot nadal dysponuje danymi (nawet jeśli tylko je przechowuje), to w rozumieniu przepisów prawa nadal je przetwarza. Co za tym idzie, w dalszym ciągu ciążą na nim obowiązki administratora danych[217] i nieskuteczne byłoby podnoszenie, że nie wykorzystuje danych w żadnych celach, a jedynie pozostały one w jego zasobach i są tylko przechowywane bez podejmowania jakichkolwiek działań. Błędem byłoby niezwrócenie uwagi na istotną kwestię związaną z tym, że przetwarzanie danych obejmuje swoim zakresem cały cykl istnienia danych, tzn. od momentu ich pozyskania, do momentu ich usunięcia. Usunięcie to zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą (definicja funkcjonowała na gruncie art. 7 pkt 3 UODO z 1997 r., prawodawca w treści RODO nie zdecydował się na sformułowanie definicji usunięcia). Rozumieć z tego należy, że za dane usunięte są uważane dane fizycznie zniszczone lub też dane, które poddano nieodwracalnemu procesowi anonimizacji, pozbawiającego dane osobowego charakteru. Przetwarzaniem będzie więc czynność niszczenia i anonimizacji danych. Ta druga opcja oznacza w praktyce, że podmiot nie przetwarza danych osobowych pomimo faktycznego przechowywania informacji, które wcześniej stanowiły dane osobowe, ale zostały one zmodyfikowane w taki sposób, że nie można ich przypisać do osoby (jedna z form

[215] Na temat pojęcia przetwarzania zob. szerzej A. Krasuski, *Dane osobowe w obrocie tradycyjnym i elektronicznym*, Warszawa 2012, s.104-109.
[216] M. Kuba [w:] T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo…, op. cit*., s. 67.
[217] Zgodnie z treścią 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.

usunięcia danych). Z powyższych uwag można zatem wywieść, że kluczowe znaczenie w definicji przetwarzania danych osobowych ma to, by dane, na których wykonywane są operacje, miały osobowy charakter. Dokonywanie tych samych operacji, ale na danych pozbawionych możliwości przypisania ich osobie (po procesie anonimizacji) nie będzie przetwarzaniem w rozumieniu przepisów prawa. W konsekwencji do operacji na takich danych nie będą miały zastosowania przepisy o ochronie danych osobowych. Na marginesie warto dodać, że w ramach przetwarzania danych osobowych wyróżnić można czynności przetwarzania ukierunkowane do wewnątrz, w stosunku do danych będących w dyspozycji przetwarzającego (np. porządkowanie, przeglądanie), jak również czynności ukierunkowane na zewnątrz, w stosunku do innych podmiotów (np. przesyłanie, rozpowszechnianie, udostępnianie).

Katalog działań wymienianych w przepisach prawa jako czynności przetwarzania ma charakter otwarty. Świadczy o tym przede wszystkim literalne brzmienie przepisu i zastosowanie sformułowania „taką jak", „lub innego rodzaju" czy „jakiekolwiek". Wynika to również z faktu, że nie jest możliwe określenie z góry wszystkich czynności, które wchodzą lub ewentualnie mogą wchodzić w zakres pojęcia przetwarzania danych osobowych[218]. Przykładowe wyliczenie operacji przetwarzania można spotkać w orzecznictwie, gdzie stwierdzono, że każde połączenie skonkretyzowanych danych osobowych z jakimkolwiek działaniem administratora danych, będzie stanowiło ich przetwarzanie[219]. Szeroka definicja i otwarty katalog operacji stanowiących przetwarzanie danych osobowych niejednokrotnie wymaga doprecyzowania w postaci interpretacji judykatury. Przykładem jest wyrok Sądu Najwyższego, gdzie uznano, że udostępnianie pełnego zapisu przebiegu posiedzenia komisji sejmowej w Systemie Informacyjnym Sejmu, jeżeli zapis ten obejmuje dane osobowe w postaci imienia i nazwiska umieszczonego w kontekście pozwalającym na identyfikację osoby fizycznej, jest przetwarzaniem danych osobowych[220]. Oprócz otwartego katalogu czynności przetwarzania, zwraca uwagę także ustawowa konstrukcja sposobów przetwarzania. Ustawodawca brał pod uwagę wszystkie możliwe sposoby, a podkreślał te wykonywane w systemach informatycznych. Podobnie postąpił prawodawca unijny, który ujął sposoby

[218] A. Dmochowska [w:] A Dmochowska, M. Zadrożny (red.), *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warszawa 2016, Legalis.
[219] Wyrok Wojewódzkiego Sądu Administracyjnego siedziba w Warszawie z dnia 9 października 2015r., II SA/Wa 40/15, Legalis nr 1364248.
[220] Wyrok Sądu Najwyższego z dnia 13 kwietnia 2017 roku, I CSK 289/16, dostępny na www.sn.pl/sites/orzecznictwo/orzeczenia3/i%20csk%20289-16-1.pdf.

przetwarzania danych równie szeroko, poprzez sformułowanie „w sposób zautomatyzowany lub niezautomatyzowany". Jako trafne należy uznać uzasadnienie powyższych sformułowań faktem, że praktycznie nieograniczone są możliwości obiegu informacji w sieci[221], dlatego przy przetwarzaniu danych za pomocą systemów informatycznych (środków zautomatyzowanych) istotna jest szczególna troska o bezpieczeństwo danych.

Z punktu widzenia prowadzonych na gruncie rozprawy rozważań, których przedmiotem jest umowa powierzenia przetwarzania danych osobowych, nie sposób nie zauważyć, że ustawodawca wśród operacji przetwarzania nie wymienia powierzenia danych. Trudno znaleźć wyjaśnienie co do intencji i ewentualnego celu nieumieszczenia powierzenia np. obok udostępnienia danych można przyjąć, że taki stan rzeczy potwierdza tezę, że definicja przetwarzania danych osobowych zawiera otwarty katalog operacji na danych. Niemniej jednak nie ulega wątpliwości, że w powierzenie mieści się w zakresie przetwarzania danych osobowych.

1.2. Zakres pojęcia powierzenia przetwarzania danych osobowych

Powierzenie przetwarzania danych osobowych nie ma sformułowanej definicji w przepisach obowiązującej wiele lat UODO z 1997 r. czy Dyrektywy 95/46/WE, ani w bezpośrednio stosowanym od 25 maja 2018 roku RODO. Podkreślić należy, że termin „powierzenie" w ogóle nie pada na gruncie aktualnych przepisów o ochronie danych osobowych. Pozostało w praktycznym użyciu, pomimo że nie obowiązuje już art. 31 UODO z 1997 r., zgodnie z którym administrator danych mógł powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Jest natomiast sformułowane w nauce prawa oraz w wypowiedziach Generalnego Inspektora Ochrony Danych Osobowych (aktualnie Prezes Urzędu Ochrony Danych Osobowych). Na gruncie RODO przedmiotowa operacja na danych nie ma swojej nazwy, prawodawca posługuje się sformułowaniem „przetwarzania przez podmiot przetwarzający". Powierzenie w ogólnym rozumieniu nie jest jednakże pojęciem obcym polskiemu systemowi prawnemu.

[221] M. Kuba [w:] T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo…, op. cit*., s. 67.

W kontekście dalszych rozważań zachodzi potrzeba analizy pojęcia powierzenia, przy czym odróżnić należy dwa aspekty. Pierwszy to czynność powierzenia (czyli jak jest ono dokonywane), a drugi to przedmiot powierzenia (czyli co może być powierzane).

Jako przykłady regulacji prawnych odnoszących się do powierzenia wskazać można regulację w Kodeksie cywilnym[222] dotyczącą winy w wyborze: kto powierza wykonanie czynności drugiemu, ten jest odpowiedzialny za szkodę wyrządzoną przez sprawcę przy wykonywaniu powierzonej mu czynności, chyba że nie ponosi winy w wyborze albo że wykonanie czynności powierzył osobie, przedsiębiorstwu lub zakładowi, które w zakresie swej działalności zawodowej trudnią się wykonywaniem takich czynności (art. 429 KC) czy też zastępstwa przy zleceniu: przyjmujący zlecenie może powierzyć wykonanie zlecenia osobie trzeciej tylko wtedy, gdy to wynika z umowy lub ze zwyczaju albo gdy jest do tego zmuszony przez okoliczności (art. art. 738 § 1 KC).

W Kodeksie rodzinnym i opiekuńczym[223] powierzenie odnosi się do wykonywania władzy rodzicielskiej: sąd może powierzyć wykonywanie władzy rodzicielskiej jednemu z rodziców, ograniczając władzę rodzicielską drugiego do określonych obowiązków i uprawnień w stosunku do osoby dziecka, jeżeli dobro dziecka za tym przemawia (art. 58 § 1a) lub też do zarządu majątkiem małoletniego: sąd opiekuńczy może także powierzyć zarząd majątkiem małoletniego ustanowionemu w tym celu kuratorowi (art. 109 § 3).

W Kodeksie pracy[224] powierzenie dotyczy głównie mienia pracodawcy, co ustawodawca reguluje w treści art. 124 § 1 stanowiącym, że pracownik, któremu powierzono z obowiązkiem zwrotu albo do wyliczenia się: pieniądze, papiery wartościowe lub kosztowności, narzędzia i instrumenty lub podobne przedmioty, a także środki ochrony indywidualnej oraz odzież i obuwie robocze, odpowiada w pełnej wysokości za szkodę powstałą w tym mieniu; czy też art. 125 § 1, zgodnie z którym pracownicy mogą przyjąć wspólną odpowiedzialność materialną za mienie powierzone im łącznie z obowiązkiem wyliczenia się.

Następnym przykładem używania terminu powierzenia w przepisach prawa jest treść art. 6a ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[225], zgodnie z którym bank może, w drodze umowy zawartej na piśmie, powierzyć przedsiębiorcy lub przedsiębiorcy

[222] t.j. Dz.U. z 2018 r. poz. 1025 ze zm., dalej KC.
[223] t.j. Dz.U. z 2017 r. poz. 682.
[224] t.j. Dz.U. z 2018 r. poz. 917.
[225] t.j. Dz.U. z 2017 r. poz. 1876.

zagranicznemu wykonywanie określonych czynności, przy czym powierzenie przez bank wykonywania tych czynności następuje na podstawie umowy agencyjnej. Podobnie kształtuje się regulacja powierzenia w treści art. 170 ustawy z dnia z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[226], gdzie ustawodawca uprawnił przedsiębiorcę telekomunikacyjnego do udzielania informacji o numerach abonentów lub powierzenia tej czynności innemu podmiotowi z zachowaniem wszystkich warunków i ograniczeń przewidzianych w przepisach niniejszego rozdziału, jak również w treści art. 35 ustawy z dnia z dnia 23 listopada 2012 r. Prawo pocztowe[227], stanowiącego, że operator pocztowy, który zawarł z nadawcą umowę o świadczenie usługi pocztowej, może po przyjęciu przesyłki pocztowej powierzyć dalsze wykonanie usługi innemu operatorowi pocztowemu na podstawie umowy o współpracę zawieranej w formie pisemnej.

Z powyższych przykładowych regulacji wynika, że na gruncie obowiązujących aktów prawa krajowego powierzenie kojarzone jest z przekazaniem czegoś przez jeden podmiot innemu podmiotowi, „zleceniem" określonych czynności, przeniesieniem wykonywania obowiązków lub praw z jednego podmiotu, by w jego imieniu wykonywał je inny podmiot. Sama czynność powierzenia jest działaniem o niejednorodnym charakterze. Można go dokonać albo poprzez czynność faktyczną (np. wręczenie rzeczy) albo poprzez czynność prawną (np. zawarcie umowy), albo też poprzez działanie władcze organu (wyrok w sprawie powierzenia władzy rodzicielskiej). Przykładem powierzenia w drodze czynności faktycznej jest wspomniane wyżej powierzenie pracownikowi odzieży roboczej przez pracodawcę (art. 124 § 1 Kodeksu pracy), jak również powierzenie płaszcza w szatni w teatrze. Trzeba jednak zauważyć, że zdarza się, że powierzenie może mieć konsekwencje dwojakiego rodzaju. Może to być działanie powodujące powstanie określonej zmiany w sferze prawnej podmiotów dokonujących między sobą powierzenia, albo też niepowodujące żadnych dodatkowych stosunków prawnych pomiędzy tymi podmiotami. Pierwszy przypadek obrazuje przykład powierzenia odzieży roboczej – jest to element stosunku pracy łączącego pracodawcę i pracownika, nie zmienia on sytuacji prawnej żadnego z podmiotów. Inaczej jest we wspomnianej sytuacji z płaszczem – w tym przypadku czynność faktyczna powierzenia rzeczy powoduje zawarcie umowy przechowania zgodnie z art. 835 KC. Zmienia się zatem sfera praw i obowiązków stron dokonujących powierzenia – powstaje stosunek zobowiązaniowy ze wszystkimi jego

[226] t.j. Dz.U. z 2017 r. poz. 1907.
[227] t.j. Dz.U. z 2017 r. poz. 1481.

konsekwencjami. Zwykle aby doszło do powierzenia, musi nastąpić wydanie przedmiotu powierzenia. Do dokonania powierzenie przetwarzania danych osobowych w drodze umowy zawartej zgodnie z art. 28 RODO często wymagane jest wydanie przedmiotu powierzenia, ale nie jest to regułą.

Przepisy prawa dopuszczają też możliwość, by czynność powierzenia została dokonana na mocy aktu władczego. W przedstawionych wyżej przypadkach jest to orzeczenie sądu w przedmiocie powierzenia władzy rodzicielskiej bądź też zarządu mieniem małoletniego przez kuratora (art. 58 § 1a i art. 109 § 3 Kodeksu rodzinnego i opiekuńczego). Powierzenie tą drogą powoduje skutki prawne po stronie tego podmiotu, któremu powierzono określone obowiązki. Wskazane sposoby dokonywania powierzenia na gruncie polskiego prawa potwierdzają, że nie jest to jednolite zagadnienie i może przybierać różne formy oraz powodować różnorodne skutki.

Sporo problemów rodzi przedmiot powierzenia, który również jest niejednorodny i trudny do usystematyzowania. W kontekście przytoczonych przykładów regulacji prawnych, przedmiotem powierzenia mogą być czynności faktyczne, czynności prawne, mienie pracodawcy, władza rodzicielska, zarząd majątkiem małoletniego, czynności bankowe, czynność udzielania informacji, wykonanie usługi pocztowej. Innymi słowy powierzyć można jakąś rzecz, działanie, prawa i obowiązki. Rzecz jest przedmiotem powierzenia przy umowie przechowania. W klasycznej umowie zlecenia przedmiotem powierzenia są czynności prawne. Z treści umowy o świadczenie usług wynika powierzenie czynności faktycznych. Jeśli chodzi o orzeczenie dotyczące powierzenia władzy rodzicielskiej, przedmiotem powierzenia są obowiązki i prawa rodzica wobec dziecka. Trudno znaleźć kryteria systematyzujące ten aspekt powierzenia, ale też wydaje się, że z praktycznego punktu widzenia nie miałyby one istotnego znaczenia dla definicji pojęcia.

Z punktu widzenia prawa, powierzenie danych osobowych do przetwarzania jest stosunkiem prawnym. Przez pojęcie to rozumiemy każdą relację pomiędzy podmiotami, polegającą na tym, że jakaś norma prawna wyznacza podmiotowi określone zachowanie odniesione w pewien sposób do osoby czy spraw innego podmiotu[228]. Relacja powierzenia zachodzi pomiędzy dwoma podmiotami, z których jeden to administrator danych

[228] P. Machnikowski [w:] E. Gniewek (red.) *System Prawa Prywatnego tom 3, Prawo rzeczowe*, Warszawa 2013, str. 8-9, Legalis.

osobowych, a drugi to przetwarzający (występujący również pod nazwą zaczerpniętą z języka angielskiego, procesor)[229]. Stosunek powierzenia polega na tym, że administrator danych „zleca" czynności przetwarzania danych innemu podmiotowi. Koresponduje to z treścią art. 4 pkt 7 i 8 RODO, gdzie zdefiniowano kim jest administrator danych, a kim podmiot przetwarzający. Przepisy nie formułują wobec administratora obowiązku, by sam dokonywał czynności przetwarzania, ma on natomiast decydować o celach i sposobach przetwarzania danych. W związku z tym, na gruncie nauki prawa wywodzi się, że dopuszczalne są sytuacje, kiedy administrator nie będzie miał kontaktu z danymi osobowymi, bo w konsekwencji jego decyzji operacje na danych będą zlecane innemu podmiotowi[230]. Zdarza się, że procesy przetwarzania danych są skomplikowane i wielowarstwowe, a administrator nie będzie mógł realizować ich samodzielnie i zdecyduje się wydelegować zadania do podmiotów zewnętrznych[231]. Podmiot ten (przetwarzający) może przetwarzać dane osobowe jedynie w imieniu administratora, w celu i w zakresie, jaki przewiduje umowa stanowiąca podstawę powierzenia, choć możliwy jest też inny niż umowa tytuł powierzenia, szczególnie w strukturach administracji publicznej[232]. Przetwarzający ma przy tym spełniać obowiązki określone przepisami prawa, jednakże nie przejmuje na siebie obowiązków nałożonych wyłącznie na administratora danych; innymi słowy poprzez dokonanie powierzenia, podmiot przetwarzający nie staje się administratorem powierzonych mu danych[233]. Wobec podmiotu, któremu „zlecono" przetwarzanie danych może być przeprowadzona kontrola przez Prezesa Urzędu Ochrony danych osobowych (wcześniej GIODO). Przedmiot kontroli może dotyczyć tego, czy dane są przetwarzane zgodnie z postanowieniami umowy powierzenia, czy przetwarzanie dokonywane jest we wskazanym zakresie i celu oraz czy podmiot, któremu powierzono przetwarzanie danych, podjął środki zabezpieczające określone w przepisach o ochronie danych osobowych[234].

Z treści art. 17 nieobowiązującej już Dyrektywy 95/46/WE można było wnioskować, że prawodawca nie sformułował całościowej regulacji powierzenia

[229] P. Barta, P. Litwiński, *Ustawa…, op. cit.,* s. 345-346.
[230] A. Śleszyńska, *Instytucja powierzenia przetwarzania danych osobowych* [w:] Temidium.pl -Portal Okręgowej Izby Radców Prawnych w Warszawie , dostęp na stronie internetowej https://www.temidium.pl/artykul/instytucja_powierzenia_przetwarzania_danych_osobowych-2172.html.
[231] G. Wanio [w:] M. Kołodziej (red.), *Vademecum administratora bezpieczeństwa informacji*, Warszawa 2016, Legalis.
[232] A. Drozd, *Ustawa..., op. cit.,* s. 209.
[233] A. Śleszyńska, *Instytucja…, op. cit*.
[234] https://edugiodo.giodo.gov.pl/pluginfile.php/36/mod_resource/content/5/KON/KON_R03.html#8

przetwarzania danych. Dopuścił jedynie możliwość, że dane osobowe nie są przetwarzane przez administratora danych, ale przez podmiot nazwany przetwarzającym, który będzie przetwarzał dane w imieniu administratora. Nie określono jednak w jakich okolicznościach dane mogły być przetwarzane przez inny podmiot. Z analizy przepisu zawartego w art. 17 Dyrektywy 95/46/WE wynika, że przetwarzający to podmiot zewnętrzny, który zostawał przez administratora danych wybrany spośród innych podmiotów. Istotnym z perspektywy prawodawcy unijnego kryterium wyboru przetwarzającego było dawanie gwarancji odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz zapewnienia ich stosowania. Ponadto powierzenie musiało odbywać się na podstawie umowy lub aktu prawnego, które przewidywały, że przetwarzający działa wyłącznie na polecenie administratora danych oraz że również jego dotyczą obowiązki określone w art. 17 ust. 1 Dyrektywy 95/46/WE. Chodziło tu o zapewnienie, że przetwarzający wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas, gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania. Co więcej, relację przetwarzającego z administratorem danych określono jako stosunek podległości. Prawodawca określił formę, w jakiej sporządzone mają być części umowy lub aktu prawnego dotyczące ochrony danych i wymagań dotyczących środków dla celów dowodowych - forma pisemna bądź inna równorzędna.

Warto tu wskazać, że przepis art. 17 ust. 4 Dyrektywy 95/46/WE nie był w pełni jasny co do formy powierzenia przetwarzania danych osobowych, tj. jakich elementów dotyczył wymóg formy pisemnej. Polski ustawodawca, implementując przepisy Dyrektywy 95/46/WE przyjął w treści art. 31 ust. 1 UODO z 1997 r.[235] jedną formę powierzenia przetwarzania danych osobowych, czyli formę umowy zawartej piśmie. Forma alternatywna została wprowadzona do ustawy dopiero w 2016 roku jako bezumowne powierzenie przetwarzania danych osobowych (art. 31 ust. 2a UODO

[235] Polski ustawodawca poświęcił zagadnieniu powierzenia przetwarzania danych osobowych zaledwie jeden artykuł UODO (art. 31). 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. 2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie (...).

z 1997r.[236]). Wśród istotnych różnic pomiędzy regulacją Dyrektywy 95/46/WE a implementującą ją UODO z 1997 r. wymienić należy również to, że przepisy ustawy nie uzależniały wyboru podmiotu przetwarzającego od tego, czy gwarantuje on zabezpieczanie danych i spełnianie określonych prawem wymogów.

Przenosząc uwagę na grunt regulacji prawnych, które zaczęły być bezpośrednio stosowane od 25 maja 2018 roku, można stanąć na stanowisku, że w porównaniu z przepisami Dyrektywy 95/46/WE oraz UODO z 1997 r., w aspekcie przetwarzania danych na zlecenie administratora nowe regulacje RODO są najbardziej szczegółowe i pełne. Uzasadnieniem tego może być fakt, że szczegółowość i konkretność przepisów jest podyktowana potrzebami praktyki - tendencja do korzystania z usług innych podmiotów zamiast samodzielnego przetwarzania danych przez administratora, aktualnie jest już nie wyjątkiem, a coraz bardziej staje się regułą.

Należy zwrócić uwagę, że w treści przepisów RODO nie mówi się o powierzeniu przetwarzania danych, używa się sformułowania przetwarzania przez przetwarzającego, przetwarzania w imieniu administratora. Z uwagi na fakt, że Dyrektywa 95/46/WE również nie posługiwała się takim terminem, uznać należy, że nazwa operacji na danych osobowych, (czy inaczej czynność przetwarzania danych, polegająca na „zleceniu" przez administratora przetwarzania innemu podmiotowi), jaką jest powierzenie przetwarzania, jest osadzona w polskim systemie prawa, a określenie to nie jest stosowane na gruncie prawa Unii Europejskiej. Ze względu na to, że termin powierzenie występuje w wypowiedziach GIODO (w tym decyzjach), literaturze przedmiotu i orzecznictwie, wydaje się, że można używać pojęcia powierzenia przetwarzania danych osobowych w odniesieniu do wszystkich regulacji, tak krajowych, jak i unijnych. Zostało ono przyjęte na gruncie nauki prawa, jak i wśród praktyków z obszaru ochrony danych osobowych, a będzie to stanowić ułatwienie terminologiczne.

Regulacji przetwarzania danych w imieniu administratora przez podmiot przetwarzający poświęcono treść art. 28 RODO. Jego istotę wyrażono jako przetwarzanie dokonywane w imieniu administratora przez podmiot przetwarzający na podstawie umowy lub innego instrumentu prawnego, które określają przedmiot i czas trwania przetwarzania,

[236] Nie wymaga zawarcia umowy między administratorem a podmiotem, o którym mowa w ust. 1, powierzenie przetwarzania danych, w tym przekazywanie danych, jeżeli ma miejsce między podmiotami, o których mowa w art. 3 ust. 1. Przepis wprowadzony Ustawą z dnia 11 lutego 2016 o pomocy państwa w wychowywaniu dzieci (t.j. Dz.U. z 2017 r. poz. 1851). Zawiera on wyjątek od zasady powierzania przetwarzania danych osobowych w drodze umowy w formie pisemnej.

charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora[237].

W treści art. 28 ust. 3 RODO prawodawca dopuszcza dwie możliwości co do formy powierzenia przetwarzania danych: na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego. W literaturze wyrażono pogląd, że pierwsza ze wskazanych powyżej podstaw prawnych powierzenia przetwarzania dotyczyć będzie w szczególności podmiotów ze sfery prawa prywatnego, natomiast druga dotyczyć będzie przede wszystkim podmiotów ze sfery prawa publicznego[238]. Zestawiając regulację w Dyrektywie 95/46/WE i w RODO (przez wiele lat ustawodawca w przepisie art. 31 ust.1 UODO z 1997r. w ogóle nie przewidywał alternatywy dla umowy), należy przyjąć, że inny instrument prawny jest pojęciem szerszym niż akt prawny. Na gruncie nauki prawa akt prawny definiowany jest jako akt, który dotyczy większej ilości ludzi, oznaczonej ogólnie, skierowany jest do niewskazanego konkretnie kręgu osób, w swej treści zawiera normy prawne, zawiera dyspozycje o charakterze ogólnym, wydany przez organ państwa (lub inny podmiot uprawniony) na podstawie upoważnienia zawartego w konstytucji lub innej ustawie, w formie przez ustawę przewidzianej i zawierający normy, które określonego rodzaju podmiotom wyznaczają określonego rodzaju zachowania się, ilekroć wystąpią przewidziane w tych normach okoliczności[239]. Według katalogu źródeł prawa zawartego w treści art. 87 Konstytucji RP, aktami prawa powszechnie obowiązującego są ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia oraz akty prawa miejscowego. Natomiast aktami prawa wewnętrznego mogą być np. uchwały, zarządzenia, instrukcje, okólniki, pisma okólne, wytyczne, regulaminy, decyzje, polecenia służbowe, komunikaty i obwieszczenia[240]. Przy czym pamiętać należy, że akty prawa wewnętrznego wiążą tylko

[237] W treści art. 28 RODO, podobnie jak w art. 17 Dyrektywy 95/46/WE i jednocześnie odmiennie niż w treści art. 31 ust. 1 UODO, prawodawca nie sformułował literalnego uprawnienia administratora danych do przetwarzania danych niesamodzielnie, a poprzez korzystanie z usług innego podmiotu.
[238] P. Litwiński (red.), *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz,* Warszawa 2018, Legalis.
[239] W. Płowiec, *Koncepcja aktu prawa wewnętrznego w Konstytucji RP*, Poznań 2006, s. 37, tekst dostępny na stronie internetowej https://repozytorium.amu.edu.pl/bitstream/10593/19276/3/Koncepcja%20aktu%20prawa%20wewn%C4%99trznego.pdf.
[240] W. Płowiec, *Koncepcja…,* s. 47-48.

organy (instytucje), do których są adresowane i mogą mieć zastosowanie tylko przy kształtowaniu stosunków między podmiotami prawa powiązanymi węzłami podległości[241].

W treści przepisów w art. 28 RODO ustanowiono jako alternatywę umowy „inny instrument prawny", który podlega prawu Unii lub prawu państwa członkowskiego i który wiąże podmiot przetwarzający i administratora. Nie określono ani nie zdefiniowano w prawie pojęcia innego instrumentu prawnego. W literaturze wyrażono pogląd, że pojęcie instrument prawny odnosi się do regulacji o różnych formach i szerokim zakresie. W szerokim rozumieniu są to ogólnie obowiązujące akty prawne: dyrektywy, ustawy; w zakresie wąskim: normy kształtujące, przepisy kompetencyjne[242]. Nie wiadomo, czy używając tego pojęcia, prawodawca unijny miał na myśli akty prawne: obowiązujące powszechnie jak i akty wewnętrzne, czy może miał intencje, by włączyć w zakres tego przepisu również akty administracyjne jak np. decyzje administracyjne, albo też inne formy prawnego działania np. porozumienia administracyjne[243].

Rodzi się tu wątpliwość, czy podstawą prawną powierzenia przetwarzania danych osobowych hipotetycznie mogłaby być decyzja. Decyzja administracyjna jest aktem administracyjnym, dotyczącym indywidualnych spraw obywateli regulowanych przez prawo publiczne; jego wydanie następuje w trybie regulowanym przez przepisy o postępowaniu przed organami administracji; rozstrzyga sprawę co do jej istoty, albo w inny sposób kończy sprawę w danej instancji; może nakazywać, zakazywać lub zezwalać na określone działanie[244]. Kluczowe znaczenie ma tu władczy charakter decyzji oraz to, że jest ona formułowana do konkretnego adresata na podstawie konkretnego przepisu prawa. Trudno obecnie znaleźć przepis, który stanowiłby podstawę prawną wydania decyzji w przedmiocie powierzenia przetwarzania danych osobowych. Uzasadnione wydaje się wyłącznie decyzji administracyjnej (która jest aktem stosowania prawa), jako alternatywy podstawy powierzenia przetwarzania danych. Natomiast porozumienie administracyjne wydaje się możliwą alternatywą dla umowy powierzenia[245]. Z definicji porozumienia administracyjnego prezentowanej w nauce prawa wynika, że jest

[241] Orzeczenie Trybunału Konstytucyjnego z dnia 29 października 1986 r., U 2/86, Legalis nr 35959.
[242] A. Erechemla, *Rola wybranych instrumentów prawa ochrony środowiska w zapewnieniu bezpieczeństwa walorów przyrodniczych i turystycznych obszarów przyrodniczo-cennych*, 2007, tekst dostępny na stronie internetowej http://www.pogorzedynowskie.pl/data/referaty/IVBS/ref_13_IVBS.pdf.
[243] Z. Niewiadomski (red.), *Prawo administracyjne*, Warszawa 2013, s. 211.
[244] E. Ura, *Prawo administracyjne*, Warszawa 2015, s. 121.
[245] Na temat charakteru prawnego porozumienia administracyjnego zob. szerzej Z. Cieślak, *Porozumienie administracyjne*, Warszawa 1985.

to niewładcza forma działania administracji, czynność prawna realizowana przez podmioty wykonujące zadania administracji publicznej, której przedmiotem są sprawy leżące w sferze prawa administracyjnego, zawierane między podmiotami na zasadzie równorzędności i współdziałania[246]. Ponadto porozumienie administracyjne, pomimo tego, że przypomina umowę cywilnoprawną (zwłaszcza pod tym względem, że podmioty porozumienia samodzielnie ustalają cel, treści oraz warunki jego dochowania), nie może być za taką umowę uznane[247]. Zatem można przyjąć, że wchodzi w zakres pojęcia innego instrumentu prawnego i hipotetycznie, jako zgodne oświadczenie woli dwóch podmiotów sektora publicznego, a nie władczy akt, może stanowić podstawę powierzenia przetwarzania danych osobowych. Warto powołać się na poglądy wyrażone na gruncie przepisów RODO wskazujące, że innym instrumentem prawnym może być akt prawny oraz jednostronna czynność prawna, o ile spełniają wszystkie przesłanki z art. 28 ust 3 i 9 RODO[248].

Na kanwie nowych przepisów RODO należy dostrzec istotną zmianę w zakresie wyboru podmiotu przetwarzającego. Przepisy UODO z 1997 r. nie uzależniały wyboru podmiotu przetwarzającego od tego, czy gwarantuje on zabezpieczanie danych i spełnianie określonych prawem wymogów. Ustawodawca pominął więc wymóg dopełnienia należytej staranności przez administratora danych. UODO z 1997 r. nie była zatem podstawą prawną do przypisania odpowiedzialności administratorowi za dokonanie wyboru nieodpowiedniego podmiotu przetwarzającego. Odmiennie ukształtował to zagadnienie prawodawca unijny w treści art. 17 ust. 3 Dyrektywy 95/46/WE, gdzie sformułowane było zobowiązanie administratora danych do wybrania przetwarzającego, o wystarczających gwarancjach odnośnie do technicznych środków bezpieczeństwa oraz rozwiązań organizacyjnych, regulujących przetwarzanie danych, oraz zapewnienia stosowania tych środków i rozwiązań. Natomiast RODO jako zasadę i wyraźny obowiązek wprowadza, by administrator korzystał z usług tylko takiego przetwarzającego, który da mu odpowiednie gwarancje, innymi słowy dopuszczalne jest powierzenie przetwarzania danych wyłącznie podmiotowi, który da dokonującemu wyboru administratorowi gwarancje określone w treści art. 28 ust. 1 RODO, a ponadto ciężar odpowiedzialności za

[246] E. Ura, *Prawo…*, op. cit., s. 130.
[247] Z. Niewiadomski (red.), *Prawo…, op. cit*., s. 214.
[248] K. Witkowska-Nowakowska [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018, s. 636.

wybór ciąży na administratorze[249]. W praktyce oznacza to, że administrator powinien przed zawarciem umowy uważnie zweryfikować standard usług oferowanych przez przetwarzającego, uwzględniając wiedzę fachową, wiarygodność i zasoby przetwarzającego. Brak uprzedniej weryfikacji potencjalnego przetwarzającego stanowi naruszenie przepisów RODO (art. 28). Problemem jest jednakże to, że *de facto* nie istnieją żadne wskazówki, jak należy rozumieć i w praktyce zastosować się do się do wymogu zapewniania gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą. Nie wypowiada się na ten temat Urząd Ochrony Danych Osobowych, a przedstawiciele nauki prawa raczej pomijają to zagadnienie, ograniczając się do sformułowań literalnych z treści przepisu art. 28 ust. 1 RODO. Można na tej podstawie powiedzieć, że poziom ogólności oraz skomplikowania przepisów RODO nie ułatwia podmiotom stosowania się do wymogów tego aktu, przez co część regulacji może z czasem okazać się nieskuteczna. Już teraz widoczny jest pewien dysonans między założeniami prawodawcy a praktyką. Często jest tak, że czynnikiem decydującym o wyborze określonego podmiotu przetwarzającego jest jakość i cena oferowanych przez niego usług (zasadniczych, z którymi wiąże się przetwarzanie danych), a dopiero treść umowy powierzenia wymusza na przetwarzającym dostosowanie swojej działalności do wymogów RODO.

W treści art. 28 ust. 3 lit. a RODO prawodawca wprowadził wymóg, by przetwarzanie danych przez podmiot przetwarzający następowało wyłącznie na udokumentowane polecenie administratora. O ile Dyrektywa 95/46/WE przewidywała, że przetwarzający działa wyłącznie na polecenie administratora danych, to jego udokumentowana forma jest nowym rozwiązaniem.

Należy przyjąć, że uregulowanie powierzenia w RODO jest budowane na bazie Dyrektywy 95/46/WE, w związku z czym zawiera wiele rozwiązań, które były znane o polskiej ustawy o ochronie danych osobowych. Prawodawca w nowym akcie prawnym również nie posługuje się pojęciem powierzenia. Przepisy RODO w zakresie powierzenia danych są dużo bardziej szczegółowe i zawierają bardziej restrykcyjne wymogi, szczególnie co do obowiązków przetwarzającego. Ani w przepisach Dyrektywy ani UODO z 1997 r. nie było szczegółowych regulacji tej kwestii, natomiast w RODO

[249] K. Witkowska-Nowakowska [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO...*, *op. cit.*, s. 635.

obowiązki zostały wymienione w treści art. 28 ust. 3 lit. a-e, czy też art. 30 ust. 2, art. 33 ust. 2, art. 35 ust. 8, art. 37 ust. 1. Uszczegółowienie regulacji powierzenia przetwarzania danych widoczne jest również w aspekcie obligatoryjnych elementów treści umowy. W Dyrektywie 95/46/WE wskazano tylko, że przetwarzający działa wyłącznie na polecenie administratora danych i że obowiązki zabezpieczenia danych dotyczą również przetwarzającego. W treści UODO z 1997r. poprzestano na wymogu określenia celu i zakresu przetwarzania, natomiast w RODO rozszerzono obligatoryjne elementy umowy o: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora (art. 28 ust. 3 RODO). W praktycznym wymiarze tego zagadnienia, zmiany, które stały się egzekwowalne z dniem 25 maja 2018 roku, powodują konieczność zweryfikowania zawartych dotąd umów powierzenia pod kątem ich treści i ewentualnego uzupełnienia o nowe wymogi, ponieważ dotychczasowe umowy nie w pełni gwarantują poziom ochrony danych osobowych przewidziany w przepisach RODO. Będzie to powodowało większe zainteresowanie zagadnieniem powierzenia przetwarzania danych osobowych, wzrost świadomości w tym zakresie oraz dążenia do uporządkowania stosunków prawnych pomiędzy podmiotami prawa.

Analizując ogólne kwestie dotyczące istoty powierzenia przetwarzania danych osobowych należy jeszcze poruszyć istotną kwestię, jaką jest odniesienie tej operacji na danych osobowych do osoby, której dane dotyczą. W literaturze przedmiotu wskazuje się, że powierzenie przetwarzania danych osobowych jest czynnością, która nie wymaga zgody osoby, której dane dotyczą[250]. Uzasadniane jest to tym że podstawą prawną powierzenia jest art. 28 RODO (wcześniej art. 31 UODO z 1997 r.), w związku z tym nie wymaga ono podstawy prawnej wynikającej z art. 6 i 9 RODO (wcześniej art. 23 czy 27 UODO z 1997r.) i dlatego nie ma potrzeby poszukiwania usprawiedliwienia w którejkolwiek z przesłanek dopuszczalności przetwarzania danych, w tym uzyskania na nie zgody[251]. Pogląd ten poparty jest przez GIODO, który w decyzji z dnia 27 lipca 2005 roku uznał, że gdyby zawieranie umów powierzenia uzależniać od każdorazowego uzyskiwania zgody od osoby, której powierzane dane dotyczą, to przedsiębiorca (będący administratorem) nie miałby możliwości funkcjonować w obrocie

[250] M. Sakowska-Baryła, *Prawo…, op. cit*., s. 162.
[251] *Ibidem*.

gospodarczym, korzystając w pełni ze swobody działalności gospodarczej[252]. Praktycznie rzecz ujmując, administrator miałby poważne trudności jeśli chodzi o prowadzenie usług, aż do czasu, kiedy otrzymałby zgodę wszystkich podmiotów danych, których dane chciałby zlecić do przetwarzania np. podwykonawcy, czy innemu usługodawcy. W związku z tym prawodawca zdecydował się nie wyposażać osoby, której dane dotyczą w możliwość decydowania o tym, czy i komu jej dane mogą zostać powierzone.

Brak wymogu uzyskiwania zgody osoby fizycznej, której dane dotyczą na powierzenie przetwarzania danych ma określone dla niej konsekwencje. W praktyce niejednokrotnie nie wie ona, kto poza administratorem danych ma dostęp do jej danych, w jakim celu je przetwarza i za pomocą jakich środków. Jak wskazują przedstawiciele nauki prawa, podmiot danych nie uczestniczy ani w procesie wyboru podmiotu, któremu administrator powierza przetwarzanie danych, ani też w procesie wyrażania zgody na przetwarzanie jego danych przez podmiot niebędący administratorem danych. Dlatego też sposób przetwarzania (a także zakres i cel) w przypadku powierzenia nie może być inny niż ten, który przewidziany jest przez administratora danych. Ponadto warto podkreślić, że największą odpowiedzialność związaną z przetwarzaniem danych (łącznie z powierzeniem) ponosi administrator danych osobowych, ale ma on też największy zakres uprawnień wobec przetwarzanych danych[253].

Od czasu wejścia w życie przepisów RODO, funkcjonuje nowe rozwiązanie polegające na informowaniu osoby o powierzeniu jej danych osobowych, w ramach realizacji obowiązku informacyjnego wynikającego z treści art. 12-14 RODO. Wynika to z treści art. 13 ust. 1 lit. e RODO, zgodnie z którym administrator podczas pozyskiwania danych osobowych podaje osobie, której dane dotyczą, szereg informacji, w tym informacje o odbiorcach danych osobowych lub o kategoriach odbiorców. Pojęcie odbiorcy oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią (art. 4 pkt 9 RODO). Z zakresu definicji odbiorcy funkcjonującej na gruncie UODO z 1997 r. wyłączone były podmioty przetwarzające. Aktualnie natomiast podmioty

[252] https://giodo.gov.pl/305/id_art/1469/j/pl.
[253] A. Krasuski, D. Skolimowska, *Dane osobowe w przedsiębiorstwie*, Warszawa 2007, s. 55.

przetwarzające mieszczą się w tej kategorii, co skutkuje obowiązkiem informowania osoby fizycznej o tym, komu jej dane zostały powierzone[254].

Wśród rozstrzygnięć zawartych w orzeczeniach sądów i decyzjach GIODO, niewiele z nich dotyczy analizowanej tu istoty powierzenia przetwarzania danych osobowych, a większość odnosi się do kwestii szczegółowych związanych z umową powierzenia. Jako przykład wypowiedzi organów stosujących prawo w zakresie ochrony danych osobowych, które mogą być pomocne przy interpretacji dość skomplikowanych regulacji prawnych, można przytoczyć tezę decyzji GIODO z 2014 roku. Znalazło się tam stwierdzenie, że istota powierzenia przetwarzania danych polega na udzieleniu przez administratora danych na rzecz innego podmiotu upoważnienia do przetwarzania danych, dla realizacji określonych celów[255]. Należy przy tym wywnioskować, że upoważnienie to wynika z treści porozumienia zawieranego pomiędzy administratorem danych a przetwarzającym. Obie możliwości postępowania administratora z danymi osobowymi (samodzielne przetwarzanie lub też powierzenie przetwarzania) potwierdzone zostały w decyzji GIODO z 2013 roku. W decyzji stwierdzono, że jakkolwiek administrator danych osobowych może przetwarzać dane samodzielnie, to art. 31 UODO z 1997 r. upoważnia go również do powierzenia, w drodze zawartej formie pisemnej umowy, przetwarzania tych danych innemu podmiotowi. W przypadku zatem, gdy administrator skorzysta z upoważnienia wynikającego z brzmienia powołanego przepisu, dochodzi do zlecenia „na zewnątrz" przetwarzania danych. Podmiot, któremu administrator powierzył przetwarzanie danych, może je jednak przetwarzać wyłączne w przewidzianym umową zakresie i w określonym w umowie celu[256]. Do istotnych wniosków prowadzi również teza decyzji GIODO z 2010 roku, gdzie organ ustalił, że powierzenie przetwarzania danych na podstawie umowy, w określonym w niej celu, jest działaniem prawnie dopuszczalnym i nie stanowi nieuprawnionego udostępnienia danych przez ich administratora innemu podmiotowi[257]. Cenne informacje co do powierzenia przetwarzania danych wynikają także z treści wyroków sądów, które stoją na stanowisku, że podmiot przyjmujący od administratora "zlecenie przetwarzania danych" może to przetwarzanie prowadzić wyłącznie w przewidzianym umową zakresie (chodzi

[254] Będzie o tym mowa przy analizowaniu zasady rzetelności oraz przejrzystości przetwarzania danych.
[255] Decyzja GIODO z dnia 1 grudnia 2014r., 1215/14/102796, Legalis nr 1336568.
[256] Decyzja GIODO z dnia 22 października 2013r., DOLiS/DEC 1113/13/69461, Legalis nr 1336564.
[257] Decyzja GIODO z dnia 14 września 2010 r. DOLiS/DEC-1103/10, Legalis nr 464232.

tu głównie o rodzaj danych) oraz w określonym umową celu (przeznaczenie danych). Zakres i cel mogą być doprecyzowane przez wskazówki i polecenia udzielone przez administratora danych[258]. Ponadto za niedopuszczalne w świetle prawa należy uznać wszelkie działania podmiotu na danych powierzonych mu do przetwarzania, które mogłyby wykraczać poza cel i zakres przetwarzania wskazany w umowie zawartej z administratorem danych[259]. Z przytoczonych fragmentów orzeczeń sądów i decyzji GIODO wyłania się doniosłość praktyczna umowy powierzenia przetwarzania danych osobowych, jak również sporo wskazówek co do stosowania skomplikowanej regulacji prawnej.

2. Zasady wynikające z przepisów o ochronie danych osobowych w świetle podstawowych funkcji zasad prawa

W opinii niemieckiego filozofa prawa R. Alexy'ego zasady są normami optymalizacyjnymi, normami nakazującymi realizację pewnego stanu rzeczy w możliwie najwyższym stopniu z uwagi na prawne i faktyczne możliwości[260]. Termin zasady prawa jest wieloznaczny, ale w podstawowym znaczeniu jest to obowiązująca norma prawna, która uznawana jest za normę szczególnie doniosłą[261]. Zgodnie z poglądami doktryny teorii prawa, termin zasada prawa pojmowany jest dwojako: w znaczeniu opisowym bądź dyrektywalnym[262]. Znaczenie opisowe implikuje rozumienie zasady prawa jako wzorca ukształtowania instytucji prawnej w szczególnie doniosłych dla tej instytucji aspektach. Chodzi o wzorzec ukształtowania określonego przedmiotu unormowania, który wskazuje sposób rozstrzygnięcia danej kwestii z danego punktu widzenia[263]. Zasada w znaczeniu dyrektywalnym oznacza natomiast wiążące prawnie normy, które należą do danego systemu prawnego, albo jego części i są nadrzędne w stosunku do innych norm tego systemu, którym wyznacza się w tym systemie role szczególne, inne niż role pozostałych norm tego systemu[264]. Są one określone w tekście prawnym w postaci przepisów

[258] Wyrok Wojewódzkiego Sądu Administracyjnego siedziba w Warszawie z dnia 15 lutego 2006 r., II SA/Wa 2055/05, Legalis nr 334989
[259] Decyzja GIODO z dnia 23 listopada 2001 r., GI-DEC-DS-178/01, Legalis nr 464277.
[260] Cyt. za T. Gizbert-Studnicki, *Zasady i reguły prawne*, „Państwo i Prawo" 1988, nr 3, s. 18.
[261] G. Maroń, *Zasady prawa. Pojmowanie i typologie a rola w wykładni prawa i orzecznictwie konstytucyjnym*, Poznań 2011, s. 11.
[262] S. Wronkowska, Z. Ziembiński, *Zarys teorii prawa*, Poznań 2001, s. 186.
[263] S. Wronkowska, Z. Zieliński, Z. Ziembiński, *Zasady prawa. Zagadnienia podstawowe,* Warszawa 1974, s. 25.
[264] S. Wronkowska, Z. Ziembiński, *Zarys…, op. cit*., s. 187.

prawnych, bądź też dają się odtworzyć z tekstu prawnego na podstawie wielu przepisów[265].

Warto zaznaczyć, że S. Prutis stoi na stanowisku, że podział na zasady dyrektywne i opisowe ma odzwierciedlenie w pełnionych przez nie funkcjach[266]. Według poglądu tego autora zasady w znaczeniu opisowym (jak np. zasada *lex retro non agit*) porządkują materiał normatywny, służą ustaleniu właściwych metod regulacji stosunków prawnych. Natomiast zasady dyrektywne (jak np. zasada autonomii woli podmiotów) pełnią funkcje ważnej dyrektywy w procesie wykładni prawa, zwłaszcza przy rekonstrukcji normy w razie luki prawnej oraz stanowią mechanizm samonapędzający w procesie wykładni i stosowania prawa[267].

Istotną kwestią z punktu widzenia dalszych rozważań jest rola, jaką zasady ogólne pełnią w systemie prawa. S. Wronkowska i Z. Ziembiński wskazują cztery szczególne role zasad prawa. Wyznaczają one kierunek działań prawodawczych, wskazując jakie stany rzeczy prawodawca powinien osiągać poprzez tworzenie prawa oraz jakich wartości w procesie prawodawczym powinien nie naruszać, a także wskazują pewne sposoby ukształtowania określonych instytucji prawnych. Zasady ukierunkowują proces interpretacji przepisów prawnych. Wskazują też kierunki stosowania prawa, a w szczególności sposoby czynienia użytku z tzw. luzów decyzyjnych. Ponadto zasady ukierunkowują sposób czynienia użytku z różnych, przysługujących określonym podmiotom praw[268]. Z. Pulka dodaje również rolę determinowania treści norm tworzących daną instytucję prawną, określania wzoru ukształtowania instytucji prawnej[269]. Reasumując, zasady prawa wpływają na proces tworzenia, interpretacji i stosowania prawa i przenikają przez cały porządek prawny, sprawiając, że jest on spójny i opiera się na wspólnych wartościach wyrażanych przez te zasady[270]. Niektóre zasady przekazują system wartości ważny dla całego porządku prawa, inne zaś są specyficzne dla poszczególnych gałęzi prawa.

---

[265] *Ibidem*.
[266] S. Prutis, *Instytucje podstawowe prawa prywatnego (w opozycji do regulacji prawa publicznego)*, Białystok 2018, s. 86.
[267] *Ibidem*, s. 86.
[268] S. Wronkowska, Z. Ziembiński, *Zarys…, op. cit*., s. 188.
[269] Z. Pulka [w:] A. Bator (red.), *Wprowadzenie do nauk prawnych : leksykon tematyczny*, Warszawa 2016, s. 171.
[270] S. Wronkowska, *Podstawowe pojęcia prawa i prawoznawstwa*, Poznań 2005, s. 111.

Można powiedzieć, iż zasady przetwarzania danych osobowych powinny być uznawane za zasady prawa w znaczeniu dyrektywalnym. Stanowią normy prawnie wiążące, zawarte są w tekście prawnym w postaci przepisu prawa. Nie są to jedynie postulaty, które interpretuje się z całokształtu regulacji, sformułowane zostały jako dyrektywy postępowania o charakterze normatywnym, nakładają obowiązki na administratorów[271]. Waga zasad przetwarzania danych nie wynika jedynie z faktu, że prawodawca wyodrębnił je w treści art. 5 RODO, otwierającego Rozdział II o tytule „Zasady", ale przede wszystkim z tego, że za naruszenie zasad przewidziana jest sankcja w postaci administracyjnej kary pieniężnej[272]. Podstawową funkcją zasad przetwarzania danych osobowych wydaje się wskazywanie kierunku wykładni przepisów RODO. Należy zauważyć, że dążąc do nadania przepisom elastyczności, prawodawca często posługuje się ogólnymi regulacjami. Nie zawsze pozwalają one rozstrzygnąć dany problem na gruncie praktyki, nie dają jednoznacznych odpowiedzi na wątpliwości w aspekcie teoretycznym. To w dużej mierze zadanie zasad wymienionych w treści art. 5 ust. 1 RODO, które ukierunkowują na rozwiązania wielu problematycznych kwestii. W praktyce niejednokrotnie zdarza się, że zasady przetwarzania danych są bardzo pomocne w rozwiązywaniu licznych problemów, np. dotyczących legalności przetwarzania. Stanowią też uzasadnienie wielu działań administratora. Pomagają znaleźć odpowiedź na pytania, co do których nie ma odpowiedzi w poszczególnych przepisach prawa. Dla przykładu, podejmując decyzję jak długo będą przetwarzane określone dane, kierunek daje zasada ograniczonego przechowywania. W przypadku decydowania, jaki zakres danych może być pozyskiwany od osób fizycznych, należy kierować się zasadą minimalizacji danych.

Zasady przetwarzania danych osobowych wynikające z przepisów prawa, zostały nazwane i scharakteryzowane na gruncie nauki prawa, choć w przepisach RODO również zostały im nadane pewne określenia. Chronologicznie pierwszym aktem prawnym, z którego wywieść można reguły postępowania z danymi osobowymi, jest Konwencja Rady Europy z 1981 roku nr 108. Zgodnie z treścią art. 5 Konwencji 108 dane osobowe będące przedmiotem automatycznego przetwarzania powinny być pozyskiwane oraz przetwarzane rzetelnie i zgodnie z prawem. Mają być gromadzone dla określonych

[271] P. Drobek [w:] E. Bielak-Jomaa, D. Lubasz (red.) *RODO..., op. cit.,* s. 325.
[272] Zgodnie z treścią art. 83 ust. 5 lit. a RODO w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

i usprawiedliwionych celów i nie mogą być wykorzystywane w sposób niezgodny z tymi celami. Wymaga się też, by były odpowiednie, rzeczowe, niewykraczające poza potrzeby wynikające z celów, dla których są gromadzone oraz dokładne i w razie potrzeby uaktualniane. Ponadto dane powinny być przechowywane w formie umożliwiającej identyfikację osób, których dotyczą, przez okres nie dłuższy niż jest to wymagane ze względu na cel, dla którego je zgromadzono.

Zakreślone przez Konwencję 108 ramy przetwarzania danych zostały zaakceptowane przez prawodawcę unijnego, który oparł na nich treść art. 6 Dyrektywy 95/46/WE. Można uznać, że zasady przetwarzania danych wynikające z Dyrektywy w sposób literalny pokrywają się z ich katalogiem sformułowanym w Konwencji 108. Prawodawca unijny w art. 6 Dyrektywy 95/46/WE wprost nałożył na administratora danych obowiązek zapewnienia przestrzegania zasad, co wydawało się dobrym rozwiązaniem w kontekście możliwości przypisania odpowiedzialności za niestosowanie się do zasad przetwarzania danych.

Na poziomie krajowym do dnia 25 maja 2018 roku regulacja prawna, z której można wywieść zasady przetwarzania, ujęta była w treści art. 26 ust. 1 UODO z 1997 r., zgodnie z którą administrator danych powinien był dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności był obowiązany zapewnić, aby dane były przetwarzane zgodnie z prawem, zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Ponadto dane miały być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich były przetwarzane oraz przechowywane w postaci umożliwiającej identyfikację osób, nie dłużej niż było to niezbędne do osiągnięcia celu przetwarzania. Treść art. 26 ust. 1 UODO z 1997 r. stanowiła w sposób wyraźny pełną implementację art. 6 Dyrektywy 95/46/WE. Prawo polskie realizowało wymienione w Dyrektywie wymogi poprzez nałożenie obowiązków na administratorów danych dokładnie w tym samym zakresie, a więc przykładano wagę do rzetelności przetwarzania danych, legalności, celowości i związania celem, merytorycznej poprawności danych, adekwatności przetwarzania, ograniczonego czasu przetwarzania.

Punktem wyjścia do dalszych rozważań jest fragment motywu 9 preambuły RODO, zgodnie z którym cele i zasady Dyrektywy 95/46/WE pozostają aktualne. Pozwala to rozpatrywać przedmiot prowadzonych rozważań również w odniesieniu do regulacji

unijnych i krajowych, które już nie obowiązują, ale nie utraciły swojej wagi w aspekcie zasad przetwarzania danych osobowych. Od 25 maja 2018 roku zasady wypełniają treść rozdziału II RODO, a w art. 5 RODO prawodawca sformułował ich nazwy i wyjaśnienia. Są to następujące zasady:

1) zgodność z prawem, rzetelność i przejrzystość,
2) ograniczenie celu,
3) minimalizacja danych,
4) prawidłowość,
5) ograniczenie przechowywania,
6) integralność i poufność,
7) rozliczalność.

Dodatkowo, z treści art. 25 RODO wywodzi się również zasadę uwzględniania ochrony danych w fazie projektowania (*privacy by design*) oraz domyślnej ochrony danych (*privacy by default*). Należy też wspomnieć o wynikającej z nowego aktu prawnego koncepcji, którą również można by rozpatrywać w kategorii zasady, choć w ten sposób nie ujął jej prawodawca. Chodzi o podejście oparte na ryzyku (ang. *risk based approach*), polegające na tym, że każdorazowo gdy przetwarzane są dane osobowe, należy analizować ryzyko, jakie może nastąpić dla prywatności osób, których dane dotyczą[273]. Trzeba podkreślić, że sformułowanie zasad integralności i poufności, rozliczalności, uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych stanowi *novum* względem dotychczas obowiązujących przepisów. RODO jest jedynym aktem spośród aktów prawnych stanowiących podstawę prowadzonych rozważań, w którym prawodawca sam literalnie wskazuje zasady przetwarzania z nazwy. Ponadto w akcie tym ujęty został najszerszy katalog zasad przetwarzania danych osobowych.

Nie ograniczając się do literalnego brzmienia przepisów prawa, podkreślenia wymaga, że zasady przetwarzania danych osobowych budzą zainteresowanie nauki prawa. Z badań literatury przedmiotu wynika, że katalogi zasad formułowane są w sposób podobny, ale nie w pełni jednolity. P. Barta i P. Litwiński zaproponowali następujący katalog: zasada rzetelności, zasada przetwarzania danych zgodnie z prawem, zasada celowości przetwarzania danych osobowych, zasada związania celem przetwarzania danych osobowych, zasada adekwatności zbieranych danych osobowych, zasada

[273] Publikacja Biura Generalnego Inspektora Ochrony Danych Osobowych, *Czy jesteś gotowy na RODO?* s. 6.

ograniczenia czasowego; nie formułują natomiast zasady merytorycznej poprawności danych[274].

Autor T. Cygan wskazuje zasadę legalności przetwarzania danych osobowych, zasadę związania celem przetwarzania danych osobowych, zasadę merytorycznej poprawności danych osobowych, zasadę adekwatności przetwarzania danych osobowych, zasadę ograniczenia czasu przetwarzania danych osobowych, ale nie formułuje wspomnianej przez innych zasady rzetelności[275].

Natomiast Generalny Inspektor Ochrony Danych Osobowych[276] wymieniał w swoich publikacjach pięć zasad: zasadę legalności, zasadę celowości, zasadę merytorycznej poprawności, zasadę adekwatności i zasadę ograniczenia czasowego[277]. Zasady te wywodzone były z treści obowiązków nakładanych przez ustawodawcę na administratorów danych.

Zauważyć jednak należy, że o ile nazewnictwo zasad nie jest jednolite wśród teoretyków w dziedzinie ochrony danych osobowych, to ważniejsze jest, że co do ich treści poglądy autorów są zgodne. Ponadto, na bardzo istotną kwestię zwrócił uwagę Wojewódzki Sąd Administracyjny w Warszawie, który w wyroku z dnia 5 listopada 2010 roku podkreślił łączny charakter wszystkich zasad przetwarzania wymienionych jako obowiązki administratora danych. W treści wyroku wyraźnie stwierdzono, że przepis art. 26 ust. 1 UODO z 1997 r. wyznacza pięć wymagających łącznego poszanowania podstawowych zasad przetwarzania danych osobowych, ujętych jako obowiązki administratora: legalności, celowości, merytorycznej poprawności, adekwatności, oraz ograniczenia czasowego[278]. Wynika z tego, że każda z zasad przetwarzania ma odrębny i samoistny charakter, ale obowiązkiem administratora danych jest spełnienie ich wszystkich łącznie.

Po przeanalizowaniu treści art. 26 ust 1 UODO z 1997 r. , art. 5 RODO oraz uwzględnieniu katalogów zasad przetwarzania danych osobowych występujących w literaturze przedmiotu, można stwierdzić, że w stosunku do wąskiego obszaru prawa, jaką jest ochrona danych osobowych, zasad jest zbyt wiele. Ponadto są one zbyt

[274] P. Barta, P. Litwiński, *Ustawa…, op. cit*., s. 304 i n..
[275] T. Cygan, *Podręcznik Administratora Bezpieczeństwa Informacji*, Wrocław 2016, s. 44.
[276] Aktualnie Prezes Urzędu Ochrony Danych Osobowych (PUODO).
[277] Materiał edukacyjny *ABC wybranych zagadnień z ustawy o ochronie danych osobowych* dostępny na stronie internetowej https://edugiodo.giodo.gov.pl/file.php/1/UST/UST_03.htm
[278] II SA/Wa 964/10, Legalis nr 379532.

szczegółowe w odniesieniu do istoty i funkcji pełnionych przez zasady w prawie. W konsekwencji wydaje się, że może to prowadzić do deprecjacji ich wartości i nadrzędnego charakteru, jako norm podstawowych, naczelnych i szczególnie doniosłych. Należy zgodzić się z poglądem wyrażonym w doktrynie, że powoływanie się na zbyt wielką liczbę zasad staje się zabiegiem nieoperacyjnym oraz stanowi automatycznie zarzewie zasadniczych sporów i kontrowersji wokół pytania, czy określona zasada istnieje. Można wyprowadzić stąd wniosek, że poprawny jest postulat zachowywania wstrzemięźliwości interpretacyjnej i ostrożności w „wynajdywaniu" nowych zasad systemu, gałęzi czy dyscypliny prawa[279].

Można w związku z tym zaproponować ujęcie zasad ochrony danych osobowych w następujący katalog:

1) zasada staranności przetwarzania danych (do której zaliczone będą zasady: rzetelności i przejrzystości, legalności, prawidłowości danych);

2) zasada niezbędności danych (w jej ramach znajdzie się zasada ograniczenia celu, zasada minimalizacji i zasada ograniczenia przechowywania);

3) zasada bezpieczeństwa danych (w zakresie której umieścić można zasadę integralności i poufności, zasadę rozliczalności przetwarzania danych i zasadę uwzględniania ochrony danych w fazie projektowania (*privacy by design*) i domyślnej ochrony danych (*privacy by default*)).

Wymienione tu zasady kształtują funkcje przepisów RODO, a przede wszystkim funkcję ochrony i bezpieczeństwa danych osób fizycznych.

Zaproponowany katalog zasad uwzględnia wszystkie zasady wymienione i nazwane przez prawodawcę w treści art. 5 RODO. Ponadto rozszerzony został o wprowadzone w treści RODO regulacje, które nie zostały literalnie określone mianem zasad przez prawodawcę, ale na gruncie nauki prawa uznawane są za zasady, z uwagi na to, że posiadają szczególne znaczenie i stanowią podstawę wykładni i stosowania innych przepisów nowego aktu prawnego[280].

[279] M. Safjan (red.), *System Prawa Prywatnego, tom I, Prawo cywilne część ogólna*, Warszawa 2012, s. 324.
[280] O zasadzie *privacy by design i privacy by default* szerzej m.in. M. Kluska [w:] M. Kołodziej (red.), *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, 2017, Legalis. O zasadzie podejścia opartego na ryzyku szerzej: Publikacja Biura Generalnego Inspektora Ochrony Danych Osobowych *Jak rozumieć podejście oparte na ryzyku*, 2017, dostępna na https://giodo.gov.pl/pl/1520282/10294.

3. Specyfika zasad przetwarzania danych osobowych i ich realizacja w sferze umów powierzenia przetwarzania danych osobowych

3.1. Zasada staranności przetwarzania danych

Warto na wstępie wyjaśnić, co stanowi podstawę i uzasadnienie objęcia zakresem ogólnej zasady staranności przetwarzania danych, zasad nazwanych w treści art. 5 RODO jako zgodność z prawem, rzetelność, przejrzystość, prawidłowość. Można stwierdzić, że podstawowym kryterium przyporządkowującym wymienione zasady do tej grupy jest to, że zasady te nakładają na administratora obowiązek dbałości o przetwarzanie danych na odpowiednim poziomie staranności i jednocześnie wyznaczają kierunek realizacji literalnie sformułowanych w treści RODO praw osób, których dane dotyczą, takich jak prawo do informacji o przetwarzaniu, prawo dostępu do swoich danych, prawo sprostowania i uaktualniania danych.

Z uwagi na sformułowanie zasady rzetelności i przejrzystości (choć bez nadania nazwy) już na gruncie uchylonych przepisów regulujących ochronę danych osobowych (w tym na początku przepisu art. 26 ust. 1 UODO z 1997 r. zgodnie z którym administrator danych przetwarzający dane powinien dołożyć szczególnej staranności w celu ochrony interesów osób, których dane dotyczą) wydaje się, że jest ona podstawowym i ogólnym standardem ochrony danych osobowych. Odnosząc się do Dyrektywy 95/46/WE, zauważyć należy, że w jej polskim tłumaczeniu używane było słowo rzetelność, a nie staranność jak w UODO z 1997 r., jednakże można przyjąć, że określenia te mają charakter synonimów. Prawodawca unijny sformułował zasadę rzetelności przetwarzania danych osobowych w treści art. 6 ust. 1 lit. a Dyrektywy 95/46/WE, gdzie poprzez sformułowanie, że państwa członkowskie zapewniają, aby dane osobowe były przetwarzane rzetelnie i legalnie, połączono ją wraz z zasadą legalności[281].

Na gruncie RODO prawodawca bardzo powierzchownie potraktował regulację zasady rzetelności, stanowiąc jedynie, że przetwarzanie ma być zgodne z prawem, rzetelne i w sposób przejrzysty dla osoby, której dane dotyczą. Istnieje więc konieczność

[281] O rzetelności wspominał prawodawca unijny już w treści preambuły Dyrektywy 95/46/WE. W motywie 28 stwierdził, że przetwarzanie danych osobowych musi być zgodne z prawem i rzetelne wobec zainteresowanych osób. Cecha rzetelności w przetwarzaniu danych osobowych rozwinięta została w treści motywu 38 preambuły Dyrektywy, zgodnie z którym jeżeli przetwarzanie danych ma być rzetelne, osoba, której dane dotyczą, musi mieć możliwość dotarcia do informacji o wystąpieniu czynności przetwarzania danych oraz, jeżeli dane są uzyskiwane od niej, musi otrzymać dokładne i pełne informacje, uwzględniające okoliczności pozyskiwania danych.

odniesienia się do przepisów obowiązujących przed dniem 25 maja 2018 roku. Pozwalają one przyjąć, że przejawem rzetelnego przetwarzania danych osobowych jest umożliwienie osobie, której dane dotyczą, uzyskania informacji o tym, że jej dane są przetwarzane a także o okolicznościach pozyskiwania danych (co można rozumieć jako informacje o tym skąd są dane, w jakim celu są zbierane, jak długo i przez kogo będą przetwarzane). Z motywu 60 preambuły RODO wynika, że zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Jednakże sama zasada jest sformułowana w art. 5 RODO nie w sposób odrębny, lecz w połączeniu z innymi. Zgodnie z jego treścią dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"). Kwestia rzetelności i przejrzystości przetwarzania na gruncie RODO nie ma wypracowanej stałej interpretacji i stanowi przedmiot interpretacji w indywidualnych przypadkach, a wpływ na nią ma m.in. postęp technologiczny czy skala przetwarzania danych i działalności administratora danych[282].

Elementem, na który trzeba zwrócić uwagę, jest przejrzystość przetwarzania danych, nie występująca wprost w przepisach Dyrektywy 95/46/WE ani też UODO z 1997 r. Można ją powiązać z zasadą transparentności procesu przetwarzania danych osobowych, która została przewidziana w punkcie 12 Rekomendacji Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami[283]. W nauce prawa wskazuje się, że realizacją zasady transparentności jest wymóg publicznego udostępnienia informacji o dokonywanym przetwarzaniu danych oraz, że zasada ta stanowi podstawy społecznej kontroli nad danymi będącymi w zasobach administratora, a co za tym idzie, buduje system kontroli jednostki nad danymi osobowymi[284].

[282] M. Krzysztofek, *Ochrona…, op. cit*., s. 58.
[283] Tekst w języku angielskim dostępny na stronie http://www.giodo.gov.pl/pl/147/713. Dokument ten to jedynie zalecenia Rady OECD, nie ma on charakteru wiążącego.
[284] M. Jagielski, *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010, s. 94.

Zasada rzetelności i przejrzystości przetwarzania danych osobowych wyraża obowiązek nałożony na administratora danych, polegający na dbaniu o interesy osoby, której dane dotyczą, w trakcie przetwarzania jej danych. W nauce prawa postrzegana jest jako wytyczna postępowania, zgodnie z którą przy podejmowaniu jakichkolwiek czynności przetwarzania administrator powinien dokładać staranności by wybrać taki sposób przetwarzania, który pozwoli mu osiągnąć cel przetwarzania, ale jednocześnie w jak najmniejszym stopniu będzie narażał interesy podmiotu danych (osoby, której dane dotyczą)[285]. Innymi słowy można powiedzieć, że istotne jest zachowanie równowagi i proporcji pomiędzy celami administratora a prawami osoby, a przetwarzanie ma być jak najmniej uciążliwe dla jej interesów. Podobnie jak w przypadku funkcjonującego do dnia 25 maja 2018 roku elementu definicji danych osobowych, jakim było ograniczenie nadmiernych kosztów czasu i działań, również w tym przypadku odwołać się należy do zasady rozsądku[286].

Przepisy o ochronie danych osobowych (zarówno uchylone jak i aktualnie obowiązujące) wymagają od administratora danych osobowych staranności na poziomie szczególnym, podwyższonej staranności profesjonalisty. Należyta staranność w zakresie prowadzonej działalności gospodarczej oceniana jest z uwzględnieniem zawodowego charakteru tej działalności. Mierniki staranności zawodowej są automatycznie uwzględniane i nie ma znaczenia, czy z charakteru stosunku, jego rodzaju i treści wynikają konkretne wskazania dotyczące wymagań od profesjonalisty[287]. Podwyższona staranność w tym przypadku wymagana jest przede wszystkim z uwagi na ochronę praw podmiotów danych.

Zdaniem Sądu Administracyjnego w Warszawie administrator przetwarzający dane osobowe powinien uwzględniać zarówno niemajątkowe, jak i majątkowe interesy osób, których te dane dotyczą. Jego działania muszą charakteryzować się "szczególną starannością", jeśli chodzi o respektowanie tych interesów. Ma to być zatem staranność większa od zwykłej, przeciętnej, czy nawet należytej[288]. Należy zgodzić się z poglądem, że obowiązek szczególnej staranności powinien być postrzegany jako obowiązek dochowania staranności najwyższej, której można oczekiwać od osoby przetwarzającej dane osobowe,

[285] M. Jagielski, *Prawo..., op. cit.,* s. 79.
[286] Zob. szerzej: K. Malinowska, *Umowa..., op. cit.,* s. 247 i n.
[287] B. Fuchs [w:] M. Habdas, M. Fras (red.) *Kodeks cywilny. Komentarz,* tom III, Warszawa 2018, s. 59.
[288] Wyrok Wojewódzkiego Sądu Administracyjnego siedziba w Warszawie z dnia 5 listopada 2010 r., II SA/Wa 964/10, Legalis nr 379532.

ponieważ przemawia za tym cel tego obowiązku, jakim jest ochrona interesów podmiotów danych[289].

Dla przykładu jako zachowanie szczególnej staranności w przetwarzaniu danych osobowych postrzegać można to, że administrator danych powinien unikać sytuacji, kiedy przetwarza dane osobowe ze świadomością, że są one pozyskiwane nielegalnie, od podmiotów lub ze źródeł, o których nielegalnym charakterze mógł się dowiedzieć przy dochowaniu należytej staranności[290]. Ponadto, należyta staranność administratora przejawia się w sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu. Administrator powinien przed dokonaniem powierzenia zweryfikować, czy podmiot przetwarzający zapewnia wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia i chroniło prawa osób, których dane dotyczą (art. 28 ust. 1 RODO). Dopiero uzyskanie takiego zapewnienia może skutkować zawarciem umowy powierzenia. Jako dobrą praktykę wykazującą dochowanie należytej staranności przez administratora można również uznać uprzednie sprawdzenie potencjalnego podmiotu przetwarzającego, jakie zabezpieczenia danych osobowych stosuje (np. poprzez rozeznanie w opiniach na temat tego podmiotu, zadanie mu pytań czy też w ramach profesjonalnego audytu bezpieczeństwa u przyszłego podwykonawcy), jak również weryfikację, czy podmiot nie będzie sprzeciwiał się zawarciu umowy powierzenia.

Przykładem naruszenia tej zasady może być umieszczenie klauzuli zgody na przetwarzanie danych osobowych w celach marketingowych pośród klauzul zgody na inne cele i objęcie ich wszystkich jednym podpisem podmiotu danych, co w konsekwencji praktycznie uniemożliwia mu odmowę wyrażenia zgody na działania marketingowe, kiedy zgadza się na przetwarzanie w reszcie wskazanych celów[291]. Innym przypadkiem niedochowania należytej staranności przez administratora będzie niesprawdzenie podmiotu przetwarzającego przed zawarciem umowy powierzenia przetwarzania danych osobowych.

Dokonując analizy przepisów UODO z 1997 r., Dyrektywy 95/46/WE, jak i RODO można wywnioskować, że realizacją zasady rzetelności przetwarzania danych osobowych

[289] P. Barta, P. Litwiński, *Ustawa…*, *op. cit*., s. 291 i cytowany tam R. Szałowski .
[290] *Ibidem*, s. 292.
[291] M. Krzysztofek, *Ochrona…, op. cit*., s. 58.

będzie spełnianie tzw. obowiązku informacyjnego[292] przez administratora danych[293]. Warto zwrócić uwagę, jak istotna jest to kwestia dla prawodawcy, skoro regulacja prawna bezpośrednio stosowana od 25 maja 2018 roku zmieniła się w sposób bardzo wyraźny. Ustawodawca w treści art. 24 UODO z 1997 r. wypunktował 4 kwestie, o których poinformowanie stanowiło obowiązek administratora danych osobowych. Były to po pierwsze, adres siedziby i pełna nazwa administratora danych, a w przypadku gdy administratorem danych jest osoba fizyczna - miejsce zamieszkania oraz imię i nazwisko; po drugie, cel zbierania danych, a w szczególności znani administratorowi w czasie udzielania informacji lub przewidywani odbiorcy lub kategorie odbiorców danych, po trzecie, prawo dostępu do treści danych oraz ich poprawiania; po czwarte, dobrowolność albo obowiązek podania danych, a jeżeli taki obowiązek istnieje, jego podstawa prawna. W treści art. 13 i 14 RODO wymagania co do treści klauzuli informacyjnej zostały znacznie rozszerzone, dla przykładu o okres, przez który dane osobowe będą przechowywane, czy też informacje o profilowaniu, realizacji szeregu praw podmiotu danych, a także o odbiorcach danych (przy czym na gruncie RODO odbiorcą jest również podmiot przetwarzający, co stanowi *novum* w odniesieniu do nieobowiązujących przepisów UODO z 1997r.)[294]. Znacznie więcej informacji ma być przekazywanych podmiotom danych, co jednocześnie może utrudniać działalność administratorów. Komplikacje w spełnianiu zasady rzetelności i przejrzystości przetwarzania po stronie administratora danych są widoczne np. w przypadku konieczności zrealizowania obowiązku informacyjnego w tak rozszerzonej formie podczas rozmów telefonicznych, które są nagrywane czy też podczas udzielania pomocy przez

[292] Zagadnienie obowiązków informacyjnych jest znane również innym dziedzinom prawa poza ochroną danych osobowych. Dla przykładu, na gruncie prawa ubezpieczeniowego obowiązki informacyjne pośredników ubezpieczeniowych są istotnym elementem ochrony konsumenta na rynku finansowym, gdzie są one obecnie znacznie rozszerzane w dyrektywach unijnych.
Szerzej na ten temat: M. Szaraniec, *Działalność ubezpieczeniowa pośredników ubezpieczeniowych. Studium publicznoprawne*, Warszawa 2017.

[293] Obowiązek informacyjny sformułowany jest w treści art. 13 RODO (był w treści art. 24 UODO) – w wersji podstawowej, gdy dane zbierane są od osoby, której dotyczą, oraz w treści art. 14 RODO (wcześniej art. 25 UODO) – w wersji rozszerzonej, w przypadku, gdy dane zbierane są nie od osoby, której dotyczą. Wersja podstawowa jest w praktyce realizowana częściej.

[294] Treść art. 4 pkt 9 RODO stanowi że „odbiorca" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania. Natomiast zgodnie z treścią art. 7 pkt 7 UODO odbiorcą był każdy, komu udostępnia się dane osobowe, **z wyłączeniem**: a) osoby, której dane dotyczą, b) osoby upoważnionej do przetwarzania danych, c) przedstawiciela, o którym mowa w art. 31a, d) **podmiotu, o którym mowa w art. 31**, e) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

ratowników medycznych. Zasada staranności przetwarzania danych uwidacznia się przede wszystkim w tym kontekście, że obowiązek informacyjny ma charakter obowiązku aktywnego, co oznacza, że to po stronie administratora danych leży inicjatywa jego wykonania, a nie biernie oczekuje wystąpienia z żądaniem udzielenia informacji przez podmiot danych[295].

Warto zauważyć, że zasada rzetelności i przejrzystości w aspekcie redakcyjnym zyskała na ważności poprzez umieszczenie jej jako pierwszej w katalogu zasad w treści art. 5 RODO, podczas gdy na gruncie UODO z 1997 r. nie była wprost nazwana i zawarto ją w odległym artykule 26. Z drugiej jednak strony można powiedzieć, że aktualnie zdeprecjonowano ją poprzez połączenie jej z zasadą zgodności z prawem i ustawienie w szeregu reszty zasad, podczas gdy w treści art. 26 UODO z 1997r. można było przyznać jej miano zasady naczelnej, która była punktem wyjścia dla innych zasad przetwarzania danych. Świadczyło o tym już samo sformułowanie, że podstawowym obowiązkiem administratora jest dołożenie szczególnej staranności w celu ochrony interesów osób, a w szczególności jest on obowiązany do spełnienia wymogów, z których wywodziły się odrębne zasady przetwarzania danych. Ponadto można powiedzieć, że wszystkie pozostałe zasady (legalności, adekwatności i niezbędności danych do celów, merytorycznej poprawności danych, ograniczonego czasu przetwarzania) stanowiły jednocześnie samodzielne dyrektywy działania i elementy składające się na zasadę rzetelności i przejrzystości przetwarzania danych osobowych.

W aspekcie przejrzystości przetwarzania danych osobowych, wypada zająć stanowisko, że realizowana jest ona przede wszystkim poprzez zobowiązanie administratora do podejmowania odpowiednich środków, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, oraz prowadzić z nią wszelką komunikację w sprawie przetwarzania (art. 12 RODO). Na gruncie nauki prawa wyjaśnia się, że o przejrzystości (transparentności) procesów przetwarzania danych można mówić tylko wtedy, jeżeli osoba, której dane dotyczą, została należycie poinformowana o istotnych dla niej aspektach tego przetwarzania[296]. Zasada przejrzystości przejawia się w wielu obowiązkach nałożonych przez prawodawcę na administratorów danych również poza treścią powołanego art. 12 RODO. Wśród nich wymienić można: uświadamianie osobom

[295] P. Barta, P. Litwiński, *Ustawa…, op. cit*. ,s. 285.
[296] P. Litwiński (red.), *Rozporządzenie... op. cit.*, Legalis.

fizycznym ryzyka, zasad, zabezpieczeń i praw związanych z przetwarzaniem danych osobowych, informowanie o prowadzeniu operacji na danych osobowych i celach przetwarzania, o dokonywaniu profilowania i jego konsekwencjach. Wymóg przetwarzania danych osobowych w sposób przejrzysty dla podmiotu danych został dodany w treści RODO, Dyrektywa 95/46/WE nie uwypuklała tej zasady w sposób tak dosłowny, ale też trudno uznać ją za *novum*, gdyż wywodzona była z zasady rzetelności już wcześniej.

Odnosząc powyższe uwagi dotyczące zasady rzetelności i przejrzystości przetwarzania danych osobowych do problematyki powierzenia przetwarzania danych osobowych, można zająć stanowisko, że aktualnie obowiązujące przepisy nie pozwalają jednoznacznie stwierdzić, czy w aspekcie powierzenia przetwarzania danych osobowych zasada ta jest w pełni realizowana. Trzeba zwrócić uwagę, że do dnia 25 maja 2018 roku administrator danych w ogóle nie miał obowiązku informować osoby, której dane dotyczą, o tym, że powierza jej dane innemu podmiotowi. W treści art. 24 UODO z 1997 r. nie było zobowiązania do informowania o fakcie powierzenia danych. Była natomiast wzmianka o obowiązku administratora poinformowania o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach danych. Jednocześnie z definicji pojęcia odbiorcy zawartej w art. 7 pkt 6 UODO z 1997 r. wyłączony był podmiot przetwarzający. Należy zatem rozumieć, że zasadą było, że osoba, której dane dotyczą nie wiedziała, że jej dane są w dyspozycji zupełnie innego podmiotu, niż administrator danych, któremu osoba podała swoje dane np. na podstawie klauzuli zgody na przetwarzanie. Taki stan rzeczy zdecydowanie powodował niepewność jeśli chodzi o rzetelność i przejrzystość przetwarzania danych. Od 25 maja 2018 roku sytuacja uległa zmianie.

Aktualnie z treści art. 13 i 14 RODO wynika obowiązek informowania podmiotu danych o odbiorcach danych osobowych lub o kategoriach odbiorców, choć bezpośrednio nie wskazuje się podmiotów przetwarzających. Istotne jest przy tym, że na gruncie RODO funkcjonuje nowe rozumienie pojęcia odbiorcy i są to zarówno podmioty, którym udostępniono dane, jak i podmioty przetwarzające dane osobowe na zlecenie administratora, a nawet podwykonawców tych podmiotów[297], ponieważ nie ma tu wyłączenia podmiotu przetwarzającego z definicji odbiorcy, które zawierał przepis art. 7 pkt 6 UODO z 1997 r.. Oznacza to, że administrator danych realizując obowiązek

[297] P. Kalina [w:] P. Walczak (red.), *Dokumentacja wewnętrzna w jednostkach sektora finansów publicznych*, 2018, Legalis.

informacyjny, jest zobowiązany do poinformowania osoby, której dane dotyczą, o tym, komu powierza przetwarzanie jej danych osobowych. Zrozumiałe jest, że na działanie administratora polegające na powierzeniu danych nie jest wymagana zgoda podmiotu danych. Wynika to z faktu, że powierzenie jest czynnością wchodzącą w zakres przetwarzania, co do którego administrator spełnia (powinien spełniać) co najmniej jedną z przesłanek dopuszczalności. Np. zgoda osoby, której dane dotyczą jest zgodą na cały proces przetwarzania, zatem zbędne jest uzyskiwanie oddzielnej i kolejnej zgody na powierzenie danych. Jednakże kwestia poinformowania osoby o powierzeniu jej danych innemu podmiotowi, stanowi jedno z podstawowych założeń zasady rzetelności i przejrzystości przetwarzania danych

Wątpliwość od strony praktycznej jednak budzi to, jaki jest zakres szczegółowości takiej informacji. Nie wiadomo dokładnie, czy w treści klauzuli informacyjnej podmioty przetwarzające mają być wymienione z nazwy, czy też mogą być określone rodzajowo. Z obserwacji rodzącej się praktyki stosowania art. 13 i 14 RODO wynika, że druga opcja jest dominująca. Nie wszystkie podmioty chcą ujawniać z kim współpracują bo może to być traktowane jako tajemnica przedsiębiorstwa. Ponadto bez wątpienia należy uznać przepis sformułowany w art. 28 ust. 1 RODO za realizujący zasadę rzetelności i przejrzystości przetwarzania danych pod kątem powierzania przetwarzania danych. Stanowi on, że 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 rozporządzenia i chroniło prawa osób, których dane dotyczą. Rzetelność przejawia się tu w dbałości administratora o staranne i bezpieczne przetwarzanie danych poprzez wybór odpowiedniego podmiotu przetwarzającego, który zagwarantuje stosowanie przepisów RODO.

Przepisy UODO z 1997r. w kontekście powierzenia nie gwarantowały spełnienia zasady rzetelności i przejrzystości. Natomiast w regulacjach RODO rzetelność i przejrzystość przetwarzania w kontekście powierzenia przetwarzania danych osobowych przejawia się w doborze odpowiedniego podmiotu przetwarzającego dane w imieniu administratora jak również w wymogu poinformowania podmiotu danych w treści klauzuli informacyjnej o odbiorcach danych, w tym o podmiotach przetwarzających dane na zlecenie administratora w drodze umowy, a także poprzez transparentną i zrozumiałą komunikację. Z perspektywy osób, których dane dotyczą, jest to zmiana pozytywna,

jednakże z perspektywy administratorów, może powodować spore utrudnienia, np. godzić w tajemnice przedsiębiorstwa. Dla zapewnienia spójności przepisów i podkreślenia wagi informacji o dokonywanym powierzeniu można zaproponować *de lege ferenda* zmianę w treści art. 28 RODO poprzez dodanie ustępu 11, który stanowiłby, że w przypadku, gdy dane osobowe są lub będą przetwarzane w imieniu administratora przez podmiot przetwarzający, administrator danych informuje o tym osobę, której dane dotyczą.

Ogólnie można powiedzieć, że zasada przetwarzania zgodnie z prawem, przyjęta powszechnie jako zasada legalności przetwarzania, wyznacza kryteria oceny tego, czy przetwarzanie w określonej sytuacji jest dozwolone czy zabronione. W nauce prawa wyrażono pogląd, że przetwarzanie nielegalne ignoruje obowiązek lub zakaz określony w przepisach prawa, w szczególności jest to przetwarzanie danych bez podstawy prawnej lub w celu niezgodnym z prawem[298].

Niejednokrotnie zasada legalności bywa traktowana jako podstawowy punkt odniesienia dla pozostałych zasad przetwarzania danych osobowych[299]. W treści RODO (art. 5 ust. 1 lit. a RODO) jest jednakże połączona z zasadą rzetelności i przejrzystości, co formalnie nie daje jej nadrzędnej pozycji nad innymi zasadami przetwarzania danych. Z drugiej jednak strony, niepodważalna wartość zasady legalności przejawia się w tym, że na jej podstawie określone zostały przesłanki dopuszczalności przetwarzania danych osobowych[300].

Rozbieżności wśród przedstawicieli nauki prawa nie budzi to, jak należy rozumieć zgodność przetwarzania z prawem. Zdaniem A. Drozda zwrot „zgodnie z prawem" jest na tyle szeroki, że obejmuje wszystkie normy prawne obowiązujące zgodnie z koncepcją źródeł prawa przyjętą w Konstytucji, a ponadto, pomimo braku wyraźnego odniesienia do klauzuli dobrej wiary czy zasad współżycia społecznego, administrator nie jest zwolniony z postępowania zgodnie z nimi, ponieważ są one częścią przyjętego porządku prawnego[301]. M. Krzysztofek twierdzi, że legalnie oznacza zgodnie z przepisami rangi ustawowej, rozporządzeniami wydanymi na podstawie ustawy, prawem materialnym, proceduralnym oraz orzecznictwem[302]. Podobnego zdania jest P. Drobek, według którego

[298] M. Krzysztofek, *Ochrona..., op. cit.,* Legalis.
[299] W ten sposób np. M. Krzysztofek, *Ochrona..., op. cit.,* Legalis, K. Świtała, *Pacjent jako beneficjent ograniczeń jawności elektronicznej dokumentacji medycznej*, 2018, Legalis.
[300] P. Barta, P. Litwiński, *Ustawa..., op. cit.,* s. 224.
[301] A. Drozd, *Ustawa..., op. cit*., s. 157
[302] M. Krzysztofek, *Ochrona..., op. cit.,* s. 56.

chodzi nie tylko o spełnienie przesłanek legalności przetwarzania ujętych w treści art. 6 i 9 RODO, ale również o zgodność z innymi przepisami o ochronie danych osobowych, jak też z całokształtem przepisów regulujących działalność podmiotów, które przetwarzają dane[303]. Wyrażono również pogląd, że zasada ta odnosi się do całego *universum* norm prawnych, w tym prawa materialnego i norm postępowania, aktów rangi ustawowej oraz aktów wykonawczych[304].

Nie budzi wątpliwości, że dla realizowania zasady legalności przetwarzania, administrator musi legitymować się podstawą prawną przetwarzania. Warto zauważyć, że mechanizm działania zasady legalności w treści RODO jest taki sam jak dotychczasowy, funkcjonujący na gruncie Dyrektywy 95/46/WE oraz UODO z 1997 r. Oznacza to, że nadal daje ona podstawy do przetwarzania zarówno danych tzw. zwykłych (art. 6 RODO), jak i danych szczególnej kategorii[305] (art. 9 RODO). Rozróżnienie opiera się na tym, że dane zwykłe mogą być przetwarzane wtedy, gdy zaistnieją przesłanki wynikające z treści art. 6 ust. 1 RODO. Wystarczy wystąpienie jednego z sześciu przypadków wymienionych w przepisie, stanowiących zarówno sytuacje faktyczne, jak i prawne. Natomiast w odniesieniu do danych szczególnej kategorii istnieje wyraźnie sformułowany zakaz ich przetwarzania (art. 9 ust. 1 RODO), chyba że spełniona zostaje jedna z przesłanek uchylających ten zakaz, wymienionych w treści art. 9 ust. 2 RODO.

Można dokonać systematyzacji podstaw prawnych przetwarzania danych osobowych, a tym samym wyznaczników realizacji zasady legalności, w drodze podziału na dwie grupy. Do pierwszej zakwalifikować należy przesłanki, na zaistnienie których ma wpływ osoba, której dane dotyczą. Jeśli chodzi o podstawy wymienione w art. 6 ust. 1 RODO, w pierwszej grupie znajdzie się zgoda na przetwarzanie danych, niezbędność do wykonania umowy, gdy osoba jest jej stroną lub żąda ona działań przed zawarciem umowy, a także niezbędność do ochrony żywotnych interesów osoby. Natomiast w przypadku podstaw wymienionych w art. 9 ust. 2 RODO, zakwalifikować tu można

[303] P. Drobek [w:] E. Bielak-Jomaa, D. Lubasz (red.) *RODO. Ogólne...., op. cit.*, s. 325.
[304] P. Litwiński (red.), *Rozporządzenie..., op. cit.*, Legalis.
[305] W katalogu danych szczególnej kategorii prawodawca wymienia następujące rodzaje danych osobowych: ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. W odróżnieniu od stanu prawnego obowiązującego do 25 maja 2018 roku, dane osobowe dotyczące wyroków skazujących oraz czynów zabronionych lub powiązanych środków bezpieczeństwa nie znajdują się w katalogu danych szczególnej kategorii, ale istnieje tu ograniczenie innego rodzaju – mogą być przetwarzane wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego (art. 10 RODO).

wyrażenie przez osobę wyraźnej zgody na przetwarzanie, niezbędność do ochrony żywotnych interesów osoby, sytuację gdy dane osobowe zostają w sposób oczywisty upublicznione przez osobę, a także w części odnoszącej się do osoby - niezbędność do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej. Do drugiej grupy należy zaliczyć te z przesłanek, których spełnienie leży po stronie administratora lub zależy od okoliczności zewnętrznych. Spośród podstaw wymienionych w art. 6 ust. 1 RODO będą to: niezbędność do wypełnienia obowiązku prawnego ciążącego na administratorze, niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi oraz niezbędność do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora. Jeśli chodzi o podstawy wynikające z treści art. 9 ust. 2 RODO, znaleźć się tu mogą: w części odnoszącej się do administratora - niezbędność do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, uprawnioną działalność prowadzoną z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, niezbędność do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy. Ponadto będą tu również: niezbędność ze względów związanych z ważnym interesem publicznym, niezbędność 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 lub zabezpieczenia społecznego oraz niezbędność ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego i niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

Trzeba zauważyć, że aktualny układ przesłanek legalizujących przetwarzanie danych osobowych ma nieco inny kształt, niż obowiązujący na gruncie przepisów UODO z 1997 r. Brakuje istotnej przesłanki funkcjonującej dotychczas w treści art. 23 UODO z 1997 r., jaką była niezbędność do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Oznaczało to, że jeśli konkretny przepis prawa przewidywał obowiązek lub prawo do przetwarzania określonych danych, to dany podmiot

miał podstawę prawną określoną w tym przepisie i w sposób legalny mógł dane przetwarzać. W aktualnym stanie prawnym nie ma problemu jeśli chodzi o kwestię obowiązku, ponieważ treść art. 5 ust. 1 lit c RODO stanowi o niezbędności do wypełnienia obowiązku prawnego ciążącego na administratorze. Nie ma tu natomiast mowy o uprawnieniu administratora wynikającym z przepisu prawa do przetwarzania danych. Przykładem takich regulacji może być art. 112b ustawy Prawo bankowe stanowiący, że banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych, albo też art. 20 ust. 2a ustawy z dnia 6 kwietnia 1990 r. o Policji[306], gdzie sformułowane jest uprawnienie Policji do pobierania, uzyskiwania, gromadzenia, przetwarzania i wykorzystywania informacji, w tym danych osobowe, np. o osobach stwarzających zagrożenie lub zaginionych, także bez ich wiedzy i zgody. Podkreślenia wymaga to, że powołane przepisy nie stanowią obowiązku, a są uprawnieniem banków i policji, które na gruncie UODO z 1997 r. wypełniało przesłankę niezbędności do zrealizowania uprawnienia wynikającego z przepisu prawa. Dlatego niewłaściwym jest oparcie przetwarzania danych przez te podmioty o przesłankę, która zawarta jest w art. 5 ust. 1 lit. c RODO (przetwarzanie niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze). Zauważyć należy, że pomimo utraty oparcia w poprzednim brzmieniu przepisu, działania wskazanych podmiotów nadal pozostają legalne, ale muszą znaleźć inną podstawę w katalogu ujętym w art. 6 ust. 1 RODO. Dla banków będzie to najprawdopodobniej przesłanka niezbędności do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (art. 6 ust. 1 lit. f RODO), a w przypadku policji niezbędność do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 6 ust. 1 lit. e RODO).

Pojawia się na tym etapie wątpliwość, czy realizacja zasady legalności polega tylko na przetwarzaniu danych osobowych w oparciu o podstawę prawną przewidzianą w przepisach art. 6 lub 9 RODO. Pomocne jest przy tym odwołanie się do poglądów wyrażonych w literaturze. Należy się zgodzić, że zgodne z prawem przetwarzanie danych to również zapewnienie informacji m.in. o celu i odbiorcach danych, zapewnienie prawa dostępu do danych, wdrożenie środków zapewniających odpowiedni poziom bezpieczeństwa przetwarzania danych, a także inne obowiązki określone w RODO i w powszechnie obowiązujących przepisach prawa, mających zastosowanie

[306] t.j. Dz.U. z 2017 r. poz. 2067.

w poszczególnych przypadkach przetwarzania danych[307]. Oznacza to, że zasada legalności odnosi się do całego procesu przetwarzania danych, od momentu pozyskiwania danych do momentu ich usunięcia.

Istotną kwestią jest również to, że zasada legalności oddziałuje na treść właściwie każdej z zasad przetwarzania danych. Dla przykładu wskazać można zasadę ograniczenia celu, w treści której dostrzega się wymóg, by cele przetwarzania były prawnie uzasadnione. W przypadku zasady ograniczonego przechowywania podkreślić należy, że niejednokrotnie przepisy prawa stanowią o okresie, w jakim dane mogą być przetwarzane. Z treści art. 74 ustawy z dnia 29 września 1994 r. o rachunkowości[308] wynika np., że obowiązek przechowywania dokumentów dotyczących rękojmi i reklamacji wynosi 1 rok po terminie upływu rękojmi lub rozliczeniu reklamacji, a karty wynagrodzeń pracowników bądź ich odpowiedniki należy przechowywać przez okres wymaganego dostępu do tych informacji, wynikający z przepisów emerytalnych, rentowych oraz podatkowych, nie krócej jednak niż 5 lat. Można zatem powiedzieć, że w sytuacji, gdy dane osobowe klientów, którzy zgłosili reklamację zakupionego towaru, będą przechowywane przez administratora dłużej niż 1 rok, to jego działanie narusza zarówno zasadę ograniczonego przechowywania, jak i zasadę legalności przetwarzania danych.

Odnosząc uwagi o zasadzie legalności przetwarzania do problematyki powierzenia przetwarzania danych, należy zauważyć, że żadna z przesłanek legalizujących prowadzenie operacji na danych osobowych (art. 6 i 9 RODO) nie odnosi się wprost do sytuacji, w której dane przetwarzane są na „zlecenie" administratora danych. Innymi słowy prawodawca nie przewidział w katalogu przesłanek dopuszczalności przetwarzania danych podstawy, którą może wylegitymować się podmiot przetwarzający, który zawarł umowę z administratorem. Wprowadza to wątpliwość czy brak ujęcia faktu, że administrator powierzył przetwarzanie danych w drodze umowy podmiotowi trzeciemu, wśród przesłanek dopuszczalności przetwarzania oznacza, że umowa powierzenia nie legalizuje procesu przetwarzania, czy też może stanowi samodzielną i odrębną od wymienionych przesłankę, ale wtedy gubi się sens regulacji zawartej w art. 6 RODO (oraz odpowiednio w stosunku do danych szczególnej kategorii – art. 9 RODO). Literalnie przepis art. 6 RODO stanowi, że przetwarzanie jest zgodne z prawem „wyłącznie w przypadkach, gdy - i w takim zakresie, w jakim - spełniony jest co najmniej jeden"

[307] M. Krzysztofek, *Ochrona..., op. cit.*, Legalis.
[308] t.j. Dz.U. z 2018 r. poz. 395.

z wymienionych w sześciu punktach warunków (przesłanek legalności przetwarzania danych). Nie ma wśród nich regulacji, że podstawą przetwarzania danych jest zawarta umowa powierzenia przetwarzania danych osobowych. W praktyce zatem podmiot przetwarzający może wykazać zawarcie umowy powierzenia przetwarzania danych z administratorem danych, ale w myśl przepisów RODO nie jest to przesłanką legalności przetwarzania. W związku z tym bez odpowiedzi pozostaje pytanie, która z przesłanek dopuszczalności przetwarzania zachodzi w przypadku powierzenia przetwarzania danych. Z drugiej jednak strony, z treści decyzji GIODO z 2001 roku wynika, że zawarcie umowy powierzenia przetwarzania danych, zgodnie z wymogami ustawy o ochronie danych osobowych, legalizuje proces przetwarzania danych przez podmiot będący stroną (zleceniobiorcą) takiej umowy[309]. Istnieje zatem uzasadniona potrzeba zaproponowania *de lege ferenda*, by wśród przesłanek legalizujących przetwarzanie danych osobowych umieścić również działanie polegające na „zlecaniu" przetwarzania danych osobowych innym podmiotom. Mogłoby to zostać ujęte w treści art. 6 ust. 1 RODO poprzez dodanie lit. „g", np. w sformułowaniu: „administrator danych powierzył przetwarzanie danych podmiotowi przetwarzającemu w drodze umowy na mocy art. 28 RODO". Dla zapewnienia spójności przepisów podobne sformułowanie mogłoby znaleźć się również w treści art. 9 ust. 2 RODO poprzez dodanie litery „k" o powyższej treści.

Formułując zasadę prawidłowości w treści art. 5 ust. 1 lit. d RODO jako zobowiązanie administratora, by przetwarzane dane były prawidłowe i w razie potrzeby uaktualniane, a także by podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane, prawodawca unijny w gruncie rzeczy przeniósł dotychczasową regulację obowiązującą na kanwie Dyrektywy 95/46/WE[310]. W nauce prawa powszechnie przyjęto nazwę zasada merytorycznej poprawności danych, taka nazwa funkcjonuje również częściej w praktyce. W przeciwieństwie do regulacji UODO z 1997 r. (art. 26 ust. 1 pkt 3

[309] Decyzja GIODO z dnia 23 listopada 2001 r., GI-DEC-DS-178/01, Legalis nr 464277.

[310] W treści nieobowiązującej już Dyrektywy 95/46/WE prawodawca w art. 6 ust. 1 lit. d stwierdził, że państwa członkowskie zapewniają, aby dane osobowe były prawidłowe oraz, w razie konieczności, aktualizowane; należy podjąć wszelkie uzasadnione działania, aby zapewnić usunięcie lub poprawienie nieprawidłowych lub niekompletnych danych, biorąc pod uwagę cele, dla których zostały zgromadzone lub dla których są dalej przetwarzane. Był to przepis bardzo rozbudowany i szczegółowy w stosunku do regulacji w prawie krajowym, która zawarta była w art. 26 ust. 1 pkt 3 UODO, zgodnie z którym administrator danych był obowiązany zapewnić, aby przetwarzane dane były merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Co istotne, ustawa odnosiła się do zagadnienia merytorycznej poprawności danych również w treści art. 35 ust. 1 UODO, stanowiącym że w razie wykazania przez osobę, której dane osobowe dotyczą, że są one niekompletne, nieaktualne, nieprawdziwe, administrator danych był obowiązany do uzupełnienia, uaktualnienia, sprostowania danych.

oraz art. 35 ust. 1), w przepisach RODO brakuje uszczegółowienia treści zasady prawidłowości. Można jednakże bazować na regulacjach zawierających wymogi dotyczące jakości przetwarzanych danych osobowych i stwierdzić, że w kontekście zasady prawidłowości danych, wymaga się od administratora danych, by były one prawidłowe (merytorycznie poprawne), aktualizowane w razie konieczności, usuwane lub poprawiane w przypadku gdy są nieprawidłowe lub niekompletne.

Trzonem omawianej zasady jest założenie, że przetwarzane dane powinny być prawidłowe. Przedstawiciele nauki prawa przedstawiają sposób rozumienia tej reguły w ten sposób, że dane, którymi dysponuje administrator danych osobowych powinny być merytorycznie poprawne, mieć swoje odzwierciedlenie w dokumentach źródłowych, być zgodne z treścią dokumentów źródłowych[311], a dokumentem takim może być np. formularz zgody na przetwarzanie danych osobowych. W wyroku z dnia z dnia 2 kwietnia 2007 r. Wojewódzki Sąd Administracyjny ustalił, że nazwisko osoby, której dane są przetwarzane winno być przetwarzane w takiej formie, w jakiej znajduje się w aktach stanu cywilnego i wystawianych na podstawie tych akt dokumentów tożsamości (np. dowodu osobistego, paszportu). Inne zapisy niż oryginalne mogą wprowadzać w błąd i są niepoprawne[312]. Aspekt prawidłowości danych oznacza również, że nie mogą one być zniekształcane ani modyfikowane w sposób niezgodny ze stanem faktycznym[313]. Mając na uwadze powyższe stwierdzenia, prawidłowość danych osobowych trzeba rozumieć jako wymóg przetwarzania danych w formie zgodnej z oryginałem wynikającym z dokumentów źródłowych, niemodyfikowanej w sposób niezgodny ze stanem faktycznym, pomimo stosowania takich operacji przetwarzania jak powielanie, kopiowanie, przenoszenie danych. Można również wywnioskować, że na administratora danych nałożono obowiązki korekcyjne – uzupełnienia lub sprostowania danych bez zbędnej zwłoki, co odczytywać należy jako działanie, którego celem jest zagwarantowanie, by przetwarzane dane były jak najlepszej jakości i jak najbardziej zbliżone do oryginału.

Drugi element omawianej zasady odnosi się do aktualizowania danych w razie konieczności. Może być traktowany jako obowiązek administratora danych do

[311] M. Krzysztofek, *Ochrona..., op. cit.,* Legalis.
[312] II SA/Wa 2328/06, Legalis nr 840404.
[313] M. Kuba, [w:] T. A. J. Banyś, E. Bielak-Jomaa, M. Kuba, J. Łuczak, *Prawo…, op. cit*., s. 116.

systematycznego przeglądu przetwarzanych danych pod kątem ich aktualizacji[314]. Wśród poglądów przedstawicieli nauki prawa można dostrzec, że element ten bywa nawet wyodrębniany jako samodzielna zasada aktualności danych – stanowiąca, że dane osobowe powinny odpowiadać aktualnemu (najnowszemu) stanowi rzeczy, na ile to możliwe oraz uzasadnione celem przetwarzania danych[315].

Wymienione wyżej elementy budzą wątpliwość w kontekście obowiązków administratora danych osobowych, poprzez które realizowana jest zasada prawidłowości. RODO nie precyzuje, czy od administratora wymaga się aktywnego podejścia i działań z jego inicjatywy w stosunku do dbałości o merytoryczną poprawność i aktualność przetwarzanych danych osobowych. Językowa wykładnia przepisu art. 6 ust. 1 lit. d Dyrektywy 95/46/WE, a w szczególności sformułowanie, że „należy podjąć wszelkie uzasadnione działania" wskazuje, że od administratora danych oczekiwało się podjęcia działań w celu zadbania o jakość przetwarzanych danych, natomiast sformułowanie „w razie konieczności" sugerowało, że działania te mają być odpowiedzią na zaistniałą konieczność, zatem nie muszą być inicjowane przez administratora. Wydaje się, że można w tym przypadku wykorzystać treść art. 35 ust 1 UODO z 1997 r., gdzie polski ustawodawca wprost sformułował obowiązek administratora, aktualizujący się *post factum* jako reakcja na wykazanie przez podmiot danych nieprawidłowości, niekompletności i nieaktualności jego danych. Jest to również pogląd wyrażony w nauce prawa, że zasada prawidłowości danych na gruncie RODO nie nakłada w sposób bezpośredni na administratora danych obowiązku aktywnego uprzedniego działania w celu dbałości o merytoryczną poprawność danych, a także, że granicą działań administratora w wykonaniu obowiązku prawidłowości danych powinny być rozsądne działania, aby dane osobowe, które są nieprawidłowe zostały niezwłocznie usunięte lub sprostowane[316]. Praktyka potwierdza słuszność spostrzeżeń poczynionych przez przedstawicieli nauki. Zauważyć warto, że jeśli rozumiemy poprawność merytoryczną przetwarzanych danych osobowych jako wymóg, by były one zgodne ze stanem faktycznym czy treścią dokumentów źródłowych, jak np. formularz zgody, to faktycznie administrator powinien z własnej inicjatywy dbać o to, by dane, które przetwarza, były danymi poprawnymi[317].

[314] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit.,* s. 474.
[315] *Ibidem*, s. 473.
[316] P. Barta, P. Litwiński, *Ustawa…, op. cit,* s. 316 oraz P. Litwiński (red.), *Rozporządzenie..., op. cit.,* Legalis.
[317] Przykładem sytuacji, która uzasadniałaby ten pogląd, może być zbieranie przez administratora od klientów formularzy z ich zgodą na przetwarzanie danych osobowych w celach marketingowych i

Argument wskazujący na powinność aktywnej dbałości o merytoryczną poprawność danych dla dobra administratora trudno jest zrównać z formalnym obowiązkiem aktywnego działania z własnej inicjatywy administratora nałożonym przez prawodawcę. W związku z tym, że należy w pełni podzielić stanowisko wyrażone w nauce prawa zgodnie z którym, jeżeli podmiot danych udowodni zaistnienie niezgodności w sferze jego danych osobowych podlegających przetwarzaniu, to w takim wypadku administrator danych ma obowiązek niezwłocznego uzupełnienia lub uaktualnienia, sprostowania danych[318].

W treści art. 5 ust. 1 lit. d RODO prawodawca zadbał o to, by waga jakości przetwarzanych danych osobowych miała odzwierciedlenie w regulacji stanowiącej zasadę przetwarzania i zastosowano tu przeniesienie przepisu Dyrektywy 95/46/WE do innego aktu prawnego bez merytorycznych modyfikacji, jedynie ze zmianami językowymi. Co ciekawe, przedstawiciele nauki prawa, wypowiadając się na temat zasady prawidłowości w kontekście RODO, idą o krok dalej, konkretyzując obowiązek zapewniania merytorycznej poprawności danych. Wyrażono to w stwierdzeniu, że administrator danych powinien oceniać wiarygodność źródła pozyskania danych, jak i wdrożyć sposób weryfikowania prawdziwości przetwarzanych danych. Administrator nie powinien zbierać danych osobowych z niewiadomych źródeł[319]. Pogląd ten rozumieć można w ten sposób, że zasięg przedmiotowej zasady obejmuje również działania administratora na samym początku procesu przetwarzania (pozyskiwania danych), a nawet na etapie przygotowań do przetwarzania (przed pozyskaniem). W kontekście zmian wprowadzonych przez RODO, a w szczególności w aspekcie zobowiązania administratorów danych do dokonywania oceny skutków dla ochrony danych, należy się zgodzić z powyższą interpretacją. Często wskazywany jest na gruncie nauki prawa przykład sytuacji, gdy dochodzi do naruszenia zasady prawidłowości danych – jako proceder zbierania danych osobowych ze źródeł niewiadomego pochodzenia, które nie są w stanie zagwarantować prawidłowości danych[320]. Przykładem naruszenia przedmiotowej

---

otrzymywanie informacji handlowej. Następnie administrator na podstawie formularzy tworzy bazę klientów, do których przesyła pocztą tradycyjną oferty swoich produktów lub usług. W sytuacji tej dbałość o to, by przetwarzane dane były poprawne merytorycznie (np. prawidłowe adresy korespondencyjne) oraz aktualne (np. usuwanie z bazy klientów nieżyjących), powinno następować poprzez aktywne działanie administratora podjęte z jego inicjatywy, chociażby dlatego, że w jego interesie jest by dysponował prawidłowymi danymi. W odwrotnym przypadku może ponosić straty, jeśli korespondencja będzie wysyłana na niepoprawny adres lub kierowana będzie do osób już nieżyjących.

[318] Tak m.in. P. Barta, P. Litwiński, *Ustawa…, op. cit.,* s. 315-316.

[319] A. Dmochowska, *Unijna…, op. cit*., Legalis

[320] *Ibidem*.

zasady w kontekście RODO może być też profilowanie oraz kategoryzowanie osoby w oparciu o dane niepotwierdzone, nieprawdziwe lub niekompletne (np. na podstawie portali społecznościowych), co może prowadzić do błędnych wniosków[321]. Warto zauważyć, że podobne sytuacje mogą jednocześnie służyć za przykład naruszania zasady szczególnej staranności przetwarzania danych. Jest to przykład przenikania się i bliskiego powiązania zasad przetwarzania danych osobowych. Jeśli chodzi o środki realizacji tej zasady, należy przyjąć pogląd, zgodnie z którym, o ile administrator danych zazwyczaj nie ma fizycznej możliwości monitorowania zmian danych klientów, np. w zakresie adresu zamieszkania, to powinien wdrożyć procedury korekty danych – tak na wniosek podmiotu danych, jak i wskutek samodzielnego powzięcia informacji o zmianach przez administratora z wiarygodnych źródeł[322].

Reasumując kwestię zasady prawidłowości przetwarzanych danych osobowych, powiedzieć można, że jej istotą jest wymóg merytorycznej poprawności, kompletności, aktualności i zgodności ze stanem faktycznym. Według stanowiska Generalnego Inspektora Ochrony Danych Osobowych[323], administrator danych powinien każdorazowo oceniać wiarygodność źródła danych osobowych; wypracowywać tryb weryfikowania prawdziwości danych (w zależności od tego, czy dane są zwykłe, czy szczególnie chronione); ustalać zasady postępowania w przypadku stwierdzenia nieprawdziwości danych[324]. Jak wykazano wyżej, bardzo problematyczną kwestią szczególnie w wymiarze praktycznym jest to, czy na administratorze danych spoczywa ustawowy obowiązek aktywnego i podejmowanego z własnej inicjatywy sprawdzania i uaktualniania, a także korekty danych. Problem ten można jednak rozwiązać, idąc w kierunku przyjęcia, że administrator nie jest formalnie do tego zobowiązany, ale dokonywanie przez niego weryfikacji i aktualizacji przetwarzanych danych z własnej inicjatywy, może być w praktyce korzystne z ekonomicznego punktu widzenia działalności administratora. Z jednej strony należy mieć na uwadze, że wprowadzenie stosownych sposobów weryfikacji i aktualizacji danych może powodować koszty po stronie administratora (takie jak zakup odpowiedniego oprogramowania czy też koszty pracownicze). Z drugiej jednak strony, w aspekcie biznesowym nie jest opłacalne przetwarzanie danych niepoprawnych i nieaktualnych, np. przy prowadzeniu marketingu na dużą skalę lub też wysyłaniu

[321] M. Krzysztofek*, Ochrona…, op. cit*., s. 71.
[322] *Ibidem*.
[323] Którym aktualnie jest Prezes Urzędu Ochrony Danych Osobowych (PUODO).
[324] M. Krasińska, S. Mizerek, *ABC wybranych zagadnień z ustawy o ochronie danych osobowych*, Warszawa 2007, s. 11.

korespondencji pocztą tradycyjną. Z powyższych względów rozstrzygnięcie należy pozostawić administratorom w oparciu o każdorazową ocenę okoliczności przetwarzania danych osobowych.

Zasada prawidłowości danych wydaje się nie rodzić większych komplikacji w sytuacjach, gdy procesy przetwarzania danych osobowych realizowane są przez administratora danych, który nie tylko ma obowiązek przestrzegania zasad przetwarzania danych osobowych, ale również jest zobowiązany wykazywać, że je przestrzega (art. 5 ust. 2 RODO). Problem może pojawić się w sytuacji gdy administrator danych sam nie przetwarza danych, bo powierzył je innemu podmiotowi na mocy art. 28 RODO. Patrząc przez pryzmat regulacji dotyczącej przetwarzania danych przez przetwarzającego w imieniu administratora danych, nie ma w niej mowy o wymogach związanych z prawidłowością powierzanych danych, które byłyby skierowane do przetwarzającego. Wywnioskować można z tego, że pomimo faktu, że prowadzenie operacji na danych powierzone zostaje innemu podmiotowi, odpowiedzialność za przestrzeganie merytorycznej poprawności danych nadal ciąży na administratorze. Wątpliwość jednak budzi to, czy ma on realną możliwość spełnienia swojego obowiązku, zwłaszcza gdy dane pozostają w dyspozycji przetwarzającego oraz czy ewentualnie możliwe jest przesunięcie tego obowiązku na przetwarzającego. To natomiast jest kwestia związana z instrumentem prawnym, w drodze którego dokonywane jest powierzenie (umowa), jak również zasady swobody umów. Wydaje się, że nie ma przeszkód co do rozwiązania polegającego na umieszczeniu w treści umowy postanowienia o tym, że to podmiot przetwarzający ma dbać o prawidłowość i aktualność przetwarzanych danych. W związku z tym można stwierdzić, że uregulowanie powierzenia przetwarzania danych zarówno w przepisach RODO, jak i nieobowiązujących od 25 maja 2018 roku przepisach o ochronie danych osobowych, nie jest spójne z zasadą prawidłowości danych i nie w pełni pozwala na jej efektywne realizowanie.

3.2. Zasada niezbędności danych

Kryterium wyodrębnienia tej grupy zasad jest zakres przetwarzania danych osobowych, zarówno w aspekcie ilościowym, jak i czasowym. Wynika to z ogólnych wytycznych, że przetwarzać można tylko te dane, które są niezbędne i tylko tak długo, jak jest to niezbędne. Elementem łączącym jest tu cel przetwarzania. W ramach tej grupy

znajdą się normatywna zasada ograniczenia celu, zasada minimalizacji danych oraz zasada ograniczenia przechowywania.

Z punktu widzenia ochrony danych osobowych cel jest jednym z najważniejszych oraz niezbędnym elementem w procesie przetwarzania danych. Można zaryzykować stwierdzenie, że bez zidentyfikowania celu przetwarzanie w ogóle nie może mieć miejsca. W treści RODO omawiana zasada otrzymała nazwę „ograniczenia celu" i ujęta jest w treści art. 5 ust. 1 lit. b RODO. Zgodnie z nią dane muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami. Wymogi co do celu przetwarzania zawarte są w motywie 39 preambuły RODO, gdzie przewidziano, że konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. W odniesieniu do powyższych regulacji, z uwagi na to, że są one bardzo zbliżone do dotychczas obowiązujących w Dyrektywie 95/46/WE oraz przepisach UODO z 1997 r., aktualne pozostają poglądy wyrażone w nauce, jak również orzecznictwie i decyzjach GIODO, dotyczące zasady celowości i związania celem (taka nazwa została przyjęta w literaturze i orzecznictwie, w ten sposób zasadę tę określano przed rozpoczęciem stosowania RODO).

Analizując regulacje aktów prawnych stanowiących podstawę prowadzonych rozważań, na pierwszy rzut oka zauważa się, że prawodawca unijny i polski ustawodawca podobnie podchodzą do zasady ograniczenia celu. W treści UODO z 1997r. zasada ujęta była w art. 26 ust. 1 i 2, zgodnie z którymi administrator danych był obowiązany zapewnić, aby dane były zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami, z zastrzeżeniem, że przetwarzanie danych w celu innym niż ten, dla którego zostały zebrane, było dopuszczalne, jeżeli nie naruszało praw i wolności osoby, której dane dotyczą, oraz następowało w celach badań naukowych, dydaktycznych, historycznych lub statystycznych. Różnice między regulacją ustawową a zawartą w Dyrektywie 95/46/WE tkwiły tylko w szczegółach[325] .

[325] W art. 6 ust. 1 lit. b Dyrektywy 95/46/WE wskazywało się, że dane osobowe mają być gromadzone do określonych, jednoznacznych i legalnych celów oraz nie poddawane dalszemu przetwarzaniu w sposób

W literaturze przedmiotu dostrzega się, że w naukowym ujęciu zasad przetwarzania danych osobowych cel występuje w dwóch aspektach, w konsekwencji czego następuje wyodrębnienie dwóch zasad: zasady celowości i zasady związania celem.

Po pierwsze, formułuje się zasadę celowości, nazywaną też zasadą określoności celu[326], jako wymóg wyraźnego określenia celu. Innymi słowy, przed rozpoczęciem przetwarzania pierwszym etapem jest wskazanie, w jakim celu przetwarzane będą dane. Nie powinno ulegać wątpliwości, po co są zbierane i czemu ma służyć ich przetwarzanie. W literaturze przedmiotu wywodzi się z tego zakaz pomijania[327] oraz zatajania[328] celu przetwarzania. Ocena spełniania zasady celowości powinna następować w dwóch aspektach: w aspekcie formalnym – ustalenie, czy cel został zidentyfikowany i określony, nie wnikając w samą jego treść, jak również w aspekcie materialnym, merytorycznym – czy cel jest zgodny z prawem. Przy czym nie określono tu, czy zgodność z prawem powinna być traktowana szeroko jako zarówno zgodność z normami prawa stanowionego, jak i zasadami współżycia społecznego i dobrymi obyczajami[329], czy też wąsko jako zgodność z normami wynikającymi z prawa stanowionego. Nie ma jednoznacznej odpowiedzi na tę wątpliwość na gruncie nauki prawa, choć z pomocą przychodzą stanowiska przedstawicieli doktryny, zgodnie z którymi cel musi być dozwolony przez prawo lub co najmniej obojętny z punktu widzenia norm prawnych, ale nie zabroniony[330]. Kolejnym etapem będzie ocena, czy przetwarzanie jest zgodne z określonym uprzednio celem. W ocenie autorytetów w dziedzinie ochrony danych osobowych ocena zgodności przetwarzania z celem jest problematyczna w praktyce, więc proponuje się ustalanie nie każdorazowo dla osiągnięcia jakiego celu realizowane jest przetwarzanie, ale czy przetwarzanie nie wykracza poza określony cel[331].

---

niezgodny z tym celem. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie jest uważane za niezgodne z przepisami pod warunkiem ustanowienia przez Państwa Członkowskie odpowiednich środków zabezpieczających.

[326] M. Jagielski, *Prawo…, op. cit.,* s. 89.

[327] A. Krasuski, *Dane…, op. cit*, s. 157.

[328] T. Szewc, *Ochrona…, op. cit.,* s. 26.

[329] Przywołać warto pogląd M. Safjana dotyczący bezprawności: „Prawo prywatne inkorporowało do pojęcia „bezprawności" zachowanie nie tylko naruszające reguły prawa stanowionego, ale także reguły słusznościowe. Zachowanie bezprawne, a więc rodzące negatywne konsekwencje dla sprawcy, przede wszystkim sankcje odszkodowawcze, to także zachowanie niegodziwe, naruszające standardy przyzwoitości w relacjach z innymi podmiotami, naruszające szeroko rozumiane reguły prawidłowego w sensie moralnym i obyczajowym postępowania", M. Safjan (red.), *System... op. cit.,* s. 357, Legalis. Na temat zasady słuszności zob. Szerzej zbiór publikacji zawarty w Białostockich Studiach Prawniczych 2014 r., z. 17.

[330] T. Szewc, *Ochrona…, op. cit*., s. 26.

[331] M. Jagielski, *Prawo…, op. cit*., s. 90.

Po drugie, w momencie, kiedy ustalony i wyraźnie określony został cel przetwarzania danych, jest on wiążący dla całego procesu przetwarzania (zasada związania celem). Cel ustalony przez administratora danych wyznacza granice przetwarzania przez niego danych, ponieważ co do zasady nie dopuszcza się wykraczania poza ramy celu, jaki ustanowiono pierwotnie. Podkreślić przy tym należy, że ustawodawca nie zabrania przetwarzania danych osobowych w celu innym niż pierwotnie ustalony, innymi słowy, nie ma wśród zasad przetwarzania danych takiej reguły jak zasada niezmienności celu przetwarzania, a jedynie zasada związania celem i wywodzony z niej zakaz przetwarzania danych w celu niezgodnym z pierwotnie określonym[332]. Oznacza to w praktyce, że jeżeli zebrano dane osobowe w określonym celu np. do procesu rekrutacji, na podstawie zgody podmiotu danych (zgoda na cel pierwotny), to przetwarzanie danych w celach marketingowych (bez uzyskania zgody na ten cel) będzie oznaczało przetwarzanie niezgodne z pierwotnym celem. Tego typu sytuacje często stanowią przedmiot rozstrzygnięć GIODO i sądów. Jako przykład powołać można decyzję GIODO z 2011 roku. Zapadło w niej rozstrzygnięcie, w którym stwierdzono, że dane osobowe Skarżącego zawarte w zaświadczeniu o zatrudnieniu zostały zebrane przez bank w celu przyznania kredytu. Dane te, pozyskane w celach służbowych, mogły być legalnie wykorzystane wyłącznie dla realizacji tych celów. Wykorzystanie tych danych w celu prywatnym, a więc innym niż ten, dla którego zostały zebrane, stanowiło naruszenie art. 26 ust. 1 pkt 2 UODO z 1997 r.[333], a aktualnie stanowiłoby naruszenie art. 5 ust. 1 lit. b RODO. Można więc wyciągnąć wniosek, że dalsze przetwarzanie danych w innym celu niż zakomunikowany osobie w momencie zbierania danych, będzie wymagało uzyskania zgody osób, których dane dotyczą, lub też spełnienia innej przesłanki legalności przetwarzania danych, zawartej w treści art. 6 RODO. Jeśli w odniesieniu do przetwarzania danych w nowym celu nie uzyska się nowej zgody, nie wystąpi żadna z przesłanek wskazanych w powołanym przepisie i nie wystąpi wyjątek określony w treści art. 5 ust. 1 lit. b RODO, przetwarzanie będzie należało traktować jako nielegalne. Tym samym uwidacznia się bardzo ścisłe powiązanie zasady celowości i związania celem z zasadą legalności przetwarzania danych osobowych. Zasada legalności ma w tym zestawieniu charakter uzupełniający.

[332] P. Barta, P. Litwiński, *Ustawa…, op. cit.,* s. 310.
[333] Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dnia 15 kwietnia 2011 r., DOLiS/DEC-304/11, Legalis nr 1348599.

Zagadnieniem wymagającym uwagi jest kwestia określania celu przetwarzania danych. Istotnym do odnotowania jest fakt, że zagadnienie ustalenia celu przetwarzania danych osobowych następuje inaczej w przypadku podmiotów sektora publicznego, a inaczej w przypadku podmiotów sektora prywatnego.

Jeśli chodzi o podmioty sektora prywatnego, zgodnie przyjmuje się na gruncie nauki prawa opinię, że administrator danych nie jest w kwestii ustalenia celu przetwarzania danych niczym nieograniczony. Uznaje się, że cel musi mieścić się w zakresie działalności prowadzonej przez administratora[334]. Dla wyjaśnienia powiązania celu przetwarzania z zakresem działalności administratora, warto powołać się na stanowisko, zgodnie z którym „administrator musi wykazać, iż dokonanie przetworzenia danych ma miejsce w ramach prowadzonej przez niego legalnej działalności i tylko w takim zakresie, w jakim cel przetworzenia danych pokrywa się z celami przedsięwzięć podejmowanych w ramach działalności"[335]. Można zatem wywnioskować, że definicja administratora danych osobowych jako podmiotu decydującego o celach i sposobach przetwarzania danych, sugerująca, że status administratora cechuje samodzielność niezależność i szerokie pole do decydowania, jest *de facto* ograniczona okolicznościami dotyczącymi działalności administratora danych.

W nauce prawa zgodnie wskazuje się, że w przypadku gdy administrator danych jest podmiotem sektora publicznego, to cele przetwarzania danych osobowych wyznaczane są w treści przepisów przyznających kompetencje do przetwarzania danych, co oznacza, że „jeżeli podmiot ze sfery prawa publicznego zbiera dane osobowe dla realizacji celów wskazanych w przepisach przyznających mu kompetencję do przetwarzania tych danych, należy uznać, że spełnia zarówno warunek przetwarzania danych osobowych dla celów zgodnych z prawem, jak i dla celów oznaczonych"[336]. Na tej podstawie można wyciągnąć wniosek, że przepisy przewidujące zadania i kompetencje podmiotu publicznego jednocześnie wyznaczają cel przetwarzania danych, a analiza tych przepisów będzie niezbędna do oceny, czy podmiot postępuje zgodnie z zasadą celowości i związania celem przetwarzania[337].

[334] A. Drozd, *Ustawa..., op. cit.,* s. 159.
[335] M. Jagielski, *Prawo…, op. cit*., s. 91.
[336] P. Barta, P. Litwiński, *Ustawa…, op. cit.,* s. 309.
[337] Przykład stanowić może art. 80a i kolejne (dotyczące danych w centralnej ewidencji pojazdów) ustawy z dnia 20 czerwca 1997r. Prawo o ruchu drogowym (t.j. Dz.U. z 2017 r. poz. 1260)

Ponadto cel przetwarzania danych osobowych niejednokrotnie wynika z przepisu prawa w sposób bezpośredni. Przykładem takiej sytuacji jest zawarcie w ustawie z dnia 29 sierpnia 1997 r. Prawo bankowe[338] art. 112b, zgodnie z którym banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych. Działalność bankowa stanowi przedmiot regulacji w art. 5 i 6 ustawy Prawo bankowe. Nie można również pominąć tego, że cel wynika bardzo często z treści umowy zawieranej między administratorem danych osobowych, a osobą, której dane dotyczą. Chodzi tu przede wszystkim o umowy w bieżących sprawach życia codziennego. Przykładem jest zawarcie umowy z operatorem telefonii komórkowej na usługi telekomunikacyjne, czy też umowa sprzedaży w sklepie internetowym. Ponadto w życiu codziennym zdarza się, że cel przetwarzania danych wynika z samej treści czynności faktycznej – osoba fizyczna podaje swoje dane osobowe przy założeniu karty bibliotecznej, po to, by móc korzystać z zasobów biblioteki i wypożyczać książki. Zasada ograniczenia celu nie będzie z punktu widzenia prawa przestrzegana w takich sytuacjach, gdy cel przetwarzania danych jest możliwy do wyinterpretowania przez osobę, której dane dotyczą, ale nie został jej zakomunikowany w sposób wyraźny i jasny.

Prawodawca nie sprecyzował, w jaki sposób ma być określany cel przetwarzania danych osobowych. Cel przetwarzania nie może być określony zbyt ogólnie, nie będzie właściwym rozwiązaniem jedynie ogólnikowa informacja np. dla celów komercyjnych[339]. W praktyce życia codziennego bardzo często spotykamy się z udzielaniem zgody na przetwarzanie danych osobowych w celach marketingowych. Jednakże wymagać należy, żeby administrator danych doprecyzował, czego dotyczy marketing i za pomocą jakich środków jest prowadzony. Należy wziąć pod uwagę, że niejednokrotnie sformułowanie celu może również rzutować na czas przetwarzania danych. Jest to kolejny argument przemawiający za postawioną na wstępie tezą o ścisłym powiązaniu, przenikaniu się i wzajemnym uzupełnianiu zasad przetwarzania danych osobowych. Jako przykład takiej sytuacji wskazuje się przetwarzanie danych przez pracodawcę w celu przeprowadzenia rekrutacji na określone stanowisko pracy – faktycznie okres przetwarzania danych będzie zależny od terminu zakończenia rekrutacji[340]. Administrator danych osobowych ma obowiązek wyraźnego oznaczenia celu, a oznaczenie powinno z reguły być zrealizowane

[338] T.j. Dz.U. z 2017 r. poz. 1876.
[339] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit.,* s. 470.
[340] A. Dmochowska, *Unijna…, op. cit*., Legalis.

w formie pisemnej, co ułatwia dokonanie oceny przestrzegania zasady związania celem[341]. Jednakże stanowisko to spotyka się z kontrargumentacją. Według odmiennej opinii ze względu na brak wymogu szczególnej formy w powołanych przepisach, nie może być uznane za słuszne stanowisko wskazujące, że oznaczenie celów przetwarzania danych powinno być z reguły zrealizowane w formie pisemnej[342]. Powyższe argumenty nie wykluczają się nawzajem i należy przyznać rację obu z nich jednocześnie, o ile interpretowane będą w ten sposób, że rzeczywiście brak wymogu szczególnej formy określenia celu przetwarzania danych w powołanych przepisach ustawy sam w sobie nie przyznaje priorytetowego znaczenia formie pisemnej spełnienia tego wymogu, ale zrealizowanie obowiązku oznaczenia celu w formie pisemnej, jako najłatwiejszej do wykazania jej skuteczności, ułatwia wykazanie przestrzegania omawianej zasady.

Według GIODO (aktualnie PUODO) zbierający dane nie może pominąć ani zataić tego celu oraz nie można określać celu przetwarzania danych w sposób ogólnikowy. Ponadto cel ten powinien być zakomunikowany zainteresowanemu przed zebraniem danych osobowych. Niedopuszczalne jest uzależnianie zawarcia umowy od wyrażenia zgody na przetwarzanie danych w zupełnie innych celach (np. marketingu produktów i usług podmiotów trzecich)[343]. Wydaje się, że niezbędnym jest uzupełnienie istoty przedmiotowej zasady. Przede wszystkim związanie celem przetwarzania nie oznacza niezmienności celu. Ustalenie celu przetwarzania danych osobowych następuje inaczej w przypadku podmiotów sektora publicznego, a inaczej w przypadku podmiotów sektora prywatnego. Co wykazano w treści powyższych rozważań, zasada ta nie zawsze daje jednoznaczne wskazówki i budzi kilka wątpliwości, których rozstrzygnięcie wymaga każdorazowej oceny okoliczności konkretnego przypadku. Z tego też względu wiele spraw zostaje skierowanych do rozpatrzenia Prezesa Urzędu Ochrony Danych Osobowych (PUODO, wcześniej GIODO) w drodze decyzji administracyjnej[344] bądź sądów w formie wyroków.

W zestawieniu powyższych uwag z zagadnieniem istoty powierzenia przetwarzania danych osobowych, nie wymaga szczegółowego uzasadnienia, że cel jest jednym z podstawowych elementów powierzenia i treści umowy powierzenia. Cel przetwarzania

[341] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit.,* s. 470.
[342] P. Barta, P. Litwiński, *Ustawa…, op. cit.,* s. 310.
[343] https://edugiodo.giodo.gov.pl/file.php/1/UST/UST_03_02.htm.
[344] Np. Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dnia 22 maja 2012 r. DOLiS/DEC-458/12/31753, Legalis nr 804426 czy też Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dnia 1 czerwca 2011 r. DOLiS/DEC-442/11, Legalis nr 464291.

literalnie znalazł się w treści art. 28 ust. 3 RODO wśród niezbędnych elementów umowy bądź innego instrumentu prawnego regulującego relację między administratorem danych Interpretować to należy w ten sposób, że określenie celu przetwarzania danych w treści umowy powierzenia stanowi konieczny warunek prawidłowości nawiązania stosunku prawnego powierzenia. Bez tego działania przetwarzającego mogą być uznane za niezgodne z prawem. Jeśli powierzenie danych następuje w określonym celu, to wszystkie działania podmiotu przetwarzającego powinny realizować dokładnie ten cel, z uwagi na fakt, że wiążą go postanowienia umowne. Można przewidywać, że zmiana celu w trakcie trwania stosunku powierzenia spowoduje konieczność zmiany umowy powierzenia. Należy uznać, że zasada ograniczenia celu jest w pełni realizowana w rozwiązaniu, jakim jest powierzenie danych do przetwarzania w drodze umowy.

Zasada minimalizacji danych sformułowana w treści art. 5 ust. 1 lit. c RODO, stanowiącego, że dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane, zastąpiła znaną z przepisów Dyrektywy 95/46/WE oraz przepisów UODO z 1997 r. zasadę adekwatności danych. Należy zwrócić uwagę, że odmiennie niż w przypadku większości zasad, które stanowią co do zasady powtórzenie pod inną nazwą uchylonych przepisów, RODO rzuca nowe światło na kwestię adekwatności przetwarzania danych. W dużej mierze jednak obie zasady są oparte na tym samym fundamencie – treściowym i ilościowym ograniczeniu przetwarzania danych. Dlatego należy podjąć się analizy zarówno zasady minimalizacji, jak i zasady adekwatności danych.

W motywie 39 preambuły RODO ustanowiono, że dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Z powołanych regulacji jasno wynika, że w nowym stanie prawnym prawodawca posuwa się o krok dalej i w miejsce zasady adekwatności kształtuje bardziej rygorystyczną zasadę minimalizacji danych[345]. Trudno wobec tego zgodzić się z odmiennym poglądem wyrażonym w nauce prawa, że zasada adekwatności została zawarta w RODO w postaci takiej, jak w ustawie o ochronie danych osobowych[346]. Świadczy o tym z jednej strony fakt, że w treści RODO poświęconej zasadom przetwarzania (art. 5) prawodawca nie wymienia zasady

[345] P. Litwiński (red.), *Rozporządzenie …, op. cit.,* Legalis.
[346] A. Dmochowska, *Unijna…, op. cit*., Legalis.

adekwatności wśród nazwanych wprost zasad, a z drugiej w treści UODO z 1997 r. nie dostrzegało się tak wyraźnego kierunku, by przetwarzanie danych mogło następować tylko wtedy, gdy inaczej nie można osiągać celu, w którym dane są przetwarzane. Z uwagi na zmianę w kierunku zwiększenia restrykcyjności przepisów, warto w pierwszej kolejności poświęcić uwagę zasadzie adekwatności funkcjonującej na gruncie Dyrektywy 95/46/WE oraz UODO 1997 r., a następnie zasadzie minimalizacji danych konstruowanej z przepisów RODO.

Zasada adekwatności danych do celów przetwarzania danych osobowych w przepisach prawa wyrażana była dość zdawkowo. Ustawodawca w treści art. 26 ust. 1 pkt 3 UODO z 1997 r. stanowił, że przetwarzane dane mają być merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane. Łączył ją razem z zasadą prawidłowości danych i nie zapewniał dodatkowych wyjaśnień. Bardziej szczegółowy był prawodawca unijny, stanowiąc wymóg w treści art. 6 ust. 1 lit. c Dyrektywy 95/46/WE, by dane były prawidłowe, stosowne oraz nie nadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone. Tutaj również reguła ta została połączona z zasadą merytorycznej poprawności danych. Należy jednak zauważyć, że faktycznie zasada adekwatności byłą bardzo blisko związana z zasadą celowości przetwarzania danych, mniej wspólnego miała z zasadą merytorycznej poprawności.

Zasada adekwatności na gruncie nauki prawa była też nazywana zasadą proporcjonalności. Odnosiła się do zakresu danych, jakie mogą być przetwarzane przez administratora danych, a konkretniej, określała stosunek zależności między celem a zakresem przetwarzania danych. Interpretować ją można jako obowiązek zapewnienia, by przetwarzane były tylko te dane osobowe, które są istotne i niezbędne dla celów przetwarzania. W literaturze przedmiotu sformułowany został pogląd, że zasadę tę konstruowały dwa wymogi – uprawnienie administratora do zbierania tylko danych niezbędnych do osiągnięcia celu przetwarzania oraz konieczność usuwania lub poddawania anonimizacji danych, które stały się zbędne do osiągnięcia celu[347]. Co warte podkreślenia, dane powinny być odpowiednie zarówno pod względem liczby, jak i ich treści[348]. Zasada adekwatności bardzo ściśle związana była z konstytucyjną zasadą proporcjonalności, co dostrzegł Trybunał Konstytucyjny w wyroku z dnia 20 listopada 2002 roku dotyczącym danych w deklaracjach majątkowych zbieranych przez urzędy

[347] M. Jagielski, *Prawo…, op. cit*., s. 87.
[348] M. Krzysztofek, *Ochrona…, op. cit.,* s. 65.

skarbowe. Znalazło się tam stwierdzenie, że relacja proporcjonalności dotyczyć ma konieczności użytego środka (deklaracja majątkowa) do założonego celu (jednego ze wskazanych w art. 31 ust. 3 Konstytucji) i to w stopniu adekwatnym do poświęconego dobra (autonomia informacyjna). Taka zaś relacja między deklaracjami majątkowymi i usprawnieniem poboru podatku dochodowego - nie zachodzi. "Celowości", "pożyteczności" nie można utożsamiać z "koniecznością" tego instrumentu (decydującą o jego konstytucyjności) w warunkach, gdy o słabości realizacji podatku dochodowego decyduje nie brak informacji, lecz nieudatność jej przetwarzania, a deklaracje majątkowe same w sobie także wymagają przetworzenia[349]. W orzeczeniach sądów administracyjnych zgodnie wyrażany jest pogląd, że zasada adekwatności powinna być rozumiana jako równowaga pomiędzy uprawnieniem osoby do dysponowania swoimi danymi, a interesem administratora danych. Równowaga będzie zachowana, jeżeli administrator zażąda danych tylko w takim zakresie, w jakim jest to niezbędne do wypełnienia celu, w jakim dane są przez niego przetwarzane[350]. Zasada adekwatności pełniła zatem podwójną funkcję. Po pierwsze, wyznaczała granice działań administratorów danych – mogą oni zbierać tylko dane w zakresie niezbędnym do celów ich przetwarzania. Po drugie, chroniła podmioty danych przed nieuzasadnioną ingerencją w ich prywatność poprzez pozyskiwanie danych osobowych w nadmiernej ilości i nadmiernej treści. W ten sposób zasada adekwatności tworzyła racjonalne proporcje i balans pomiędzy interesami administratora danych, a dobrem podmiotu danych.

Z zasady minimalizacji danych wynika obowiązek administratora do ograniczenia zakresu przetwarzanych danych osobowych jedynie do takich, bez których nie będzie możliwe osiągnięcie zamierzonego celu przetwarzania[351]. Na podstawie wypowiedzi przedstawicieli nauki można wyeksponować dwa aspekty minimalizacji. Chodzi tu o potrzebę wyselekcjonowania jedynie tych danych, które są potrzebne do danej działalności oraz ograniczenie okresu przechowywania danych[352]. Co za tym idzie, administratorzy danych powinni aktualnie zweryfikować, czy przetwarzane w ramach ich

[349] K 41/02, Legalis nr 55361.
[350] Wyrok Wojewódzkiego Sądu Administracyjnego siedziba w Warszawie z dnia 26 sierpnia 2010 r. II SA/Wa 923/10 LEX nr 456399, Wyrok Naczelnego Sądu Administracyjnego z dnia 30 listopada 2011 roku, I OSK 2118/10, http://orzeczenia.nsa.gov.pl/doc/6A2A1D2737.
[351] P. Litwiński (red.), *Rozporządzenie…, op. cit.,* Legalis.
[352] A. Jankowska-Galińska, K. Sawicka, *RODO: Zmiany w zasadach przetwarzania danych osobowych*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/RODO-zmiany-w-zasadach-przetwarzania-danych-osobowych.html.

działalności dane osobowe są adekwatne do celu przetwarzania[353]. Z samego sformułowania przepisu art. 5 ust. 1 lit. c RODO można wywnioskować, że zasada minimalizmu objęła swoim zakresem zasadę adekwatności, przez co ma szerszy zakres treściowy niż adekwatność. Zawiera się w niej wymóg, by dane były adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane, co oznacza *de facto* połączenie elementów zasad adekwatności, celowości, ograniczonego czasu przetwarzania oraz prawidłowości. Zasada ta koresponduje z treścią art. 51 ust. 2 Konstytucji RP, zgodnie z którym władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym. O zasadzie minimalizacji danych wspominano w literaturze przedmiotu już dużo wcześniej niż znana była treść przepisów RODO[354]. Ponadto warto podkreślić, że analizując fragment preambuły o tym, że dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami, można przyjąć, że sugerują one w sposób generalny ograniczenie procesów przetwarzania danych. Trzeba zwrócić uwagę na konotację z rzadko wspominaną na gruncie nauki prawa zasadą nullifikacji, którą przewidziano w treści art. 3 lit. a niemieckiej federalnej ustawy o ochronie danych osobowych. Stwierdzono, że systemy przetwarzania danych powinny być zaprojektowane i wybrane by nie gromadzić, przetwarzać i używać danych osobowych w ogóle, albo w tak niewielkim stopniu jak to tylko możliwe[355]. Zasada nullifikacji jest ostrzejszym środkiem niż zasada minimalizacji danych. Przy nullifikacji regułą byłoby dążenie do (w miarę możliwości) wyeliminowania operacji przetwarzania danych albo przetwarzania w marginalnym stopniu na zasadzie wyjątku, natomiast minimalizację charakteryzuje dopuszczenie przetwarzania, ale z zapewnieniem, by odbywało się w jak najmniej szkodliwym stopniu. Zestawiając zacytowany przepis niemieckiej ustawy z treścią RODO, można wyciągnąć wniosek, że prawodawca unijny, ustanawiając nowe przepisy nie sięgnął po ostateczne środki, działał zachowawczo i racjonalnie, czego efektem jest dalej posunięta ochrona danych niż przewidywała to Dyrektywa 95/46/WE, ale z zachowaniem racjonalnych proporcji.

W kwestii rozstrzygnięcia, czy przetwarzając określone dane osobowe, administrator danych wywiązuje się z obowiązku przetwarzania danych adekwatnych,

[353] D. Michalski, *RODO: przetwarzanie danych pod kątem adekwatności*, Rzeczpospolita, 6 października 2017 roku, http://www.rp.pl/Firma/310069981-RODO-przetwarzanie-danych-pod-katem-adekwatnosci.html.
[354] M. Jagielski w 2010r. pisał o zasadzie minimalizmu.
[355] Cyt. za M. Jagielski, *Prawo…, op. cit.*, s. 88.

stosownych oraz ograniczonych do tego, co niezbędne do celów, stwierdzić należy, że nie istnieje kryterium odniesienia w postaci generalnego katalogu danych, które w sposób powszechny mogą być przetwarzane (np. imię i nazwisko) jako dane zawsze niezbędne do celu przetwarzania. Nie ma też uniwersalnego katalogu danych, uznanych z góry za nieadekwatne (np. skan wzoru siatkówki oka jako dane zbędne, które zawsze mogą być zastąpione innym rodzajem danych mniej ingerujących w sferę prywatności osoby). Często punktem odniesienia przy ocenie adekwatności mogą być przepisy prawa, pozwalające podmiotom na przetwarzanie określonych danych w określonego typu sytuacjach[356]. W praktyce często istnieje konieczność indywidualnej interpretacji zasady adekwatności w poszczególnych przypadkach oraz oceny, czy zestaw przetwarzanych danych zawiera wyłącznie dane niezbędne do osiągnięcia celu[357].

Kwestia interpretacji zasady minimalizacji danych pojawia się często w sprawach z życia codziennego. Niejednokrotnie sądy wypowiadają się bardzo ogólnie, nie podając rozwiązań bezpośrednio i wprost[358]. Bywa również tak, że sądy konkretyzują zakres przetwarzanych danych lub jednoznacznie stwierdzają, w jakich przypadkach proporcjonalności brakuje[359]. Z dorobku judykatury można wyciągnąć wniosek, że zasada minimalizacji decyduje o tym, czy administrator może przetwarzać określone dane

[356] Jako przykłady wskazać można art. 112b ustawy Prawo bankowe: Banki mogą przetwarzać dla celów prowadzonej działalności bankowej informacje zawarte w dokumentach tożsamości osób fizycznych; art. 60b ustawy Prawo telekomunikacyjne: Abonent (…) podaje dostawcy usług następujące dane: imię i nazwisko, numer PESEL, jeżeli go posiada, albo nazwę, serię i numer dokumentu potwierdzającego tożsamość, a w przypadku cudzoziemca, który nie jest obywatelem państwa członkowskiego albo Konfederacji Szwajcarskiej - numer paszportu lub karty pobytu; art. 22^1 Kodeksu Pracy: Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących: imię (imiona) i nazwisko; imiona rodziców; datę urodzenia; miejsce zamieszkania (adres do korespondencji); wykształcenie; przebieg dotychczasowego zatrudnienia.

[357] M. Krzysztofek, *Ochrona…, op. cit.,* s. 65.

[358] Jako przykład zacytować można treść wyroku Sądu Apelacyjnego w Lubinie z dnia 11 maja 2016 roku, I ACa 874/15, Legalis nr 1470120: Zakres danych i informacji udostępnianych właścicielom lokali powinien być adekwatny do ich potrzeb związanych ze zgodnym z prawem celem udostępniania. (…) niedopuszczalne jest udostępnianie członkom wspólnoty tylko tych danych, których przetwarzanie nie jest niezbędne do współdziałania w zarządzie nieruchomością wspólną oraz do sprawowania kontroli działalności zarządu. Natomiast nie ulega wątpliwości, że skoro wszyscy właściciele lokali są współwłaścicielami nieruchomości wspólnej i tworzą wspólnotę mieszkaniową, to powinni mieć wiedzę o tym komu jeszcze to prawo przysługuje. Z zacytowanego orzeczenia nie wiadomo, jakie konkretnie dane mogą być udostępniane współwłaścicielom nieruchomości.

[359] Takim przykładem, kiedy na gruncie orzecznictwa uwidacznia się istotność zasady adekwatności oraz pomocny charakter rozstrzygnięć sądów, jest wyrok Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 4 listopada 2011 r.(II SA/Wa 1002/11, Legalis nr 400297): W ocenie Sądu, organ prawidłowo w uzasadnieniu zaskarżonej decyzji wykazał brak istnienia ustawowego celu i adekwatności przetwarzania danych osobowych w przypadku, gdy pracodawca żąda podania *en bloc* od organizacji związkowej danych osobowych pracowników należących do związku bez powołania się na wyżej wskazane okoliczności (np. wynikające z art. 38 lub art. 52 Kodeksu pracy), dopuszczające przetwarzanie przez pracodawcę takich danych.

osobowe, w tym, czy może je udostępniać innym podmiotom. Ponadto powołanie się na tę zasadę pomaga podmiotom danych ograniczać chęć pozyskiwania danych w nadmiernej liczbie i zbędnej treści przez administratorów.

Rozważenia wymaga również sytuacja, gdy administrator danych za zgodą podmiotu danych pozyskuje dane osobowe, które nie są niezbędne do celu, w jakim dane są przetwarzane. Innymi słowy, chodzi tu o zgodę na przetwarzanie danych w szerszym zakresie, wychodzącym poza granice adekwatności do celu. Czy zgoda ta stanowi wystarczające usprawiedliwienie i niweluje obowiązek przestrzegania zasady adekwatności? Odpowiedź na to pytanie może ułatwić orzecznictwo sądów administracyjnych. Z treści wyroku Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 7 grudnia 2009 r. wynika, że nawet wykazanie przez administratora danych, że legitymuje się przynajmniej jedną z przesłanek przewidzianych w art. 23 ust. 1 UODO z 1997 r. (aktualnie art. 6 ust. 1 RODO), nie wyłącza oceny adekwatności danych osoby w stosunku do celów, w jakich są one przetwarzane. Podkreślić należy, że zasada adekwatności ma charakter bezwzględnie obowiązujący[360]. Ponadto, podrzędny charakter zgody wobec zasady adekwatności wykazany został w wyroku Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 1 grudnia 2005 r. Sąd przyjął, że udzielenie zgody na przetwarzanie danych osobowych w zakresie szerszym niż wyznaczony zasadą adekwatności danych do celu nie może być prawnie skuteczne[361].

W praktyce życia codziennego zasada minimalizacji bywa niejednokrotnie łamana, często administratorzy danych mają intencje pozyskiwania danych „na zapas". Potwierdzeniem powyższego stanowiska jest fakt, że GIODO (aktualnie PUODO) stosunkowo często podejmuje działania w zakresie weryfikacji przestrzegania zasady adekwatności przez administratorów danych. Przykładem takiej interwencji było sprawdzenie w 2010 roku na skutek sygnałów ze strony klientów, zgodności z przepisami o ochronie danych osobowych zakresu danych pozyskiwanych przez Polskie Górnictwo Naftowe i Gazownictwo S.A. (PGNiG) przy zawieraniu umów z klientami[362]**.** W 2017

[360] II SA/Wa 1094/09, Legalis nr 213824.
[361] II SA/Wa 917/05, Legalis nr 293064.
[362] W trakcie postępowania GIODO ustalił m.in., że gazownia ma prawo żądać od klientów podania imienia, nazwiska, adresu zamieszkania oraz numeru PESEL oraz że dla potwierdzenia prawa do lokalu wystarczy złożenie stosownego oświadczenia, a przedstawianie lub przesyłanie w tym celu aktu notarialnego jest zbędne. W efekcie wydanej przez organ decyzji dnia 22 lipca 2010r. (DOLiS/DEC-957/10/29459/10, treść dostępna na stronie http://www.giodo.gov.pl/560/id_art/3637/j/pl), PGNiG dokonało modyfikacji w formularzach przedstawianych klientom, dostosowujących je do wymogów ustawy o ochronie danych osobowych. Podmiot zapewnił, że kopie dowodów tożsamości są albo niszczone natychmiast po weryfikacji

roku przedmiotem interwencji GIODO jako skutek sygnałów otrzymywanych od mieszkańców, była praktyka kopiowania dowodów osobistych osób wnioskujących o wydanie karty seniora w jednym z urzędów miasta[363]. Kolejnym przykładem sytuacji w której zarzuca się nieprzestrzeganie zasady adekwatności, jest przetwarzanie danych biometrycznych pracowników przez pracodawcę, co stanowiło przedmiot rozstrzygnięcia Naczelnego Sądu Administracyjnego w 2009 roku[364]. Problem ten pojawia się również w późniejszych wyrokach[365]. Faktycznie jednak w przepisach prawa pracy i ochrony danych osobowych nie odnajduje się zakazów przetwarzania danych biometrycznych przez pracodawcę. Można zatem wnioskować, że przetwarzanie danych biometrycznych przez pracodawcę możliwe jest w sposób zgodny z prawem oraz w poszanowaniu zasady adekwatności, jeśli zostanie to uzasadnione niezbędnością i szczególnym charakterem okoliczności (np. skanowanie linii papilarnych do kontroli dostępu do pomieszczeń, gdzie znajdują się dokumenty tajne i poufne).

Zasada minimalizacji danych, opierająca się na fundamencie zasady adekwatności, jest bardzo blisko związana z zasadą ograniczenia celu (co potwierdza tezę o konieczności łącznej interpretacji zasad przetwarzania danych osobowych). Zasada minimalizacji danych ma charakter pochodny w stosunku do zasady celowości. Oznacza to, że najpierw musi zostać określony cel przetwarzania, a dopiero na tej podstawie będzie można określić zakres danych, jakie będą niezbędne do jego osiągnięcia. Adekwatność będzie musiała zawsze być rozpatrywana w odniesieniu do celu przetwarzania. Brak kryteriów uznawania przetwarzania za adekwatne, jak również duża liczba spraw podlegających rozpoznaniu

---

danych klienta, albo dokument jest okazywany jedynie do wglądu, bez dalszego przetwarzania. Ponadto, kserokopia dokumentu potwierdzającego prawo do lokalu nie jest już od klientów żądana.

[363] Ustalono, że do uzyskania karty potrzebne są tylko imię i nazwisko, adres zamieszkania, data urodzenia i numer karty. Natomiast dowód tożsamości zawiera dużo szerszy zakres danych, niż wymienione, dlatego gromadzenie jego kserokopii zostało uznane za praktykę prowadzącą do naruszenia zasady adekwatności, o której mowa w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych. W konsekwencji interwencji GIODO, rada miasta zmieniła regulamin poprzez zniesienie obowiązku dołączania kserokopii dowodu osobistego do wniosku o wydanie karty seniora. Szerzej na stronie internetowej: http://www.giodo.gov.pl/pl/1520301/10243.

[364] Wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009 r. I OSK 249/09, Legalis nr 332309. Sąd uznał, że: Uznanie faktu wyrażenia przez pracownika zgody na przetwarzanie jego danych za okoliczność legalizującą pobranie od pracownika innych danych niż wskazane w art. 22[1] KP stanowiłoby naruszenie tego przepisu Kodeksu pracy. Wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania w rozumieniu art. 26 ust. 1 pkt 3 UODO.

[365] Wyrok Naczelnego Sądu Administracyjnego z dnia 6 września 2011 r., I OSK 1476/10, Legalis nr 369758: Skoro zasada proporcjonalności wyrażona w art. 26 ust. 1 pkt 3 ustawy o ochronie danych osobowych jest głównym kryterium przy podejmowaniu decyzji dotyczących przetwarzania danych biometrycznych, to stwierdzić należy, że wykorzystanie danych biometrycznych do kontroli czasu pracy pracowników jest nieproporcjonalne do zamierzonego celu ich przetwarzania.

przez GIODO (aktualnie PUODO) i sądy, to argumenty potwierdzające, że przestrzeganie przez administratorów zasady minimalizacji danych stanowi nieustannie istotny problem na gruncie i teorii i praktyki.

Jeśli chodzi o uregulowanie sytuacji, kiedy administrator danych zleca przetwarzanie danych innemu podmiotowi w drodze umowy powierzenia, bezpośrednie przełożenie na zasadę adekwatności ma treść art. 28 ust. 3 RODO, gdzie prawodawca wśród elementów umowy wymienia rodzaj danych osobowych oraz kategorie osób, których dane dotyczą. Oznacza to, że zasadę minimalizacji danych ma realizować administrator poprzez wskazanie przetwarzającemu, jakie konkretnie dane mają być przez niego powierzane. Jednakże również przetwarzający powinien przestrzegać zasady minimalizacji, przetwarzając jedynie te dane, które zostały mu w drodze umowy powierzone. Zatem należy wywnioskować, że uregulowanie powierzenia przetwarzania danych jest spójne z zasadą minimalizacji i pozwala ją efektywnie realizować.

Zasada ograniczonego przechowywania jest ściśle związana z kwestią niezbędności przetwarzania danych osobowych. Do 25 maja 2018 roku wynikała ona z treści art. 26 ust. 1 pkt 4 UODO z 1997 r., zgodnie z którym należało zapewnić, aby dane były przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania. W literaturze przedmiotu najczęściej zasada ta występowała pod nazwą zasady ograniczonego czasu przetwarzania.

W treści przepisów RODO prawodawca poświęca sporo uwagi zasadzie ograniczonego przechowywania, stanowiąc w treści art. 5 ust. 1 lit. e RODO, że dane muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Przede wszystkim prawodawca podkreśla wyjątek polegający na tym, że dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem wdrożenia odpowiednich środków technicznych i organizacyjnych wymaganych przepisami rozporządzenia. Ponadto w przepisach RODO istotną zmianą jest również to, że prawodawca wprowadził obowiązek poinformowania osoby, której dane dotyczą, jak długo jej dane będą przetwarzane przez administratora danych. Wymóg ten wynika z treści art. 13 ust. 2 lit. a RODO i stanowi uzupełnienie zasady ograniczonego przechowywania danych.

Administrator podczas pozyskiwania danych osobowych podaje osobie, której dane dotyczą okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu. Administrator powinien więc jeszcze przed rozpoczęciem przetwarzania danych ustalić termin usunięcia danych (okres retencji) lub też opracować kryteria, za pomocą których ten okres zostanie wyznaczony.

Z powierzchownej interpretacji powołanych regulacji mogłoby wynikać, że zasada ograniczonego przechowywania odnosi się jedynie do przechowywania danych osobowych. Interpretacja taka nie wydaje się poprawna, ponieważ należy tę zasadę stosować przez cały proces przetwarzania danych. Ograniczanie realizacji tej zasady wyłącznie do jednej operacji przetwarzania danych mijałoby się z celem regulacji. Możliwe, że prawodawca chciał zaakcentować fakt, że po osiągnięciu celu przetwarzania nie można wykonywać żadnych czynności na danych osobowych, a nawet bierne ich przechowywanie będzie naruszało zasadę ograniczonego czasu przetwarzania danych.

W literaturze przedmiotu zgodnie twierdzi się, że zasada ograniczenia przechowywania danych wyrażona jest poprzez obowiązek przetwarzania danych osobowych tylko tak długo, jak długo realizowany jest cel przetwarzania przez administratora danych[366]. Innymi słowy, dane osobowe przetwarzane przez administratora danych muszą podlegać określonym okresom retencji[367]. Celem tej reguły jest zabezpieczenie interesów podmiotu danych. Bardziej bezpośrednio wyrażane są poglądy na gruncie orzecznictwa, czego przykładem jest orzeczenie, w którym jednoznacznie stwierdzono, że w sytuacji gdy cel przetwarzania danych został osiągnięty, dalsze ich przetwarzanie należy uznać za nielegalne[368]. Przykładem, który przywoływany jest w literaturze przedmiotu, ale też często występuje w praktyce życia codziennego, jest przechowywanie dokumentów rekrutacyjnych kandydatów, w tym ich CV, pomimo tego, że rekrutacja na to stanowisko została już zakończona. Zasada ograniczonego czasu przetwarzania danych zostaje w takim przypadku naruszona, chyba że zgoda kandydata obejmuje przetwarzanie jego danych osobowych nie tylko w celu prowadzenia tej jednej, konkretnej rekrutacji, ale również rekrutacji kolejnych prowadzonych w przyszłości przez tego pracodawcę.

[366] Tak m.in. A. Krasuski, *Dane..., op. cit*., s. 160
[367] M. Krzysztofek, *Ochrona…, op. cit*., s. 72.
[368] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 22 lutego 2005 r., II SA/Wa 2030/04, Legalis nr 75127.

Okres przetwarzania danych może być oznaczony na różne sposoby. Po pierwsze, może wynikać z przepisu prawa np. czas określony jest w treści art. 74 ustawy o rachunkowości[369], czy też w art. 51u ustawy o narodowym zasobie archiwalnym i archiwach[370]. Po drugie, może być określony w treści zawartej umowy np. zlecenia prowadzenia usług księgowych. Może też wynikać z treści klauzuli zgody podmiotu danych. Jako przykład z życia codziennego przywołać można sytuację rozpatrywaną przez Wojewódzki Sąd Administracyjny w Warszawie i tezę jego wyroku[371]. Sposobem oznaczenia czasu przetwarzania danych osobowych staje się termin określony w umowie kredytu lub umowie rachunku bankowego.

Zasada ograniczenia czasowego przetwarzania danych osobowych w praktyce nastręcza wątpliwości. Przede wszystkim pojawiają się trudności, jeżeli nie ma możliwości określenia terminu zrealizowania celu przetwarzania danych, chociażby z tego względu, że cel realizowany jest w sposób ciągły w działalności administratora danych. Najczęściej z taką sytuacją mamy do czynienia przy działalności marketingowej. Zgodnie z poglądami wyrażonymi w doktrynie, decyzję o zakończeniu przetwarzania danych może podjąć albo administrator danych poprzez ich usunięcie, albo podmiot danych, w drodze wycofania zgody na przetwarzanie danych (o ile przetwarzanie odbywa się na podstawie klauzuli zgody) albo sprzeciwu wobec dalszego przetwarzania[372]. Wydaje się, że rozwiązanie to ma przede wszystkim walor teoretyczny, a nie praktyczny. Świadomość osób, których dane dotyczą, nie jest jeszcze na tyle rozwinięta, by w drodze oświadczeń o wycofaniu zgody na przetwarzanie danych powodowały one zakończenie procesu przetwarzania. Dodatkowo trzeba pamiętać, że interesem administratora prowadzącego działalność marketingową zazwyczaj jest dążenie do jak najdłuższego przetwarzania danych osobowych jak największej liczby osób. Dlatego można przyznać, że realizacja zasady ograniczenia przechowywania w największym stopniu zależy od efektywnego stanowienia prawa oraz skutecznego podejmowania decyzji przez organy stosowania prawa. Należy przewidywać, że prawidłowe realizowanie obowiązku przechowywania danych osobowych, czyli nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania, nie będzie łatwe z uwagi na kryteria ekonomiczne w działalności administratorów danych w obrocie gospodarczym.

[369] Ustawa z dnia 29 września 1994 roku, t.j. Dz.U. z 2016 r. poz. 1047.
[370] Ustawa z dnia 14 lipca 1983 roku, t.j. Dz.U. z 2016 r. poz. 1506.
[371] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 22 lutego 2005 r, II SA/Wa 2030/04, Legalis nr 75127. Sąd podkreślił, że z chwilą całkowitej spłaty kredytu lub zamknięcia rachunku bankowego kończy się prawne zezwolenie na przetwarzanie danych osobowych tych osób, których rachunki zostały zamknięte. Osiągnięty zostaje wówczas cel, w jakim dane te były przetwarzane.
[372] P. Barta, P. Litwiński, *Ustawa…, op. cit,* s. 317.

Pojawia się też kwestia co należy uczynić z danymi, po zakończeniu okresu kiedy były one niezbędne do osiągnięcia celu przetwarzania. Na gruncie przepisów RODO należy przyjąć, że powinny one zostać usunięte z zasobów administratora danych. Przy czym zaznaczyć trzeba, że usunięcie według regulacji prawnej to nie tylko fizyczne zniszczenie danych ale również taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą[373]. Sam ustawodawca wskazuje literalnie, że w dalszym ciągu po zrealizowaniu celów, dane nie mogą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą. Zatem mogą one ewentualnie pozostać w zasobach administratora jako informacje pozbawione charakteru osobowego (zanonimizowane). Możliwym rozwiązaniem jest też przekazanie danych przez administratora podmiotowi, który jest uprawniony ich przejęcia.

Prawodawca unijny w treści art. 5 ust. 1 lit e RODO wprowadza wyjątek od zasady ograniczonego przechowywania danych, przewidując, że dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą. Wątpliwość wzbudza sposób, w jaki należy zrealizować obowiązek wdrożenia odpowiednich środków zabezpieczających dane przechowywane dłużej niż do momentu osiągnięcia celów przetwarzania, dla potrzeb archiwalnych, naukowych, historycznych lub statystycznych. Można odnieść wrażenie, że RODO nie wskazuje jakie środki zabezpieczające dane mają ustanowić administratorzy z uwagi na przedłużenie okresu retencji.

Zdarzają się sytuacje gdy to przepis prawa krajowego ingeruje w kwestię zakończenia przetwarzania danych, stanowiąc jednocześnie wyjątek od zasady ograniczonego czasu przetwarzania. Można to wykazać na przykładzie ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną[374]. Z treści art. 19 tej ustawy wynika zasada, że usługodawca nie może przetwarzać danych osobowych usługobiorcy po zakończeniu korzystania z usługi świadczonej drogą elektroniczną, która jest *de facto* zbieżna z omawianą zasadą ograniczonego czasu przetwarzania danych. Jednakże dalej ustawodawca wprowadził wyjątek, stwierdzając, że po zakończeniu korzystania z usługi

[373] Taka definicja usunięcia danych funkcjonowała na gruncie art. 7 pkt 3 UODO z 1997 r.
[374] t.j. Dz.U. z 2017 r. poz. 1219.

świadczonej drogą elektroniczną usługodawca może przetwarzać tylko te dane, które są niezbędne do rozliczenia usługi oraz dochodzenia roszczeń z tytułu płatności za korzystanie z usługi, niezbędne do celów reklamy, badania rynku oraz zachowań i preferencji usługobiorców z przeznaczeniem wyników tych badań na potrzeby polepszenia jakości usług świadczonych przez usługodawcę, za zgodą usługobiorcy. Ponadto podobna możliwość została dopuszczona, jeżeli dane są niezbędne do wyjaśnienia okoliczności niedozwolonego korzystania z usługi. Możliwość przetwarzania danych po zakończeniu korzystania z usługi dają też przepisy odrębnych ustaw lub umowy. Sytuacje wyżej wskazane są niejednokrotnie rozpatrywane przez GIODO (aktualnie PUODO). Organ w decyzji z 2013 roku[375] zarzucił administratorowi danych brak wykazania celu ani podstawy prawnej dla dalszego przetwarzania danych osobowych. W związku z tym, z uwagi na niespełniane przez administratora danych osobowych przesłanek uzasadniających dalsze przetwarzanie danych, GIODO nakazał ich usunięcie.

Problematykę zasady ograniczenia przechowywania danych osobowych można ująć jako obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania. Z punktu widzenia praktyki GIODO i PUODO[376] jako organu stosowania prawa, po osiągnięciu ustalonego celu, administrator danych ma kilka możliwości: usunięcia danych, zanonimizowania danych lub też przekazania podmiotowi uprawnionemu do ich przejęcia od administratora (np. archiwum państwowe). Ponadto GIODO formułował obowiązek administratora danych do stałego nadzorowania zawartości swoich zbiorów pod kątem konieczności usuwania danych zbędnych[377], natomiast przepisy RODO zobowiązują do ustalenia terminu usunięcia danych (okresu retencji) lub też opracowania kryteriów, za pomocą których ten okres zostanie wyznaczony, jeszcze przed rozpoczęciem przetwarzania danych

Z literalnego brzmienia obowiązujących przepisów RODO nie wynika czy i jak realizowana jest zasada ograniczenia przechowywania w sytuacji zlecenia przetwarzania danych podmiotom zewnętrznym. Jednakże pamiętać należy, że instrumentem prawnym, za pomocą którego dokonywane jest powierzenie przetwarzania danych osobowych jest umowa. W umowie wskazywany jest okres, na jaki jest ona zawierana (może być to czas

[375] Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dnia 17 września 2013 r., DOLiS/DEC-982/13/60210, Legalis nr 831157.
[376] https://edugiodo.giodo.gov.pl/file.php/1/UST/UST_03_05.htm
[377] *Ibidem*.

określony bądź nieokreślony). Często błędnym zapisem w umowie powierzenia przetwarzania danych osobowych jest postanowienie, że umowę zawiera się na czas nieokreślony. Zdecydowanie przeczy to zasadzie ograniczonego przechowywania. Na gruncie przepisów RODO, z zasadą ograniczonego czasu przetwarzania można powiązać bezpośrednio treść regulacji w art. 28 ust. 3 RODO wskazującej, że umowa między administratorem a podmiotem powierzającym ma określać czas trwania przetwarzania. Ponadto w treści art. 28 ust. 3 lit. g RODO, przewidziano, że 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. Wyraźnie wskazano tu, że przetwarzający przetwarza dane jedynie do momentu zakończenia świadczenia usługi, z wyjątkiem sytuacji, gdy ma obowiązek ich przechowywania (najprawdopodobniej w celach archiwizacyjnych). W praktyce jednak może okazać się, że określenie czasu przetwarzania nie będzie łatwym zadaniem, bo nie zawsze można przewidzieć datę zakończenia świadczenia usługi. *De lege ferenda* sformułować można uzupełnienie treści przepisów dotyczących obowiązku określania czasu trwania przetwarzania danych przez podmiot przetwarzający na zlecenie administratora o sformułowanie: W przypadku braku możliwości precyzyjnego określenia czasu trwania przetwarzania, należy wskazać kryteria ustalania tego okresu. Taka regulacja byłaby wtedy spójna z innymi przepisami RODO, które odnoszą się do czasu przetwarzania danych, jak art. 13 ust. 2 lit. a, na mocy którego administrator danych podaje informacje o okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu.

3.3. Zasada bezpieczeństwa danych

Jest to zasada wyodrębniona z uwagi na obowiązki odnoszące się do działań administratora skierowanych na zabezpieczanie danych i wykazywania przestrzegania zasad przetwarzania. Działania te mają uwzględniać zagrożenia dla prywatności szczególnie w aspekcie nowych technologii, jak i ryzyko zagrożeń. W ramach tej grupy umieścić można zasadę integralności i poufności, zasadę rozliczalności przetwarzania danych, jak również zasadę uwzględniania ochrony danych w fazie projektowania (*privacy by design*) i domyślnej ochrony danych (*privacy by default*).

Zasada integralności i poufności do czasu pojawienia się RODO nie była sformułowana wprost w treści obowiązujących regulacji Dyrektywy 95/46/WE oraz UODO z 1997 r. Do momentu stosowania przepisów RODO można było mówić jedynie o regulacji jednego z obowiązków administratora danych, a nie o zasadzie przewodniej przetwarzania danych osobowych. Pojęcia integralność i poufność nie zostały zdefiniowane w treści RODO, ale pomocny może być tekst Normy PN-ISO/IEC 27000:2014[378]. Zgodnie z nią poufność to właściwość polegająca na tym, że informacja nie jest udostępniana ani ujawniana nieautoryzowanym osobom, podmiotom lub procesom, natomiast integralność należy rozumieć jako właściwość polegająca na zapewnieniu dokładności i kompletności[379].

Prawodawca unijny zawarł zasadę integralności i poufności danych osobowych w treści art. 5 ust. 1 lit. f RODO, zgodnie z którym dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych. Wzmiankę o zasadzie integralności i poufności danych zawiera też motyw 39 preambuły RODO[380].

Aktualnie zasada integralności i poufności danych została skonkretyzowana w treści art. 32 RODO. Po pierwsze, prawodawca wskazuje tu przykładowe środki techniczne i organizacyjne, które mogą służyć zapewnieniu bezpieczeństwa danych osobowych (np. pseudonimizacja i szyfrowanie danych)[381]. Co istotne, w przepisach

[378] Norma PN-ISO/IEC 27000 Technika Informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Przegląd i Terminologia, s. 9 i 12.

[379] Do 25 maja 2018 funkcjonowały również definicje na gruncie §2 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 roku (Dz.U. 2004 Nr 100, poz. 1024), zgodnie z którym przez integralność danych rozumie się właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany, a przez poufność danych - właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom.

[380] 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.

[381] Jako przykład zabezpieczeń technicznych i jednocześnie realizację zasady integralności i poufności danych, traktować można zawarte w treści motywu 49 preambuły RODO zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu "odmowa usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej. Natomiast do zabezpieczeń organizacyjnych odnosi się treść motywu 78 preambuły i wymóg, że administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych.

prawa nie odnajduje się żadnego katalogu zabezpieczeń, nawet otwartego, a jedynie nadmienia się ich przykłady. Po drugie, wskazuje kwestie, które należy brać pod uwagę przy dokonywaniu oceny, jakie środki należy zastosować: 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 zagrożenia. Zgodzić się należy ze stanowiskiem zaproponowanym na gruncie nauki prawa, iż z treści art. 32 RODO wynika, że w razie naruszenia fizycznej lub technicznej ochrony danych, ich integralności i/lub poufności – środki techniczne i organizacyjne zapewniały zdolność do szybkiego przywrócenia dostępności danych i dostępu do nich. Chodzi więc o jak najszybsze przywrócenie możliwości dostępu do danych osobom upoważnionym, jak również przywrócenie im możliwości dokonywania operacji na danych[382].

Zasada integralności i poufności danych w sposób bezpośredni nie nawiązuje do pozostałych zasad wymienionych w treści art. 5 ust. 1 RODO, wprowadzając odrębne obowiązki administratora danych. Jednakże jest ona pośrednio powiązana *de facto* z każdą z zasad[383].

Analiza obecnie obowiązujących przepisów pozwala wywnioskować, że prawodawca w treści RODO podnosi rangę regulacji dotyczącej bezpieczeństwa przetwarzania danych do poziomu zasady przewodniej. Uogólnia jej treść, w odróżnienia od poprzednich regulacji - nie formułuje konkretnego obowiązku wobec administratora danych ani też katalogu zabezpieczeń. Można przyjąć, że jest to zasada spinająca pozostałe zasady. Znajdujemy tu bezpośrednie nawiązanie do Dyrektywy 95/46/WE (zagrożenia dla danych osobowych (np. utrata, zniszczenie, uszkodzenie) oraz do narzędzi realizacji wymogu zapewnienia bezpieczeństwa danych – wprowadzenie odpowiednich środków organizacyjnych i technicznych. Uwaga prawodawcy skupiła się na dwóch rodzajach zagrożeń przed którymi należy chronić dane osobowe. Po pierwsze, są to zagrożenia

[382] P. Litwiński (red.), *Rozporządzenie..., op. cit.,* Legalis.

[383] Stanowisko to uzasadnić można następującymi argumentami. Wdrożenie środków organizacyjnych i technicznych w praktyce musi opierać się o podstawy prawne przetwarzania danych osobowych, a środki organizacyjne niejednokrotnie wynikają wprost z przepisów prawa (np. dokumentacja opisująca przetwarzanie danych), co wiąże się z zasadą legalności przetwarzania. Zastosowanie zabezpieczeń fizycznych jak np. dokonywanie przeglądów danych i aktualizowanie ich koresponduje z zasadą ograniczonego czasu przetwarzania danych. Wdrożenie w organizacji procedur weryfikacji oraz prostowania danych realizuje zasadę merytorycznej poprawności przetwarzanych danych. Realizacja przez administratora danych obowiązku informacyjnego wobec np. klientów związane jest z zasadą staranności przetwarzania danych, ale również zasadę celowości i związania celem przetwarzania. Wszystkie wymienione działania należy uznać za spełnianie zasady integralności i poufności danych osobowych, ponieważ stanowią one środki organizacyjne i techniczne zapewniające odpowiednie bezpieczeństwo danych osobowych.

związane z czynnikami fizycznymi (ochrona przed zniszczeniem, uszkodzeniem). Po drugie, przewidziane zostały zagrożenia związane z czynnikami ludzkimi (ochrona przed niezgodnym z prawem przetwarzaniem, niedozwolonym ujawnieniem lub dostępem). Trzeba więc przyjąć, że podniesienie rangi regulacji zawartej w art. 32 RODO do jednej z zasad przetwarzania danych osobowych to krok w kierunku zintensyfikowania ochrony danych, nie tyle poprzez poszerzenie katalogu obowiązków administratorów danych, co przez wzmocnienie roli regulacji prawnej. Jak wykazano powyżej, łączy się ona z pozostałymi zasadami przewodnimi przetwarzania danych osobowych. Treść tej zasady jest bardzo istotna i potrzebna z punktu widzenia praktyki przetwarzania danych osobowych. Przepis art. 5 ust. 1 lit. f RODO można uznać za pozytywną zmianę, z tym zastrzeżeniem, że w celu zapewnienia jego efektywności konieczne jest wzmożenie działań kontrolnych przez organ ochrony danych osobowych, zwłaszcza w początkowym okresie obowiązywania regulacji.

Jeśli chodzi o realizowanie zasady integralności i poufności w odniesieniu do powierzenia przetwarzania danych osobowych innemu podmiotowi, trzeba zająć stanowisko, że uregulowanie powierzenia jest zgodne i spójne z tą zasadą. Świadczy o tym fakt, że zgodnie z treścią art. 28 ust. 3 lit. c RODO, umowa łącząca administratora i podmiot przetwarzający ma stanowić o tym, że przetwarzający podejmuje wszelkie środki wymagane na mocy art. 32 RODO (czyli odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa przetwarzania jak np. szyfrowanie danych osobowych czy zdolność do ciągłego zapewnienia poufności, integralności i odporności systemów i usług przetwarzania). Przepis ten zobowiązuje w swej treści przetwarzającego do przestrzegania zasady integralności i poufności danych, co ma zostać zapisane w umowie zawieranej pomiędzy nim a administratorem. Przy czym należy zauważyć, że takie sformułowanie nakłada na przetwarzającego obowiązek w sposób podwójny, gdyż w treści art. 32 ust. 1 RODO literalnie ujęto ponownie, że administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa przetwarzania. Ponadto, w regulacji art. 28 ust. 3 lit. f RODO po raz kolejny prawodawca odnosi się do zapewniania bezpieczeństwa, poufności i integralności danych, tym razem poprzez zobowiązanie podmiotu przetwarzającego do pomocy administratorowi w wywiązywaniu się z obowiązków określonych w art. 32-36 RODO. To kilkukrotne podkreślenie obowiązku zabezpieczenia integralności i poufności danych sugeruje wagę tego obowiązku i zapewnienie realizacji zasady integralności

i poufności danych w aspekcie powierzenia danych do przetwarzania przez obie strony umowy.

Regulacją, która dotąd formalnie nie funkcjonowała w kształcie, w jakim obowiązuje od dnia 25 maja 2018 roku, jest treść art. 5 ust 2 RODO, stanowiąca, że administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność"). Nie brak jednak głosów, że zasada rozliczalności jako taka nie jest nowa. Jej wyraźne uznanie można zauważyć w wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD) dotyczących ochrony prywatności przyjętych w 1980 r. Zgodnie z zawartą w nich zasadą rozliczalności: administrator danych powinien odpowiadać za przestrzeganie środków, które nadają skuteczność [istotnym] zasadom[384]. Jest to rozwiązanie skutkujące nałożeniem ciężaru dowodu odnośnie przestrzegania zasad przetwarzania na administratorów danych. Innymi słowy, to nie organ ma dowieść, że administrator nie wypełnia obowiązków wynikających z treści zasad przetwarzania danych, ale po stronie administratora leży wykazanie, że działa zgodnie z prawem. To dopełnienie regulacji i podniesienie rozliczalności do rangi zasady przewodniej przetwarzania danych należy ocenić pozytywnie z perspektywy osób, których dane dotyczą. Z perspektywy administratorów danych nowy przepis ustanawia dodatkowe obowiązki i wprost wymaga od nich aktywnego podejścia do ochrony danych osobowych. To na nich spoczywa ciężar udowodnienia, że działają zgodnie z prawem.

Termin rozliczalność nie jest pojęciem ugruntowanym w języku prawnym w polskim systemie prawa, w treści UODO z 1997 r. w ogóle ono nie występowało[385]. Powołując się pomocniczo na ustalenia Grupy Roboczej art. 29, można przyjąć, że w ujęciu ogólnym termin ten wyraża sposób wykonywania odpowiedzialności i umożliwienie stosownej weryfikacji. Odpowiedzialność (ang. *responsibility*)

[384] Opinia Grupy Roboczej art. 29 nr 3/2010. Tekst w języku angielskim dostępny na stronie http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp173_en.pdf (dalej jako Opinia 3/2010), s. 7.

[385] Do tej pory rozliczalność była postrzegana jedynie przez pryzmat Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 roku (Dz.U. 2004 Nr 100, poz. 1024). W §2 rozporządzenia zdefiniowano rozliczalność jako właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi. Natomiast z treści przepisu §7 rozporządzenia wynika sposób realizacji rozliczalności poprzez możliwość odnotowania m.in. kto i kiedy wprowadził dane osobowe do systemu informatycznego, w którym dane są przetwarzane.

i rozliczalność (ang. *accountability*) stanowią dwie strony tego samego medalu i są istotnymi składnikami dobrego zarządzania[386].

W koncepcji RODO zasada rozliczaności składa się z dwóch części. W pierwszej części prawodawca ustanawia odpowiedzialność administratora danych osobowych za przestrzeganie zasad ochrony danych osobowych. W drugiej części na administratora danych nałożony został obowiązek wykazania przestrzegania przepisów. Można przyjąć, że rozliczalność ma nowy kontekst, którym jest możliwość przypisania odpowiedzialności za przetwarzanie danych osobowych administratorom danych oraz obowiązek wykazania przez nich prowadzenia działań zgodnych z przepisami RODO. Natomiast jeśli chodzi o wykazywanie przestrzegania zasad ochrony danych wynikających z treści RODO, prawodawca może mieć tu na myśli np. wykazywanie realizacji obowiązku informacyjnego, wykazywanie pozyskania zgody osoby na przetwarzanie jej danych, czy też prowadzenie kontroli administratora przez organ ds. ochrony danych osobowych i obowiązek wykazania posiadania wymaganej przepisami prawa dokumentacji ochrony danych osobowych.

Zasada rozliczalności w nowym kształcie wprowadzanym przez RODO jest *de facto* klamrą spinającą i podsumowującą wszystkie zasady przetwarzania danych osobowych. Nie ma realnej możliwości przestrzegania jej w oderwaniu od reszty zasad. Nowy kontekst przepisu poprzez sformułowanie zobowiązania administratorów do działań proaktywnych (wykazywania stosowania się do zasad przetwarzania), a nie tylko jak dotąd działań reaktywnych (zabezpieczania danych), może wpłynąć na zapewnienie skutecznego przestrzegania przepisów.

W kontekście powierzenia przetwarzania danych osobowych, warto zauważyć, że na gruncie RODO powierzenie przetwarzania danych osobowych koresponduje z zasadą rozliczalności w pełnym wymiarze, rozliczalność przeważa jednak po stronie podmiotu przetwarzającego. W przypadku przetwarzającego prawodawca wymaga, by nie tylko spełniał on wymogi z art. 28 ust. 1 RODO, czyli zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, ale też powinien dołożyć starań, by móc wykazać spełnienie tych wymogów. Zgodnie z treścią art. 28 ust. 5 RODO wystarczające gwarancje, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, lub zatwierdzonego

[386] Opinia 3/2010, s. 8.

mechanizmu certyfikacji. Bezpośrednio zasadę tę wyraża prawodawca w treści art. 28 ust. 3 lit. g RODO, gdzie nakłada na przetwarzającego obowiązek udostępniania administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków. Powyższe argumenty uzasadniają pogląd, że powierzenie przetwarzania danych osobowych realizuje zasadę rozliczalności. W przepisach UODO z 1997 r. następowało to w zakresie przypisania odpowiedzialności, natomiast na gruncie RODO - w pełni, poprzez przypisanie odpowiedzialności oraz nałożenie obowiązku wykazania spełniania wymogów prawnych.

Zasada uwzględniania ochrony danych w fazie projektowania (*privacy by design*) oraz domyślnej ochrony danych (*privacy by default*), ujęta w treści art. 25 RODO, ma zupełnie nowy charakter i dopiero rodzi się praktyka jej stosowania.

Zasada ta wymaga uwzględnienia stanu wiedzy technicznej, kosztu wdrażania oraz charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka naruszenia praw lub wolności osób fizycznych, przy wdrażaniu przez administratora odpowiednich środków technicznych i organizacyjnych (takich jak pseudonimizacja), mających gwarantować skuteczną realizację zasad ochrony danych oraz zapewnić przetwarzaniu niezbędne zabezpieczenia, tak by spełnić wymogi rozporządzenia oraz chronić prawa osób, których dane dotyczą. Prawodawca nakłada na administratora danych obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, np. pseudonimizacji danych, jeszcze przed rozpoczęciem przetwarzania na etapie opracowania jego systemu albo też w trakcie przetwarzania, po to, by zapewnić spełnienie wymogów RODO. Administrator musi przy tym uwzględniać stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych. Wydaje się, że przepis zawarty w art. 25 RODO pozostawia administratorowi pole do decyzji dotyczącej zastosowania zabezpieczeń, na podstawie własnej oceny m.in. okoliczności przetwarzania. Interpretację tego przepisu ułatwia motyw 78 preambuły RODO, zgodnie z którym jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych. W kwestii interpretacji zasady *privacy by design* należy również uwzględnić stanowisko GIODO. Z punktu widzenia organu zasada

ta wyraża proaktywne podejście, w którym ochrona prywatności powinna być wbudowana w każdy nowy projekt nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz jest wbudowana w jego konstrukcję tak, że jest składową projektu[387]. Chodzi tu zarówno o systemy teleinformatyczne, jak i procesy biznesowe związane z przetwarzaniem danych osobowych. Przykładem zastosowania zasady w praktyce życia codziennego może być zmiana w polityce działania producentów domowych routerów sieci bezprzewodowej. Zaprzestają oni ustalania takich samych haseł dla każdego urządzenia, co ułatwiało osobom nieupoważnionym dostęp do sieci, a przez to też do informacji o charakterze prywatnym[388].

Domyślna ochrona danych uregulowana jest w treści art. 25 ust. 2 RODO. W myśl tej regulacji administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do różnych aspektów przetwarzania - ilości danych, zakresu i czasu przetwarzania, dostępności. Środki te mają zapewniać, by domyślnie dane osobowe nie były udostępniane bez interwencji osoby, której dotyczą. Ponadto GIODO wyjaśnia, że „domyślnie" oznacza bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą – i to w kluczowym dla użytkownika momencie przyłączenia się do danego systemu[389]. Regulacja ta ma związek z innymi zasadami przetwarzania danych osobowych, w tym z zasadą celowości, adekwatności i minimalizacji, ograniczonego czasu przetwarzania. Prawodawca wyraża za jej pomocą postulat uwzględnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu[390]. Przykład stosowania domyślnej ochrony danych dotyczy aktywności internautów na portalach społecznościowych. Zamieszczane treści przez użytkowników powinny być z założenia nieupublicznione dla nieokreślonej liczby osób. Dopiero użytkownik sam powinien móc każdorazowo zmieniać ustawienia prywatności, decydując się na publikację treści[391].

Z formalnego punktu widzenia można twierdzić, że skoro koncepcja uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych została wyłączona

[387] http://www.giodo.gov.pl/pl/1520281/10023.
[388] L. Kępa, *Reforma ochrony danych osobowych w UE. 24 kluczowe zmiany*, Warszawa 2016, s. 10, opracowanie dostępne na stronie internetowej https://odo24.pl.
[389] http://www.giodo.gov.pl/pl/1520281/10023.
[390] *Ibidem*.
[391] L. Kępa, *Reforma…, op. cit*., s. 10.

poza katalog zasad przetwarzania wywodzony z treści art. 5 RODO, a nawet poza rozdział poświęcony zasadom, to ma ona na tyle nowy charakter, że nie ma jeszcze rangi zasady przetwarzania. Jednakże biorąc pod uwagę całokształt regulacji, prawodawca jako zasadę traktuje przedmiotowe zagadnienie w preambule RODO. Również Rzecznicy Ochrony Danych Osobowych i Prywatności w 2010 roku w Jerozolimie w treści Rezolucji w sprawie Prywatności w Fazie Projektowania nadali mu charakter zasady[392]. Dlatego należy podzielić stanowisko, że koncepcję uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochronę danych należy rozpatrywać w kategorii jednej z zasad, na których opiera się przetwarzanie danych osobowych w poszanowaniu przepisów nowego aktu prawnego. Przemawiają za tym po pierwsze, słowa preambuły RODO, gdzie w treści motywu 78 stwierdza się, że administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Po drugie, świadczą o tym przyjęte we wspomnianej Rezolucji kierunki jak uznanie prywatności w fazie projektowania za niezbędny element podstawowej ochrony prywatności czy też dążenie do wspierania włączania podstawowych zasad prywatności w fazie projektowania w zakres polityki prywatności i ustawodawstwa w poszczególnych porządkach prawnych[393]. Po trzecie, pamiętać należy, że zasada uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych opatrzona została przez unijnego prawodawcę sankcją za jej naruszenie, jak pozostałe zasady ujęte w treści art. 5 RODO (choć jest to administracyjna kara pieniężna w wysokości niższej, art. 83 ust. 4 lit. a RODO). Za naruszenie obowiązku uwzględniania ochrony danych osobowych w fazie projektowania i ustanawiania mechanizmów ochrony domyślnej przez administratora lub podmiot przetwarzający RODO przewiduje administracyjną karę pieniężną w wysokości do 10 mln euro, a w przypadku przedsiębiorstwa – do 2% całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Można odnieść wrażenie, że RODO za pomocą zasady uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, nakłada na administratorów danych obowiązek zintensyfikowania dbałości o dane osobowe. Ten obowiązek pojawia się jeszcze przed rozpoczęciem przetwarzania, już na etapie organizacyjnym (*privacy by design*) oraz ma być zagwarantowany z góry bez ingerencji

[392] http://www.giodo.gov.pl/pl/1520084/3830
[393] Tekst projektu Rezolucji w sprawie Prywatności w Fazie Projektowania dostępny na stronie internetowej http://www.giodo.gov.pl/pl/1520084/3830

podmiotu danych (*privacy by default*). Do chwili rozpoczęcia stosowania RODO faktycznie obowiązek taki nie istniał na gruncie przepisów prawa powszechnie obowiązującego. Wydaje się, że dzięki przepisom zawartym w art. 25 RODO, można będzie odczuć wzrost bezpieczeństwa danych osobowych.

Ogólnie można stwierdzić, że dla realizacji każdej z zasad przetwarzania danych osobowych z art. 5 ust. 1 RODO konieczne jest przestrzeganie odpowiednich przepisów RODO odpowiadających danej zasadzie i jednocześnie przestrzeganie samej zasady[394]. W odniesieniu nowo sformułowanej w treści RODO zasady uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych, do problematyki powierzania przetwarzania danych osobowych, powiedzieć należy, że trudno na chwilę obecną dostrzec realizację tej zasady na etapie powierzania. Należy pozostawić to jako kwestię otwartą do rozstrzygnięcia dopiero rodzącej się praktyce.

[394] J. Rzymowski, *Zasada rozliczalności w RODO*, [w:] ABI EXPERT 2018 nr 1, s. 38. Zasadę zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit a RODO) realizuje przede wszystkim przetwarzanie danych w zgodzie z art. 6, 9 i 12-14 RODO; zasadę ograniczenia celu (art. 5 ust. 1 lit. b RODO) – głównie art. 17 ust. 1 lit. a, art. 25 ust. 2 RODO; zasadę minimalizacji danych (art. 5 ust. 1 lit c RODO) – tak jak poprzednią zasadę głównie art. 17 ust. 1 lit. a, art. 25 ust. 2 RODO; zasadę prawidłowości (art. 5 ust. 1 lit d RODO) - np. art. 16 ODO; zasadę ograniczenia przechowywania (art. 5 ust. 1 lit e RODO) - głównie art. 18, art. 25 ust. 2 RODO; zasadę integralności i poufności (art. 5 ust. 1 lit f RODO) - art. 32 RODO. Zgodzić się należy z J. Rzymowskim, że powyższe uwagi mają bezpośrednie przełożenie na kwestię odpowiedzialności administracyjnej administratora. Poszczególne przepisy RODO pomagają spełnić zasady przetwarzania danych, ale jeżeli nie zostanie spełniony wymóg określony w konkretnym przepisie RODO, to można wywnioskować, że nie zostanie spełniona zasada wynikająca z art. 5 RODO. Konsekwencją tego może być nałożenie kary administracyjnej.

ROZDZIAŁ III

Normatywne ukształtowanie umowy powierzenia przetwarzania danych osobowych

1. Próba umiejscowienia umowy powierzenia przetwarzania danych osobowych w systematyzacji umów w obrocie

1.1. Klasyczne systematyzacje umów w prawie cywilnym a umowa powierzenia przetwarzania danych osobowych

Tradycyjnie na gruncie prawa cywilnego i nauki prawa umowy zawierane w obrocie dzieli się na umowy nazwane, nienazwane i mieszane. Umowy nazwane, wywodzące się z tradycji rzymskich (*contractus nominatus*) i wynikające ze szczegółowej części przepisów regulujących umowy[395], to według teoretyków prawa takie umowy, które mogą zostać przyporządkowane ustawowemu typowi umowy, ponieważ posiadają one cechy charakteryzujące dany typ umowy[396]. Według innych są to umowy powtarzające się w obrocie, które mniej lub bardziej szczegółowo normowane są w przepisach obowiązującego prawa, ich *essentialia negotii* są objęte przepisami ustawy, a przepisy często nadają im nazwy[397]. Kolejna grupa przedstawicieli postrzega określenie umowy nazwanej w powiązaniu z ustawowo określonymi wzorami – umowami zaproponowanymi przez ustawodawcę w drodze uregulowania konstruujących je postanowień w przepisach prawa cywilnego[398]. Umowy nazwane bywają również różnicowane w ramach tej kategorii na podgrupy. Pierwszą podgrupę stanowią umowy, które zawarte są w Kodeksie cywilnym (np. sprzedaż, umowa agencyjna), a drugą te, które uregulowane są w ustawach szczegółowych (np. umowy z bankiem, umowy spółek handlowych)[399]. Do zaliczenia określonej umowy do kategorii umów nazwanych jest niezbędne nie tyle, by umowa posiadała nazwę, co to, aby określone zostało minimum jej składników – podmioty (strony), przedmiot, treść (prawa i obowiązki stron) – czyli tradycyjne *essentialia negotii*

[395] Z. Radwański, *Teoria umów*, Warszawa 1977, s. 208-209.
[396] Z. Radwański, J. Panowicz-Lipska, *Zobowiązania –część szczegółowa*, Warszawa 2015, s. 7.
[397] W. Czachórski, *Zobowiązania. Zarys wykładu*, Warszawa 2009, s. 133.
[398] J. Jezioro [w:] E. Gniewek, P. Machnikowski (red.), *Zarys prawa cywilnego*, Warszawa 2016, s. 403.
[399] W. J. Katner [w:] W. J. Katner (red.) *System Prawa Prywatnego T. 9 – Prawo zobowiązań – umowy nienazwane*, Warszawa 2015, s. 7.

czynności prawnej. Przykładem może być umowa o świadczenie usług telekomunikacyjnych uregulowana w ustawie Prawo telekomunikacyjne[400].

Jeśli chodzi o cel wyodrębnienia umów nazwanych, w literaturze przedmiotu wskazuje się, że jest nim możliwość wskazania właściwej dla danej umowy regulacji prawnej i zastosowania do niej właściwych dla tego typu umowy przepisów, co ułatwia zawarcie umowy i kształtowanie jej treści[401]. Klasyfikacja umów ma też znaczenie na etapie wykonywania umów i odpowiedzialności z tytułu niewykonania lub nienależytego wykonania umowy. Warty uwagi jest również sposób, w jaki przepisy kodeksowe regulują umowy nazwane, który można wyinterpretować na podstawie wybranych umów uregulowanych w Kodeksie cywilnym. Pierwszą z nazwanych umów regulowanych w Kodeksie cywilnym jest umowa sprzedaży. Zgodnie z treścią art. 535 KC przez umowę sprzedaży sprzedawca zobowiązuje się przenieść na kupującego własność rzeczy i wydać mu rzecz, a kupujący zobowiązuje się rzecz odebrać i zapłacić sprzedawcy cenę. Strukturalnie przepis ten składa się z nazwy umowy (Przez umowę sprzedaży…), wskazania stron umowy (sprzedawca, kupujący), obowiązków jednej strony (sprzedawca zobowiązuje się przenieść na kupującego własność rzeczy i wydać mu rzecz…), obowiązków drugiej strony (…a kupujący zobowiązuje się rzecz odebrać i zapłacić sprzedawcy cenę). Drugą przykładową umową jest zamiana uregulowana w treści art. 603 KC, który stanowi, że przez umowę zamiany każda ze stron zobowiązuje się przenieść na drugą stronę własność rzeczy w zamian za zobowiązanie się do przeniesienia własności innej rzeczy. W strukturze tego przepisu wyróżnić można nazwę umowy (Przez umowę zamiany…), brak określenia stron umowy (każda ze stron… na drugą stronę), obowiązki łącznie określone dla obu stron (…każda ze stron zobowiązuje się przenieść na drugą stronę własność rzeczy w zamian za zobowiązanie się do przeniesienia własności innej rzeczy) Trzecim przykładem może być umowa rachunku bankowego wynikająca z treści art. 725 KC, zgodnie z którym przez umowę rachunku bankowego bank zobowiązuje się względem posiadacza rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych. Strukturalnie przepis ten składa się z nazwy umowy (Przez umowę rachunku bankowego…), wskazania stron umowy (bank, posiadacz rachunku), określenia obowiązków jednej ze stron (…bank zobowiązuje się względem posiadacza

[400] *Ibidem*. t.j. Dz.U. z 2018 r. poz. 1954 ze zm.
[401] W. Czachórski, *Zobowiązania*…, *op. cit*., s. 134.

rachunku, na czas oznaczony lub nieoznaczony, do przechowywania jego środków pieniężnych oraz, jeżeli umowa tak stanowi, do przeprowadzania na jego zlecenie rozliczeń pieniężnych). Na podstawie powyższych przykładów umów uregulowanych w Kodeksie cywilnym można wyciągnąć wniosek, że nie ma jednego przyjętego wzoru układu redakcyjnego dla kodeksowych umów nazwanych. Bywają regulacje całościowe (nazwa, określenie obu stron i określenie obowiązków obu stron), ale zdarzają się również regulacje niepełne (np. brak nazwania obu stron, łączne określenie obowiązków lub wskazanie obowiązków tylko jednej strony). Co należy uznać za regułę w aspekcie redakcyjnym, to fakt, że w każdym przypadku ustawodawca formułuje nazwę umowy. Ogólnie można stwierdzić, że w odniesieniu do kodeksowych regulacji w zakresie poszczególnych umów, przepisy zawierają zawsze nazwę, a w większości przypadków bez problemu można zidentyfikować strony umowy, katalog praw i obowiązków stron, przedmiot umowy czy też dokonać jej charakterystyki[402].

Warto również spojrzeć na pozakodeksowe sposoby uregulowania umów nazwanych. Przykład stanowić może umowa kredytu, którą ustawodawca uregulował w treści art. 69 ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe, zgodnie z którym przez umowę kredytu bank zobowiązuje się oddać do dyspozycji kredytobiorcy na czas oznaczony w umowie kwotę środków pieniężnych z przeznaczeniem na ustalony cel, a kredytobiorca zobowiązuje się do korzystania z niej na warunkach określonych w umowie, zwrotu kwoty wykorzystanego kredytu wraz z odsetkami w oznaczonych terminach spłaty oraz zapłaty prowizji od udzielonego kredytu. Ustawodawca w treści przepisu ustawy szczególnej zawarł nazwę umowy (umowa kredytu), nazwy stron (bank, kredytobiorca), obowiązki jednej strony (bank zobowiązuje się oddać do dyspozycji kredytobiorcy na czas oznaczony w umowie kwotę środków pieniężnych z przeznaczeniem na ustalony cel) oraz obowiązki drugiej strony (kredytobiorca zobowiązuje się do korzystania z niej na warunkach określonych w umowie…). Można uznać, że schemat regulacji kodeksowej został w tym przypadku w pełni zrealizowany. Drugi przykład stanowić może umowa o świadczenie usług telekomunikacyjnych, będąca przedmiotem regulacji art. 56 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne.

Strony mają również prawo do zawierania umów, które nie mają oparcia w regulacjach prawnych, dzięki czemu mogą wypełnić treść umowy uzgodnionymi

[402] Tak również J. Ignaczewski, *Umowy nienazwane,* Warszawa 2004, s. 2.

postanowieniami dopasowanymi do ich indywidualnych potrzeb, nie będąc jednocześnie związanymi szczegółowymi przepisami prawa[403]. Wynika to przede wszystkim z zasady swobody umów jak i swobody działalności gospodarczej, poparte jest też regulacją rangi konstytucyjnej (art. 20 Konstytucji RP stanowi, że społeczna gospodarka rynkowa oparta na wolności działalności gospodarczej, własności prywatnej oraz solidarności, dialogu i współpracy partnerów społecznych stanowi podstawę ustroju gospodarczego Rzeczypospolitej Polskiej). Celu zawierania takich umów upatrywać można w dążeniu do zaspokojenia coraz nowszych potrzeb kontrahentów, jak również braku uwzględniania przez katalog umów nazwanych zmieniających się sytuacji gospodarczych[404]. Można powiedzieć, że jest to uzasadnienie wyróżniania na gruncie prawa cywilnego kategorii umów nienazwanych, według tradycji rzymskich zwanych *contractus innominatus*.

W literaturze przedmiotu można spotkać różne wyjaśnienia pojęcia umów nienazwanych. Twierdzi się najczęściej, że są to „(...) umowy, których nie da się przyporządkować jakiemukolwiek typowi ustawowemu"[405], albo „czynności prawne, w których pojawiają się elementy nieswoiste dla danego typu umowy (…) gdy treść nie jest przewidziana przez żadną z postaci umów nazwanych"[406]. Ponadto przedstawiciele doktryny zajmują stanowisko, że „poprzez przeciwstawienie umowie nienazwanej umowie nazwanej, można przyjąć, że jest to umowa nieuregulowana przepisami prawa"[407], oraz że umowy nienazwane nie mają i mieć nie mogą ze swej istoty *essentialia negotii* a wyróżnienie w stosunku prawnym składników przedmiotowo istotnych czyniłoby z nich niedookreśloną normatywnie relację prawną[408]. Również orzecznictwo sądów jest pomocne, szczególnie w zakresie rozumienia pojęcia umowy nienazwanej. W wyroku Sądu Apelacyjnego w Katowicach z dnia 13 stycznia 2016 r., zajęto stanowisko, że jeśli strony umowy w jej ramy ujęły regulacje odnoszące się do innych umów nazwanych i dostosowały je do potrzeb zamierzonego skutku prawnego, co nie pozwala na

[403] J. Rajski, *Prawo o kontraktach w obrocie gospodarczym*, Warszawa 2002, s.27.
[404] *Ibidem*.
[405] Z. Radwański, J. Panowicz-Lipska*, Zobowiązania…, op. cit.,* s. 9.
[406] W. Czachórski, *Zobowiązania…, op. cit*., s. 134.
[407] J. Ignaczewski, *Umowy..., op. cit.,* s. 2. Ten pogląd, jak zresztą wskazuje sam autor, prowadzi do niepoprawnego wniosku, że umowy nienazwane funkcjonują w ustawowej próżni. Wyjaśnia to następująco: „Reżim prawny umów nienazwanych wyznaczony jest niejednokrotnie przez przepisy szczególne ustanowione bądź to wyłącznie dla oznaczonych typów umów nienazwanych, bądź też łącznie dla oznaczonych typów umów nazwanych i nienazwanych. W tym ostatnim przypadku umowy nienazwane, jak każda inna umowa, przyporządkowane są prawu obligacyjnemu. Mają więc do nich zastosowanie przepisy dotyczące wykonania zobowiązania oraz skutków niewykonania lub nienależytego wykonania zobowiązania. Bez ograniczeń podlegają one zamieszczonym w Księdze I KC ogólnym przepisom prawa cywilnego. Umowy nienazwane zatem, tak jak i umowy nazwane, podlegają prawnej regulacji".
[408] W. J. Katner [w:] W. J. Katner (red.) *System..., op. cit.,* s. 12.

odwoływanie się wprost do zapisów ustawy o umowach nazwanych, to taki stosunek umowny stron należy zakwalifikować jako umowę nienazwaną, dopuszczalną w świetle art. 353^1 KC[409]. Natomiast w wyroku Sądu Najwyższego z dnia 13 grudnia 2012 r. odniesiono się do postępowania z umowami tego typu, stanowiąc, że: do zawartej przez strony umowy, której nie można zakwalifikować jako wyszczególnionego w ustawie typu umowy, stosuje się bezpośrednio zawarte w Kodeksie cywilnym przepisy ogólne, dotyczące umów oraz w drodze analogii przepisy regulujące umowę nazwaną, do której umowa nienazwana jest najbardziej zbliżona charakterem prawnym[410]. Podobnie jak kategoria umów nazwanych, w przypadku umów nienazwanych również można wyróżnić dwie grupy: umowy tworzące w rozumieniu praktyki gospodarczej zupełnie nowy i odrębny typ umowy np. factoring, oraz umowy stanowiące podtyp umowy nazwanej, np. umowy związane ze świadczeniem usług[411]. Ponadto zwrócić należy uwagę, że wbrew temu, co sugeruje sformułowanie umowa nienazwana, niejednokrotnie okazuje się, że umowa taka posiada swoją nazwę w obrocie (jak np. umowa factoringu czy umowa know-how). Istotną wartość dla przedmiotu niniejszych rozważań jak i dalszych badań, ma opracowanie katalogu przesłanek stanowiących warunki prawne umowy nienazwanej. Według J. W. Katnera dopiero ich łączne spełnienie stanowi o tym, że dany stosunek prawny stanowi umowę nienazwaną:

1. dwustronna czynność prawna, będąca ważną umową;
2. brak jej nazwania, choć to nazwanie nie musi wystąpić wprost przez jakiś tytuł, pojęcie itp., może wynikać z kontekstu lub opisania;
3. brak określenia *essentialia negotii* takiej umowy w KC lub w innej ustawie, mimo że mogą być tam umieszczone wskazania, co umowa ma w swej treści zawierać;
4. brak tożsamości umowy z umową nazwaną albo takiego prawdopodobieństwa, które wskazuje na rodzaj umowy nazwanej;
5. określenie stron umowy, jej przedmiotu i treści, w tym zwłaszcza praw i obowiązków stron;
6. pozostawanie w zgodzie z porządkiem prawnym, tzn. w zgodności kreowanego stosunku prawnego (jego treści i celu) z jego właściwościami (naturą), ustawami i zasadami słuszności, jak też dobrymi obyczajami (nazywanymi obecnie w art. 353^1 KC zasadami współżycia społecznego)[412].

Zagadnienie, które wymaga uwagi z kontekście prowadzonych rozważań to elementy umowy określane jako *essentialia negotii*. Kwestia ta należy do szerszego zagadnienia

[409] V ACa 874/15, Legalis nr 1408581.
[410] V CSK 30/12, Legalis nr 667433.
[411] W. J. Katner [w:] W. J. Katner (red.) *System…, op. cit.,* s. 13.
[412] *Ibidem*, s. 16-17.

elementów treści czynności prawnych. *Essentialia negotii* to jeden z trzech członów klasycznego podziału treści czynności prawnej, występujący obok *naturalia negotii* i *accidentalia negotii*[413]. Powszechnie i niezmiennie przyjmuje się, że *essentialia negotii* to elementy umowy przedmiotowo istotne, cechy konstytutywne danego typu czynności prawnej, służące jej identyfikacji, przyporządkowaniu do określonego rodzaju, co w konsekwencji pozwolić ma na ustalenie właściwych przepisów prawa, które określają konsekwencje prawne danej czynności niewyrażone w oświadczeniach woli stron[414]. Są one wskazane przez ustawodawcę w regulacji konkretnego typu umowy (np. w przypadku sprzedaży w treści art. 535 KC wskazano strony, przedmiot sprzedaży i cenę), a wybór danego typu umowy będzie determinował elementy, które strony muszą uwzględnić w jej treści[415]. *Essentialia negotii,* jak wskazuje łacińska nazwa, to elementy umowy o charakterze koniecznym, bez nich umowa nie będzie mogła dojść do skutku. W kontekście umów nienazwanych przytoczyć należy pogląd wyrażony przez Z. Radwańskiego, zgodnie z którym w odniesieniu do nienazwanych umów typowych można wyróżnić pewien zespół charakteryzujących je ważnych cech, które ułatwiają następnie kwalifikację umów konkretnych i określenie ich konsekwencji prawnych. Mimo to należy podkreślić, że zamknięcie czy usztywnienie cech, wyrażające się w *essentialia negotii* umów nazwanych, dokonuje się w typowych umowach nienazwanych w inny sposób, który decyduje o tym, że typy te mają bardziej elastyczny kształt niż typy umów nazwanych[416]. Stwierdzenie to można uznać za bazę do konstruowania swoistych dla danej umowy cech w drodze praktyki[417].

Trzeci z klasycznych rodzajów umów stanowią umowy mieszane. Rozumiane są na gruncie nauki prawa jako konstrukcje o charakterze złożonym, stanowiące kompilację wybranych przez strony elementów różnych umów nazwanych[418]. Niejednokrotnie zdarza się również tak, że w treści takiej umowy występują zarówno elementy typowe dla umowy nazwanej, jak i elementy, które nie są spotykane dla umów nazwanych[419]. Ich układ tworzy jednakże nową jakość. Sformułowaniem umowy mieszane określa się zbiór różnorodnych umów, w których znaleźć się może połączenie elementów treści

[413] Z. Radwański [w:] Z. Radwański (red.), *System Prawa Prywatnego, Tom 2 – Prawo cywilne część ogólna*, Warszawa 2008, s. 248.
[414] *Ibidem*, s. 249.
[415] K. Górska [w:] *Zarys…, op. cit*., s. 161.
[416] Z. Radwański, *Teoria…, op. cit*., s. 249-250.
[417] Z. Radwański [w:] Z. Radwański (red.) *System…, op. cit*., s. 250.
[418] J. Ignaczewski, *Umowy…, op. cit.,* s. 1.
[419] Z. Radwański, J. Panowicz-Lipska*, Zobowiązania…, op. cit.,* s. 10.

występujących w innych umowach (najczęściej nazwanych) - przy czym procedura postępowania w przypadku takich umów kształtuje się według określonego schematu. Jeśli w umowie mieszanej przeważa główny rodzaj zobowiązania, a odmienne są świadczenia uboczne – stosuje się przepisy umowy nazwanej odpowiadającej głównemu zobowiązaniu; natomiast jeśli w umowie dochodzi do równorzędnego połączenia różnych rodzajów zobowiązań – odpowiednio stosowane będą przepisy właściwe dla każdego ze świadczeń[420]. Należy przychylić się do przyjętego przez znaczną część przedstawicieli doktryny, ale nie pozbawionego kontrowersji poglądu, zgodnie z którym brak jest podstaw pozwalających na wyróżnienie trzech równorzędnych kategorii umów: nazwanych, nienazwanych i mieszanych[421]. W konsekwencji prowadzi to do dwupodziału umów na nazwane i nienazwane. O ile w literaturze przedmiotu spotyka się stanowiska, że umowy mieszane, z uwagi na to, że zidentyfikowanie swoistej metody postępowania zmierzającego do ustalenia ich reżimu prawnego jest trudne, będą traktowane albo jako umowy nazwane albo jako nienazwane[422], bardziej przekonujące wydaje się stanowisko, że umowy mieszane jako ogólna kategoria, stanowią rodzaj umów nienazwanych[423]. Potwierdza to m.in. pogląd, że pomiędzy umową nienazwaną a mieszaną zachodzi stosunek krzyżowania, a nie wyłączania. W efekcie umowa nienazwana może być jednocześnie umową mieszaną, tak jak i umowa mieszana może równocześnie mieć miano umowy nienazwanej[424]. Stopień skomplikowania poruszanego zagadnienia zmniejszyć może wyrażony w nauce prawa pogląd, zgodnie z którym dana umowa może być albo nazwana, albo nienazwana, zaś umowy nienazwane mogą być albo czystymi umowami nienazwanymi, albo umowami mieszanymi[425]. Trzeba by dodać, że czysta umowa nienazwana wykazuje w całości odrębne cechy od jakiegokolwiek normatywnego typu umowy i nie da mu się przyporządkować żadnym swoim elementem[426]. Przekonujący jest przy tym argument, że dokonywanie dekonstrukcji struktury umowy jako złożonej całości, w konsekwencji prób zastosowania przepisów regulujących umowy nazwane w celu realizacji umowy, doprowadzi do zachwiania równowagi ochrony interesów kontrahentów i w związku z tym potencjalnym rozwiązaniem byłoby poddanie umów mieszanych

[420] M. Pannert [w:] T. Mróz (red.), *Zobowiązania*, Warszawa 2016, s. 90.
[421] W ten sposób twierdzą: J. Jezioro [w:] *Zarys…, op. cit*., s. 403-404, W. J. Katner [w:] W. J. Katner (red.) *System ..., op. cit*., s. 10.
[422] J. Jezioro [w:] *Zarys…, op. cit*., s. 404.
[423] J. Rajski, *Prawo…, op. cit.*, s. 28.
[424] I. Ignaczewski, *Umowy…, op. cit*., s. 4.
[425] S. Włodyka [w:] S. Włodyka, *Prawo..., op. cit*., s. 33.
[426] *Ibidem*, s. 34.

ogólnemu reżimowi kontraktowemu, przy uwzględnieniu możliwości odpowiedniego stosowania przepisów dotyczących określonych umów nazwanych, uzasadnionego istotnym podobieństwem sytuacji, o ile nie byłoby to sprzeczne z właściwościami (naturą) danej umowy[427].

Na podstawie powyższych uwag należy podjąć próbę ustalenia, czy umowa powierzenia przetwarzania danych osobowych może zostać zakwalifikowana jako umowa nazwana, czy jako umowa nienazwana, a może mieszana. W celu podkreślenia zmian w regulacji przedmiotu dysertacji w związku z nowymi przepisami RODO, kwalifikacja powinna zostać dokonana w dwóch etapach. Po pierwsze, w oparciu o przepisy prawa obowiązujące do dnia 25 maja 2018 roku oraz po drugie, w oparciu o przepisy prawa obowiązujące po dniu 25 maja 2018 roku. Wynika to z faktu, że jest różnica w regulacjach umowy powierzenia przetwarzania danych osobowych.

Odnosząc się do treści art. 31 ust. 1, 2 i 3 UODO z 1997 r.[428], należy stwierdzić, że ustawodawca nie nazwał przedmiotowej umowy, ale określił jej formę. Ustawodawca wskazał tylko jedną ze stron umowy – administratora danych, drugą stronę nazywa jako inny podmiot albo podmiot, o którym mowa w ust. 1 co *de facto* nie stanowiło żadnej wskazówki dla stosujących niniejszy przepis. Ponadto zostały sformułowane obowiązki tylko jednej strony umowy – podmiotu przetwarzającego. Bez głębszej analizy można powiedzieć, że ustawowa regulacja była zbyt wąska i zawierała zbyt mało treści, by móc umowę powierzenia przetwarzania danych osobowych uznać za umowę nazwaną. Faktycznie ustawodawca w treści art. 31 UODO dokonał jedynie szczątkowego uregulowania dotyczącego przedmiotowej umowy. Polegało ono jedynie na wskazaniu, że ustawodawca dopuszczał możliwość powierzenia danych osobowych do przetwarzania innemu podmiotowi. Takie działanie mogło nastąpić w drodze umowy, zaś umowa ta miała mieć formę pisemną. Jedynymi elementami, które można było uznać za *essentialia negotii* umowy powierzenia były zakres oraz cel przetwarzania danych przez przetwarzającego, przy czym nie istniały żadne dodatkowe regulacje, jak należało rozumieć zakres i cel. Określono obowiązki jednej ze stron umowy poprzez odesłanie

[427] *Ibidem*, s. 28.

[428] 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. 2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. 3. Podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a. W zakresie przestrzegania tych przepisów podmiot ponosi odpowiedzialność jak administrator danych.

do treści innych przepisów ustawy. Ponadto określono, czego raczej nie przewidują umowy nazwane, kwestię rozłożenia odpowiedzialności na strony stosunku powierzenia danych. Na tej podstawie za uzasadniony można uznać wniosek, że umowa powierzenia przetwarzania danych osobowych wynikająca ze szczątkowego uregulowania w treści art. 31 UODO z 1997 r., nie stanowiła umowy nazwanej. Jej kształt wynikał w dużej mierze z poglądów przedstawicieli nauki prawa, jak również, (a może przede wszystkim) z praktyki jej stosowania w obrocie.

Przede wszystkim próby zakwalifikowania umowy powierzenia przetwarzania danych osobowych do typu umowy nazwanej bądź umowy nienazwanej, należy dokonać na podstawie regulacji w art. 28 ust. 3 RODO[429]. Pojawiają się tu wyraźnie nowe elementy umowy powierzenia. Analizę powołanego przepisu należy oprzeć o przytoczony wcześniej katalog przesłanek, których łączne spełnienie pozwala przyznać danej umowie status umowy nienazwanej. Podążając za tokiem rozważań W. J. Katnera[430], analizy wymaga po kolei każda z przesłanek uznania umowy za umowę nienazwaną.

Pierwszą przesłankę stanowiło to, by czynność podlegająca kwalifikowaniu stanowiła dwustronną czynność prawną będącą ważną umową. Wydaje się, że nie ma potrzeby szerszego rozpatrywania tego kryterium ponieważ umowa powierzenia przetwarzania danych osobowych ze swej natury jest dwustronną czynnością prawną oraz można powiedzieć że stanowi ważną umowę, bo podstawą prawną jest przepis prawa przewidujący jej zawarcie w przypadku „zlecania" przetwarzania danych osobowych podmiotowi innemu niż administrator.

Jeśli chodzi o kolejną przesłankę, to przedstawiciel doktryny, który zaproponował katalog przesłanek wyodrębnił wymóg, by poddawana analizie umowa nie posiadała sformułowanej nazwy, choć zaznaczył, że nazwa nie musi wynikać wprost, a może z kontekstu lub opisu. Kryterium nadania umowie nazwy odnosi się w większości do umów kodeksowych, natomiast w przypadku umów pozakodeksowych, nazwy zazwyczaj tworzone są na gruncie języka prawniczego w doktrynie i orzecznictwie, jak np. umowa

[429] Treść przepisu jest następująca: 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, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający (…) – prawodawca w ośmiu punktach wymienia obowiązki podmiotu przetwarzającego.
[430] W. J. Katner [w: W. J. Katner (red.), *System…, op. cit.,* s. 16-17.

o pośrednictwo w obrocie nieruchomościami[431]. Ta przesłanka wzbudza wątpliwości, ponieważ o ile prawodawca w przepisie nie formułuje nazwy literalnie (np. tak jak czyni to ustawodawca w regulacji kodeksowej umowy sprzedaży czy najmu), to trudno jednoznacznie powiedzieć, czy nazwa wynika z kontekstu przepisów prawa. Ani razu w treści RODO nie używa się słowa powierzenie w odniesieniu do „zlecenia" przetwarzania danych – zagadnienie to nazywane jest jako przetwarzanie dokonywane w imieniu administratora, lub też przetwarzanie przez podmiot przetwarzający. Jednakże sformułowanie umowa powierzenia jest rozpowszechnione zarówno w literaturze przedmiotu, jak i publikacjach organu ds. ochrony danych osobowych (GIODO)[432]. Trudno zająć jednoznaczne stanowisko, ale można przyjąć, że nazwa przedmiotowej umowy jest raczej wytworem zarówno rozwijającej się nauki jak i praktyki w obszarze ochrony danych osobowych, nie wynika z aktualnie obowiązujących przepisów prawa.

Trzecia z wymienionych przesłanek mieści się w założeniu, że umowa będąca przedmiotem kwalifikacji nie ma określonych *essentialia negotii* ani w Kodeksie cywilnym ani w innych ustawach, ale może mieć ogólne wskazania, co powinna zawierać. Odnosząc to do regulacji rozważanej umowy w treści RODO, wydaje się, że pomocny będzie fragment przepisu zawartego w treści art. 28 ust. 3 RODO, wskazujący że umowa wiąże podmiot przetwarzający i administratora, określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Zestawiając powyższe elementy z ogólnie przyjętym tradycyjnym rozumieniem *essentialia negotii* jako elementów składowych konstytuujących umowę, przedmiotowo istotnych dla treści umowy, takich, bez których umowa nie będzie skutecznie zawarta, można stanąć na stanowisku, że przepis RODO, w odróżnieniu od przepisu funkcjonującego na gruncie UODO z 1997 r., zawiera (nie jak wcześniej w szczątkowym zakresie) elementy przedmiotowo istotne dla umowy powierzenia przetwarzania danych osobowych[433], bez których nie można mówić o tej umowie, a nie jedynie wskazania co taka umowa ma zawierać w swojej treści. Faktycznie trudno byłoby mówić o właściwym i skutecznym umownym zleceniu dokonywania operacji na danych osobowych innemu podmiotowi,

[431] M. Grochowski, *„Nieuregulowane" umowy o świadczenie usług na gruncie art. 750 KC,* Monitor Prawniczy 2016 nr 23, Legalis.
[432] Np. przygotowany przez GIODO materiał „Czy jesteś gotowy na RODO?" dostępny na stronie internetowej https://www.giodo.gov.pl/pl/1520281/10255, str. 31-32.
[433] Wymienione w treści art. 28 ust. 3 RODO elementy umowy kwalifikuje jako *essentialia negotii* umowy również M. Sakowska Baryła (M. Sakowska Baryła (red.), *Ogólne..., op. cit*., Legalis).

bez określenia przede wszystkim o jakie dane osobowe chodzi i w jakim celu następuje ich powierzenie przez administratora podmiotowi zewnętrznemu. W przypadku braku wymienionych elementów umowa, po pierwsze nie spełnia wymogów wynikających z przepisów prawa, a po drugie nie pozwala na prawidłowe wykonanie zobowiązania.

Kolejną przesłanką warunkującą zakwalifikowanie danej umowy do kategorii umów nienazwanych jest według przyjętego schematu brak tożsamości lub podobieństwa pomiędzy tą umową a umową nazwaną. W odniesieniu do umowy powierzenia przetwarzania danych osobowych należy stwierdzić, że trudno byłoby znaleźć w przepisach prawa umowę nazwaną, do której umowa powierzenia byłaby podobna. W związku z tym, że próba przyporządkowania umowy powierzenia do ustawowych typów umów nie kończy się powodzeniem, należy stwierdzić, że jest ona istotnie różna od umów przewidzianych na gruncie obowiązującego prawa, w konsekwencji czego spełnia omawiane kryterium braku tożsamości z umowną nazwaną.

Piątym elementem w katalogu analizowanych przesłanek kształtujących warunki umowy nienazwanej jest określenie stron umowy, przedmiotu i treści, praw i obowiązków stron. Można przyjąć, że większość tych elementów wynika z treści art. 28 RODO, przy czym jedne w sposób literalny, a inne wymagają wyinterpretowania. Wprost prawodawca wskazał strony umowy (w treści ust. 3 nazwane jako podmiot przetwarzający i administrator) oraz przedmiot umowy (w treści ust. 1 określone jako przetwarzanie dokonywane w imieniu administratora). Jeśli chodzi o treść umowy, zwłaszcza prawa i obowiązki stron, kwestia ta nie przedstawia się jednolicie.

W związku z tym, że zagadnienie to jest przedmiotem szczegółowych rozważań w innym miejscu niniejszej dysertacji, poświęconym prawom i obowiązkom stron umowy powierzenia przetwarzania danych osobowych, w tym miejscu należy jedynie zasygnalizować najistotniejsze kwestie. Z perspektywy podmiotu przetwarzającego, jego obowiązki są przede wszystkim wypunktowane literalnie w treści art. 28 ust. 3 lit. a-h RODO, a także art. 30 ust. 2 czy też art. 32 RODO. W odniesieniu do praw przetwarzającego, nie wynikają one z przepisów wprost, jednakże z treści regulacji można wyinterpretować, (np. że przetwarzający ma prawo do korzystania z usług innego podmiotu przetwarzającego). Natomiast patrząc z perspektywy administratora, można powiedzieć, że z uwagi na brak bezpośrednich sformułowań, jego prawa są interpretowane z korelacji z obowiązkami przetwarzającego, np. jeśli obowiązkiem przetwarzającego jest

udostępnianie administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków (art. 28 ust. 3 lit. h RODO), to administrator ma prawo żądać takich informacji. Jeśli chodzi o obowiązki administratora, to o ile prawodawca wskazał w treści art. 28 ust. 1 RODO obowiązek korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje, to odnosi się on do sytuacji przed zawarciem umowy i nie jest on obowiązkiem wobec drugiej strony umowy. Ponadto, nigdzie nie wspomina się np. o wynagrodzeniu dla przetwarzającego czy też o kwestiach związanych z przekazaniem danych do przetwarzania dla przetwarzającego. Z treści przepisu można jednakże wyinterpretować obowiązek administratora w postaci dawania udokumentowanych poleceń podmiotowi przetwarzającemu. Na podstawie powyższego trudno jednoznacznie ocenić, czy omawiane kryterium określenia stron umowy, przedmiotu i treści, praw i obowiązków stron, warunkujące status umowy nienazwanej zostaje spełnione w pełnym zakresie. Można stanąć na stanowisku, że przesłanka ta zostaje zrealizowana w części dotyczącej określenia stron umowy i jej przedmiotu, natomiast wątpliwości może budzić kwestia praw i obowiązków stron.

Kwalifikacja umowy do typu umów nienazwanych wymaga też rozważenia przesłanki pozostawania danej umowy w zgodzie z porządkiem prawnym (naturą stosunku prawnego, ustawami, zasadami słuszności, dobrymi obyczajami). Wydaje się, że w praktyce do oceny spełnienia tego kryterium umowa powierzenia przetwarzania danych osobowych potrzebuje jeszcze czasu. Aktualnie jej funkcjonowanie w obecnym kształcie jest na zbyt wczesnym i niedostatecznie zaawansowanym etapie, by móc dokonać kwalifikacji pod kątem tego kryterium i uwzględniając praktykę. W związku z tym należy uznać, że umowa powierzenia ma pewne cechy umowy nazwanej, ale w kontekście aktualnej regulacji zawartej w treści art. 28 RODO należy zakwalifikować ją do kategorii umów nienazwanych.

Umowy, postrzegane jako najważniejsze źródło stosunków zobowiązaniowych[434], podlegają na gruncie nauki prawa cywilnego wielu innym podziałom. Systematyzacja umów według jednych przedstawicieli doktryny jest typologią[435], według innych klasyfikacją[436], jak również bywa traktowana i jako typologia i jako klasyfikacja[437].

[434] Tak m.in. A. Stelmachowski, *Wstęp do teorii prawa cywilnego,* Warszawa 1984, s. 346, K. Zagrobelny [w:] E.Gniewiek, P. Machnikowski (red.), *Zarys…, op. cit.*, s. 240.
[435] Z. Radwański, *Teoria…, op. cit.*, s. 207.
[436] M.in. W. Czachórski, *Zobowiązania…, op. cit.,* s. 131, J. Rajski, *Prawo…, op. cit*., s. 24.
[437] S. Włodyka [w:] S. Włodyka, *Prawo umów w obrocie gospodarczym*, Warszawa 2001, s. 27 i n.

Zgodnie z klasycznymi na gruncie prawa cywilnego podziałami umów wyróżnia się następujące rodzaje umów: rozporządzającą i zobowiązującą; jednostronnie zobowiązującą i dwustronnie zobowiązującą; konsensualną i realną; odpłatną i nieodpłatną; kauzalną i abstrakcyjną; swobodnie negocjowaną i adhezyjną.

Podział czynności prawnych na rozporządzające i zobowiązujące wynika z faktu, że wywołują one inny skutek. Umowy zobowiązujące, zgodnie z treścią art. 353 KC polegają na tym, że wierzyciel może żądać od dłużnika świadczenia, a dłużnik powinien świadczenie spełnić. Ich skutkiem jest powiększenie pasywów u jednej ze stron oraz powiększenie aktywów u drugiej ze stron. Jako przykład wskazać można umowę składu uregulowaną w treści art. 853 KC. Natomiast umowa rozporządzająca polega na spowodowaniu zmian w prawach majątkowych (natychmiastowych lub odłożonych w czasie), których skutkiem jest negatywne oddziaływanie na sferę praw podmiotowych dokonującego rozporządzenia (przeniesienie, obciążenie, ograniczenie lub zniesienie prawa podmiotowego, zmiana pierwszeństwa) oraz zmniejszenie aktywów rozporządzającego i powiększenie aktywów kontrahenta[438]. Umowy zobowiązujące stanowią większość umów w obrocie gospodarczym. Dodać przy tym należy, że prawo polskie przyjmuje koncepcję umów o podwójnym skutku zobowiązująco-rozporządzającym, co oznacza, że umowa zobowiązująca do rozporządzenia na ogół wywołuje także skutki rozporządzające, bez potrzeby dokonywania odrębnej czynności rozporządzającej i które stanowią szczególną postać umów zobowiązujących[439]. Przepisy Kodeksu cywilnego przewidują również odrębne umowy rozporządzające (art. 508 KC – zwolnienie dłużnika z długu), jak również dopuszczają je w przypadku, gdy osiągnięcie skutku rozporządzającego w umowie zobowiązującej nie było w danej chwili możliwe lub strony wyłączyły ten skutek.

Odnosząc uwagi ogólne dotyczące umów zobowiązujących i rozporządzających do problematyki umowy powierzenia przetwarzania danych osobowych, bezspornym wydaje się fakt, że administrator dokonujący zlecenia przetwarzania danych osobowych na rzecz innego podmiotu, kształtuje zobowiązanie na mocy art. 353 §1 KC[440]. Umowa powierzenia nie stanowi rozporządzenia, nie powoduje zmian w prawach majątkowych

[438] A. Brzozowski [w:] E. Łętowska (red.), *System Prawa Prywatnego Tom 5 Prawo zobowiązań – część ogólna,* Warszawa 2012, s. 448.
[439] *Ibidem*, s. 449.
[440] Zobowiązanie polega na tym, że wierzyciel może żądać od dłużnika świadczenia, a dłużnik powinien świadczenie spełnić.

administratora, nadal to on decyduje o celach i sposobach przetwarzania danych. Zobowiązanie wynikające z umowy powierzenia należy rozważyć w klasycznym podziale na trzy elementy: podmiot, przedmiot i treść.

W aspekcie podmiotowym tradycyjnie powierzenie kształtuje się jako relacja wierzyciela i dłużnika. Przypisując role wierzyciela i dłużnika do stron umowy powierzenia przetwarzania danych, można powiedzieć, że wierzycielem, jako stroną uprawnioną, jest administrator danych, natomiast dłużnikiem, jako stroną zobowiązaną, jest przetwarzający. Warto zauważyć, że po stronie dłużnika może występować więcej niż jeden podmiot – z uwagi na fakt, że przepisy prawa, jak i treść umowy powierzenia, mogą dopuszczać tzw. podpowierzenie, w omawianym stosunku możliwe jest wystąpienie również tzw. podprzetwarzającego (jako wykonawcy podmiotu przetwarzającego).

Aspekt przedmiotowy zobowiązania stanowi świadczenie, które jest przedmiotem zobowiązania i spoczywającego na dłużniku długu, zachowaniem (a częściej zespołem zachowań), które dłużnik powinien podjąć w interesie wierzyciela realizuje nie dokona rozporządzenia danymi[441]. Świadczenie jest oznaczane poprzez treść czynności tworzącej zobowiązanie oraz przepisy prawa, zatem w kontekście umowy powierzenia przetwarzania danych osobowych można przyjąć, że świadczeniem będzie przetwarzanie danych - dokonywanie przez podmiot przetwarzający w imieniu administratora operacji na danych osobowych, wyłącznie na udokumentowane polecenie administratora (zgodnie z art. 28 RODO). Z uwagi na szerokie rozumienie pojęcia przetwarzania, wydaje się słusznym przyjęcie, że świadczenie obejmuje zarówno czynności faktyczne (większość przypadków, np. przechowywanie, powielanie, niszczenie), jak i czynności prawne – możliwość podpowierzenia przetwarzania innemu podmiotowi), ponadto może być zarówno działaniem (większość przypadków, np. zbieranie, udostępnianie), jak i zaniechaniem (nieudostępnianie osobom niepowołanym). Można przy tym podnieść, że wątpliwości może budzić stanowisko przedstawiciela nauki prawa, według którego jako przedmiot umowy powierzenia nie powinien być kwalifikowany jedynie dostęp (wgląd) do danych osobowych przez przetwarzającego nieprzechowywującego ich, niezwiązany z wykonywaniem jakichkolwiek operacji na danych osobowych w imieniu administratora[442]. Z uwagi na szeroki zakres definicji przetwarzania, wgląd do danych również należy uznać za operację na danych osobowych. Jako przykład można wskazać

[441] P. Machnikowski [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, 2017, Legalis.
[442] J. Byrski, *Umowne…, op. cit*., Legalis.

sytuacje, gdy umowy powierzenia przetwarzania danych osobowych są zawierane przez podmioty z przedsiębiorstwami z branży informatycznej, których usługi na zasadzie helpdesk polegają na zdalnej pomocy użytkownikowi określonego systemu informatycznego. W takim przypadku przedsiębiorca nie przechowuje danych osobowych, ale ma do nich dostęp poprzez wgląd w czasie udzielania zdalnej pomocy użytkownikowi i w związku z tym faktem wymaga się zawarcia z nią umowy powierzenia przetwarzania danych osobowych[443].

Warto przyjrzeć się systematyzacji świadczeń na gruncie nauki prawa cywilnego i odnieść ją do świadczenia z omawianej umowy. Po pierwsze, pod względem kryterium wpływu czasu na świadczenie, wyróżnia się świadczenie jednorazowe, okresowe i ciągłe. Świadczenie jednorazowe rozumiane jest w ten sposób, że treść i rozmiar świadczenia są oznaczone wyczerpująco wyłącznie przez wskazanie zachowania się dłużnika, do którego jest on obowiązany, upływ czasu nie ma wpływu na rozmiar świadczenia[444]. Przedmiotem umowy powierzenia może być świadczenie jednorazowe, co potwierdza wyrażony w nauce prawa pogląd, że przedmiotem umowy powierzenia przetwarzania danych osobowych może być czynność jednorazowa[445]. Przykładem takiej sytuacji jest oferowana na rynku usługa polegająca na niszczeniu papierowych dokumentów poufnych czy też niszczeniu elektronicznych nośników danych. Zważywszy, że usuwanie danych stanowi operację na danych i jest literalnie wymienioną czynnością wchodzącą w zakres pojęcia przetwarzania danych osobowych (art. 4 pkt 2 RODO), nie budzi wątpliwości, że zlecenie tej czynności przez administratora danych innemu podmiotowi, czyli skorzystanie z usług niszczenia oferowanych na rynku, będzie wymagało zawarcia umowy powierzenia przetwarzania danych osobowych z podmiotem świadczącym tę usługę, mimo, że jest ona jednorazową czynnością (świadczeniem jednorazowym). W przypadku umowy powierzenia może też wystąpić świadczenie ciągłe. Zgodnie z powszechnie przyjętymi w nauce prawa cywilnego poglądami, świadczenie takie polega na określonym, stałym i w zasadzie niezmiennym zachowaniu się dłużnika przez czas trwania stosunku zobowiązaniowego[446]. Można powiedzieć, że ten rodzaj świadczenia jest dominujący, z uwagi na to, że czynności mieszczące się w zakresie przetwarzania danych osobowych mają charakter ciągłego zachowania (np. zbieranie, przechowywanie). Świadczeniem

[443] https://sylwiaczub.pl/powierzenie-danych-wedlug-rodo/.
[444] P. Machnikowski [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks…, op. cit.,* Legalis.
[445] J. Byrski, *Umowne…, op. cit*., Legalis.
[446] W. Borysiak [w:] K. Osajda (red.), *Kodeks cywilny. Komentarz, 2018*, Legalis.

ciągłym może być np. obsługa kadrowo-płacowa realizowana na rzecz przedsiębiorcy przez wyspecjalizowany podmiot zewnętrzny. Natomiast jeśli chodzi o świadczenie okresowe, za takie nauka prawa uznaje zgodnie świadczenie pieniędzy lub innych rzeczy zamiennych, następujące w określonych, regularnych odstępach czasu, a poszczególne świadczenia nie składają się na żadną z góry określoną wielkość i zachowują swoją jurydyczną samodzielność[447]. W tym wypadku wydaje się, że świadczenie przetwarzającego nie do końca odpowiada temu rodzajowi świadczenia, a przynajmniej trudno byłoby wskazać przykład z praktyki, gdzie przedmiotem umowy powierzenia przetwarzania danych osobowych mogłoby być zachowanie kwalifikowane jako świadczenie okresowe. Z drugiej jednak strony, jeśli w przedmiotowej umowie zostałoby zastrzeżone wynagrodzenie dla przetwarzającego z tytułu przetwarzania danych osobowych w imieniu administratora, to świadczenie mogłoby być rozpatrywane w kategorii świadczenia okresowego.

Doktryna prawa cywilnego odróżnia przedmiot zobowiązania od przedmiotu świadczenia, za który uznaje się np. przedmiot sprzedaży czy kwotę pieniężną wynikającą z umowy pożyczki. W omawianym kontekście przedmiotem świadczenia są dane osobowe powierzane przez administratora, mogą występować w każdej formie, zarówno papierowej, jak i elektronicznej. Z uwagi na przedmiot świadczenia, świadczenia dzielą się na indywidualne (gdy przedmiot jest oznaczony co do tożsamości) i rodzajowe (gdy przedmiot jest oznaczony co do gatunku). Przedmiotem zobowiązania w umowie powierzenia przetwarzania danych osobowych jest świadczenie rodzajowe. Po pierwsze, wynika to z interpretacji przepisu z art. 28 ust. 3 RODO – literalnie sformułowanym wymogiem wobec umowy powierzenia jest określenie w niej rodzaju danych osobowych które w imieniu administratora będzie przetwarzał podmiot przetwarzający*;* po drugie, trudno wyobrazić sobie w praktyce sytuację, gdy administrator będzie zlecał przetwarzanie danych oznaczonych co do tożsamości – czyli jednostkowych danych indywidualnej osoby.

Z uwagi na treść art. 379 § 2 KC[448] wyróżnia się świadczenia podzielne i niepodzielne. Ogólnie można przyjąć, że Podział ten nie jest przydatny do przedmiotu umowy powierzenia przetwarzania danych osobowych, zważywszy na jego specyfikę –

[447] M. Safjan [w:] *K. Pietrzykowski* (red.), *Kodeks cywilny. T. I. Komentarz*, Warszawa 2015, Legalis.
[448] Świadczenie jest podzielne, jeżeli może być spełnione częściowo bez istotnej zmiany przedmiotu lub wartości.

dokonywanie operacji na danych osobowych nie może być rozpatrywane w kategoriach podzielności (gdy istnieje możliwość spełnienia świadczenia w częściach bez istotnej zmiany przedmiotu lub wartości) lub niepodzielności (*a contrario* w przypadku gdy częściowe spełnienie określonego świadczenia wiąże się z istotną zmianą jego przedmiotu lub wartości).

W ujęciu klasycznym, trzecim z wymienionych elementów zobowiązania jest jego treść. Powszechnie przyjętym na gruncie prawa cywilnego jest pogląd, że na treść każdego stosunku zobowiązaniowego składa się istnienie uprawnienia po stronie wierzyciela (co nazywane jest wierzytelnością) i skorelowanego z nim obowiązku oznaczonego działania lub zaniechania po stronie dłużnika (co nazywane jest długiem)[449]. W doktrynie prawa cywilnego bezspornie przyjmuje się też, że przedmiotem obowiązku dłużnika jest spełnienie świadczenia, działanie w określony sposób bądź zaniechanie określonego działania, natomiast przedmiotem uprawnienia wierzyciela jest prawo podmiotowe pozwalające żądać od dłużnika spełnienia świadczenia, czyli zachowania się w określony sposób bądź zaniechanie określonego działania[450]. W przypadku umowy powierzenia przetwarzania danych osobowych, i biorąc pod uwagę tylko tę umowę, a nie fakt, że jest ona umową towarzyszącą innemu stosunkowi prawnemu pomiędzy stronami, za obowiązek dłużnika (przetwarzającego) generalnie uznać można powinność wykonywania woli administratora danych. Natomiast wierzytelność (uprawnienie administratora) stanowi w ujęciu ogólnym prawo żądania spełnienia świadczenia czyli zgodnego z prawem i umową przetwarzania danych osobowych w imieniu administratora. Szczegółowemu ujęciu praw i obowiązków stron będzie poświecony podrozdział o treści umowy powierzenia przetwarzania danych.

Wracając do kwestii kwalifikowania umowy powierzenia przetwarzania danych osobowych jako czynności zobowiązującej, a nie rozporządzającej, należy wyjaśnić, dlaczego w przypadku powierzenia nie następuje rozporządzenie. W konsekwencji podjęcia decyzji o zleceniu przetwarzania danych osobowych podmiotowi zewnętrznemu, *de facto* nie następuje żadna zmiana w sferze praw majątkowych administratora danych. Ponadto po dokonaniu powierzenia to administrator nadal dysponuje danymi, na nim ciążą obowiązki wynikające z przepisów prawa i odpowiedzialność z tytułu przetwarzania danych. Na akceptację zasługuje pogląd wyrażony w nauce prawa, że intencją

[449] *Ibidem*.
[450] M. Gutowski [w:] M. Gutowski (red.), *Prawo cywilne. Komentarz, T. I*, Warszawa 2016, Legalis.

ustawodawcy było to, aby podmiot przetwarzający nie był traktowany jako administrator danych[451], co widać było wyraźnie w nieobowiązującej już treści art. 31 ust. 4 UODO z 1997 r., dotyczącej odpowiedzialności obu stron umowy[452]. Powierzenie przetwarzania danych nie jest umową rozporządzającą również dlatego, że administrator danych nie traci statusu decydenta wobec danych, a podmiot przetwarzający jedynie realizuje wolę administratora i (zgodnie z przepisami RODO) ma działać wyłącznie na polecenie administratora. Potwierdzenie powyższego argumentu znaleźć można w decyzjach GIODO, który w decyzji z dnia z dnia 14 grudnia 2007 r., stwierdził, że działanie podmiotu, który powierzył dane nie zwalnia go z obowiązków nałożonych na niego ustawą o ochronie danych osobowych, bowiem w świetle przepisów wskazanego aktu prawnego, nie traci on przymiotu administratora danych[453].

Jeśli chodzi o podział na umowy jednostronnie i dwustronnie zobowiązujące, dokonywany jest on w oparciu o kryterium interesów kontrahentów lub inaczej tego, czy obowiązek świadczenia ciąży na jednej, czy na obu stronach umowy. W przypadku umów jednostronnie zobowiązujących celem jest realizacja i ochrona interesów jednego z kontrahentów, świadczenia dokonuje natomiast drugi z nich. Przykład stanowić może darowizna. Natomiast jeśli chodzi o umowy dwustronnie zobowiązujące (dla przykładu najem, dzieło, pożyczka), ich celem jest zaspokojenie obu kontrahentów, obie strony zobowiązane są do świadczenia, ponadto umowy te stanowią podstawę wymiany dóbr i usług i główny instrument obrotu towarowo-pieniężnego[454]. W literaturze przedmiotu wskazuje się na możliwość, że dany rodzaj umowy może stanowić w zależności od okoliczności i umowę jednostronnie zobowiązującą i umowę dwustronnie zobowiązującą (umowa przedwstępna)[455]. Ponadto jako szczególny rodzaj umów dwustronnie zobowiązujących wskazuje się umowy wzajemne. Wyróżnienie tej kategorii opiera sie na tym, że świadczenia obu stron są ekwiwalentne, równoważne, stanowią odpowiedniki (na podstawie subiektywnych ocen kontrahentów a nie rzeczywistej wartości świadczeń), jak

[451] J. Barta, P. Fajgielski, R. Markiewicz, *Komentarz…, op. cit.,* s. 505.
[452] W przypadkach, o których mowa w ust. 1-3, odpowiedzialność za przestrzeganie przepisów niniejszej ustawy spoczywa na administratorze danych, co nie wyłącza odpowiedzialności podmiotu, który zawarł umowę, za przetwarzanie danych niezgodnie z tą umową.
[453] Decyzja GIODO z dnia 14 grudnia 2007 r., DOLIS/DES-2/440/07, Legalis nr 465536.
[454] A. Brzozowski [w:] A. Brzozowski, J. Jastrzębski, M. Kaliński, E. Skowrońska-Bocian, *Zobowiązania. Część ogólna,* Warszawa 2016, s. 139.
[455] Z. Radwański, A. Olejniczak, *Zobowiązania - część ogólna*, Warszawa 2016, s. 121.

również na tym, że pomiędzy świadczeniami istnieje więź polegająca na fakcie, że jedna strona świadczy w celu uzyskania świadczenia od drugiej strony[456].

Rozważania nad podziałem umów na jednostronnie zobowiązujące i dwustronnie zobowiązujące stanowią podstawę do wyciągnięcia wniosku, że umowa powierzenia przetwarzania danych osobowych należy do kategorii umów dwustronnie zobowiązujących (a dokładniej wzajemnych). O ile przeważającym jej celem jest zaspokojenie interesów administratora, a z kontekstu regulacji wynika jedynie zobowiązanie do świadczenia podmiotu przetwarzającego, to praktyka stosowania tego instrumentu prawnego nie pozwala uznać, że podmiot przetwarzający przyjmuje na siebie zobowiązania bez świadczenia administratora w zamian. Logicznym jest, że najczęściej przetwarzający otrzymuje w zamian za realizowane obowiązki związane z powierzeniem danych wynagrodzenie określone w pieniądzu

W kontekście podziału umów na konsensualne i realne, kwalifikacja umowy powierzenia przetwarzania danych osobowych budzi wątpliwości. Pierwszy rodzaj obejmuje umowy, które są zawierane wskutek tego, że strony składają zgodne oświadczenia woli (porozumienie, konsens). Jest to zasada we współczesnym prawie zobowiązań, ponieważ do większości umów wystarczy samo złożenie odpowiednich oświadczeń woli (np. sprzedaż, pożyczka, dzierżawa). W umowach realnych natomiast dodatkowo do dojścia do skutku zgodnych oświadczeń woli wymaga się jeszcze przeniesienia władztwa nad określoną rzeczą lub innymi przedmiotami, niezbędne jest wydanie przedmiotu umowy, którego objęcie we władanie stanowi istotny element umowy[457]. Oznacza to, że umowa dochodzi do skutku nie automatycznie w momencie złożenia oświadczeń woli, a dopiero w momencie wręczenia rzeczy w następstwie zgodnych oświadczeń (które może nastąpić w tym samym czasie bądź później). Konieczność ta zachodzi m.in. przy umowie składu, przechowania, użyczenia. Trzeba podkreślić, że strony korzystając z zasady swobody umów, zawarcie każdej umowy mogą uzależnić od faktu wręczenia rzeczy, w konsekwencji czego umowie konsensualnej nadają charakter umowie realnej. Można zatem uznać, że jest to podział teoretyczny i niewiążący.

[456] M. Pannert [w:] T. Mróz (red.), *Zobowiązania…, op. cit*., s. 87.
[457] A. Brzozowski [w:] E. Łętowska (red.), *System…, op. cit*., Legalis.

Z jednej strony można powiedzieć, że umowa powierzenia przetwarzania danych osobowych ma konsensualny charakter[458]. Uzasadnieniem tego stanowiska jest fakt, że przedmiotowa umowa zawierana jest w konsekwencji złożenia zgodnych oświadczeń woli stron, a nie ma konieczności wręczenia rzeczy (w takim przypadku najprawdopodobniej nośnika z danymi, czy to papierowego czy elektronicznego). Administrator może powierzyć przetwarzanie danych osobowych nawet wtedy, kiedy sam tymi danymi nie dysponuje (np. „zleca" zebranie danych do bazy klientów w formie telefonicznej lub mailingowej). Na gruncie nauki prawa wskazuje się również możliwość odmienną. Strony w drodze wspólnych uzgodnień mogą nadać umowie powierzenia charakter umowy realnej. Możliwe jest sformułowanie następującego postanowienia w treści umowy: Administrator powierza Usługobiorcy do przetwarzania dane osobowe objęte zbiorem danych, a Usługobiorca zobowiązuje się do ich przetwarzania zgodnego z prawem i niniejszą umową. Usługobiorca będzie przetwarzać dane osobowe objęte zbiorem danych w swojej siedzibie[459]. W takim wypadku przedmiotowy zbiór danych musi być wydany podmiotowi przetwarzającemu, aby mógł realizować zobowiązanie. Z uwagi na to, że powierzenie przetwarzania danych osobowych rozumiane jest jako wykonywanie operacji na danych w imieniu administratora, na jego zlecenie, trudno byłoby przetwarzać te dane bez uzyskania do nich dostępu. Wydaje się, że umożliwienie podmiotowi przetwarzającemu dostępu do danych może nastąpić w różny sposób, np. poprzez przesłanie pliku z danymi, przekazanie dokumentacji w formie papierowej, udostępnienie folderu z danymi umieszczonego w chmurze, przekazanie przenośnego dysku z danymi. Jeśli dane nie zostaną przez administratora fizycznie przekazane bądź wirtualnie udostępnione przetwarzającemu, trudno mówić o dokonaniu powierzenia. W związku z tym uzasadnionym wydaje się przyjęcie, że umowa powierzenia przetwarzania danych osobowych w pewnych okolicznościach może mieć charakter umowy konsensualnej, a w innych - realnej.

Umowę powierzenia przetwarzania danych osobowych należy też rozważyć w kontekście kwalifikacji umów jako odpłatnych i nieodpłatnych. Umowy odpłatne to umowy przysparzające, czyli polegające na tym, że jedna strona dokonuje przysporzenia drugiej strony i w zamian uzyskuje określoną korzyść majątkową, która o ile nie musi stanowić ekwiwalentu według obiektywnej wartości rynkowej, to powinna mieć wartość

[458] W ten sposób A. Krasuski, D. Skolimowska, *Dane osobowe w przedsiębiorstwie*, Warszawa 2007, s. 130.
[459] *Ibidem* s. 130-131.

realną[460]. Natomiast umowy nieodpłatne, nazywane też darmymi i będące jednocześnie niewzajemnymi, to takie umowy, gdzie nie zastrzeżono żadnej korzyści majątkowej dla strony dokonującej przysporzenia (dla przykładu darowizna, użyczenie) albo też przewidziano korzyść symboliczną (sprzedaż za symboliczną złotówkę). W nauce prawa wskazuje się, że waga przedmiotowego podziału polega na tym, że w przypadku umów nieodpłatnych dłużnik ma zazwyczaj mniejszy zakres obowiązków niż w umowach odpłatnych, jak również na tym, że czynności nieodpłatne są słabiej chronione przez prawo cywilne[461]. Większość umów uregulowanych w Kodeksie cywilnym to umowy odpłatne, np. zamiana, komis, najem.

Nie budzi większych wątpliwości kwalifikacja umowy powierzenia przetwarzania danych osobowych do kategorii umów odpłatnych. Analiza dostępnych wzorów umów, jak również wypowiedzi przedstawicieli nauki zajmujących się problematyką ochrony danych osobowych pozwala wyciągnąć wniosek, że są trzy główne sposoby na określenie kwestii związanych z wynagrodzeniem podmiotu przetwarzającego. Po pierwsze, w umowie powierzenia można zawrzeć uzgodnienia dotyczące wynagrodzenia, określające jego kwotę. Można też ustalić, że wynagrodzenie przetwarzającego z tytułu wykonywania zobowiązań z umowy jest objęte wynagrodzeniem określonym w umowie zasadniczej. Nie ma problemu, jeżeli w treści umowy powierzenia nie zawarto żadnego postanowienia odnoszącego się do wynagrodzenia. W takim wypadku nie oznacza to, że umowa powierzenia jest umową nieodpłatną, bo wynagrodzenie jest ustalone w umowie zasadniczej za całość usługi świadczonej na rzecz administratora. Na podstawie dokonanych badań wzorów umów powierzenia przetwarzania danych osobowych, można sformułować wniosek, że faktycznie wynagrodzenie pieniężne rzadko jest przewidziane w samej umowie powierzenia, najczęstszą opcją jest trzecia z wyżej wymienionych - strony ustanawiają całościowe wynagrodzenie w umowie zasadniczej, zawierając w niej klauzulę o zawarciu umowy powierzenia jako integralnej części umowy zasadniczej

W oparciu o kryterium powiązane z celem zawarcia umowy, wyróżnia się umowy kauzalne (przyczynowe) i abstrakcyjne (oderwane), co ma znaczenie głównie w przypadku czynności przysparzających (powiększających aktywa osoby lub zmniejszających jej pasywa). W nauce prawa wyjaśnia się to w ten sposób, że kontrahenci zawierając umowy kierują się określonymi motywami (*causa*). Jeśli ważność oraz skutki prawne umowy są

[460] W. Czachórski, *Zobowiązania…, op. cit*., s. 138.
[461] *Ibidem*.

uzależnione od istnienia odpowiedniej podstawy, to mamy do czynienia z umową kauzalną. Natomiast jeśli przyczyna (*causa*) jest prawnie obojętna, ponieważ ważność i skutki prawne zawartej umowy są niezależne od istnienia odpowiedniej podstawy prawnej, będzie to umowa abstrakcyjna, jak np. weksel lub przejęcie długu[462]. Od czasów rzymskich wyróżnia się trzy główne podstawy prawne przysporzenia: nabycie prawa lub uzyskanie innej korzyści majątkowej przez przysparzającego, zwolnienie się przez przysparzającego od ciążącego na nim obowiązku, wzbogacenie kontrahenta kosztem dokonującego przysporzenia[463]. O ile tradycyjnie kauzalność umów była uznawana za zasadę, to w nowszej literaturze przedmiotu spotyka się krytykę tego poglądu i stanowisko, zgodnie z którym „za dominujący obecnie należy uznać pogląd, zgodnie z którym w obowiązujących przepisach brak jest podstaw do obrony koncepcji generalnej zasady kauzalności czynności prawnych. Kauzalność przysporzenia może wynikać z uregulowania ustawowego (np. art. 156, 510 § 2 KC). W pozostałym zakresie strony mogą ukształtować czynność prawną jako kauzalną lub abstrakcyjną"[464]. Można wnioskować, że podobnie jak w przypadku umów konsensualnych i realnych, podział na umowy kauzalne i abstrakcyjne jest podziałem teoretycznym, natomiast decyzja co do kwalifikacji może leżeć po stronie kontrahentów konkretnej umowy.

Choć trudno zająć w tym aspekcie jednoznaczne stanowisko i je przekonująco uzasadnić, to mając na uwadze okoliczności faktyczne zawierania umowy powierzenia przetwarzania danych osobowych, wydaje się słusznym uznanie jej za umowę kauzalną. Kluczowe znaczenie ma przy tym akcesoryjny, niesamodzielny charakter umowy powierzenia. Nie jest ona w praktyce zawierana bez towarzyszącej jej umowy zasadniczej (dla przykładu umowa sklepu internetowego z podmiotem zajmującym się usługami kurierskimi na realizację dostaw produktów sklepu do klienta). Nie miałoby uzasadnienia ani sensu zawieranie umowy powierzenia między wymienionymi podmiotami, jako umowy samodzielnej, bez przyczyny, bez oparcia na podstawie prawnej, jaką jest zawarta między nimi umowa zasadnicza, gdyby nie chodziło o realizację dostaw. Można więc uznać, że ważność oraz skutki prawne umowy powierzenia przetwarzania danych osobowych są uzależnione od istnienia odpowiedniej podstawy prawnej, jaką będzie każdorazowo umowa zasadnicza, określająca czynności, do realizacji których niezbędne jest powierzenie przetwarzania danych.

[462] A. Brzozowski [w:] E. Łętowska (red.), *System…, op. cit.,* s. 456.
[463] *Ibidem.*
[464] *Ibidem*, s. 457.

Kolejne zagadnienie do rozważenia stanowi wyróżnianie umów podlegających swobodnym negocjacjom stron oraz umów adhezyjnych. Co do zasady strony układają stosunek prawny wedle swojego uznania, ale w granicach swobody umów (zgodnie z art. 353^1 KC) strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego. Po zakończeniu negocjacji i w konsekwencji wzajemnych ustępstw finalnym etapem jest zaakceptowanie przez obie strony wypracowanych warunków umowy. Tak zawierane umowy należą do rodzaju umów swobodnie negocjowanych. Zdarzają się jednakże takie sytuacje, gdy to jedna ze stron opracowuje postanowienia umowy *de facto* bez ustaleń z kontrahentem i bez negocjacji, pozostawiając drugiej stronie swobodę podjęcia decyzji jedynie w zakresie tego, czy przystąpi do takiej umowy czy nie. Ten rodzaj umów, charakteryzujący się jednostronnością w ustalaniu z góry praw i obowiązków stron, brakiem możliwości modyfikacji postanowień, zawieraniem poprzez przystąpienie nazywany jest umową adhezyjną[465]. Z umowami tego typu mamy do czynienia np. przy usługach dostawy energii lub usługach telefonii, w których przystępuje się do jednostronnie ustalonych warunków, zwykle dyktowanych przez monopolistę.

Jeśli chodzi o próbę zakwalifikowania umowy powierzenia przetwarzania danych osobowych jako umowy swobodnie negocjowanej bądź umowy adhezyjnej, analiza treści umów nie pozwala sformułować wniosku o jednoznacznej kwalifikacji do jednego z tych dwóch rodzajów. Obserwując tendencje na rynku usług oraz korzystając z własnych doświadczeń, można zająć stanowisko, że nie ma wypracowanej zasady i umowy powierzenia przetwarzania danych osobowych mogą być zarówno umowami swobodnie negocjowanymi jak i adhezyjnymi. Niejednokrotnie zdarzają się przypadki, kiedy strony nie negocjują warunków umowy, a stosunek prawny powierzenia następuje poprzez przystąpienie do umowy bez negocjacji, lub też nie zostaje nawiązany w sytuacji, gdy dany podmiot nie zdecyduje się na przystąpienie. Istotną rolę odgrywa tu przede wszystkim kwestia konkurencyjności na rynku usług. Jeśli daną usługę np. przetwarzania chmurowego, proponuje podmiot, który ma pozycję dominującą na rynku (dla przykładu: usługi geolokalizacyjne Google) to umowa powierzenia przetwarzania danych, zawierana przez podmiot, który w swojej działalności opiera się na tych usługach, może być umową adhezyjną – Google najprawdopodobniej będzie zajmował pozycję ustalającego warunki

[465] W. Czachórski, *Zobowiązania…, op. cit.*, s. 141.

umowy. Podobnie może być w sytuacji, gdy agent będzie zawierał umowę z podmiotem świadczącym usługi ubezpieczeniowe np. PZU SA- nie wydaje się, by w sytuacji przedstawienia warunków umowy przez ubezpieczyciela kontrahent mógł je swobodnie negocjować. Jednakże inaczej wygląda sytuacja podmiotu, np. szkoły językowej, korzystającej z usług innego przedsiębiorcy np. biura rachunkowego. W takich przypadkach umowy powierzenia będą raczej umowami swobodnie negocjowanymi, przede wszystkim z uwagi na fakt, że usługi księgowo-rachunkowe oferowane są przez dużo szerszy zakres podmiotów, a ich podejście do klienta jest bardziej zindywidualizowane z uwagi na stosunkowo dużą konkurencję na rynku.

Podsumowując próby określenia charakteru umowy powierzenia przetwarzania danych osobowych, można powiedzieć, że umowa powierzenia przetwarzania danych osobowych jest umową związaną, przede wszystkim z uwagi na to, że nie jest umową samodzielnie występującą w obrocie. Oznacza to, że zawierana jest w powiązaniu z inną umową, ma charakter akcesoryjny, sama nie kreuje zasadniczej relacji prawnej pomiędzy stronami tak jak np. umowa zlecenia, ale ją uzupełnia. Innymi słowy, administrator danych oraz przetwarzający nie zawierają umowy powierzenia przetwarzania danych osobowych, tylko dlatego, że administrator, realizując ustawowe uprawnienie, podejmuje decyzję o tym, że przetwarzanie danych zleci podmiotowi zewnętrznemu. W tym momencie brakowałoby jednego z najistotniejszych i niezbędnych elementów stosunku prawnego powierzenia przetwarzania danych osobowych, jakim jest cel powierzenia. Takim celem byłaby realizacja umowy zasadniczej jak np. zlecenie prowadzenia spraw księgowych biuru rachunkowemu, umowa na usługę hostingu strony internetowej. W związku z tym można sformułować wniosek o niesamodzielnym charakterze umowy powierzenia przetwarzania danych. Każdorazowo wymagane jest jej oparcie o określony cel, który realizowany będzie przez jakieś działanie, a w jego konsekwencji zaistnieje konieczność formalnego uzupełnienia go o powierzenie przetwarzania danych w drodze umowy. Akcesoryjność umowy powierzenia powoduje, że nie może ona podlegać systematyzacji umów samodzielnie, ale łącznie z umową zasadniczą.

Można sformułować wniosek, że umowie powierzenia przetwarzania danych osobowych, której istota wynika z przepisu art. 28 RODO, w odróżnieniu od uregulowanej do niedawna w treści art. 31 UODO z 1997 r., nie można przypisać charakteru typowej umowy nienazwanej. Aktualnie prawodawca europejski znacznie bardziej szczegółowo traktuje przedmiotowy instrument prawny, wskazując, by umowa zawierała co najmniej

sześć wymienionych wymagań: przedmiot przetwarzania, czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych, kategorie osób, których dane dotyczą, obowiązki i prawa administratora. W świetle całej regulacji art. 28 RODO można powiedzieć, że prawodawca podaje sporo informacji na temat umowy powierzenia przetwarzania danych osobowych, które poddają w wątpliwość, czy nadal będzie to umowa nienazwana. Analiza katalogu przesłanek, które zdaniem W. J. Katnera stanowią warunki prawne umowy nienazwanej, pozwala na wyciągnięcie wniosku, że regulacja przedmiotowej umowy w RODO nie spełnia kumulatywnie sześciu wskazanych przesłanek (m.in. ponieważ określa które elementy umowa ta ma obligatoryjnie zawierać), wskazuje strony), zatem idąc tym tokiem rozumowania, nie wydaje się poprawnym uznanie umowy powierzenia za klasyczną umowę nienazwaną, jak np. umowa franchisingu czy forfaitingu. Błędem jednakże byłoby przyznanie jej charakteru umowy nazwanej. Mając na uwadze zagadnienie umowy powierzenia przetwarzania danych osobowych, należy zgodzić się z poglądem, że podział umów na nazwane i nienazwane może być tylko pozornie precyzyjny, ponieważ ani w dorobku orzecznictwa ani nauki prawa nie odnajduje się uniwersalnego mechanizmu pozwalającego na jednoznaczną identyfikację tych umów i oddzielenie ich od siebie[466]. Uzasadnia to pogląd, że w kontekście art. 28 RODO, mamy do czynienia z przepisem, który zmienia dotychczasową bardzo powściągliwą regulację krajową dotyczącą „zlecania" przez administratora czynności przetwarzania danych na zewnątrz. Można zatem postrzegać umowę powierzenia przetwarzania danych osobowych jako umowę nienazwaną, choć dość nietypową, zawierającą cechy umowy nazwanej.

Jeśli chodzi o klasyczną systematyzację umów w prawie cywilnym, wynikiem uwag poczynionych w oparciu o źródła o charakterze teoretycznym, jak i odniesienia do praktyki funkcjonowania powierzania danych osobowych do przetwarzania innym podmiotom przez administratora danych, udało się ustalić, że umowa powierzenia przetwarzania danych osobowych może być zakwalifikowana do kategorii umów zobowiązujących, dwustronnie zobowiązujących (w tym wzajemnych), realnych, odpłatnych, kauzalnych i swobodnie negocjowanych lub adhezyjnych.

[466] M. Grochowski, *„Nieuregulowane" ..., op. cit*., Legalis.

1.2. Kwestia charakteru prawnego umowy powierzenia przetwarzania danych osobowych

Klamrę zamykającą tę część rozważań stanowią próby w zakresie zakwalifikowania umowy powierzenia przetwarzania do konkretnego typu umowy cywilnoprawnej. Z analizy poglądów przedstawicieli nauki prawa wynika, że zazwyczaj zgodnie i bez szczegółowych analiz powtarzane jest stanowisko, w którym umowa powierzenia przetwarzania danych osobowych jest umową o świadczenie usług[467]. Dostępne wzory umowy powierzenia wymagają analizy pod kątem elementów charakterystycznych dla umowy zlecenia, umowy o dzieło i nienazwanej umowy o świadczenie usług, w celu ustalenia, do którego z powyższych rodzajów umów jest przedmiotowej umowie najbliżej, a w konsekwencji, które przepisy mogą być do niej stosowane.

Umowa o świadczenie usług stanowi umowę nienazwaną. W treści Kodeksu cywilnego poświęcono jej dosłownie jedno zdanie (w art. 750 KC), stanowiącego, że do umów o świadczenie usług, które nie są uregulowane innymi przepisami, stosuje się odpowiednio przepisy o zleceniu[468]. Pomimo bardzo okrojonej regulacji, uważa się, że umowy te należą do najczęściej zawieranych w obrocie, ponieważ dotykają niemal wszystkich sfer życia społecznego i gospodarczego[469]. W pierwszej kolejności, ale tylko w niezbędnym zakresie, trzeba odnieść przetwarzanie danych osobowych w konsekwencji powierzenia do kategorii usług. Pojęcie usługi nie zostało zdefiniowane na gruncie Kodeksu cywilnego, ale świadczenie usług ma definicję legalną sformułowaną w ustawie z dnia 11 marca 2004 r. o podatku od towarów i usług[470]. Definicja ta jest stosunkowo szeroka i można powiedzieć, że powierzenie przetwarzania danych mieści się w niej zarówno w aspekcie przedmiotowym (każde świadczenie), jak i podmiotowym (na rzecz osoby fizycznej, osoby prawnej lub jednostki organizacyjnej niemającej osobowości

[467] M.in. M. Kołodziej (red.), *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, Warszawa 2017, Legalis.
[468] Na temat pojęcia świadczenia usług oraz przepisów dotyczących świadczenia usług zob. szerzej P. Zakrzewski [w:] M. Habdas, M. Fras (red.), *Kodeks cywilny. Komentarz. Tom IV. Zobowiązania. Część szczegółowa (art. 535-764*(1) Warszawa 2018, s. 667 i nast. oraz bogate orzecznictwo tam powołane.
[469] R. Morek, M. Raczkowski [w:] K. Osajda (red.), *Kodeks …, op. cit*., Legalis.
[470] T.j. Dz.U. z 2017 r. poz. 1221. Przez świadczenie usług, o którym mowa w art. 5 ust. 1 pkt 1, rozumie się każde świadczenie na rzecz osoby fizycznej, osoby prawnej lub jednostki organizacyjnej niemającej osobowości prawnej, które nie stanowi dostawy towarów w rozumieniu art. 7, w tym również: 1) przeniesienie praw do wartości niematerialnych i prawnych, bez względu na formę, w jakiej dokonano czynności prawnej; 2) zobowiązanie do powstrzymania się od dokonania czynności lub do tolerowania czynności lub sytuacji; 3) świadczenie usług zgodnie z nakazem organu władzy publicznej lub podmiotu działającego w jego imieniu lub nakazem wynikającym z mocy prawa.

prawnej). Co więcej, można też stanąć na stanowisku, że powierzenie przetwarzania danych osobowych może odpowiadać uszczegółowieniu, które ustawodawca sformułował w punkcie 1 powołanego przepisu (przeniesienie praw do wartości niematerialnych i prawnych, bez względu na formę, w jakiej dokonano czynności prawnej). Jako argumenty wskazać można po pierwsze, że powierzenie przetwarzania danych osobowych stanowi czynność prawną (podstawowym instrumentem dokonania powierzenia jest przecież umowa), po drugie, dane osobowe mogą być uznane za wartości niematerialne i prawne (jest to zgodne z wnioskami wynikłymi z rozważań nad pojęciami informacji i danych, dokonanymi w pierwszym rozdziale rozprawy), a po trzecie, konsekwencją powierzenia jest przeniesienie praw, z racji tego, że prawo do przetwarzania danych osobowych posiada administrator danych, który na mocy umowy powierzenia przenosi część swoich praw na podmiot przetwarzający (który bez zawarcia przedmiotowej umowy nie miałby żadnych praw do tych danych). W ślad za powyższymi ustaleniami należy uznać, że przetwarzanie danych osobowych w konsekwencji powierzenia stanowi świadczenie usług zdefiniowane na gruncie języka prawnego w treści ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług[471].

Z uwagi na przyjęte wyżej ustalenia oraz fakt, że na gruncie nauki prawa nie są wyraźnie zarysowywane poglądy przeciwstawne do większościowego, zgodnie z którym umowa powierzenia przetwarzania jest umową o świadczenie usług, należy poprzeć to stanowisko i traktować je jako niewymagające argumentacji. Jednakże jednocześnie warto zaznaczyć wewnętrzną niejednolitość w ramach umowy tego typu, ponieważ z praktyki zawierania umów powierzenia można odnieść wrażenie, że część z nich będzie miała charakter umowy o świadczenie usług z wyraźnymi elementami umowy zlecenia, a część (choć zdecydowanie mniejsza) – charakter umowy o świadczenie usług z wyraźnymi elementami umowy o dzieło. Trzeba zwrócić uwagę przede wszystkim na fakt, że przedmiotem umowy powierzenia przetwarzania danych osobowych jest świadczenie polegające na przetwarzaniu danych. Natomiast przetwarzanie to nie tylko czynności faktyczne, ale również czynności prawne. Czynnością prawną w zakresie pojęcia przetwarzania danych osobowych będzie podpowierzenie (dalsze powierzenie) przetwarzania danych, które następuje w drodze umowy z podwykonawcą (tzw. podprzetwarzającym).

[471] T.j. Dz.U. z 2017 r. poz. 1221.

Zgodnie ze stanowiskiem Sądu Najwyższego odpowiednie stosowanie przepisów o zleceniu do umowy o świadczenie usług oznacza konieczność uwzględnienia specyfiki konkretnej sytuacji. Może więc wchodzić w grę stosowanie określonych przepisów wprost, z dostosowującymi do okoliczności modyfikacjami, a nawet wyłączenie stosowania pewnych przepisów z uwagi na odmienne cechy danego przypadku, wynikające ze swobodnego ukształtowania przez strony stosunku prawnego (art. 353^1 KC)[472]. Można powiedzieć, że w tej drugiej sytuacji będzie możliwe powoływanie się na przepisy regulujące umowę u dzieło, z uwagi na odmienne cechy danego przypadku, czyli wtedy gdy umowa powierzenia przetwarzania danych osobowych będzie miała cechy umowy rezultatu, a nie umowy starannego działania (np. w usłudze niszczenia danych).

Do oceny tego, czy do konkretnej umowy powierzenia przetwarzania danych osobowych należy stosować odpowiednio przepisy o zleceniu, czy też dana umowa jest jednak bardziej podobna do umowy o dzieło, każdorazowej analizy wymaga przedmiot umowy, a dokładniej jakie operacje wchodzące w zakres przetwarzania danych osobowych będzie obejmowała umowa. W przypadku gdy administrator danych powierza np. takie czynności jak zbieranie, przechowywanie, porządkowanie, powielanie danych, to z uwagi na fakt, że są to czynności traktowane jako staranne działanie, to faktycznie przepisy o zleceniu są bardziej odpowiednie biorąc pod uwagę, że jest to umowa starannego działania i nie oczekuje się by strona odpowiadała za efekt swoich działań. Umowa powierzenia stanowi w tym przypadku umowę o świadczenie usług z wyraźnymi elementami umowy zlecenia. Natomiast w przypadku, kiedy umowa powierzenia jest integralną częścią umowy np. na usługę niszczenia czy to dokumentów w formie papierowej, czy też elektronicznych nośników informacji, dotyczy ona rezultatu działania przetwarzającego – chodzi o efekt usunięcia danych. Ten rodzaj operacji dokonywanych na danych powinien być rozpatrywany w kategorii dzieła jako umowy rezultatu, a nie zlecenia, jako starannego działania podmiotu świadczącego usługi niszczenia dokumentów. W takiej sytuacji umowa powierzenia może być rozpatrywana jako umowa o świadczenie usług z wyraźnymi elementami umowy zlecenia. Skłania to również do sformułowania wniosku, że charakter umowy powierzenia w głównej mierze jest zależny od umowy zasadniczej, z którą jest związana. Jeśli umowa zasadnicza jest umową starannego działania i ma cechy zlecenia (np. archiwizacja akt osobowych pracowników, wynajęcie miejsca na serwerze), to umowa powierzenia również ma ten charakter.

[472] Wyrok Sądu Najwyższego z dnia 23 stycznia 2008 r., V CSK 377/07, Legalis nr 140220.

Natomiast jeśli umowa zasadnicza ma cechy dzieła jako umowa rezultatu (np. przeprowadzenie jednorazowej akcji reklamowej i zwrócenie danych klientów administratorowi) – to i umowa powierzenia przetwarzania danych osobowych będzie miała takie właśnie cechy. Potwierdza to występowanie obu umów w relacji umów akcesoryjnych, choć akcesoryjność nie wynika z *essentialia negotii* umowy powierzenia przetwarzania danych ujętych w treści art. 28 ust. 3 RODO.

Oczywiście nietrudno wywnioskować, że zdecydowaną większość umów powierzenia przetwarzania danych osobowych będą stanowiły umowy o świadczenie usług, do których odpowiednio należy stosować przepisy o zleceniu, natomiast wyjątkowo będzie się zdarzało, że określona umowa powierzenia stanowi umowę o świadczenie usług podobną do umowy o dzieło. Uzasadnia to stanowisko, że charakter prawny umowy jest *de facto* uzależniony od rodzaju czynności przetwarzania, których dotyczy konkretna umowa. W związku z tym, w przypadku, gdy będzie to czynność starannego działania, odpowiednie zastosowanie znajdą przepisy odnoszące się do umowy zlecenia, a gdy przedmiotem umowy będzie działanie rezultatu, można powoływać się na przepisy dotyczące umowy o dzieło. Wnioskiem z powyższych rozważań jest też to, że umowa powierzenia przetwarzania danych osobowych okazuje się rodzajem umowy niejednolitym pomimo zgodnego zakwalifikowania jej do kategorii umów o świadczenie usług. Nie można zatem poprzestać na abstrakcyjnych rozważaniach, uniknąć każdorazowej analizy konkretnej umowy, ani też nadać jej charakter odgórnie i w sposób jednoznaczny.

1.3. Umowa powierzenia przetwarzania danych osobowych w świetle zasady swobody umów

Z punktu widzenia stron umowy doniosłym i interesującym jest zagadnienie regulacji prawnej umowy powierzenia przetwarzania danych osobowych w kontekście zasady swobody umów. Wydaje się, że o ile trudno jest uznać tę umowę za umowę nazwaną, to sposób, w jaki została uregulowana w treści art. 28 RODO daje podstawę do uznania, że zasada swobody umów jest tu wyraźnie i mocno ograniczona. Warto to zauważyć chociażby dlatego, że to swoboda umów jest normatywną podstawą do konstruowania umów nienazwanych[473]. Dla zbadania istoty i celu ograniczenia zasady swobody umów w przypadku umowy powierzenia przetwarzania danych osobowych

[473] W. J. Katner (red.), *System*…, tom 9, *op. cit.*, s. 3.

niezbędna wydaje się krótka analiza konstrukcji normatywnej i dogmatycznej zasady swobody umów.

Swoboda umów jest przejawem szerszego pojęcia autonomii woli, rozumianego jako umożliwienie przez system prawny regulowania stosunków prawnych przez podmioty prawa według ich woli za pomocą czynności prawnych[474]. Innymi słowy, chodzi o wolę podmiotów, będącą kreatorem dynamiki obrotu prawnego w drodze czynności prawnych, które są aktami woli autonomicznych podmiotów[475]. Twierdzi się również, że zasada autonomii woli podmiotów jest podstawową zasadą prawa prywatnego, a zasadę swobody umów powinno się pojmować w sensie techniczno-prawnym, jako określony prawem zakres działań, który w ramach autonomii woli stron pozwala na kształtowanie stosunków prawnych za pomocą umów[476].

Normatywny kształt swobody umów określony został w treści art. 353^1 Kodeksu cywilnego, który stanowi, że strony zawierające umowę mogą ułożyć stosunek prawny według swego uznania, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego. Z treści tego przepisu wynika, że strony mogą zawrzeć umowę dowolnej treści i o dowolnym celu, jednak obowiązujące prawo, zasady współżycia społecznego (coraz częściej zastępowane zasadą słuszności), a także natura stosunku prawnego nie mogą zostać naruszone[477]. W tym zrębowym dla swobody umów przepisie wyróżnić można następujące elementy: podmiot kompetencji (strony), czynność konwencjonalna (umowa), zachowanie nakazane adresatowi (obowiązek ułożenia stosunku prawnego w sposób niesprzeciwiający się naturze stosunku, ustawie i zasadom współżycia), adresat (strony, które dokonują czynności)[478].

Jeśli chodzi o treść zasady swobody umów, przedstawiciele nauki prawa prezentują różne stanowiska, ale najczęściej wyróżnia się jej cztery elementy. Pierwszym jest swoboda zawarcia lub niezawarcia umowy, czyli *de facto* podjęcia decyzji o wejściu bądź

[474] Z. Radwański, *System Prawa Prywatnego*, tom 2, Warszawa 2008, s. 4 i n.
[475] S. Prutis, *Instytucje..., op. cit*., s. 89.
[476] S. Prutis, *Instytucje..., op. cit*., s. 89, A. Stelmachowski, *Zarys teorii prawa cywilnego*, Warszawa 1998, s. 88.
[477] E. Łętowska, J. Woleński, *Czy prawo zatruwa wolność?* [w:] Przegląd Filozoficzny – Nowa Seria R. 22: 2013, Nr 3, artykuł dostępny na stronie internetowej http://www.czasopisma.pan.pl/Content/94028/PDF/pfns-2013-0064.pdf?handler=pdf.
[478] A. Brzozowski, P. Machnikowski [w:] E. Łętowska (red.), *System Prawa Prywatnego*, tom 5, Warszawa 2013, s. 482

nie w stosunek zobowiązaniowy. Drugi element to możliwość swobodnego wyboru kontrahenta, czyli decyzji z kim zawrzeć określoną umowę. Następny element to swoboda co do zasady dowolnego ukształtowania treści umowy. Ostatnim z wyróżnianych przejawów jest forma umowy zależna od woli stron, co stanowi uwolnienie stron od formalizmu prawnego. Trzeba jednak tu zaznaczyć, że w praktyce, w swej idealnej, czystej postaci swoboda umów jest rzadkością. Zwykle ograniczają ją w sposób mniejszy lub większy przepisy prawa oraz szereg czynników pozaprawnych, jak np. warunki ekonomiczne. Swobody umów nie należy więc traktować jako wartości absolutnej, z którą nigdy nie może konkurować żadne inne dobro.

Wśród poglądów przedstawicieli nauki prawa podkreślenia wymaga stanowisko, że wymienione elementy swobody z reguły umów nie występują łącznie. Zawsze zawierają prawne lub pozaprawne ograniczenia, na które składają się czynniki ustrojowe, normatywne, gospodarcze czy społeczne. Stąd uzasadnione jest przyjęcie trwałości samej idei swobody umów, ale zmienności jej treści[479]. W treści art. 353^1 KC wymienione są trzy czynniki stanowiące granice swobody umów. Zakres kompetencji stron co do kształtowania stosunku umownego jest wyznaczony poprzez właściwość (naturę stosunku), ustawę i zasady współżycia społecznego. Wskazuje się, że wymienione w treści przepisu ograniczenia są jedynymi, co oznacza, że nie ma innych jak np. istniejące zwyczaje, a ponadto o kompetencji stron decyduje chwila zawarcia umowy (późniejsze zmiany stanu prawnego nie mają znaczenia)[480].

Jeśli chodzi o pierwsze z ograniczeń zasady swobody umów, spotyka się ono z trudnościami w interpretacji, jest niejasne i wątpliwe. Pełen Skład Izby Cywilnej Sądu Najwyższego podjął uchwałę, zgodnie z którą ograniczenie, polegające na konieczności respektowania (natury) danego stosunku prawnego, jest interpretowane w sposób szeroki i wąski. W szerszym rozumieniu za sprzeczne z naturą zobowiązania uznawane jest takie zniekształcenie umowy typowej, które wykracza poza ramy stosunku umownego, akceptowanego w sferze danego ustawodawstwa, gdy jednocześnie nie istnieje podstawa do rozumienia stosunku jako umowy mieszanej, zgodnej z wolą stron. Natomiast interpretacja węższa oznacza sprzeczność przewidywanych warunków umowy z jakąkolwiek rozsądną wykładnią stosunku prawnego mieszczącego się w sferze

[479] T. Mróz, *Dekompozycja zasady swobody umów? Próba klasyfikacji i oceny niektórych czynników kształtujących tę zasadę*, [w:] B. Gnela (red.), *Ustawowe ograniczenia zasady swobody umów. Zagadnienia wybrane*, Warszawa 2010, s. 42-43.
[480] P. Machnikowski, *Swoboda umów według art. 353^1 KC. Konstrukcja prawna*, Warszawa 2005, s.175.

dostępnych naszemu ustawodawstwu instytucji[481]. Kryterium właściwości (natury) stosunku prawnego zostało wyjaśnione przez jednego z przedstawicieli nauki prawa jako zapobieżenie takim sytuacjom umownym, które pod płaszczykiem umów przewidzianych w prawie miałyby realizować zupełnie inne cele[482]. Interesującą kwestią jest też możliwość odwołania do natury stosunku umownego nienazwanego. Jest to uznane za dopuszczalne, z zastrzeżeniem, iż kryterium natury zobowiązania może znaleźć zastosowanie jedynie poprzez odwołanie się do ogólnych, podstawowych cech stosunku obligacyjnego nienazwanego, bez których jest on pozbawiony swojego sensu gospodarczego[483].

W nauce prawa zgodnie twierdzi się, że ograniczenie zasady swobody umów z uwagi na ustawę występuje najczęściej i sprowadza się do niedopuszczalności ustalenia treści stosunku zobowiązaniowego (czyli uprawnień i obowiązków stron) lub jego celu, które powodowałoby naruszenie przepisu o charakterze *iuris cogentis*. Wyjaśnić należy, że chodzi tu zarówno o przepisy Kodeksu cywilnego jak i innych aktów[484], przy czym ma to być przepis rangi ustawowej lub rozporządzenia wydanego na podstawie wyraźnej delegacji ustawowej[485]. Wyłączone z tego zakresu są natomiast pozakonstytucyjne źródła prawa prywatnego, akty wewnętrzne organów administracji, ogólne warunki umów, statuty i umowy dotyczące osób prawnych, uchwały organów osób prawnych[486]. Można uznać, że z uwagi na rangę wyższą niż ustawy, przepisy rozporządzenia unijnego tym bardziej mogą stanowić ograniczenia swobody umów należące do tej kategorii. Co istotne, ograniczenia swobody określania treści umowy przez same strony, statuowane przez imperatywne przepisy prawa, mogą przybierać różną postać. Mogą polegać na wskazaniu, co (albo jak) strony muszą postanowić w treści umowy. Ponadto mogą wskazywać, czego stronom zawrzeć w umowie nie wolno (umowa będzie nieważna, chyba że właściwy przepis przewiduje inny skutek). Możliwe jest też, że prawo nadaje zachowaniom stron

[481] Uchwała Pełnego Składu Izby Cywilnej Sądu Najwyższego z dnia 28 kwietnia 1995 r., III CZP 166/94, nr Legalis 29265.
[482] A. Stelmachowski, *Zarys..., op. cit.,* s. 97.
[483] M. J. Skrodzka, K. Skrodzki, *Źródła zasady swobody umów oraz wybrane aspekty jej granic – w świetle orzecznictwa*, Białostockie Studia Prawnicze 2008 z. 3, s. 94-95.
[484] Zob. Szerzej powoływaną tu publikację pod red. B. Gneli, w której przedstawiono przykładowe ograniczenia swobody umów wynikające m.n. z prawa własności intelektualnej, prawa zamówień publicznych, prawa upadłościowego czy prawa spółek.
[485] M. Szaraniec, *Publicznoprawne ograniczenia swobody kontraktowej w działalności krajowego zakładu ubezpieczeń – zagadnienia wybrane* [w:] B. Gnela (red.), *Ustawowe...*, op. cit., s. 135. S. Prutis dodaje do tego katalogu również akty prawa miejscowego o ile realizują odpowiednio skonstruowane upoważnienie ustawowe.
[486] S. Prutis, *Instytucje..., op. cit*., s. 99.

określonego przez prawo znaczenia, niezależnie od tego, czy strony tego rzeczywiście chciały[487].

Trzecia kategoria ograniczeń swobody kształtowania treści stosunku prawnego to zasady współżycia społecznego, które powszechnie przyjęto na gruncie cywilistyki jako normy moralne. Co istotne, w nauce prawa wskazuje się, że kwestionowanie ważności czynności prawnej wobec jej sprzeczności z zasadami współżycia społecznego wymaga każdorazowo wskazania, o jakie dokładnie zasady chodzi. Najważniejsze wartości, których nieprzestrzeganie może prowadzić do stwierdzenia niezgodności z zasadami współżycia społecznego i nieważności umowy na podstawie art. 353^1 w zw. z art. 58 § 2 KC, to m.in. wolność człowieka, w tym wolność działalności gospodarczej, równość faktyczna stron, słuszność kontraktowa, ochrona osób trzecich, wolna konkurencja[488]. Ponadto wskazuje się w literaturze, że należy szeroko traktować sprzeczność stosunku zobowiązaniowego z zasadami współżycia społecznego, co oznacza, że nie tylko treść i cel umowy powinny być poddawane ocenie moralnej, ale również postępowanie stron prowadzące do zawarcia umowy[489]. Jako przykładowe sprzeczności umowy z zasadami współżycia społecznego wskazać można umowę zawartą z lekarzem uzależniającą wysokość wynagrodzenia od wyleczenia chorego czy też *pactum de non licitando* (powstrzymanie się od udziału w licytacji).

Odnosząc powyższe ogólne uwagi dotyczące swobody umów do umowy powierzenia przetwarzania danych osobowych, należy ustalić, które z wymienionych elementów zasady swobody umów są respektowane w przypadku tego zobowiązania, a które doznają znacznych ograniczeń.

Już na początku pojawia się trudność co do swobody zawarcia lub niezawarcia umowy. Wątpliwości wzbudza przede wszystkim to, że przepisy prawa konstruują obowiązek zawarcia umowy powierzenia, w przypadku gdy administrator poleca przetwarzanie danych w swoim imieniu innemu podmiotowi. Obowiązek ten wyinterpretować można zarówno z treści art. 28 ust. 3 RODO, zgodnie z którym przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, jak również z treści motywu 81 preambuły RODO, stanowiącej, że

[487] E. Łętowska, J. Woleński, *Czy prawo..., op cit.*, http://www.czasopisma.pan.pl/Content/94028/PDF/pfns-2013-0064.pdf?handler=pdf.
[488] M. Gutowski [w:] M. Gutowski (red.), *Kodeks cywilny. Tom II. Komentarz*, Warszawa 2019, Legalis.
[489] S. Prutis, *Instytucje..., op. cit.*, s. 102.

przetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym instrumentem prawnym. Ponadto jako przejaw braku swobody co do samego nawiązania stosunku umownego między administratorem i podmiotem przetwarzającym postrzegać można przepisy dotyczące kar administracyjnych. Zgodnie z treścią art. 83 ust. 4 lit. a) RODO naruszenie obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25–39 oraz 42 i 43 RODO, podlega administracyjnej karze pieniężnej w wysokości do 10 000 000 euro, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu. Obowiązki zawarte w treści art. 28 RODO dotyczącego przetwarzania danych przez podmiot przetwarzający, bez wątpienia mieszczą się w zakresie tej regulacji. Tutaj należy pamiętać o akcesoryjnym charakterze umowy powierzenia. Jest to umowa powiązana z umową zasadniczą dotyczącą określonej usługi, w ramach której dochodzi do przetwarzania danych osobowych przez podmiot zlecający czynności podmiotowi zewnętrznemu. Można zatem stwierdzić, że w oparciu o aktualne brzmienie przepisów RODO zasada swobody umów nie ma zastosowania w aspekcie swobody zawarcia umowy, samego nawiązywania stosunku zobowiązaniowego. Natomiast w większości przypadków zasada swobody umów realizowana jest co do umowy zasadniczej, ponieważ w gestii administratora danych leży to, czy określone zadania będzie realizował w oparciu o własne zasoby, czy też „zleci" je podmiotowi zewnętrznemu.

Podobnie kształtuje się kwestia spełniania swobody wyboru kontrahenta w przypadku regulacji umowy powierzenia przetwarzania danych osobowych. Jako umowa akcesoryjna, umowa powierzenia nie może być zawarta z dowolnym podmiotem. Stosunek powierzenia może być nawiązany jedynie z tym podmiotem, z którym administrator zawarł umowę zasadniczą na określoną usługę, np. biurem rachunkowym czy firmą kurierską. Podobnie jak w przypadku swobody zawarcia umowy, swoboda wyboru kontrahenta może być realizowana na etapie podejmowania decyzji o skorzystaniu z usług podmiotu zewnętrznego i dokonania jego wyboru (np. na podstawie dobrej opinii, atrakcyjnej ceny, jakości usług). Jednakże tu RODO wprowadza dodatkowe ograniczenie. Zgodnie z treścią 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 RODO i chroniło prawa osób, których dane dotyczą. Z przepisu tego bez wątpienia wynika

ograniczenie w wyborze kontrahenta. Jeśli bowiem administrator chciałby „zlecić" kampanię marketingową podmiotowi, który został wybrany na podstawie kryterium ceny, ale nie daje on gwarancji, że będzie przetwarzać dane osobowe w imieniu administratora, uwzględniając wymogi określone w RODO, to współpraca z takim podmiotem będzie oznaczała naruszenie art. 28 ust. 1 RODO oraz umożliwi zarzucenie administratorowi niedopełnienie należytej staranności.

Kolejnym ważnym obszarem zasady swobody umów, który należy odnieść do regulacji umowy powierzenia przetwarzania danych osobowych jest swoboda dowolnego ukształtowania treści umowy. Trudno powiedzieć, aby strony umowy powierzenia mogły ukształtować treść umowy według własnej woli. Elementy, które ma zawierać umowa prawodawca narzucił w treści art. 28 ust. 3 RODO, wskazując na przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Co więcej, prawodawca ustalił w treści przepisów art. 28 ust. 3 pkt a-h RODO sferę obowiązków podmiotu przetwarzającego, jako minimalne wymagania. Nie wydaje się, żeby strony mogły postanowić, że któryś z obowiązków nie będzie w ogóle realizowany lub też przechodzi na administratora. Tak szczegółowe zobowiązania leżące po stronie podmiotu przetwarzającego nie powinny jednak być kopiowane do postanowień konkretnych umów. Jak wskazuje się w literaturze przedmiotu, w praktyce obowiązki wynikające z art. 28 ust. 3 pkt a-h RODO będą wymagać skonkretyzowania w sposób adekwatny do zadań, operacji przetwarzania, zaplecza logistycznego, kategorii danych i osób, których dane dotyczą, ram czasowych i terytorialnych powierzonego przetwarzania[490]. Wydaje się jednak, że strony mimo to mają sporą swobodę w zakresie treści wymaganych zapisów, w tym zasad kształtowania sposobu realizowana obowiązków podmiotu przetwarzającego (dla przykładu, jak często można przeprowadzać audyt przetwarzania danych i z jakim wyprzedzeniem informować o nim podmiot przetwarzający).

Ostatni z elementów swobody umów jest swoboda co do wyboru formy zawarcia umowy. Ogólnie rzecz biorąc, prawodawca w przypadku umowy powierzenia przetwarzania danych osobowych nie zwolnił stron z formalizmu prawnego, stanowiąc w treści art. 28 ust. 9 RODO że umowa ma formę pisemną, w tym formę elektroniczną. Można to tłumaczyć generalnym podejściem stosowanym na gruncie przepisów RODO

[490] M. Sakowska-Baryła (red.), *Ogólne..., op. cit*., Legalis.

do skrupulatnego dokumentowania działań związanych z ochroną danych osobowych. W odniesieniu do akcesoryjnego charakteru umowy powierzenia względem umowy zasadniczej, wygląda na to, że umowa zasadnicza może mieć dowolną formę, zaś będąca jej częścią umowa powierzenia zawsze musi być zawierana na piśmie bądź elektronicznie.

Reasumując, zgodnie z szeroko uznanym na gruncie nauki prawa poglądem, swoboda umów to przekazanie przez państwo swych kompetencji normotwórczych samym stronom, przez co państwo rezygnuje z władczego uregulowania stosunków wzajemnych stron[491]. W przypadku umowy powierzenia przetwarzania danych osobowych nie można powiedzieć o całkowitej rezygnacji z kompetencji prawodawcy do władczego ukształtowania stosunku prawnego zachodzącego między administratorem i podmiotem przetwarzającym. Przepisy prawa skrupulatnie przewidują zakres praw i obowiązków stron umowy, jednoznacznie wskazują formę umowy, jasno formułują wymogi co do elementów jej treści.

Kluczowe znaczenie ma tu charakter przepisów RODO odnoszących się do umowy powierzenia przetwarzania danych osobowych – czy są to przepisy imperatywne (bezwzględnie obowiązujące) czy też dyspozytywne (względnie obowiązujące). Należy zgodzić się z rozumowaniem przedstawionym przez E. Łętowską i J. Woleńskiego, zgodnie z którym w przypadku przepisów imperatywnych decyduje wola ustawodawcy wyrażona w treści przepisów, a nie wola stron. Regulacja prawna zajmuje arbitralnie miejsce tego, co strony miałyby uregulować same, wobec czego ich wola musi ustąpić przed wolą prawodawcy, ponieważ umowa jest tu subsydiarna względem prawa. Natomiast w przypadku gdy przepisy prawa mają charakter dyspozytywny, sytuacja jest odwrotna. To przepisy są subsydiarne względem umowy, a ich zastosowanie ma miejsce wtedy, gdy strony w umowie nie uregulowały jakiejś kwestii inaczej[492]. Chociażby z uwagi na konsekwencje naruszenia postanowień RODO administracyjnymi karami pieniężnymi, bez wątpienia jego przepisy mają charakter imperatywny. Można w związku z tym stwierdzić, że swoboda umów jest znacznie ograniczona w przypadku umów powierzenia przetwarzania danych osobowych.

Można też wywnioskować, że najczęściej swoboda umów znajduje zastosowanie dopiero wtedy, gdy minimalne wymogi wynikające z treści art. 28 RODO zostają

[491] A. Stelmachowski, *Zarys..., op. cit.,* s. 89.
[492] E. Łętowska, J. Woleński, *Czy prawo..., op. cit.*, http://www.czasopisma.pan.pl/Content/94028/PDF/pfns-2013-0064.pdf?handler=pdf.

spełnione. W ten sposób należałoby interpretować treść motywu nr 109 preambuły RODO, zgodnie z którym należy zachęcać administratorów i podmioty przetwarzające, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie minimalnych wymogów. Ponadto, na podstawie poczynionych rozważań można przyjąć, że z trzech czynników wyznaczających granice swobody umów, najczęściej występują ustawowe ograniczenia tej zasady i mają one swoje źródło w przepisach RODO.

Należy podkreślić, że istotne w praktyce są również faktyczne ograniczenia możliwości korzystania ze swobody umów. również faktyczne ograniczenia możliwości korzystania ze swobody umów. W nauce prawa rozumie się je jako różnorodne zjawiska o charakterze prawnym lub pozaprawnym, które ograniczają rzeczywistą swobodę podejmowania decyzji przez jedną lub obie strony umowy, a najczęściej wskazuje się faktyczną nierównorzędność stron[493]. Zdarza się, że jedna ze stron ma nad drugą przewagę ekonomiczną, w konsekwencji czego zawarcie umowy ma mniejsze znaczenie dla tej strony niż dla jej kontrahenta. Może ona wywierać presję w kierunku zawarcia umowy o określonej treści, szczególnie gdy alternatywą jest odrzucenie warunków i ostatecznie niezawarcie umowy[494]. Wstępnie można powiedzieć, że w umowie powierzenia przetwarzania danych osobowych zdarzają się sytuacje, gdy stronom umowy trudno przypisać cechę równorzędności, ale kwestie te zostaną rozwinięte w poniższych uwagach dotyczących stron umowy powierzenia przetwarzania danych osobowych.

Wydaje się, że ograniczenia swobody umów są uzasadnione, z uwagi na to że wynikają z szczególnego rodzaju dóbr, jakimi są dane osobowe. Należy podkreślić, że powszechnie doceniana wartość zasady umowy nie ma charakteru wartości absolutnej i może być ograniczana z uwagi na ochronę innego dobra, w przypadku umowy powierzenia przetwarzania danych osobowych tym dobrem są dane osobowe. Trudno jest jednakże stwierdzić generalnie, czy ograniczenia te w sposób dostateczny zapewniają ochronę danych osobowych, jest to kwestia indywidualnego przypadku.

[493] A. Brzozowski, P. Machnikowski [w:] E. Łętowska (red.), *System..., op. cit*., s. 496 i n.
[494] *Ibidem*.

2. Strony umowy powierzenia przetwarzania danych osobowych

2.1. Charakterystyka podmiotów stosunków prawnych w procesie przetwarzania danych osobowych

Stronami umowy powierzenia przetwarzania danych osobowych są administrator danych osobowych oraz podmiot przetwarzający, nazywany również procesorem. W źródłach anglojęzycznych odpowiednikiem administratora danych jest *data controller,* a przetwarzającego – *data procesor*[495]. Strona uprawniona - administrator - została nazwana bezpośrednio w treści przepisów prawa regulujących przetwarzanie danych w imieniu administratora. Można powiedzieć, że administrator danych pełni najważniejszą rolę nie tylko w stosunku powierzenia przetwarzania danych, ale globalnie, w całym procesie przetwarzania, z uwagi na to, że ma uprawnienia decyzyjne. Od jego woli oraz działania zależy *de facto*, czy zaistnieje relacja administratora z każdym innym podmiotem uczestniczącym w przetwarzaniu danych osobowych. Dlatego zazwyczaj najważniejszym okazuje się dokonanie właściwej identyfikacji podmiotu, który jest administratorem danych. Nie jest to zadanie proste i niejednokrotnie może prowadzić do niejednoznacznych ustaleń.

W celu wyjaśnienia kontekstu rozważań warto powołać się na pogląd wyrażony w nauce prawa, dotyczący podmiotów procesu przetwarzania danych osobowych[496]. W ramach tego procesu wyróżniono dwa stosunki: wewnętrzny i zewnętrzny. W stosunku wewnętrznym (wewnątrzorganizacyjnym) uczestniczą administrator danych osobowych i osoby, które zostały upoważnione do przetwarzania danych (na mocy art. 29 RODO). Natomiast w stosunku zewnętrznym wyróżnia się udział administratora danych, przetwarzającego, odbiorcy danych i przedstawiciela (zdefiniowany w art. 4 pkt 17 RODO, oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia). Omawiając podmiotowy aspekt przetwarzania danych należy również

[495] Opracowanie w języku angielskim, *Data controllers and data processors: what the difference is and what the governance implications are*, dostępne na stronie internetowej https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf.
[496] A. Krasuski, D. Skolimowska, *Dane..., op. cit.*, s. 55.

zwrócić uwagę na podmiot zdefiniowany w art. 4 pkt 10 RODO), czyli stronę trzecią[497], która oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe. Krótkie wyjaśnienie tych pojęć jest bardzo istotne z perspektywy dalszych rozważań, ponieważ implikuje wniosek, który wynika również z wypowiedzi Komisji Europejskiej: przetwarzający jest podmiotem zewnętrznym w stosunku do administratora danych, nie jest elementem jego struktury organizacyjnej[498]. W najnowszej literaturze przedmiotu wyrażono inny pogląd w kontekście podmiotów procesu przetwarzania danych[499]. Zgodnie z nim, dane osobowe mogą być przetwarzane przez podmioty należące do jednej z dwóch kategorii: administrator danych osobowych lub podmiot przetwarzający. Wydaje się, że jest to stanowisko, które prowadzi do zbytniego uproszczenia relacji istniejących w ramach przetwarzania danych i w konsekwencji do wyciągnięcia wniosków, które prowadzić mogą do niewłaściwego ustalenia statusu podmiotu zaangażowanego w przetwarzanie. Jednakże można się z tym zgodzić, jeśli mówimy o przetwarzaniu danych osobowych w stosunku powierzenia danych, wtedy bowiem dwupodział kategorii uczestników procesu przetwarzania jak najbardziej jest uzasadniony.

Chronologicznie pierwszym aktem, na który można się powołać przy analizie podmiotów stosunku prawnego powierzenia przetwarzania danych osobowych jest Konwencja Rady Europy nr 108 z 1981 roku. Faktycznie jednak treść Konwencji 108 nie rozwiązuje problemu, gdyż zawarto w niej pojęcie administratora zbioru danych, a nie administratora danych, natomiast brakuje definicji przetwarzającego. Zgodnie z treścią art. 2 lit. d Konwencji pod pojęciem administratora zbioru danych rozumie się osobę fizyczną lub prawną, władzę publiczną, agencję lub każdy inny organ właściwy na podstawie prawa wewnętrznego do określenia celu, któremu ma służyć zautomatyzowany zbiór danych, kategorii gromadzonych danych osobowych oraz sposobu przetwarzania, jakiemu dane będą poddawane. Z biegiem czasu, na etapie prac nad aktem prawnym wiążącym państwa

[497] W polskiej ustawie nie identyfikuje się tego pojęcia.
[498] *"The data processor is usually a third party external to the company. However, in the case of groups of undertakings, one undertaking may act as processor for another undertaking."* (https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en).
[499] P. Litwiński [w:] D. Szostek (red.), *Bezpieczeństwo danych i IT w kancelarii prawnej radcowskiej/ adwokackiej/ notarialnej/ komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej*, Warszawa 2018, Legalis.

członkowskie Unii Europejskiej (Dyrektywa 95/46/WE), zdecydowano o zmianie administratora zbioru danych na administratora danych. Nie jest to jednak tylko zmiana terminologiczna, ale nowe podejście do podmiotu procesu przetwarzania danych. Wskazuje się na to w treści Opinii 1/2010 w sprawie pojęć administrator danych i przetwarzający[500] przyjętej w dniu 16 lutego 2010 roku przez Grupę Roboczą ds. ochrony danych powołaną na mocy art. 29 Dyrektywy 95/46/WE.

Administrator danych i przetwarzający występowali już na gruncie Dyrektywy 95/46/WE, w treści art. 17 ust. 2 Dyrektywy 95/46/WE Państwa Członkowskie zobowiązywały administratora danych, w przypadku przetwarzania danych w jego imieniu, do wybrania przetwarzającego. Polski ustawodawca nie formułował nazwy podmiotu przetwarzającego, a posługiwał się w treści art. 31 UODO z 1997 r. sformułowaniem nieokreślonym: „innemu podmiotowi", a następnie opisowo „podmiot, o którym mowa w ust. 1". Trudno logicznie uargumentować zasadność takiego zabiegu, wydaje się, że nazwanie drugiej strony stosunku powierzenia zapewniłoby ułatwienie stosowania przepisów i porządek terminologiczny. Natomiast w treści RODO proponuje się rozwiązanie polegające na wskazaniu z nazwy obydwu podmiotów, znane z Dyrektywy 95/46/WE. W treści art. 4 pkt 7 RODO mowa jest o administratorze, który 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. Wprost jest też wskazany podmiot przetwarzający, który oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO). W związku z powyższym, dla zachowania porządku terminologicznego warto pozostać przy nazewnictwie wypracowanym na gruncie prawa Unii Europejskiej.

W ramach ogólnych uwag dotyczących stron umowy powierzenia przetwarzania danych osobowych należy rozważyć kwestię wzajemnej relacji administratora i podmiotu przetwarzającego. Już na podstawie regulacji prawnej zawartej w treści art. 28 RODO można wywnioskować brak równorzędności stron umowy powierzenia, w większości przypadków z przewagą administratora. Na pierwszy rzut oka jest to widoczne w sposobie

[500] Dalej jako Opinia 1/2010. Tekst dostępny na stronie internetowej http://www.giodo.gov.pl/pl/1520057/3595.

ukształtowania sfery praw i obowiązków stron, gdzie prawodawca wyszczególnił szereg obowiązków po stronie podmiotu przetwarzającego, a nie odniósł się do treści zobowiązania z perspektywy administratora. Ponadto z praktycznego punktu widzenia, niejednokrotnie zdarza się, że brak woli podmiotu przetwarzającego co do zawarcia umowy powierzenia w kształcie zaproponowanym przez administratora stanowi powód niedojścia do skutku umowy zasadniczej tj. dla przykładu umowy o świadczenie usług kadrowo-płacowych. Innymi słowy bywa, że administrator decyduje się nie zlecać określonych czynności podmiotowi, który nie akceptuje postanowień umowy powierzenia przetwarzania danych osobowych. Oznacza to, że może się zdarzyć, że umowa powierzenia będzie miała charakter adhezyjny[501]. Na podstawie obserwacji kształtującej się praktyki stosowania instrumentu ochrony danych osobowych, jakim jest umowa powierzenia, można też powiedzieć, że w większości przypadków zlecania przetwarzania danych podmiotom zewnętrznym, treść umowy powierzenia jest konstruowana przez administratorów. W związku z tym nie ulega wątpliwości, że jej postanowienia będą bardziej korzystne właśnie dla tej strony. Jednakże zdarza się też tak, że to podmiot przetwarzający, oferując swoje usługi, przewidział również warunki co do zawarcia oraz samej treści umowy powierzenia. Postanowienia umowy są wtedy konstruowane jednostronnie przez podmiot przetwarzający, najczęściej w taki sposób, aby to jego interesy były chronione. Administrator staje wtedy przed wyborem albo zawarcia takiej umowy albo zrezygnowania z tego zleceniobiorcy i szukania nowego. Tego typu sytuacje występują najczęściej w odniesieniu do podmiotów zajmujących się infrastrukturą informatyczną, np. dostawcy usług chmurowych czy hostingodawców. Można powiedzieć, że są to przedsiębiorcy więksi i silniejsi ekonomicznie od potencjalnych klientów (będących w tym układzie administratorami) i dlatego nierównorzędność stron umowy powierzenia zostaje tu odwrócona. Podkreślenia wymaga, że przepis art. 28 ust. 3 RODO nie przesądza, czy na zawarciu umowy powierzenia bardziej powinno zależeć administratorowi, czy podmiotowi przetwarzającemu. Prawodawca ujął tę kwestię ogólnie, stanowiąc, że przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego. Wydaje się, że obie strony powinny być w tym samym stopniu zainteresowane, by do zawarcia umowy doszło. W przeciwnym razie można by powiedzieć, że administratorowi grozi zarzut udostępnienia danych

[501] Takie sytuacje będą miały miejsce najczęściej przy usługach związanych z dostarczaniem infrastruktury informatycznej, wynajmowaniu przestrzeni na serwerach, usługach chmurowych.

nieuprawnionemu podmiotowi, natomiast podmiotowi przetwarzającego – zarzut przetwarzania danych bez podstawy prawnej.

2.2. Administrator danych

W treści RODO pojęcie administratora danych zdefiniowano jako jedno z podstawowych pojęć w art. 4 pkt 7, jako osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych[502]. Z definicji wynikają zatem dwa elementy: pierwszy dotyczy aspektu podmiotowego (osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot), a drugi funkcjonalnego (samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych), i *de facto* ten drugi jest decydujący i konstytuuje status administratora danych. Łącząc powyższe elementy, należy zgodzić się z poglądem, że dla uznania podmiotu za administratora danych wymagane jest kumulatywne spełnienie dwóch przesłanek (dwa powyższe elementy)[503]. O ile pierwszy z elementów nie wymaga szczegółowych wyjaśnień, to problem natury praktycznej pojawia się najczęściej w odniesieniu do elementu funkcjonalnego. Dalsza część powołanego przepisu stanowi o tym, że administrator może zostać wyznaczony (lub mogą zostać określone konkretne kryteria jego wyznaczania) w prawie Unii lub w prawie państwa członkowskiego). Nie zawsze proste jest ustalenie w sposób oczywisty i pewny, kto faktycznie powinien pełnić rolę administratora danych osobowych. Wśród przykładów form prawnych administratorów danych wymienić można spółki kapitałowe, spółdzielnie, stowarzyszenia, fundacje, organy państwowe i samorządu terytorialnego, spółki osobowe prawa handlowego, osoby fizyczne lub prawne[504]. Ponadto, można powiedzieć, że w oparciu o inne ustalenia będą identyfikowani administratorzy danych w przypadku podmiotów sektora publicznego i prywatnego.

W przypadku podmiotów sektora prywatnego, bezspornie przyjmuje się, że to przedsiębiorca jest administratorem danych osobowych wykorzystywanych w związku z prowadzącą przez siebie działalnością gospodarczą[505]. Zaznacza się przy tym, że wykonywanie czynności administratora danych będzie przypisane konkretnej osobie lub grupie osób, w zależności od formy prawnej w jakiej działa przedsiębiorca, jak również

[502] Pojęcie to niewiele różni się od definicji administratora danych obowiązującej na gruncie art. 7 ust. 4 UODO z 1997 r., w rozumieniu którego administratorem był organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych.
[503] M. Sakowska-Baryła, *Prawo…, op. cit*., s. 135.
[504] M. Krzysztofek, *Ochrona…, op. cit*., s. 204.
[505] P. Kowalik, D. Wociór, [w:] D. Wociór (red.) *Ochrona...*, op. cit., Legalis.

obowiązującym regulacjom wewnętrznym. Oznacza to konieczność indywidualnego podejścia w każdym rozpatrywanym przypadku.

W odniesieniu do podmiotów sektora publicznego, podstawowe znaczenie dla zidentyfikowania administratora mają źródła prawa, jak i opracowania naukowe, decyzje GIODO i orzeczenia sądów. Często decydującym w omawianym zakresie jest kryterium formalne - niejednokrotnie bywa, że administratora danych wskazują literalnie przepisy prawa. Jest to najprostszy i najszybszy i budzący najmniej wątpliwości sposób na ustalenie tożsamości administratora danych. Jako przykłady bezpośredniego wskazania administratora danych w treści przepisu prawa wskazać można: art. 13 § 5 ustawy z dnia 28 stycznia 2016 r. Prawo o prokuraturze[506], zgodnie z którym Prokuratura Krajowa jest administratorem danych przetwarzanych w ogólnokrajowych systemach teleinformatycznych powszechnych jednostek organizacyjnych prokuratury; w treści art. 11 ust. 1 ustawy z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego[507] ustanowiono, że Minister właściwy do spraw administracji publicznej jest administratorem danych w rozumieniu UODO z 1997 r. przetwarzanych w systemie; ponadto w art. 39 ustawy z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym[508] wskazano, że ewidencję prowadzi, w systemie teleinformatycznym, minister właściwy do spraw transportu, który jest administratorem danych zgromadzonych w ewidencji, natomiast w art. 21 ust. 2 ustawy z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny[509] przewidziano, że administratorami danych osobowych przetwarzanych w zakresie niezbędnym do realizacji zadań wynikających z niniejszej ustawy są wójt oraz minister właściwy do spraw rodziny.

Takich sytuacji, kiedy administratora danych osobowych literalnie wskazuje przepis, nie jest jednak wiele, a dodatkowo zauważyć należy, że przepisy prawa są pomocne raczej tylko w kontekście podmiotów sektora publicznego. Mając na uwadze wielość relacji prawnych wymagających przetwarzania danych osobowych, można stwierdzić, że przepisy prawa w niewystarczającym stopniu wskazują administratorów danych. Wskazywanie administratorów przez ustawodawcę stanowiłoby ułatwienie, przede wszystkim z perspektywy osób, których dane są przetwarzane, ale również innych podmiotów procesu przetwarzania, np. przedsiębiorstw oferujących usługi wymagające współpracy z administratorem danych. Istnieje zatem potrzeba, by *de lege ferenda*

[506] T.j. Dz.U. z 2017 r. poz. 1767.
[507] T.j. Dz.U. z 2018 r. poz. 867.
[508] T.j Dz.U. z 2017 r. poz. 2136.
[509] T.j. Dz.U. z 2017 r. poz. 1832.

ustawodawca określił, kto pełni funkcję administratora danych osobowych np. na uczelni wyższej, w przedszkolu, szpitalu, urzędzie, straży miejskiej, spółce skarbu państwa, itp.

W nauce prawa wyrażono stanowisko, że forma prawna administratora danych nie ma znaczenia, byleby umożliwiała nabywanie praw i zaciąganie zobowiązań, czyli ustalanie celów i sposobów przetwarzania danych, które może następować w ramach działalności gospodarczej, zawodowej lub statutowej[510]. Administratorem danych może być po pierwsze, zarówno podmiot o strukturze jednoosobowej (komornik, minister), jak i wieloosobowej (wspólnota). Po drugie, może to być i organ władzy publicznej (wójt) i jednostka wymiaru sprawiedliwości (Sąd Najwyższy) i funkcjonariusz publiczny (komornik). Nie ma zatem żadnej zasady przyznawania statusu administratora danych w przepisach prawa. Nie w pełni zrozumiałe jest też to, dlaczego status administratora nadawany jest spółdzielni a nie na zarządowi spółdzielni, czy też wspólnocie a nie zarządowi wspólnoty, jako strukturom decyzyjnym i reprezentacyjnym[511]. Wszystko to jest oczywiście spójne z szerokim kręgiem podmiotów ujętych w definicji legalnej administratora danych, ale jednocześnie powoduje problemy z rozstrzygnięciem, kogo *de facto* uznać za administratora, na kim ciążą obowiązki prawne i kto ponosi odpowiedzialność za ich nieprzestrzeganie.

Najczęściej jednak nie ma w przepisach prawa wskazania, kto jest administratorem danych. Pozostając w obszarze podmiotów sektora publicznego (a przede wszystkim sfery administracji publicznej), wątpliwości na gruncie praktyki nieustannie budzi, czy administratorem danych będzie organ administracji czy może jednostka organizacyjna. W takich przypadkach pomocnym, ale nadal często nie dającym jednoznacznej odpowiedzi działaniem jest każdorazowa analiza konkretnych przepisów prawa, określających rodzaj i charakter nadawanych kompetencji z obszaru spraw publicznych oraz ustawowo wyznaczone zadania[512]. Argumentem potwierdzającym zasadność tego działania jest to, że faktycznie w treści przepisów prawa jest wyznaczony cel przetwarzania danych (mniej lub bardziej ogólnie), natomiast podmiot decydujący (czyli administrator) dokonuje tylko konkretyzacji jego zakresu tak, aby był on zgodny

[510] M. Krzysztofek, *Ochrona…, op. cit*., s. 204.
[511] GIODO argumentuje to następująco: „Spółdzielnia mieszkaniowa jest administratorem danych osobowych jej członków, zaś zarząd spółdzielni na czele z jego prezesem jest organem umocowanym jedynie do kierowania działalnością spółdzielni. W związku z powyższym to na spółdzielni, a nie na jej organach spoczywają określone obowiązki wynikające z przepisów ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.), przede wszystkim obowiązek legalnego przetwarzania danych". Decyzja GIODO z dnia 9 stycznia 2013 roku, DOLiS/DEC-18/13/1245, Legalis nr 813845.
[512] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit.*, s. 333.

z potrzebami szczegółowo określonego zadania publicznego realizowanego przez ten podmiot[513]. Analiza zakresu kompetencji może zatem umożliwić wskazanie administratora danych poprzez ocenę, kto decyduje o konkretyzacji celów i sposobów przetwarzania. Zauważyć przy tym warto, że w konsekwencji tego związania przepisem prawa, swoboda podmiotów sektora publicznego w zakresie decydowania o celach i sposobach przetwarzania danych jest zazwyczaj niewielka[514]. A to jest czynnik różniący administratorów danych sektora publicznego (np. Zakład Ubezpieczeń Społecznych) od administratorów danych sektora prywatnego (np. przedsiębiorcy świadczący usługi deweloperskie), którzy mogą być związani np. przepisami branżowymi, jednakże dysponują szerszym zakresem decyzyjności.

W przypadku zarówno podmiotów publicznych, jak i prywatnych, gdy przepisy prawa nie określają, kto jest administratorem danych, a ma to najczęściej miejsce w przypadku podmiotów sektora prywatnego, należy zidentyfikować administratora w oparciu o inne możliwości. Jako pierwsze intuicyjnie przychodzi na myśl umowne określenie kto jest administratorem danych osobowych (a jednocześnie wskazanie kto jest przetwarzającym) w treści umowy. W przypadku umownego podziału ról należy jednak zachować ostrożność i zdrowy rozsądek, ponieważ treść umowy okazuje się nie być ostatecznym i miarodajnym środkiem rozstrzygającym o statusie administratora danych. Wniosek ten wypływa z analizy decyzji GIODO, gdzie stwierdzono, że to, że w umowie pomiędzy podmiotami wskazano jeden z podmiotów jako administratora danych, a drugiego jako podmiot, któremu powierzono przetwarzanie danych, nie przesądza o tym, kto rzeczywiście jest administratorem tych danych. Jeżeli zarówno z innych postanowień umowy jak i samego procesu przetwarzania danych wynika, iż podmiot wskazany w umowie jako ten, któremu powierzono przetwarzanie danych, w rzeczywistości decyduje o celach i sposobach, należy uznać iż administratorem danych jest właśnie ten podmiot[515]. W podobnym kierunku interpretować można wyrok Naczelnego Sądu Administracyjnego, gdzie ustalono, że status administratora danych nie wynika z samego faktu posiadania danych, ale ze sprawowania faktycznej kontroli nad ich przetwarzaniem, obejmującej dwa elementy - decydowanie o celach i środkach przetwarzania danych[516].

[513] *Ibidem*, s. 334.
[514] P. Litwiński, *Administrator danych osobowych w sektorze publicznym po zmianach w ustawie o ochronie danych osobowych wprowadzonych ustawą „500+" [w:] Informacja w Administracji Publicznej* 2016, Nr 2, str. 40.
[515] Decyzja GIODO z dnia 15 lipca 2015 roku, DIS/DEC 594/15/62961, Legalis nr 1336609.
[516] Wyrok NSA z dnia 18 sierpnia 2016 roku, I OSK 864/16, dostępny na stronie internetowej http://orzeczenia.nsa.gov.pl/doc/CA1E71D70A.

Można w związku z tym odnieść wrażenie, że poza niewymagającymi dalszych interpretacji przypadkami, kiedy status administratora danych bezpośrednio wynika z przepisów prawa, innym sposobem na zidentyfikowanie administratora danych jest ustalenie, kto faktycznie ustala cele i sposoby przetwarzania danych. Chodzi tu zatem o kryterium faktyczne, a nie formalne. Podkreślenia wymaga, że rzeczywiste administrowanie danymi osobowymi oznaczałoby zarazem brak możliwości przeniesienia statusu administratora na inny podmiot, upoważnienia innego podmiotu do działania jako administrator danych, zlecenia innemu podmiotowi pełnienia zadań administratora danych. Jednakże z drugiej strony pamiętać należy, że aby być administratorem danych, nie istnieje konieczność osobistego wykonywania czynności przetwarzania ani fizyczne dysponowanie danymi[517]. Stanowisko co do ustalania administratora danych w oparciu o okoliczności faktyczne znajduje uzasadnienie w treści wyroku Wojewódzkiego Sądu Administracyjnego w Warszawie, który wyraził pogląd, że okolicznością przesądzającą o tym, czy określonemu podmiotowi można przypisać miano administratora danych osobowych, nie jest status prawny danego podmiotu, lecz ustalenie, czy to on decyduje o celach i środkach przetwarzania tych danych[518].

Kryterium faktycznego ustalania celów i sposobów przetwarzania danych jest niezwykle istotne z punktu widzenia podmiotów sektora prywatnego. W literaturze przedmiotu wskazuje się przykłady administratorów w tym obszarze, takie jak bank, fundusz emerytalny, spółka (ale też wspólnicy spółki cywilnej), podmiot świadczący usługi ubezpieczeniowe. Ponadto, co stanowi bardzo ważną uwagę, administratorem danych osobowych jest podmiot jako całość, a nie osoba pełniąca funkcję kierowniczą (jak np. prezes, dyrektor, zarząd)[519]. W praktyce życia codziennego takie podejście może zastanawiać w aspekcie faktycznego wykonywania obowiązków administratora danych. Dla przykładu, jeśli administratorem danych jest podmiot świadczący usługi ubezpieczeniowe, rodzi się pytanie, kto powinien podpisywać upoważnienia do przetwarzania danych osobowych nadawane przez administratora danych[520]. Podobnie, kto powinien zawierać umowy powierzenia przetwarzania danych osobowych. Można przyjąć, że nawet jeśli jako administratora danych osobowych będziemy traktować całość organizacji (np. spółkę), to *de facto* i tak obowiązki administratora danych będzie

[517] M. Sakowska-Baryła*, Prawo…, op. cit*., s. 140.
[518] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 23 marca 2006 roku, II SA/Wa 2047/05, Legalis nr 280899.
[519] J. Barta, P. Fajgielski, R. Markiewicz*, Ochrona…, op. cit.*, s. 334.
[520] Zgodnie z treścią art. 37 UODO: *Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych*.

wykonywać osoba (lub osoby) pełniąca funkcje kierownicze lub posiadająca prawo do reprezentacji. Aktualnie obowiązujące prawo, jak również przepisy obowiązujące dotychczas, nie przewidują takiego rozwiązania, by możliwe było scedowanie zadań administratora danych osobowych określonej osobie. Dla przykładu nie ma możliwości zatrudnienia pracownika do pełnienia funkcji administratora danych osobowych w przedsiębiorstwie. Z praktycznego punktu widzenia można zaproponować rozwiązanie, by administrator danych (np. spółka z o.o.) był reprezentowany przez określoną osobę, np. poprzez ustalenie, że obowiązki administratora pełni dyrektor, prezes, członek zarządu.

Jeśli chodzi o osobę fizyczną nieprowadzącą działalności gospodarczej, jako administratora danych osobowych, wydaje się, że takie przypadki nie zdarzają się zbyt często, choć prawo dopuszcza taką możliwość. Zgodnie z treścią art. 2 ust. 2 lit. c RODO, nie ma ono zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. Posiadanie przez osobę fizyczną statusu administratora danych oznaczałoby w praktyce przypadki indywidualnego i niezinstytucjonalizowanego przetwarzania danych[521], co byłoby raczej sytuacją niecodzienną z uwagi na to, że przetwarzanie danych musi odbywać się zgodnie z zasadami przewidzianymi prawem, np. w oparciu o określony cel. W literaturze przedmiotu jako przykład sytuacji, gdy osoba fizyczna postrzegana jest jako administrator danych przedstawia się naukowca, który w pracy badawczej przeprowadza ankiety - zbiera dane osobowe, przechowuje je, opracowuje[522]. Należy przyznać, że są to jednak działania o charakterze sporadycznym, z uwagi na fakt, że prace naukowe zazwyczaj opierają się raczej na danych statystycznych niż na danych osobowych.

Pomocniczo traktować można dorobek Grupy Roboczej art. 29[523], która w treści Opinii 1/2010 wśród możliwych sposobów ustalenia administratora danych wspomina również o kryterium tzw. dorozumianej kompetencji[524]. Polega ono na odwołaniu się – w przypadku, gdy ustalenie administratora danych osobowych nie jest możliwe na podstawie wyraźnego sformułowania w przepisie prawa, czy też nie da się wyinterpretować z treści przepisów kompetencyjnych - do utrwalonych praktyk w różnych

[521] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit.*, s. 334.
[522] G. Sibiga, *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003, s. 54.
[523] Grupę Roboczą zastąpiła Europejska Rada Ochrony Danych, zgodnie z treścią art. 94 ust. 2 RODO odesłania do Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowionej w art. 29 dyrektywy 95/46/WE, należy traktować jako odesłania do Europejskiej Rady Ochrony Danych, ustanowionej rozporządzeniem.
[524] Opinia 1/2010 s. 12.

dziedzinach i istniejących tradycyjnych ról i związanej z nimi odpowiedzialności[525]. Jako przykład wskazuje się uznanie za administratora pracodawcę w odniesieniu do danych pracowników bądź stowarzyszenia w stosunku do danych jego członków, w konsekwencji naturalnego powiązania zdolności do określania celów i środków przetwarzania danych z funkcjonalną rolą podmiotu. Kryterium to jest cenną wskazówką przy identyfikacji administratora danych, jednakże zaznaczyć trzeba, że jest ono najbardziej ryzykowne i ma największe prawdopodobieństwo błędu. Opiera się raczej na kwestiach interpretacyjnych i ocennych, niż na elementach znajdujących gruntowne uzasadnienie, co trudniej podważyć. Z tego względu powinno być raczej stosowane jako rozwiązanie pomocnicze, na zasadzie ostateczności w przypadkach, gdy inne z powyższych kryteriów nie doprowadziły do ustalenia kto jest administratorem danych osobowych.

W odniesieniu do ustalania celu i sposobów przetwarzania przedstawiciele nauki prawa proponują cenne, ale niejednoznaczne wskazówki. Pomocnym przy identyfikacji administratora danych może być ustalenie trzech następujących elementów. Po pierwsze, cel musi być całkowicie związany z administratorem, po drugie, administrator podejmuje decyzje o realizacji celu przetwarzania w sposób samodzielny, a ponadto, administrator podejmuje decyzje w sposób faktyczny[526]. Pierwszy element dotyczy stosunku prawnego istniejącego pomiędzy administratorem danych a podmiotem danych (osobą fizyczną, której dane dotyczą, np. umowa o pracę). W drugim chodzi o samodzielne podejmowanie decyzji we własnym imieniu. Ostatni element polega na rzeczywistym a nie pozornym podejmowaniu decyzji. Warto dodać, że jeśli chodzi o samodzielność decyzji, w nauce prawa twierdzi się, że administrator nie zawsze będzie w pełni decyzyjny w stosunku do każdego aspektu przetwarzania danych, ale ma podejmować decyzje o zasadniczym znaczeniu dla przetwarzania[527]. Inny pogląd sugeruje, że decydowanie o środkach i celach należy rozumieć jako faktyczne podejmowanie decyzji we własnym imieniu i na własną rzecz, o tym, w jakim celu i w jaki sposób przetwarzane będą dane osobowe[528]. W sposób najpełniejszy i najbardziej klarowny zagadnienie sposobów i celów przetwarzania przedstawiono w Opinii 1/2010. Grupa Robocza stoi na stanowisku, że określanie celów i sposobów sprowadza się do określenia odpowiednio dlaczego i jak prowadzi się pewne czynności przetwarzania danych[529]. Jeśli chodzi o sposoby, Grupa Robocza ustaliła, że nie

[525] *Ibidem*.
[526] A. Krasuski, *Dane…, op. cit*., s. 120.
[527] K. Witkowska-Nowakowska [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…, op. cit*., s. 217.
[528] M. Sakowska-Baryła, *Prawo…, op. cit.,* s. 143.
[529] Opinia 1/2010 s. 14.

odnoszą się tylko do technicznych sposobów przetwarzania danych osobowych, ale także do tego jak odbywa się przetwarzanie, co obejmuje zagadnienia: które dane się przetwarza, jakie osoby trzecie mają dostęp do tych danych, kiedy usuwa się dane itp.[530]. Określeniem sposobów objęto kwestie techniczne i organizacyjne, np. sprzętu komputerowego i oprogramowania, długości procesu przetwarzania danych. Innymi słowy, sposoby powinny reprezentować uzasadnioną drogę osiągania celu[531].

Należy podkreślić, że określenie, kto w całym procesie przetwarzania danych jest administratorem ma znaczenie przede wszystkim dla osoby, której dane dotyczą. Chodzi tu przede wszystkim o realizację obowiązku informacyjnego wynikającego z treści art. 12-14 RODO. Przepisy prawa gwarantują, że osoba, której dane dotyczą ma wiedzieć, kto jest administratorem jej danych oraz gdzie mieści się jego siedziba. Tożsamość administratora ma kluczowe znaczenie w odniesieniu do realizacji praw osób, których dane dotyczą, jak np. prawo dostępu do danych, cofnięcia zgody na przetwarzanie danych czy prostowania swoich danych. Po trzecie, tożsamość administratora danych jest szczególnie istotna w kontekście odpowiedzialności za niewłaściwe przetwarzanie danych osobowych (np. pozbawione podstawy prawnej bądź sprzeczne z zasadami przetwarzania). To administratorowi przypisywana jest odpowiedzialność administracyjna, cywilna i karna (jeśli objęty jest zakresem odpowiedzialności karnej).

Nowy podmiot procesu przetwarzania danych wprowadzony przez prawodawcę w treści art. 26 RODO to współadministrator danych[532]. Z literalnego brzmienia przepisu wynika, że współadministrowanie danymi osobowymi zachodzi wtedy, gdy cele i sposoby przetwarzania danych są ustalane nie przez jednego administratora (co przyjmowane jest jako zasada), a przez co najmniej dwa podmioty.

Z pluralizmem po stronie administratora danych mieliśmy do czynienia już na gruncie Dyrektywy 95/46/WE, gdzie w definicji administratora danych występowała możliwość, by samodzielnie lub wspólnie z innymi podmiotami określał cele i sposoby przetwarzania danych. Brakowało jej natomiast w definicji administratora danych osobowych wynikającej z polskiej ustawy, gdzie ustawodawca posługiwał się liczbą pojedynczą. Słusznie zaznacza się w nauce prawa, że UODO z 1997 r. dopuszczała inną konfigurację wielości administratorów niż RODO. Zgodnie z interpretacją regulacji UODO z 1997 r. więcej niż jeden podmiot może pełnić rolę administratora w odniesieniu

[530] *Ibidem*, s. 15.
[531] *Ibidem*, s. 16.
[532] Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami.

do tych samych danych osobowych, jednakże każdy z nich przetwarza dane osobowe we własnych celach i podejmuje samodzielnie decyzje co do celów i środków przetwarzania[533].

Współadministrowanie danymi osobowymi odnosi się do możliwości, kiedy w pojedynczej operacji przetwarzania danych kilka stron może wspólnie określić cel i sposoby przewidywanego przetwarzania danych. Pociąga to za sobą nałożenie na każdego współadministratora zobowiązań wynikających z ochrony osób fizycznych, których dane są przetwarzane[534]. Pojawia się tu kwestia jak ukształtuje się stosunek prawny w sytuacji, gdy jeden ze współadministratorów podejmie decyzję w przedmiocie zlecenia przetwarzania danych w swoim imieniu innemu podmiotowi. Wątpliwość budzi to, czy stroną umowy powierzenia przetwarzania danych osobowych może być jeden ze współadministratorów, czy wymagane byłoby porozumienie co do tego działania wszystkich współadministratorów.

Prawodawca nie określił konkretnych wymagań dotyczących wewnętrznej relacji pomiędzy współadministratorami, poza ustanowieniem wymogu, by wypracowane zostały wspólne uzgodnienia współadministratorów. Na tej podstawie wywnioskować można, że podmioty te zobowiązane są do poczynienia uzgodnień, ale prawodawca pozostawił im elastyczność co do ustalenia i podziału obowiązków i odpowiedzialności, w treści art. 26 RODO stanowiąc, że wspólne uzgodnienia mają obejmować uzgodnienia co do zakresów obowiązków wynikających z RODO, relacji pomiędzy współadministratorami a osobami, których dane dotyczą, jak również zakresów odpowiedzialności dotyczącej wypełniania obowiązków. Regulacja nie zawiera wskazań co do formy uzgodnień. Niemniej jednak, można wyinterpretować z treści przepisu, z którego wynika, że zasadnicza treść uzgodnień jest udostępniana podmiotom, których dane dotyczą (art. 26 ust. 2 RODO), iż musi być to forma umożliwiająca zapoznanie się z uzgodnieniami przez podmioty danych (zatem nie może to być forma ustna). Na bazie motywu 79 preambuły RODO podjęto próbę określenia kryteriów odpowiedzialności współadministratorów dotyczących wypełniania obowiązków wynikających z RODO. Chodzi tu o przejrzysty i transparentny podział zadań i obowiązków, zagwarantowanie rozliczalności przez każdego ze współadministratorów, precyzja ustaleń, zgodność ustaleń ze stanem faktycznym i rzeczywistymi ramami współpracy[535]. Regulacja stanowiąca

[533] P. Litwiński, *Rozporządzenie..., op. cit*., Legalis.
[534] Opinia 1/2010, s. 19.
[535] K. Witkowska-Nowakowska [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO..., op. cit*., s. 614.

przedmiot rozważań pozwala uznać, że współadministratorzy mają samodzielność w kreowaniu relacji współadministrowania. Każdy z nich ma przy tym swój rozgraniczony zakres obowiązków i odpowiedzialności za nie, który musi być kompatybilny z zakresem innego współadministratora, co zostaje zagwarantowane w drodze wspólnych uzgodnień. Jednocześnie zakres ten musi odpowiadać wspólnym ustaleniom co do celów i sposobów przetwarzania danych. W Opinii 1/2010 wskazuje się zasadnie, że udział stron we wspólnym określaniu celów i sposobów może jednak przyjąć różne formy i nie musi być równo rozłożony[536], co związane jest z dużą różnorodnością i złożonością aktualnych realiów w zakresie przetwarzania danych osobowych.

Mając na uwadze powyższe uwagi, można zająć stanowisko, że dopuszczalne jest rozwiązanie polegające na tym, że umowę powierzenia przetwarzania danych osobowych z przetwarzającym może zawrzeć jeden ze współadministratorów, bądź kilku z nich albo też wszyscy, czyli nie ma konieczności, by stroną tej umowy byli wszyscy współadministratorzy. Z uwagi na sformułowanie w treści przepisu, że co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, można interpretować, iż co do zasady wspólnie powinni oni podejmować decyzje o zleceniu przetwarzania danych innemu podmiotowi i wspólnie zawierać umowy powierzenia. Jednakże, biorąc pod uwagę elastyczność co do zakresu uzgodnień oraz jasne, precyzyjne i transparentne rozgraniczenie zakresów obowiązków i odpowiedzialności, wydaje się, że nic nie stoi na przeszkodzie, by jeden ze współadministratorów mógł stać się stroną umowy powierzenia przetwarzania danych. Jednak powinien być przy tym respektowany zakres uprawnień przyznany współadministratorowi względem celów i sposobów przetwarzania danych osobowych[537]. Podkreślenia wymaga w takim przypadku to, by zawarcie tej umowy nie było sprzeczne z wspólnymi uzgodnieniami współadministratorów. Mogą oni z drugiej strony, wspólnie podjąć decyzję o wyłączeniu możliwości powierzenia przetwarzania danych osobowych[538]. Jeśli okaże się, że powierzenie danych do przetwarzania innemu podmiotowi sprzeniewierza wspólne uzgodnienia, należy je uznać za niedopuszczalne, ponieważ mogłoby to wtedy oznaczać pozbawienie współadministratorów pluralistycznej kontroli nad przetwarzaniem danych.

[536] Opinia 1/2010, s. 21.
[537] J. Byrski, *Umowne ..., op. cit.*, Legalis.
[538] *Ibidem*.

Przykładem obrazującym relację polegającą na współadministrowaniu danymi osobowymi jest sytuacja przedstawiona przez Komisję Europejską[539]. Dotyczy ona przedsiębiorstwa świadczącego usługę opieki nad dziećmi obsługiwaną poprzez platformę online. Jednocześnie przedsiębiorstwo to ma umowę zawartą z innym podmiotem zajmującym się dodatkowymi usługami, np. umożliwianiem rodzicom wypożyczenia gier lub filmów DVD, które opiekunka otrzymująca zlecenie za pośrednictwem platformy dostarcza dziecku. Oba przedsiębiorstwa zdecydowały się na używanie tej samej platformy, w konsekwencji czego niejednokrotnie mają dostęp do danych osobowych tych samych klientów. Jak wskazuje Komisja, przedsiębiorstwa te są współadministratorami danych nie tylko dlatego, że uzgodniły oferowanie usługi łączonej, ale również dlatego, że zaprojektowały i wdrożyły wspólną platformę.

Inny przykład przedstawiono w Opinii 1/2010, gdzie podmiot świadczący usługi rekrutacji X współpracował z przedsiębiorcą poszukującym pracowników Y[540]. Podmioty zawarły umowę, zgodnie z którą firma X jako przetwarzający przetwarza dane osobowe kandydatów w imieniu firmy Y będącej administratorem danych. Jednocześnie jednak podmiot X jest administratorem danych osób poszukujących pracy, stanowiących zbiór globalny, a nie tylko danych z CV przekazywanych przez przedsiębiorcę Y. Zdaniem przedstawicieli Grupy art. 29, pomimo umownego przypisania roli przetwarzającego, podmiot X należy uznać za wspólnie administrującą danymi z przedsiębiorcą Y, w zakresie danych z rekrutacji w przedsiębiorstwie Y.

W odniesieniu do powyższych przykładów, trzeba zwrócić uwagę na rozróżnienie kwestii współadministrowania danymi od powierzenia przetwarzania danych. Oba rozwiązania z powodu tego, że dane przetwarzane są przez więcej niż jeden podmiot (administratora), mogą być trudne do odróżnienia na gruncie praktyki[541]. W nauce prawa wskazuje się, że współadministrowanie danymi od powierzenia danych różni kwestia faktycznej kontroli nad ustaleniem celów i sposobów przetwarzania[542]. Można przyjąć, że przy współadministrowaniu zachodzi wspólne określanie celów i wspólne ustalanie sposobów przetwarzania danych, natomiast przy powierzeniu powyższe kwestie decyzyjne pozostają po stronie administratora danych, a przetwarzający *de facto* nie ma na nie wpływu, jest wykonawcą decyzji administratora. Po drugie, współadministratorzy

[539] https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en..
[540] Opinia 1/2010, s. 21.
[541] Na problem ten zwraca uwagę K. Witkowska-Nowakowska w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…, op. cit*., s. 617.
[542] *Ibidem*.

wspólnie sprawują pluralistyczną kontrolę nad przetwarzaniem, natomiast w stosunku powierzenia to administrator sprawuje kontrolę nad przetwarzającym.

Podsumowując, można sformułować wniosek, że współadministrowanie opiera się na równorzędności podmiotów i braku pomiędzy nimi stosunku zobowiązaniowego (nie ma wśród nich podmiotu uprawnionego i podmiotu zobowiązanego), natomiast w przypadku powierzenia wyinterpretować można zależność podmiotów tej relacji mającą cechy podległości, zobowiązanie jednej strony i uprawnienie drugiej strony. Ponadto w aspekcie dokonywania powierzenia przetwarzania danych osobowych innemu podmiotowi, istnieje kilka możliwości. Po pierwsze, wszyscy współadministratorzy nawiązują stosunek powierzenia z przetwarzającym w odniesieniu do całości procesów przetwarzania danych. Po drugie, tylko wybrani współadministratorzy nawiązują stosunek powierzenia z przetwarzającym w odniesieniu do procesów przetwarzania danych dokonywanych przez tych współadministratorów. Trzecia możliwość polega na tym, że jeden współadministrator nawiązuje stosunek powierzenia z przetwarzającym w odniesieniu do całości procesów przetwarzania danych[543]. Decydujące będą w tej kwestii ustalenia poczynione w ramach wzajemnych uzgodnień współadministratorów.

Kolejnym istotnym zagadnieniem dotyczącym statusu prawnego administratora w procesie przetwarzania danych osobowych są jego obowiązki. W przepisach prawa obowiązki administratora danych nie zostały ujęte w uporządkowanym katalogu, wynikają z treści poszczególnych przepisów RODO. W nauce prawa sformułowano katalog obowiązków wynikających z przepisów UODO z 1997 r. w następujących kształcie: 1) zabezpieczenia przetwarzanych danych osobowych, 2) prowadzenia dokumentacji przetwarzania danych i powołania administratora bezpieczeństwa informacji, 3) dołożenia szczególnej staranności w celu ochrony interesów osób, których dane przetwarza, 4) zapewnienia prawidłowego przetwarzania danych w przypadku powierzenia ich przetwarzania podmiotowi zewnętrznemu, 5) spełnienia wynikających z UODO z 1997r. obowiązków informacyjnych[544]. Można powiedzieć, że katalog ten jest szczegółowy i pod pewnymi względami wymaga modyfikacji. Dla przykładu aktualnie nie ma literalnie sformułowanego w przepisach RODO obowiązku prowadzenia dokumentacji przetwarzania danych osobowych, natomiast w poprzednim stanie prawnym nie było obowiązku powołania administratora bezpieczeństwa informacji. Dlatego warto podjąć

[543] M. Kwiatkowska-Cylke [w:] D. Lubasz (red.), RODO w e-commerce, Warszawa 2018, s. 231-232.
[544] K. Kędzierska, [w:] A. Brzezińska, S. Gajewski, A. Gawrońska-Baran, B. Jakacka, K. Kędzierska, Ł. Kudelski, W. Mende, P. Mrozek, E. Pawka-Nowak, B. Pietrzak, M. Rączka, M. Sroczyński, A. Wicik, M. Zając, *Vademecum dyrektora jednostki pomocy społecznej*, Warszawa 2017, Legalis.

próbę nowego usystematyzowania obowiązków administratora i zaproponować ich podział na trzy grupy.

W pierwszej grupie można umieścić obowiązki związane z legalnością przetwarzania danych osobowych, które prawodawca wskazuje w treści art. 5-7, 9 i 44-50 RODO. Znajduje się tu obowiązek realizacji zasad przetwarzania oraz wykazywanie przestrzegania przepisów; obowiązek przetwarzania danych osobowych jedynie w oparciu o przynajmniej jedną z wymienionych podstaw prawnych; obowiązek wykazywania, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Ponadto jest to też obowiązek powstrzymywania się od przetwarzania danych szczególnej kategorii, chyba że zachodzi jedna z przesłanek oraz obowiązek przestrzegania zasad przy przekazywaniu danych do państw trzecich.

Do drugiej grupy mogą zostać zaliczone obowiązki związane z prawami osób, których dane dotyczą. Chodzi to o spełnienie obowiązku informacyjnego wobec osoby, której dane dotyczą (art. 12-14 RODO), obowiązek realizacji praw osób, których dane dotyczą art. (15-22 RODO) oraz obowiązek zawiadamiania podmiotu danych o naruszeniu ochrony danych osobowych (art. 34 RODO).

W trzeciej najliczniejszej grupie znajdują się obowiązki administratora związane z zabezpieczaniem danych. Wyróżnić tu można obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i wykazywanie tego (art. 24 RODO); obowiązek uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25 RODO); obowiązek wyznaczenia przedstawiciela w Unii (art. 27 RODO). Ponadto jest tu obowiązek korzystania wyłącznie z usług podmiotów dających gwarancje spełniania wymogów RODO, jeśli dane są powierzane do przetwarzania innemu podmiotowi (art. 28 RODO); obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych (art. 30 RODO); obowiązek współpracy z organem nadzorczym (art. 31 RODO). Jako kolejne obowiązki pojawiają się również wdrożenie odpowiednich środków technicznych i organizacyjnych (art. 32 RODO); obowiązek zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu i dokumentowanie naruszeń (art. 33 RODO); obowiązek dokonywania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych (art. 35 RODO) oraz obowiązek wyznaczenia inspektora ochrony danych obowiązkowo w określonych sytuacjach (art. 37 RODO).

Można sformułować wniosek, że znaczną część przepisów całego RODO stanowią obowiązki administratora danych. Potwierdza to tezę, że odgrywa on kluczową

rolę w procesie przetwarzania danych. Ponadto, administrator po reformie w ochronie danych osobowych związanej z rozpoczęciem stosowania RODO, ma więcej obowiązków niż dotychczas. Po pierwsze, są to zupełnie nowe działania, co do których zobowiązuje go prawodawca. Jako przykład wskazać można prowadzenie rejestru czynności przetwarzania danych osobowych czy też dokonywanie oceny skutków operacji przetwarzania dla ochrony danych osobowych. Po drugie, część obowiązków istniejących na gruncie UODO z 1997 r. zostaje znacznie rozszerzona i zintensyfikowana, np. szerszy zakres informacji, jaki ma być przekazywany osobie w ramach realizacji obowiązku informacyjnego czy też poprzedzające powierzenie przetwarzania danych zbadanie, czy podmiot daje gwarancje spełniania wymogów RODO. Po trzecie, zmienia się ciężar przeprowadzenia dowodu działania zgodnie z przepisami RODO. Ponadto istotne *novum* stanowi to, że zakres obowiązków aktualnie dywersyfikuje struktura administratora danych (wielkość zatrudnienia). Można ocenić, że najistotniejszą zmianą jest to, że administrator danych musi wykazywać, że spełnia nałożone na niego obowiązki. W dotychczasowym stanie prawnym sytuacja była odwrotna – to po stronie GIODO leżało działanie zmierzające do wykazania, że administrator danych naruszał przepisy o ochronie danych osobowych[545]. Natomiast od 25 maja 2018 roku, zgodnie z interpretacją zasady rozliczalności ujętej w treści art. 5 ust. 2 RODO, prawodawca przerzuca ciężar z organu na administratora, który będzie musiał wykazywać, że jego działania w zakresie przetwarzania danych osobowych są zgodne z przepisami RODO. Należy to rozumieć jako „obowiązek aktywnego działania, wykazywania inicjatywy, bez oczekiwania na skargi i wnioski klientów lub zarzuty i rekomendacje organów nadzorczych”[546]. Wydaje się, że o ile przestrzeganie tej zasady przez administratorów będzie efektywnie weryfikowane przez organ nadzorczy, przepis ten ma ogromną szansę skutecznie wpłynąć na podwyższenie standardów ochrony danych osobowych.

Ogólnie przyjmuje się, że administrator danych to podmiot, charakteryzujący się zdolnością do przekazania uprawnienia do przetwarzania danych osobowych innemu podmiotowi, ustalający cele i sposoby przetwarzania danych. Główną cechą charakteryzującą administratora i odróżniającą go od podmiotu przetwarzającego jest decyzyjność, ponieważ podmiot przetwarzający to podmiot, który przetwarza dane

[545] Potwierdzała to treść art. 18 UODO z 1997r. , zgodnie z którym w przypadku naruszenia przepisów o ochronie danych osobowych Generalny Inspektor z urzędu lub na wniosek osoby zainteresowanej, w drodze decyzji administracyjnej, nakazuje przywrócenie stanu zgodnego z prawem.
[546] M. Krzysztofek, *Ochrona…, op. cit.,* Legalis.

w imieniu i na rzecz administratora danych, co do zasady nie podejmując w tym zakresie samodzielnych decyzji.

Odwołując się do źródeł obcojęzycznych, można przytoczyć wnioski wypracowane przez brytyjskiego odpowiednika GIODO, który proponuje dokonywanie rozróżnienia pomiędzy administratorem danych a przetwarzającym, w oparciu o to, na jakie kwestie oba podmioty mają decydujący wpływ. Brytyjski organ ds. danych osobowych przypisuje administratorowi determinowanie takich kwestii jak to, czy należy zbierać dane osobowe a jeśli tak to na jakiej podstawie; dane jakiej treści mają być zbierane; cel lub cele, dla jakich dane mają być przewarzane. Co więcej, administrator decyduje w kwestii tego o jakich podmiotach dane mają być zbierane; czy dane mogą być ujawnione a jeśli tak, to komu. Kolejnym zagadnieniem, które określa administrator jest to, czy będzie znajdowało zastosowanie prawo dostępu podmiotu do danych i inne prawa podmiotu danych oraz ewentualne wyjątki w tym zakresie, jak również to, jak długo mają być przechowywane dane oraz czy/jak mają być poprawiane i aktualizowane[547].

Podmiot przetwarzający ma wpływ na to, jakie systemy informatyczne lub inne metody gromadzenia danych osobowych znajdą zastosowanie, czy też jak przechowywać dane osobowe. Po jego stronie leży decyzja co do zabezpieczeń związanych z danymi osobowymi, środków wykorzystywanych do przekazywania danych, metod zapewniających, że przechowywanie danych jest zgodne z założeniami, a także środków wykorzystywanych do usuwania bądź innych form pozbywania się danych[548].

Ogólnie rzecz ujmując, w literaturze przedmiotu sygnalizuje się niejednokrotnie problemy z rozstrzygnięciem, jaki status w stosunku do określonych danych osobowych przysługuje określonemu podmiotowi. Dla przykładu przytoczyć można sprawę, która stanowiła przedmiot rozstrzygnięcia GIODO, a dotyczyła wątpliwości co do statusu kancelarii prawnej w stosunku do przetwarzanych przez nią danych. W konsekwencji wniesionej skargi GIODO ustalił, że kancelaria, działająca w imieniu i na rzecz swojego mocodawcy, jest odbiorcą danych, który przetwarza je, dla wypełnienia prawnie usprawiedliwionych celów oraz że kancelaria nie może w niniejszej sprawie być uznana za administratora danych, gdyż działa wyłącznie w granicach umocowania wyznaczonych

[547] Opracowanie w języku angielskim, *Data controllers and data processors: what the difference is and what the governance implications are*, dostępne na stronie internetowej https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf, s. 6-7.
[548] *Ibidem*, s. 7.

zakresem pełnomocnictwa[549]. Treść tej decyzji poddana została krytyce przedstawiciela nauki prawa, który opowiada się za dwupodziałem kategorii podmiotów uczestniczących w przetwarzaniu danych – administrator danych i przetwarzający[550]. W swojej kontrargumentacji autor ten zarzuca decyzji, że ustalenia GIODO „się wzajemnie wykluczają – skoro kancelaria nie jest administratorem danych, to musi być podmiotem przetwarzającym, bo nie istnieje trzecia możliwość; skoro kancelaria jest odbiorcą danych, to nie może być podmiotem przetwarzającym"[551]. Wyważając powyższe argumenty można powiedzieć, że w stanie faktycznym stanowiącym przedmiot powołanej decyzji, kancelaria będzie administratorem danych w stosunku do danych skarżącej (bo pozyskała dane od skarżącej w celu prowadzenia sprawy, co do której jest pełnomocnikiem i ustala cele i sposoby przetwarzania). Kancelarii nie można uznać za podmiot przetwarzający - nie zawarła umowy powierzenia, a skarżąca jest podmiotem danych, a nie administratorem swoich danych więc nie może powierzyć informacji o sobie w drodze umowy. Wydaje się zatem, że GIODO nie do końca prawidłowo przyznał kancelarii status odbiorcy danych (definicja w art. 4 pkt 9 RODO).

Przy rozważaniu statusu kancelarii prawnej należy najpierw wziąć pod uwagę, w stosunku do jakich danych ma być określona jej pozycja w procesie przetwarzania danych osobowych. Jeśli chodzi o dane osobowe, które pozostawiają kancelarii jej bezpośredni klienci, jak również dane pracowników kancelarii i jej współpracowników - kancelaria wydaje się zajmować pozycję administratora tych danych. W sytuacji, gdy kancelaria prawna prowadzi stałą obsługę np. przedsiębiorstwa czy instytucji na podstawie umowy, będziemy tu mieli do czynienia z koniecznością umownego powierzenia przetwarzania danych, zatem kancelaria będzie miała status przetwarzającego. Kluczowe są zatem okoliczności przetwarzania danych przez kancelarię, ustalenie czyje są to dane oraz na jakiej podstawie będą przetwarzane. Co należy dodać, na etapie prac nad nową ustawą o ochronie danych osobowych istniała szansa na uproszczenie tego problemu, poprzez literalne wskazanie w przepisach prawa, kto ma wykonywać obowiązki administratora danych. Według projektu z dnia 12 września 2017 roku ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych[552], administratorami danych mieli

[549] Decyzja GIODO z dnia 2 sierpnia 2005 r., GI-DEC-DS-233/05, dostępna na stronie internetowej https://giodo.gov.pl/pl/307/1505.
[550] P. Litwiński [w:] D. Szostek (red.), *Bezpieczeństwo …, op. cit.,* Legalis.
[551] *Ibidem*.
[552] Tekst projektu dostępny na stronie internetowej https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-przepisy-wprowadzajace-ustawe-o-ochronie-danych-osobowych.html.

być adwokaci i radcowie prawni – w przypadku danych osobowych przetwarzanych w ramach wykonywania zawodu. Ostatecznie zmiany nie weszły w życie.

Nie można również pomijać istotnej kwestii, że przetwarzający też bywa administratorem danych. Dzieje się tak dlatego, że na przetwarzającym, dla przykładu przedsiębiorcy, również ciążą obowiązki administratora w stosunku do danych, co do których podejmuje decyzje o sposobach i celach przetwarzania. Najczęściej będą to dane pracowników podmiotu przetwarzającego, klientów, dostawców itp. Jako przykład wskazać można biuro rachunkowe, które jest przetwarzającym w stosunku do danych osobowych, wobec których administratorem jest klient, powierzonych mu w drodze umowy przez klienta w ramach obsługi księgowej. Natomiast z drugiej strony biuro to jest administratorem danych osobowych własnych pracowników oraz klientów indywidualnych (osób fizycznych). Można z powyższych uwag sformułować wniosek, że niemożliwe jest jednoczesne pełnienie funkcji zarówno administratora, jak i przetwarzającego w stosunku do tego samego zakresu danych. Innymi słowy, w stosunku do określonego zakresu danych można być albo administratorem, albo przetwarzającym (bądź też innym podmiotem procesu przetwarzania danych, który pozostaje poza zakresem prowadzonych rozważań).

Należy przy tym rozważyć, czy zaproponowany w nauce prawa dwupodział podmiotów procesu przetwarzania danych, nie warto by jednak rozszerzyć również o inne podmioty faktycznie funkcjonujące w procesie przetwarzania a nie mieszczące się w żadnej z tych dwu kategorii. Takie podmioty wskazywane są przecież literalnie w treści RODO. Jest to odbiorca oraz strona trzecia. W stosunku do obu wymienionych kategorii podmiotów trzeba stwierdzić, że nie zostały one sprecyzowane na gruncie RODO, ich katalog jest otwarty. Można więc powiedzieć, że w przetwarzaniu danych poza administratorem i przetwarzającym mogą też uczestniczyć odbiorcy – z treści art. 4 pkt 9 RODO wynika, że mogą to być osoby fizyczne, osoby prawne i organy publiczne (jednak nie te organy, które mogą otrzymywać dane w ramach konkretnego postępowania), którym ujawnia się dane osobowe. Innymi słowy są to podmioty, które choćby potencjalnie mają możliwość poznania danych osobowych – chodzi tu o faktyczne przekazanie danych lub umożliwienie dostępu do danych, bez znaczenia w jaki sposób to następuje[553]. Kolejnym uczestnikiem procesu przetwarzania danych osobowych może być strona trzecia, czyli zgodnie z treścią art. 4 pkt 10 RODO osoba fizyczna lub prawna, organ publiczny,

[553] M. Sakowska-Baryła (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018, Legalis.

jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe. Nawet bez analizy przepisów dotyczących statusu odbiorcy i strony trzeciej można zająć stanowisko, że w przetwarzaniu danych osobowych nie uczestniczy tylko administrator i podmiot przetwarzający. W konsekwencji tego trudno zgodzić się ze stwierdzeniem, że jeśli ten, kto przetwarza określone dane nie jest ich administratorem, to jest podmiotem przetwarzającym.

2.3. Przetwarzający

Na wstępie zauważyć należy, że byt podmiotu przetwarzającego i jego obecność w procesie przetwarzania danych osobowych jest w zupełności zależny od administratora. Oznacza to, że podmiot przetwarzający nie zaistnieje, jeśli administrator nie skorzysta z uprawnienia do przetwarzania danych osobowych za pomocą innych podmiotów. Decyzja administratora co do niesamodzielnego przetwarzania danych jest jedynym sposobem powstania relacji powierzenia. Nie ma takiej możliwości, by określony podmiot stał się przetwarzającym z mocy prawa. Nie wydaje się też możliwe, by nakazać podmiotowi pełnienie funkcji przetwarzającego w drodze decyzji administracyjnej.

Druga strona umowy powierzenia przetwarzania danych osobowych jest w porównaniu do administratora danych uregulowana w sposób bardziej powściągliwy. Polski ustawodawca w przepisach UODO z 1997 r. tylko w jednym artykule odnosił się do przetwarzającego i to nie wprost[554], poza tym nie sformułował nawet nazwy tego podmiotu. W konsekwencji braku ustawowego określenia, na gruncie praktyki drugą stronę umowy powierzenia przetwarzania danych nazywa się niejednolicie: jako przetwarzającego, procesora, zleceniobiorcę, wykonawcę, administrującego. Prawodawca unijny uczynił postęp w tym zakresie, ponieważ zamieścił definicję legalną podmiotu przetwarzającego wśród innych definicji pojęć podstawowych na gruncie RODO. Zgodnie z treścią art. 4 pkt 8 RODO podmiot przetwarzający oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. To działanie prawodawcy ma szansę dać efekt w postaci ujednolicenia i uporządkowania terminologicznego treści umów powierzenia.

[554] Art. 31 UODO z 1997 r.: 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. 2. Podmiot, o którym mowa w ust. 1, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

W praktyce podmiotami przetwarzającymi najczęściej bywają: przedsiębiorcy świadczący usługi IT (w tym rozwiązania chmurowe), podmioty świadczące usługi brokerskie, biura rachunkowe, kancelarie prawne, przedsiębiorcy świadczący usługi kurierskie, windykacyjne, archiwizacyjne i niszczenia dokumentów, agenci ubezpieczeniowi, podmioty świadczące usługi reklamowe i marketingowe. W stosunku prawnym powierzenia danych wystąpić mogą również podmioty przekazujące dane klientów w postępowaniu reklamacyjnym bądź też serwisom gwarancyjnym przy realizacji umowy gwarancji jakości[555]. Można powiedzieć, że z usług co najmniej jednego z powyższych podmiotów korzysta *de facto* każdy podmiot obrotu gospodarczego- zarówno przedsiębiorcy, jak i podmioty sektora publicznego.

Zestawiając regulacje dotyczące podmiotu przetwarzającego obowiązujące na gruncie poprzedniego stanu prawnego z aktualną definicją, można zaryzykować stwierdzenie, że pomimo braku sformułowania nazwy podmiotu oraz jego definicji, z treści art. 31 UODO z 1997 r. wyinterpretować można było więcej szczegółów dotyczących przetwarzającego niż z aktualnego brzmienia art. 4 pkt 8 i art. 28 RODO. Niewątpliwie bardziej wyraźne było dotychczas to, że przetwarzający stanowił odrębny byt prawny w stosunku do administratora danych. Sugerowało to wprost literalne sformułowanie „powierzyć innemu podmiotowi". Takie ujęcie przetwarzającego zostało przyjęte i nie zmieniło się to, że powierzenie danych osobowych następuje na zewnątrz, poza strukturę administratora. Z treści art. 28 RODO wynika wprost to, że to administrator kreuje stosunek powierzenia przetwarzania danych, to on decyduje, czy dane przetwarza samodzielnie, czy korzysta z innego podmiotu. Potwierdzono w nauce prawa, że administrator danych może bądź sam przetwarzać dane, bądź powierzyć to innemu podmiotowi[556]. Oznacza to, że status przetwarzającego nie wynika z kryterium formalnego, ani też z kryterium faktycznego, ani z kryterium dorozumianych kompetencji. W nauce prawa stwierdzono, że umowa powierzenia przetwarzania danych osobowych jest elementem wtórnym i nie powinna być traktowana jako kryterium istnienia powierzenia bo nie ona kreuje to powierzenie[557]. Dokonanie powierzenia w sposób czysto faktyczny (bez umowy, nawet ustnej) może powodować trudność z ustaleniem, czy w rzeczywistości doszło do powierzenia, czy do udostępnienia danych lub umożliwienia

[555] J. Sobczak, D. Wociór, [w:] D. Wociór (red.) *Ochrona…, op. cit.,* s. 65.
[556] J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona…, op. cit.*, s. 504.
[557] K. Witkowska-Nowakowska [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…, op. cit*., s. 634.

dostępu do nich osobom nieupoważnionym (art. 107 UODO z 2018 r.[558]). Podsumowując, źródłem stosunku prawnego powierzenia danych, a tym samym statusu przetwarzającego, jest czynność prawna – powierzenie przetwarzania danych w drodze umowy zawartej pomiędzy administratorem a przetwarzającym.

Na ważną kwestię zwrócono uwagę w literaturze przedmiotu, jako konsekwencję i zarazem uzasadnienie, że podmiot przetwarzający ma być podmiotem zewnętrznym w stosunku do struktury organizacyjnej administratora. Innym podmiotem z art. 31 ust. UODO z 1997 r. nie mogła być osoba fizyczna posiadająca upoważnienie nadane przez administratora danych z art. 37 UODO z 1997 r.[559]. Bardzo często pojawia się dylemat, czy dana osoba (np. zleceniobiorca) powinna zostać upoważniona do przetwarzania danych osobowych, czy należy z nią zawrzeć umowę powierzenia przetwarzania danych osobowych. O rozgraniczeniu pomiędzy osobami upoważnionymi do przetwarzania danych a podmiotami przetwarzającymi stanowi treść art. 29 RODO, zgodnie z którym podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora. W przepisie nie ma odpowiedzi na postawione pytanie. Praktyka i doświadczenie w obszarze ochrony danych osobowych przekonuje, że upoważnienia do przetwarzania danych osobowych dotyczą osób fizycznych nieprowadzących działalności gospodarczej funkcjonujących wewnątrz struktury organizacyjnej administratora danych osobowych (głównie są to pracownicy i zleceniobiorcy działający w strukturze administratora). Natomiast umowy powierzenia przetwarzania danych osobowych dotyczą podmiotów przetwarzających funkcjonujących poza strukturą organizacyjną administratora, wykonujących zadania zdalnie, na własnym sprzęcie, w oparciu o własne zasoby i mających określoną formę prawną (np. jednoosobowa działalność gospodarcza czy spółka). Faktycznie nie jest to jednak przewidziane w treściach regulacji w związku z czym dopuszczać należy również kontrargumentację.

Można sformułować pytanie, czy administrator danych, jako podmiot zarządzający i decydujący w kwestiach przetwarzania danych osobowych, w każdych okolicznościach może dokonać powierzenia przetwarzania danych, czy istnieją ograniczenia lub też okoliczności uniemożliwiające polecenie przetwarzania danych innemu podmiotowi. Jest

[558] Dz. U z 2018 r., poz. 1000, ze zm., dalej jako: UODO z 2018 r.
[559] J. Byrski, *Umowne…, op. cit*., Legalis.

to zarazem pytanie o to, czy istnieją ograniczenia możliwości bycia przetwarzającym. Przepisy RODO w tej kwestii nie zawierają żadnych wyjątków. Z prowadzonych badań regulacji prawnych pod kątem ich odniesień do zagadnień ochrony danych osobowych wynika, że istnieje literalny zakaz powierzania przetwarzania danych. Zawarto go w treści art. 8 ust. 2 ustawy z dnia 6 lipca 2001 r. o usługach detektywistycznych[560], stanowiącego, że detektyw nie może powierzać przetwarzania danych osobowych innemu podmiotowi. Można to interpretować również tak, że żaden podmiot nie może pełnić funkcji przetwarzającego w stosunku do danych przetwarzanych przez detektywa. Wyłączenie uprawnienia detektywa jako administratora danych do powierzania danych innemu podmiotowi zgodnie z ogólnym uprawnieniem do powierzania wynikającym z treści art. 28 RODO, należy uznać za racjonalne działanie ustawodawcy. Zakaz ten jest uzasadniony przede wszystkim tym, że zgodnie z treścią art. 3 powołanej ustawy o usługach detektywistycznych, świadczenie usług detektywistycznych jest działalnością regulowaną i wymaga uzyskania wpisu do rejestru działalności detektywistycznej. Ponadto, zakaz powierzania danych stanowi gwarancję tego, że dane osobowe będzie przetwarzał tylko detektyw zgodnie z zakresem swoich uprawnień.

Inne ograniczenie możliwości powierzania przetwarzania danych wywieść można z przepisów ustawy Prawo bankowe. Zgodnie z treścią art. 6a tej ustawy bank może, w drodze umowy zawartej na piśmie, powierzyć przedsiębiorcy lub przedsiębiorcy zagranicznemu, wykonywanie w imieniu i na rzecz banku pośrednictwa oraz czynności faktycznych związanych z działalnością bankową. Przy powierzeniu wymienionych działań (jak np. zawieranie umów o kartę płatniczą, których stroną jest konsument), niejednokrotnie niezbędnym elementem będzie również powierzenie danych osobowych. Ustawodawca zastrzegł jednak wyjątek, że powierzenie wykonywania czynności nie może obejmować: zarządzania bankiem i przeprowadzania audytu wewnętrznego banku. Konsekwentnie należałoby przyjąć, że oznacza to, że bank nie może powierzyć przetwarzania danych osobowych innemu podmiotowi w celu zarządzania bankiem i prowadzenia audytu. A to z kolei oznacza, że przedsiębiorca lub przedsiębiorca zagraniczny nie może stać się przetwarzającym w zakresie wymienionych działań banku.

W praktyce są nierzadko spotykane sytuacje trudne do jednoznacznej oceny, który z podmiotów jest administratorem danych, a który przetwarzającym. Skomplikowanym

[560] T.j. Dz.U. z 2017 r. poz. 556.

przypadkiem z życia codziennego może być np. przystąpienie pracodawcy do programu oferowanego przez podmiot świadczący usługi sportowo-rekreacyjne i zawarcie umowy o świadczenie usług przez dany podmiot dla pracowników pracodawcy. Pracodawca jako administrator danych pracowników jest zobowiązany do przekazania określonych w umowie danych po to, by pracownicy jako członkowie programu benefitowego otrzymali karty wstępu do obiektów usługodawcy. W dalszych postanowieniach umownych okazuje się, że pracodawca staje się przetwarzającym, natomiast administratorem danych uczestników programu sportowo-rekreacyjnego jest podmiot świadczący usługę. Takich przypadków, gdy administrator danych jest jednocześnie przetwarzającym (i w odwrotnej konfiguracji) oraz gdy trudno jest jednoznacznie stwierdzić, który z podmiotów jest faktycznie administratorem, a który przetwarzającym, jest wiele. Każdy stosunek prawny tego typu wymaga indywidualnej oceny okoliczności, choć posiłkować się można wskazówkami wynikającymi z nauki prawa. Sugeruje się, że kluczowym elementem wyróżniającym przetwarzającego, jak również odróżniającym przetwarzającego od administratora jest stopień samodzielności (niezależności) w stosunku do danych osobowych, jaki ma dany podmiot[561].

Podkreślenia wymaga fakt, że przetwarzający na gruncie RODO jest zdecydowanie bardziej zauważalnym podmiotem procesu przetwarzania danych osobowych, niż było to pod rządami UODO z 1997 r. Jest to widoczne chociażby z tego względu, że treść przepisów RODO wprost odnosi się do podmiotu przetwarzającego. Głównie chodzi tu o to, że przetwarzający jest podmiotem praw i obowiązków, co bezpośrednio sformułowane jest w przepisach RODO, a nie występowało na gruncie UODO z 1997 r.

Biorąc pod uwagę sferę obowiązków przetwarzającego, należy przyjąć zaproponowany w najnowszej literaturze przedmiotu podział obowiązków na dwie grupy[562]. Pierwszą z nich stanowią obowiązki podmiotu przetwarzającego wynikające z treści umowy powierzenia przetwarzania danych osobowych. Będą one stanowiły przedmiot rozważań w dalszej części rozprawy. Druga grupa to obowiązki, jakie przepisy RODO nakładają na przetwarzającego, w oderwaniu od umowy. Wśród nich wskazać należy wyznaczenie przedstawiciela w Unii (art. 27 RODO), przetwarzanie wyłącznie na polecenie administratora (art. 29 RODO), prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 RODO).

[561] A. Krasuski, D. Skolimowska, *Dane…, op. cit*., s. 70.
[562] M. Sakowska-Baryła (red.), *Ogólne..., op. cit.,* Legalis.

Ponadto w grupie tej wyróżnić można współpracę z organem nadzorczym (art. 31 RODO), wdrażanie odpowiednich środków technicznych i organizacyjnych adekwatnych do ryzyka (art. 32 RODO). Będą tu również obowiązki zgłaszania naruszeń ochrony danych osobowych administratorowi (art. 33 RODO), wyznaczenia inspektora ochrony danych (art. 37 RODO), czy też korzystania z kodeksów postępowań i certyfikacji (art. 40-42 RODO). Dla kontrastu, przepisy UODO z 1997 r. nie kreowały żadnego z powyższych obowiązków w stosunku do przetwarzającego.

Istotnym i nowym aspektem dotyczącym podmiotu przetwarzającego jest zbliżenie w przepisach RODO jego pozycji prawnej do administratora danych. Jest to widoczne w tym, że często RODO obok administratora adresatem swoich przepisów ustanawia podmiot przetwarzający[563]. Dla przykładu powołać można art. 37 RODO, zgodnie z którym zarówno administrator, jak i podmiot przetwarzający mają obowiązek wyznaczenia inspektora ochrony danych w trzech wskazanych przypadkach, czy też art. 32 RODO stanowiący, że oba podmioty wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku. Faktycznie to zbliżenie pozycji administratora i przetwarzającego dostrzegalne jest tylko w sferze obowiązków, jakie nakładają na nich przepisy prawa.

Stosunki powierzania przetwarzania danych osobowych mogą być bardzo zróżnicowane pod względem obowiązków stron, ale przede wszystkim mogą mieć różny zakres podmiotowy. Po pierwsze, administrator może korzystać z więcej niż jednego podmiotu przetwarzającego (nawet w stosunku do tego samego celu przetwarzania danych). Przykładem jest hotel, który może współpracować z kilkoma serwisami internetowymi, za pomocą których dokonywane są rezerwacje. Po drugie, mogą zaistnieć też takie przypadki, że jeden podmiot przetwarzający zawrze więcej niż jedną umowę powierzenia z tym samym administratorem[564]. Takie sytuacje występują w praktyce rzadziej, ale jako przykład można wskazać korzystanie przez przedsiębiorstwo z obsługi oferowanej przez dużą korporację o szerokim profilu działalności, np. w zakresie doradztwa podatkowego oraz osobno prowadzenia rekrutacji pracowników. Z uwagi na różne cele przetwarzania i różne zakresy danych osobowych, wymagane są tu odrębne umowy powierzenia przetwarzania danych osobowych z tym samym podmiotem

[563] *Ibidem*.
[564] *Ibidem*.

przetwarzającym. Problematyka praw podmiotu przetwarzającego jest w treści RODO potraktowane bardzo lakonicznie.

Można przyjąć, że wobec potrzeb biznesowych jak i rozwoju uwarunkowań rynkowych, istnieje faktyczna potrzeba, aby podmiot, któremu administrator danych „zleca" przetwarzanie danych osobowych w swoim imieniu, korzystał z usług innego podmiotu. Na gruncie literatury przedmiotu i w praktyce ochrony danych osobowych taką relację prawną, w której przetwarzający nie przetwarza powierzonych mu danych osobowych samodzielnie, a z pomocą innego podmiotu, nazywa się podpowierzeniem przetwarzania danych osobowych[565]. Tworzy się wówczas tzw. łańcuch powierzeń[566].

Konstrukcja prawna tego działania w ogóle nie występowała na gruncie Dyrektywy 95/46/WE ani UODO z 1997 r.[567]. Potrzebę uregulowania tzw. łańcucha powierzeń dostrzeżono na etapie prac nad RODO, czego efektem jest po raz pierwszy ujęcie podpowierzenia w akcie prawnym. Zgodnie z treścią 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 podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian. Wynika z powyższego przepisu, że zagwarantowano administratorowi wpływ i kontrolę w aspekcie udziału w procesie przetwarzania danych osobowych innego podmiotu niż przetwarzający. Innymi słowy, podmiot przetwarzający nie może „zlecić" dalszego przetwarzania danych podprzetwarzającemu, bez uprzedniej akceptacji administratora, czy to w formie szczegółowej (osobno w stosunku do każdego podmiotu) czy ogólnej (jednorazowej bez konkretyzacji podmiotu) pisemnej zgody. Ponadto w myśl art. 28 ust 4 RODO, jeżeli przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot nałożone zostają te same obowiązki ochrony danych jak w umowie między

[565] „Przez podpowierzenie przetwarzania danych osobowych będziemy rozumieli sytuację, w której podmiot, któremu powierzono przetwarzanie (przetwarzający, procesor), dalej powierza ich przetwarzanie kolejnemu podmiotowi (podwykonawca, subprocesor)". G. Sibiga, *Podpowierzenie przetwarzania danych osobowych*, [w:] Dodatek do Monitora Prawniczego 2012 nr 7, Legalis.

[566] Szerzej o podpowierzeniu przetwarzania danych osobowych zob. J. Byrski, *Outsourcing w działalności dostawców usług płatniczych*, Warszawa 2018, Legalis.

[567] Problematyki podpowierzenia przetwarzania danych osobowych dotyczy Decyzja Komisji Europejskiej 2010/87/WE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich, na mocy dyrektywy 95/46/WE, Dz. Urz. L Nr 39/5.

administratorem a podmiotem przetwarzającym[568]. W kwestii odpowiedzialności przewidziano, że jeżeli podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, to pełną odpowiedzialność wobec administratora będzie ponosił podmiot przetwarzający.

Pomimo faktu, że przed rozpoczęciem stosowania RODO przepisy UODO z 1997 r. nie przewidywały możliwości zaangażowania innych podmiotów w relację administratora z przetwarzającym, to mając na uwadze, że korzystanie przez podmiot przetwarzający z usług podwykonawców było i nadal jest częstym rozwiązaniem, można uznać praktykę podpowierzania przetwarzania danych osobowych za ugruntowaną[569]. Przedstawiciele nauki prawa formułują przesłanki, których spełnienie warunkuje legalność podpowierzenia. Wśród nich występują: wskazanie w treści umowy powierzenia przetwarzania danych (przed jej zawarciem) tożsamości podmiotów, które mogą być podwykonawcami przetwarzającego; uzyskanie przez przetwarzającego pisemnej zgody administratora (w trakcie realizowania umowy) na korzystanie z usług wskazanego co do tożsamości podmiotu. We wszystkich przypadkach działania podprzetwarzającego muszą mieścić się w granicach zakresu i celu przetwarzania określonych w treści umowy powierzenia[570]. W związku z tym, aby podpowierzenie było zgodne z wymogami RODO, w umowie powierzenia musi zaistnieć umocowanie do podpowierzenia danych innemu podmiotowi. Umocowanie to realizowane może być poprzez wyrażenie przez administratora zgody na wskazane konkretnie w umowie podmioty, którym dane mogą zostać podpowierzone, albo poprzez zawarcie klauzuli mówiącej o tym, że przed przekazaniem danych wykonawcy podmiot przetwarzający musi uzyskać akceptację administratora, bądź przynajmniej poinformować administratora i umożliwić mu ewentualny sprzeciw wobec podpowierzenia[571]. W treści przepisu art. 28 ust. 4 RODO wskazano, w jakiej formie ma nastąpić podpowierzenie przetwarzania danych osobowych. Jest to umowa lub inny akt prawny, które podlegają prawu Unii lub prawu państwa członkowskiego. W praktyce jest to umowa dalszego powierzenia (podpowierzenia)

[568] W szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom rozporządzenia

[569] Autorytety w dziedzinie ochrony danych osobowych twierdzą, że o ile podpowierzenie znajduje uzasadnienie w treści art. 31 UODO (bo czynności mieszczące się w ramach podpowierzenia mieszczą się w ramach powierzenia przetwarzania danych), to mamy do czynienia z luką w prawie dotyczącą warunków podpowierzania (G. Sibiga, *Podpowierzenie…, op. cit., Legalis).*

[570] P. Litwiński [w:] M. Jagielski, M. Krasińska, P. Litwiński, P. Kawczyński, K. Wojsyk, A. Sieradzka, E. Bielak-Jomaa, K. Andres, *Ochrona danych osobowych medycznych*, Warszawa 2013, Legalis.

[571] G. Sibiga, *Podpowierzenie…, op. cit.,* Legalis.

przetwarzania danych, na mocy której na podprzetwarzającego nałożone zostają te same obowiązki ochrony danych, co w umowie między administratorem a przetwarzającym. Należy pamiętać, że podmiot przetwarzający, który podpowierza przetwarzanie danych nie ma przy tym administratora w stosunku do podpowierzanych danych.

Należy więc stwierdzić, że w odróżnieniu od regulacji obowiązujących przed dniem 25 maja 2018 roku, prawodawca unijny w treści RODO dokonał szczegółowej i kompleksowej regulacji podpowierzenia przetwarzania danych osobowych, które przede wszystkim musi zostać uregulowane w umowie podpowierzenia. Po pierwsze, z treści art. 28 ust. 2 sformułowano wyraźnie uprawnienie podmiotu przetwarzającego do korzystania z usług innych podmiotów przy przetwarzaniu danych osobowych „zleconym" przez administratora. Po drugie, określono warunki korzystania z tych usług, czyli albo uzyskanie zgody szczegółowej (gdy jest konkretny podmiot będący podwykonawcą przetwarzającego), albo zgody ogólnej o charakterze blankietowym (gdy nie wiadomo jeszcze na tym etapie kto będzie podprzetwarzającym). Co więcej, prawodawca w treści art. 28 ust. 4 wymaga, aby podprzetwarzający również zapewniał wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych (wybór odpowiedniego podmiotu), jak też, by przestrzegał tych samych obowiązków co podmiot przetwarzający w relacji z administratorem[572]. Wydaje się, że należy pozytywnie ocenić regulację podpowierzenia przetwarzania danych osobowych. Jest ona wystarczająco szczegółowa i w przeciwieństwie do przepisów obowiązujących przed 25 maja 2018 r., pozwala na ustanowienie przejrzystych ram współpracy podmiotów w łańcuchu powierzeń. Dodatkowo regulacja zawarta w treści art. 82 RODO dotycząca odpowiedzialności podmiotu przetwarzającego za działania i zaniechania podmiotów przetwarzających, zabezpiecza interesy administratora.

Należy powiedzieć, że podpowierzenie przetwarzania danych osobowych stanowi uprawnienie podmiotu przetwarzającego oraz jest bardzo częstą sytuacją. Przyczyną takiego stanu rzeczy jest to, że po pierwsze, procesy przetwarzania danych osobowych bywają naprawdę skomplikowane i złożone, a po drugie, podmioty w obrocie gospodarczym są coraz bardziej wyspecjalizowane w ściśle określonych usługach, co *de facto* prowadzi do przekazywania realizacji fragmentów usług podwykonawcom[573]. Z racji tego, należy bardzo pozytywnie ocenić podejście prawodawcy unijnego, który

[572] M. Kwiatkowska-Cylke [w:] D. Lubasz (red.), *Rodo…, op. cit*., s. 241.
[573] *Ibidem*, s. 238.

sformułował w treści RODO regulację prawną, pozwalającą na stosowanie tego instrumentu w oparciu o przepis prawa nie budzący większych wątpliwości interpretacyjnych.

3. Elementy przedmiotowe umowy powierzenia przetwarzania danych osobowych

Brzmienie przepisu art. 31 UODO z 1997 r. skłaniało do przyjęcia, że kształtowanie treści umowy powierzenia przetwarzania danych osobowych odbywało się na zasadzie swobody kontraktowania, która ograniczona była przepisami UODO z 1997 r. tylko w niewielkim stopniu. Gdyby nie wskazówki wypracowane na gruncie nauki prawa, orzecznictwa i działania organu ds. ochrony danych osobowych (np. publikacje internetowe GIODO), administrator danych osobowych nie został wyposażony w podstawowy zakres informacji, jak powinien realizować obowiązek zawierania umów powierzenia. Od 25 maja 2018 roku umowa powierzenia przetwarzania zyskała na znaczeniu, a jej ranga wzrosła. Regulacja w treści art. 28 RODO jest wyraźnie precyzyjniejsza od dotychczasowej, co może pozwolić na upowszechnienie tego instrumentu prawnego w obrocie, a tym samym na podniesienie standardów ochrony danych osobowych.

Interpretacja regulacji art. 31 UODO z 1997 r. pozwalała na wyodrębnienie tylko dwóch elementów, które ustawodawca uznał za niezbędne w treści umowy powierzenia, czyli zakres przetwarzania i cel przetwarzania. Pozostałe elementy treści umowy mogły być kształtowane w oparciu o zasadę swobody umów. Natomiast z treści art. 28 ust. 3 RODO wynika następujący katalog elementów umowy powierzenia przetwarzania danych osobowych: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Zestawiając obie regulacje można powiedzieć, że w zasadzie elementem wspólnym wymogów co do treści umowy powierzenia wynikających z UODO z 1997 r. i RODO jest określenie celu przetwarzania. Ponadto można przyjąć, że dotychczasowy wymóg określenia zakresu powierzenia obejmuje w aktualnym brzmieniu przepisu przedmiot powierzenia, charakter, rodzaj danych osobowych oraz kategorie osób.

Pierwszym z elementów obowiązkowych w treści umowy powierzenia przetwarzania danych osobowych uznanym za priorytetowy zarówno przez polskiego ustawodawcę, jak i prawodawcę unijnego, jest cel powierzenia. Można powiedzieć, że nie

budzi on większych wątpliwości, tak na gruncie teoretycznym, jak i praktycznym. Nauka prawa, wypowiedzi przedstawicieli GIODO (aktualnie PUODO), orzecznictwo oraz praktyka pozwalają na wniosek, że cel powierzenia jest bardzo blisko związany z celem przetwarzania danych osobowych w imieniu administratora danych przez przetwarzającego. Należy przede wszystkim mieć na uwadze to, że umowa powierzenia nie jest umową samodzielną, a umową akcesoryjną. Generalnie rzecz ujmując, jej celem będzie realizacja zobowiązań wynikających z umowy zasadniczej, której wykonanie wymaga powierzenia danych. Ogólny cel powierzenia danych przetwarzającemu jest pochodną celu przetwarzania danych przez administratora. Cel zawarcia przedmiotowej umowy zawsze musi być związany z celem przetwarzania danych przez administratora. Administrator danych nie może „zlecić" przetwarzającemu przetwarzania danych w celu, który nie jest zgodny z celem, dla którego on sam określone dane przetwarza. Nie oznacza to, że muszą to być cele tożsame. Po pierwsze, może zdarzyć się tak, że administrator zbiera określone dane osobowe (np. imię, nazwisko, adres, numer konta bankowego) w celu zawarcia i zrealizowania umowy (np. zlecenia), a powierzy te same dane podmiotowi zewnętrznemu w celu realizowania usług kadrowo płacowych. Sprowadza się to *de facto* do tego samego celu, do którego nastąpiło zebranie danych (tożsamość celu przetwarzania danych przez administratora i celu umowy powierzenia). W innej sytuacji np. administrator danych przetwarza dane klientów w celach marketingowych, natomiast powierzenie dotyczy tych danych w aspekcie zdalnej usługi helpdesk w systemie informatycznym. Dane klientów są przetwarzane (związanie celu przetwarzania danych przez administratora z celem umowy powierzenia, ale brak tożsamości).

Niewłaściwym z punktu widzenia zasady celowości i minimalizacji danych osobowych byłoby powierzenie danych w celu zupełnie niepowiązanym z celem dokonywania operacji przetwarzania przez administratora danych. Na podstawie analizy treści dostępnych umów powierzenia można sformułować wniosek, że najczęstszym celem zawarcia umowy powierzenia przetwarzania danych osobowych jest realizacja umowy zasadniczej łączącej administratora danych i przetwarzającego (np. umowę na usługi w zakresie ochrony, umowę hostingu strony internetowej). Rozważenia wymaga też kwestia, czy skoro żadne wymogi co do celu powierzenia nie wynikają z treści przepisu prawa, to hipotetycznie administrator może powierzyć dane osobowe przetwarzającemu, w celu prowadzenia przez niego własnej działalności zarobkowej. Jako przykład można wskazać powierzenie przez podmiot prowadzący przychodnię weterynaryjną danych

osobowych klientów (właścicieli zwierząt) na prośbę podmiotu prowadzącego sklep internetowy z artykułami zoologicznymi. Strony na podstawie art. 28 RODO zawierają umowę w formie pisemnej, określającej cel – marketing i sprzedaż towarów oferowanych przez sklep, zakres (w tym przedmiot powierzenia, charakter, rodzaj danych osobowych oraz kategorie osób) oraz czas trwania przetwarzania, obowiązki i prawa administratora. Wydaje się, że trzeba udzielić odpowiedzi negatywnej na pytanie o powierzanie danych w celu prowadzenia własnej działalności zarobkowej przez podmiot przetwarzający. Taka sytuacja nie mieści się w konstrukcji powierzenia przetwarzania danych osobowych (28 RODO). Pamiętać przy tym należy, co zostało wcześniej wykazane, że to administrator inicjuje powierzenie danych osobowych, wobec których jest decydentem i zleca ich przetwarzanie w swoim imieniu. Ponadto powierzenie danych musi być związane z jakimś działaniem leżącym w gestii administratora, które angażuje dane osobowe, np. przekazanie prowadzenia spraw księgowych administratora podmiotowi zewnętrznemu. We wskazanym przypadku sklep zoologiczny będzie przetwarzał dane osobowe we własnym imieniu i na własną rzecz, będzie więc podmiotem samodzielnym w stosunku do otrzymanych danych osobowych (to on stanie się decydentem). Z tych względów nie można traktować go jak przetwarzającego, a przekazania danych przez przychodnię weterynaryjną jako powierzenia przetwarzania danych osobowych.

Pod rządami UODO z 1997 r. większość elementów umowy powierzenia przetwarzania danych osobowych była określona jednym zbiorczym pojęciem zakresu przetwarzania. Można przyjąć, że w ramach stosowanego dotychczas ogólnego pojęcia zakresu przetwarzania można ująć przedmiot powierzenia, charakter, rodzaj danych osobowych oraz kategorie osób i rozważyć te elementy łącznie. Dlatego z powodzeniem można się posiłkować literaturą przedmiotu opublikowaną przed 25 maja 2018 roku oraz poglądami wyrażonymi w orzecznictwie, ponieważ nie tracą one na aktualności. Analiza literatury przedmiotu pozwala wyodrębnić różne sposoby rozumienia pojęcia zakresu powierzenia danych. Pierwszy pogląd przedstawia to zagadnienie jako wskazanie, jakie dane osobowe może przetwarzać przetwarzający[574]. Innymi słowy, chodzi o rodzaje (kategorie) danych osobowych powierzanych przetwarzającemu[575]. Pogląd ten został również przyjęty w orzecznictwie. Wojewódzki Sąd Administracyjny w Warszawie w wyroku z dnia 15 lutego 2006 r. wyjaśnił, że podmiot przyjmujący od administratora

[574] A. Krasuski, D. Skolimowska, *Dane..., op. cit.,* s. 139.
[575] J. Byrski, *Umowne…, op. cit*., Legalis.

"zlecenie przetwarzania danych" może to przetwarzanie prowadzić wyłącznie w przewidzianym umową zakresie (chodzi tu głównie o rodzaj danych)[576]. Na podstawie badań własnych w zakresie treści umów powierzenia zawieranych przez różne podmioty sektora publicznego i prywatnego, można jako przykład realizacji tego wymogu wskazać np. postanowienie umowne o następującej treści: „Administrator danych osobowych powierza Przetwarzającemu następujący zakres danych osobowych: imię i nazwisko, numer telefonu, adres zamieszkania, adres email". Wymaga podkreślenia, że nie zawsze możliwym będzie takie wyszczególnienie konkretnych rodzajów powierzanych danych. Niejednokrotnie strony uogólniają zapis w umowie dotyczący zakresu powierzanych danych, np. „Przetwarzający ma prawo przetwarzać dane osobowe wyłącznie w zakresie niezbędnym do realizacji umowy zasadniczej na (…)". Inną opcją, która w praktyce bywa często wykorzystywana, jest grupowanie danych w kategorie. Może to być sformułowane następująco: „Przetwarzający na mocy niniejszej umowy zostaje uprawniony do przetwarzania danych osobowych kwalifikowanych do kategorii danych identyfikacyjnych oraz danych o stanie zdrowia". Dwa ostatnie sposoby formułowania zakresu powierzanych danych występują najczęściej, przede wszystkim z uwagi na to, że na etapie zawierania umowy powierzenia (czyli zgodnie z wymogami jeszcze przed rozpoczęciem przetwarzania danych przez podmiot przetwarzający), strony mogą nie wiedzieć, jakie dane konkretnie będą stanowiły przedmiot powierzenia i jakich kategorii osób będą dotyczyły. W praktyce zdarza się, że rodzajów powierzanych danych jest na tyle dużo bądź też są niewyodrębnione, że strony umowy nie są w stanie enumeratywnie wymienić wszystkie ich rodzaje. Te same problemy można dostrzec co do kategorii osób, których dane dotyczą. Sformułowaniem tym posługiwano się też na gruncie UODO z 1997 r. i nie wzbudza ono większych wątpliwości. GIODO wyjaśnił je jako wskazanie, jakich kategorii osób dotyczą przetwarzane dane (np. klienci, darczyńcy)[577]. Natomiast na gruncie nauki prawa proponuje się rozumienie kategorii osób, których dane dotyczą, jako informacje dotyczące charakterystyki określonej grupy podmiotów danych np. osoby ubezpieczone, klienci sklepów internetowych, użytkownicy określonego serwisu internetowego itd."[578]. Wydaje się, że realizacja tego wymogu nie powinna sprawiać większych problemów praktycznych.

[576] Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 15 lutego 2006 r., II SA/Wa 2055/05, Legalis nr 334989.
[577] https://edugiodo.giodo.gov.pl/file.php/1/REJ/REJ_R06_03.html.
[578] P. Litwiński (red.), *Rozporządzenie…, op. cit*., Legalis.

Należy zwrócić uwagę na zakres powierzenia, którego odpowiednikiem w treści RODO jest przedmiot powierzenia. Polega na określeniu zakresu czynności dokonywanych na danych osobowych, katalog operacji wykonywanych na danych osobowych[579]. W takim świetle zakresem (przedmiotem) powierzenia mogłoby być np. zbieranie, przechowywanie czy archiwizowanie danych. W ten sposób administrator może skonkretyzować działania podmiotu przetwarzającego, Ten sposób rozumienia pojęcia zakres (przedmiot) jest powodem problemów dla stron na etapie sporządzania umowy. Wymaga bowiem ustalenia jakie dokładnie operacje na danych będzie na mocy umowy prowadził przetwarzający. Nie jest to zadanie proste po pierwsze, z uwagi na fakt, że rzadko kiedy da się na wstępie przewidzieć wszystkie operacje na danych, których będzie wymagała realizacja umowy zasadniczej. Pamiętać należy że pojęcie przetwarzania danych jest pojęciem szerokim, ustawodawca i prawodawca unijny sformułowali jedynie przykładowy katalog czynności wchodzących w zakres przetwarzania.

Kolejnym elementem wynikającym z treści art. 28 ust. 3 RODO, a stanowiącym składową dotychczas stosowanego zakresu powierzenia jest charakter przetwarzania. W najnowszej literaturze przedmiotu wyrażane są poglądy, że charakter przetwarzania danych to sposób dokonywania operacji na danych, w tym np. częstotliwość, powtarzalność, długoterminowość, masowość, z uwzględnieniem rodzajów zastosowanych technologii[580]. Jedynie przewidywać można, że spełnieniem tego wymogu RODO może być np. wskazanie w treści umowy, czy przetwarzanie powierzonych danych będzie następowało przy użyciu specjalistycznych systemów informatycznych, jeśli tak, jakich konkretnie programów, albo też czy będzie obejmowało profilowanie i zautomatyzowane podejmowanie decyzji. Praktyka stosowania umów powierzenia z pewnością pokaże, w jaki sposób realizowany będzie ten wymóg prawny.

Kwestię rodzaju danych kategorii osób, których powierzane dane dotyczą, może być rozpatrywana łącznie, jako zakres powierzanych danych. W praktyce najczęściej sięga się po ogólne rozwiązania. Rodzaj danych można określić np. jako dane kontaktowe, możliwe jest też wymienienie kategorii danych np. imiona, nazwiska, adresy email, numery telefonów. Jeśli chodzi o kategorię osób, często spotyka się określenia takie jak dane pracowników, dane klientów. Podkreślenia wymaga, że zakres powierzanych danych musi być taki sam (bądź węższy) jak zakres danych, co do których przetwarzania

[579] J. Byrski, *Umowne…, op. cit*., Legalis.
[580] *Ibidem.*

administrator danych posiada podstawę prawną. Oznacza to, że administrator nie może powierzyć szerszego zakresu danych niż te, co do których sam jest upoważniony[581]. Dla przykładu, jeśli administrator przetwarza określone dane klientów w oparciu o przesłankę legalności przetwarzania ujętą w treści art. 6 ust. 1 lit. b RODO (stanowiącego, że przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy), to niezgodne z prawem będzie powierzenie szerszego zakresu danych (np. danych, które administrator posiada, ale nie są one niezbędne do realizacji umowy).

Czas trwania przetwarzania jest elementem, do którego nie odnosiły się dotychczasowe regulacje (UODO z 1997 r. i Dyrektywy 95/46/WE). W nauce prawa wskazuje się, że „czas trwania przetwarzania winien być określony, przy czym możliwe jest zarówno odniesienie go do czasu oznaczonego, jak i nieoznaczonego"[582]. O ile pod rządami UODO z 1997 r. określenie czasu trwania przetwarzania danych przez przetwarzającego nie było wymogiem prawnym, to z badań własnych nad tekstami umów powierzenia można wyciągnąć wniosek, że umowy zawierane przed datą rozpoczęcia stosowania RODO, co do zasady określały czas trwania przetwarzania. Po raz kolejny uwidacznia się akcesoryjny charakter umowy powierzenia w stosunku do zasadniczej umowy na usługę, która pociąga za sobą konieczność powierzenia przetwarzania danych. Można powiedzieć, że czas trwania przetwarzania danych przez podmiot przetwarzający jest determinowany czasem realizacji umowy zasadniczej, czyli czasem trwania określonej usługi i zawartej na jej realizację umowy. Przykładowo, jeśli powierzenie przetwarzania danych jest związane z faktem, że administrator danych zlecił obsługę prawną swojej działalności kancelarii prawnej (stającej się podmiotem przetwarzającym), to czas trwania przetwarzania danych przez przetwarzającego jest determinowany czasem trwania umowy na obsługę prawną. Można więc podsumować, że czas trwania przetwarzania może być określony bądź nieokreślony i jest determinowany zasadniczą umową. Ponadto nie należy zapominać, że przedmiotem umowy może być również czynność jednorazowa, czyli przetwarzanie danych przez przetwarzającego może też stanowić jednostkowe i krótkotrwałe działanie jak np. usunięcie danych z dysku komputera.

[581] A. Krasuski, D. Skolimowska, *Dane..., op. cit.*, s. 139.
[582] P. Litwiński (red.), *Rozporządzenie…, op. cit*., Legalis.

Ostatnim z wymienionych elementów w strukturze przepisu w art. 28 ust. 3 RODO, obowiązkowym wymogiem co do treści umowy łączącej administratora danych z podmiotem przetwarzającym, jest określenie obowiązków i praw administratora. Nasuwa się tu automatycznie pytanie, dlaczego prawodawca uwzględnił tu tylko perspektywę administratora, pozostawiając poza zakresem tej regulacji sferę praw i obowiązków podmiotu przetwarzającego. Ogólnie można powiedzieć, że treść art. 28 RODO jest przykładem niesymetrycznego uregulowania sfery praw i obowiązków obu stron umowy. Obowiązki przetwarzającego są wprost wyliczone w treści art. 28 ust. 3 lit. a-h RODO. W drodze interpretacji można wywieść z nich prawa administratora. Prawodawca w treści art. 28 RODO odgórnie i sztywno uregulował obowiązki strony zobowiązanej, a pozostawił do ustalenia zakres praw i obowiązków strony uprawnionej z tytułu umowy powierzenia, przede wszystkim dlatego, że zlecenie przez administratora przetwarzania danych osobowych podmiotowi zewnętrznemu, nie zwalnia go z odpowiedzialności za niezgodne z prawem przetwarzanie tych danych. Z uwagi na to, że powierzenie danych nie prowadzi do zmiany statusu administratora to administrator powinien dopracować warunki współpracy z podmiotem przetwarzającym, by mógł realizować swoje obowiązki również wobec powierzonych danych[583]. Ponadto, aby móc egzekwować określony obowiązek od podmiotu przetwarzającego, musi on wynikać z przepisu prawa lub postanowienia umowy, natomiast uprawnienia administratora stosunkowo łatwo wyinterpretować z katalogu obowiązków przetwarzającego.

Należy zwrócić uwagę również na to, że prawodawca w treści art. 28 ust. 3 RODO wymienia jedynie minimalny zakres elementów umowy powierzenia przetwarzania danych osobowych. Strony zgodnie z zasadą swobody umów mogą dowolnie wypełnić treść tego stosunku prawnego, byleby jego treść lub cel nie sprzeciwiały się właściwości (naturze) stosunku, ustawie ani zasadom współżycia społecznego (art. 353^1 Kodeksu cywilnego). W nauce prawa spotkać można stanowisko o dopuszczalności przewidzenia kary umownej w treści umowy powierzenia przetwarzania danych osobowych. Potencjalnie można ją zastrzec np. w przypadku przekroczenia przez przetwarzającego zakresu upoważnienia do przetwarzania danych osobowych wynikającego z umowy (czyli przekroczenia zakresu umowy powierzenia) albo np. gdy organy nadzorujące przestrzeganie zasad ochrony danych osobowych stwierdzą brak respektowania tych zasad

[583] K. Witkowska-Nowakowska [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…, op. cit*., s. 639-640.

przez przetwarzającego[584]. Po drugie, wskazuje się na możliwość ujęcia w umowie powierzenia kwestii roszczeń regresowych. Następnym nieobowiązkowym postanowieniem umownym może być kwestia uregulowania uprawnień kontrolnych administratora nad przetwarzaniem powierzonych danych przez podmiot przetwarzający[585]. Warto już w treści umowy ustalić zasady współpracy stron np. w kontekście audytów, w tym ramy prowadzenia działań sprawdzających przez administratora, zasady dostępu do informacji o sposobach przetwarzania danych przez przetwarzającego i stosowanych przez niego zabezpieczeniach. Kolejna propozycja dotyczy wynagrodzenia podmiotu przetwarzającego. We wcześniej poruszanym wątku zaproponowanych zostało kilka możliwości rozwiązania tej kwestii, mając na uwadze akcesoryjny charakter umowy powierzenia przetwarzania danych osobowych. Wśród dodatkowych elementów przedmiotowej umowy w literaturze przedmiotu wymienia się też kwestię wyboru prawa właściwego w przypadku gdy zobowiązanie ma charakter transgraniczny[586]. Można w pełni podzielić pogląd, że zawarcie wymienionych nieobowiązkowych elementów w treści umowy jest bardzo istotne chociażby w celu uniknięcia w przyszłości potencjalnych sporów między stronami.

Wszystkie z wymienionych w treści art. 28 ust. 3 RODO elementy *de facto* są filarami konstrukcji umowy powierzenia i kształtują cały stosunek zobowiązaniowy pomiędzy stronami. Dlatego racją jest, że wymienione elementy powinny być w umowie określone bardzo precyzyjnie, aby nie wzbudzały wątpliwości co do granic, w jakich podmiot przetwarzający może posługiwać się danymi osobowymi[587]. Może zdarzyć się taka sytuacja, że administrator dokonuje powierzenia przetwarzania danych w drodze umowy, ale w treści tej umowy w ogóle nie określa zakresu, celu przetwarzania danych, czy też obowiązków i praw administratora. W takim przypadku można przychylić się do wyrażonego w nauce prawa poglądu, zgodnie z którym jeżeli nie przewidziano w treści umowy zakresu i celu przetwarzania danych osobowych, to uznać należy, że nie dochodzi do powierzenia ale nie jest ono zgodne z treścią art. 28 RODO[588]. Ponadto kwestia ustalenia zakresu i celu przetwarzania danych osobowych stanowi też rozróżnienie pozycji administratora danych od przetwarzającego. W przypadku wątpliwości co do tego, kto w danym stosunku prawnym pełni rolę administratora, a kto przetwarzającego, pomocnym

[584] A. Krasuski, D. Skolimowska, *Dane…, op. cit*., s. 150-151.
[585] A. Krasuski, D. Skolimowska, *Dane…, op. cit*., s. 149-150.
[586] M. Kwiatkowska-Cylke [w:] D. Lubasz (red.), *Rodo…, op. cit*., s. 238.
[587] M. Sakowska-Baryła, *Prawo…, op. cit*., s. 159.
[588] A. Drozd, *Ustawa… op. cit.,* s. 210.

może być właśnie to ustalenie – administrator określa przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, swoje obowiązki i prawa, natomiast przetwarzający jest ograniczony w sferze decydowania, gdyż przetwarza dane wyłącznie w zakresie i celu przewidzianym w umowie[589].

Konstrukcja umowy powierzenia przetwarzania danych osobowych wynikająca z treści RODO jest zdecydowanie bardziej precyzyjna i konkretna niż ta, która szczątkowo uregulowana była w treści UODO z 1997 r. Można zaryzykować stwierdzenie, że taki kształt regulacji pozwoli na szersze zastosowanie tego instrumentu ochrony danych osobowych oraz na to, że umowy powierzenia przetwarzania danych osobowych zaczną stanowić coraz bardziej powszechne zabezpieczenie danych w obrocie gospodarczym. Umowy zawarte przed datą rozpoczęcia stosowania RODO należy dostosować do wymogów RODO, zaś umowy, które będą zawierane po dacie 25 maja 2018 roku od początku muszą uwzględniać nowe podstawy prawne. Prawodawca unijny, uwzględniając dynamiczne uwarunkowania prowadzenia działalności gospodarczej, nowe trendy biznesowe oraz zmieniające się potrzeby administratorów danych i przetwarzających, jak i podmiotów danych, założył uproszczenie i usprawnienie zlecania przetwarzania danych osobowych na zewnątrz. W najbliższej przyszłości okaże się, czy zmiany w prawie przyniosą pożądane skutki w sferze praktyki życia codziennego.

4. Zakres praw i obowiązków stron umowy powierzenia przetwarzania danych osobowych

4.1. Prawa administratora danych

W treści przepisów UODO z 1997 r. ustawodawca nie odnosił się do sfery uprawnień administratora danych związanych z zawarciem przedmiotowej umowy, poza sformułowaniem ogólnego prawa do powierzenia danych innemu podmiotowi w drodze umowy. Przepis art. 31 ust. 1 UODO z 1997 r. stanowił, że administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych. Na gruncie RODO sytuacja uległa zmianie o tyle, że uprawnienia administratora przede wszystkim można wyinterpretować ze skorelowanych z nimi, a wskazanych

[589] P. Barta, P. Litwiński, *Ustawa…, op. cit,* s. 349.

literalnie umowie, obowiązków przetwarzającego, ponadto prawodawca formułuje jednostkowe uprawnienia w treści przepisu w art. 28 RODO.

Zakres praw administratora można wyinterpretować na zasadzie korelacji, z uwagi na fakt, że prawodawca wypunktował w treści art. 28 ust. 3 lit. a-h RODO obowiązki podmiotu przetwarzającego. Na tej podstawie można sformułować katalog uprawnień administratora z tytułu powierzania przetwarzania danych osobowych podmiotowi przetwarzającemu.

Przede wszystkim należy wyróżnić prawo do wydawania poleceń przetwarzającemu i żądania, by dane były przetwarzane tylko na podstawie wydanych poleceń i tylko w ich zakresie. Bardzo często strony postanawiają, że ogólnym poleceniem administratora przetwarzania danych przez przetwarzającego jest sama treść umowy powierzenia. Strony mogą na etapie zawierania umowy ustalić, że polecenie to może być później konkretyzowane i uzupełniane, jednakże należy mieć na uwadze cel powierzenia przetwarzania danych osobowych. Ponadto istotne jest dokumentowanie dyspozycji, w toku współpracy i adekwatnie do okoliczności i potrzeb wynikających z tej współpracy[590]. W treści umowy warto przewidzieć, w jakiej formie będą występowały polecenia (na piśmie, telefonicznie, mailowo). Zdarzyć się może, że polecenie administratora będzie przekraczało zakres powierzenia albo też będzie wymagało działań przetwarzającego naruszających treść RODO. Zastosowanie znajdzie wtedy art. 28 ust. 3 lit. h RODO (drugi akapit), zgodnie z którym podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie rozporządzenia lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

Istotne znaczenie ma prawo do żądania od przetwarzającego zobowiązania osób przetwarzających dane osobowe do zachowania tajemnicy, a także egzekwowania tego od tych osób. Warto zauważyć, że w poprzednim stanie prawnym to administrator danych upoważniał osoby do przetwarzania danych osobowych[591]. Aktualnie w praktyce powszechnie stosowanym rozwiązaniem jest zawieranie w umowie zapisu o tym, że przetwarzający upoważnia np. swoich pracowników do przetwarzania danych powierzonych przez administratora oraz przedstawia administratorowi listę

[590] Tak w odniesieniu do obowiązku przetwarzającego: M. Kwiatkowska-Cylke [w:] D. Lubasz (red.), *Rodo…, op. cit.*, s. 235.
[591] Art. 37 UODO z 1997 r.: Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.

upoważnionych osób. Nową regulację wynikającą z RODO i przenoszącą obowiązek upoważniania do przetwarzania danych osobowych na podmiot przetwarzający należy ocenić pozytywnie, gdyż uporządkuje ona kwestię podmiotu odpowiedzialnego za upoważnianie.

Należy też wskazać prawo do żądania i egzekwowania podjęcia przez przetwarzającego wszelkich środków wymaganych na mocy art. 32 RODO (odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa). W tym momencie wątpliwość budzi to, kto wymaga i decyduje o tym, czy zabezpieczenie powierzanych danych przez podmiot przetwarzający jest odpowiednie i wystarczające: administrator czy przetwarzający. Z definicji administratora wynika, że jest to podmiot, który ustala cele i sposoby przetwarzania danych osobowych, a ponadto to na nim ciąży odpowiedzialność za powierzone dane, oraz to on dokonuje wyboru podmiotu przetwarzającego, który daje odpowiednie gwarancje wdrożenia środków technicznych i organizacyjnych, można skłonić się do opinii, że to administrator określa wymagania, a przetwarzający ma obowiązek je spełnić[592].

Jeśli chodzi o prawo do weryfikacji i egzekwowania przestrzegania przez przetwarzającego warunków korzystania z usług innego podmiotu przetwarzającego, to odnosi się ono do tzw. podpowierzenia, czyli możliwości korzystania przez podmiot przetwarzający z usług innego podmiotu przetwarzającego przy przetwarzaniu powierzonych danych. Należy dodać, że możliwa jest sytuacja, że administrator danych ma prawo wyłączyć możliwość podpowierzenia danych przez powierzającego podmiotowi trzeciemu (wykonawcy przetwarzającego). Zapis o charakterze ogólnym wyłączający dalsze powierzanie danych może znaleźć się w treści umowy, a ponadto pamiętać należy, że już na etapie realizacji umowy administrator ma wpływ na podpowierzanie bo treść art. 28 ust. 2 RODO gwarantuje, że podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora.

Ważne jest również prawo do otrzymania od przetwarzającego pomocy (z uwzględnieniem charakteru przetwarzania oraz dostępnych mu informacji) przy wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w art. 15-22 RODO. Administrator ma

[592] Podobnie, ale w odniesieniu do obowiązku przetwarzającego: M. Kwiatkowska-Cylke [w:] D. Lubasz (red.), *Rodo…, op. cit*., s. 235.

prawo do otrzymania wsparcia w realizacji praw podmiotów danych (takich jak prawo sprostowania danych czy prawo do usunięcia danych). Szczególnie chodzi o sytuacje, gdy administrator nie ma bezpośredniego dostępu do danych, które zostały powierzone i sam bez aktywnego udziału podmiotu przetwarzającego nie będzie w stanie zrealizować obowiązków wobec osób, których dane dotyczą[593]. Należy zastanowić się, czy prawo to obejmuje również realizację uprawnienia osoby której dane dotyczą, stanowiącego element prawa do usunięcia danych, wynikającego z treści art. 17 ust. 2 RODO[594]. Przeciw stanowisku, że administrator może na podstawie powołanego przepisu żądać od przetwarzającego usunięcia łącz, kopii i replikacji danych podlegających usunięciu, przemawia to, że przetwarzający nie jest administratorem, zatem nie odnosi się do niego treść tego przepisu. Jednakże pamiętać należy, że w przypadku powierzenia danych osobowych administrator nadal ma władztwo nad danymi i nawet dane fizycznie powierzone innemu podmiotowi stanowią zasób, którym zarządza administrator. Zatem, jeśli otrzyma on żądanie usunięcia danych, to obowiązek dokonania usunięcia będzie opierał się na treści art. 17 ust. 1 i na tej podstawie administrator może żądać usunięcia przez wszystkie podmioty przetwarzające.

Należy wyróżnić także prawo do otrzymania od przetwarzającego pomocy co do wywiązywania się z obowiązków określonych w art. 32–36 RODO (obowiązki związane z bezpieczeństwem danych). Prawo to odnosi się do współpracy administratora i przetwarzającego np. przy wykonywaniu oceny skutków dla ochrony przetwarzanych danych i dokonywania konsultacji z organem nadzorczym, czy też zgłaszania naruszeń ochrony danych osobowych organowi nadzorczemu. Będzie to przede wszystkim prawo do otrzymywania informacji od przetwarzającego o przetwarzaniu przez niego powierzonych danych. Ponadto, w tym obszarze umieścić należy prawo administratora do bycia poinformowanym o naruszeniu ochrony danych osobowych przez podmiot przetwarzający. Obowiązek poinformowania o naruszeniu nie został ujęty wśród innych obowiązków z art. 28 ust. 3 RODO, ale sformułowano go osobno - zgodnie z treścią art. 33 ust. 2 RODO podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi. W treści zawieranej umowy

[593] *Ibidem*, s. 236.

[594] Jeżeli administrator upublicznił dane osobowe, a na mocy ust. 1 ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

strony powinny ustalić termin na poinformowanie administratora o każdej sytuacji naruszenia, tak, by miał on realną możliwość oceny, czy ma obowiązek zgłoszenia tego faktu do organu nadzorczego (zgodnie z treścią art. 33 ust. 1 RODO administrator zgłasza naruszenie w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia zgodnie z art. 55 RODO).

Istotne znaczenie praktyczne ma również prawo do żądania i egzekwowania od przetwarzającego po zakończeniu świadczenia usług związanych z przetwarzaniem usunięcia lub zwrotu wszelkich danych osobowych (zależnie od decyzji administratora) oraz usunięcia wszelkich kopii, chyba że prawo nakazuje ich przechowywanie. To administrator ma prawo zdecydować, czy po zakończeniu umowy na określoną usługę, z którą związane jest powierzenie przetwarzania danych osobowych, podmiot przetwarzający ma te dane usunąć, czy zwrócić (administrator powinien przy tym uwzględnić charakter usługi i wykonywane kopie zapasowe). Prawo administratora jest jednak ograniczone z uwagi na to, że prawo Unii lub prawo państwa członkowskiego mogą nakazywać przechowywanie danych osobowych.

Nie można też pominąć prawa do umożliwienia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji oraz prawo do wsparcia administratora w ich czasie. Wynika z tego prawo administratora do nadzorowania przetwarzania danych osobowych przez podmiot przetwarzający. W literaturze przedmiotu wskazuje się, że kwestie zasad współpracy przy audycie powinny być szczegółowo ustalone w treści umowy powierzenia przetwarzania danych osobowych[595]. Trzeba mieć na względzie to, że administrator nie dysponuje prawem do kontroli pod kątem tego, czy przetwarzający realizuje operacje na powierzonych danych zgodnie z prawem (to uprawnienie przysługuje Prezesowi Urzędu Ochrony Danych Osobowych), ale może on kontrolować pod względem kryterium zgodności z postanowieniami umowy zawartej z przetwarzającym, co *de facto* pośrednio i tak będzie odnosiło się do zgodności z prawem. Według opinii GIODO, uzasadnieniem uprawnień kontrolnych administratora jest fakt, że ponosi on odpowiedzialność za bezpieczeństwo danych powierzonych innemu podmiotowi[596].

Nadal jednak nie istnieje żaden zamknięty katalog uprawnień administratora danych i z uwagi na zasadę swobody umów strony często kreują je według swojego

[595] Ibidem, s. 237.
[596] https://giodo.gov.pl/317/id_art/3254/j/pl.

uznania. W analizowanych treściach umów powierzenia przetwarzania danych osobowych najczęściej pojawiają się takie uprawnienia administratora jak np. prawo do uzyskania informacji na temat wszczęcia kontroli w zakresie przetwarzania danych osobowych prowadzonej przez organ nadzorczy u przetwarzającego oraz jej wyników, czy też prawo do informacji o osobach upoważnionych do przetwarzania danych osobowych w strukturze podmiotu przetwarzającego.

Uprawnienie administratora, które nie wywodzi się bezpośrednio z przepisów prawa, jednakże z praktyki zawierania umów powierzenia przetwarzania danych osobowych to uprawnienie do uzyskania informacji na temat kontroli w zakresie przetwarzania danych osobowych prowadzonej u przetwarzającego przez organ ochrony danych osobowych. Jest to bardzo istotne z punktu widzenia administratora. Uprawnienie to może być rozpatrywane jako należące do kategorii uprawnień kontrolnych. Strony umowy mogą zgodnie postanowić, że w przypadku, gdy Prezes Urzędu Ochrony Danych Osobowych (PUODO) wszczyna kontrolę podmiotu przetwarzającego pod kątem zgodności przetwarzania danych osobowych z przepisami prawa, to przetwarzający ma obowiązek niezwłocznego poinformowania o tym fakcie administratora danych, który powierzył mu przetwarzanie danych osobowych. Ponadto uprawnienie to może być rozszerzone na podstawie zgodnych ustaleń stron i obejmować nie tylko informację o wszczęciu takiej kontroli, ale również o jej wyniku. Taki zapis w umowie może pozytywnie wpłynąć na sferę interesów administratora z uwagi na fakt, że po uzyskaniu informacji o negatywnym wyniku kontroli może on zareagować np. zakończeniem stosunku prawnego (wypowiedzeniem umowy) w celu ochrony swoich interesów. Pamiętać należy, że powierzenie przetwarzania danych osobowych innemu podmiotowi nie zdejmuje z administratora ciężaru odpowiedzialności za przetwarzane dane, dlatego ukształtowanie w treści umowy powierzenia tego uprawnienia administratora danych jest jak najbardziej uzasadnione.

Kolejne z praw administratora, które kształtuje praktyka zawierania stosunku powierzenia przetwarzania danych osobowych innemu podmiotowi dotyczy uprawnienia do informacji na temat tego, kto w strukturze przetwarzającego został upoważniony do przetwarzania powierzonych danych. Pomimo faktu, że z treści art. 28 ust. 3 lit. b RODO wynika tylko, że przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, strony umowy mogą

uzgodnić, że administrator będzie informowany kto ma upoważnienie do przetwarzania powierzonych danych w strukturze przetwarzającego. Rozwiązanie, że to przetwarzający upoważnia swoich pracowników i współpracowników do przetwarzania danych powierzonych przez administratora jest sprawnym rozwiązaniem, ułatwiającym organizację dokonywania operacji na danych dla obu stron umowy. W takim układzie przetwarzający ma stałą kontrolę nad tym, kto przetwarza powierzone dane i może na bieżąco i szybko dostosowywać się do potrzeb przetwarzania, natomiast administrator, który otrzymuje aktualizowaną listę osób upoważnionych (czyli ma kontrolę nad upoważnieniami), nie wnika w wewnętrzną strukturę podmiotu przetwarzającego, nie zajmuje się upoważnianiem pracowników przetwarzającego, co *de facto* oszczędza czas, działania i związane z tym koszty. Na gruncie RODO kwestia upoważniania do przetwarzania danych osobowych została uregulowana w sposób nie budzący wątpliwości ponieważ prawodawca dopuścił możliwość upoważniania osób przez podmiot przetwarzający w treści art. 29 RODO (Podmiot przetwarzający oraz każda osoba działająca z upoważnienia administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego).

4.2. Obowiązki administratora danych

Sfera obowiązków administratora danych wynika z kilku kwestii. Po pierwsze, jak już wspomniano, intencją ustawodawcy było rozgraniczenie pozycji administratora od pozycji przetwarzającego tak, aby przetwarzający nie był traktowany jako administrator danych. Po drugie, obowiązki administratora danych wynikają z wielu przepisów RODO, dla przykładu jest to spełnianie zasad przetwarzania wywodzonych z treści art. 5 RODO i omówionych w II rozdziale dysertacji.

Można sformułować ogólny wniosek, że prawodawca nałożył na administratora danych bardzo dużą liczbę obowiązków, ale w odniesieniu do powierzenia danych osobowych do przetwarzania innemu podmiotowi, wypowiedział się bardziej powściągliwie. W efekcie tego, obowiązki te w dużej mierze należy interpretować z ogółu przepisów RODO, a w szczególności należy je wywodzić z zasady rozliczalności.

W treści RODO obowiązek administratora decydującego się na zlecenie przetwarzania danych osobowych na zewnątrz własnej struktury organizacyjnej, wynika z pierwszych słów regulacji zawartej w art. 28 ust. 1 RODO, zgodnie z którym 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. Wynika z tego zobowiązanie administratora do skrupulatnego poznania podmiotów oferujących interesujące go usługi (których świadczenie będzie angażowało dane osobowe) i weryfikacji ich poziomu pod kątem ochrony danych osobowych, a także do dokonania starannego i uważnego wyboru odpowiedniego podmiotu. Wynika też z tego, że w przypadku postępowań przetargowych, kryterium wyboru wykonawcy nie może być tylko cena. Motyw 81 preambuły RODO wskazuje, co powinien uwzględniać administrator dokonując wyboru podmiotu przetwarzającego: wiedzę fachową, wiarygodność i zasoby - wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Odpowiedzialność za dokonanie wyboru podmiotu, który nie zapewnia wystarczających gwarancji, ciąży na administratorze[597]. Można powiedzieć, że prawodawca wspiera administratora wskazówkami, jak dokonać dobrego wyboru podmiotu przetwarzającego, wskazując w treści art. 28 ust. 5 RODO, że wystarczające gwarancje 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 RODO.

4.3. Prawa podmiotu przetwarzającego

Bezpośrednio z treści art. 28 RODO (ani wcześniej 31 UODO z 1997 r.) nie wynikają żadne uprawnienia przetwarzającego. Jednak błędem byłoby uznanie, że powierzenie przetwarzania danych osobowych kreuje dla przetwarzającego same zobowiązania, skoro wyżej stwierdzono i uzasadniono, że przedmiotowa umowa jest umową dwustronnie zobowiązującą i odpłatną. Musi to oznaczać, że przetwarzający również odnosi z niej jakieś korzyści w sferze swoich interesów. Pamiętać jednakże należy o tym, że umowa powierzenia przetwarzania danych osobowych ma charakter umowy

[597] K. Witkowska-Nowakowska [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO…, op. cit*., s. 635.

akcesoryjnej, a nie samoistnej. Dlatego, jeśli rzeczywiście dana umowa powierzenia nie odnosi się do sfery praw przetwarzającego, to w umowie zasadniczej należy szukać odpowiednich świadczeń drugiej strony stanowiących korelat obowiązków przetwarzającego. Przykładem takiej korelacji jest np. zawarcie umowy powierzenia przetwarzania danych osobowych pomiędzy centrum handlowym a podmiotem świadczącym usługi ochroniarskie. W umowie zasadniczej strony określają zasady świadczenia usługi ochrony oraz wynagrodzenie. Natomiast w umowie powierzenia stanowiącej integralną część tej umowy, strony ustalają kwestie związane z bezpieczeństwem danych osobowych, których administratorem jest centrum handlowe, a podmiot świadczący usługi ochroniarskie będzie przetwarzać w ramach umowy o świadczenie usług ochroniarskich (np. wizerunek klientów i pracowników centrum). W praktyce strony umowy powinny ustalić kwotę wynagrodzenia za wykonywanie usług ochroniarskich i mogą albo osobno uzgodnić wynagrodzenie za przetwarzanie powierzonych danych, albo ująć tę kwotę w zasadniczym wynagrodzeniu (co w praktyce występuje częściej). Alternatywą wynagrodzenia, stanowiącą uprawnienie podmiotu przetwarzającego, może być ustalenie przez strony, że w zamian za realizowanie zadań przez przetwarzającego, poza wynagrodzeniem za świadczenie usług przetwarzający będzie korzystał nieodpłatnie z usług administratora (np. gdy administratorem jest bank - założenie darmowego konta albo świadczenie usług doradczych w zakresie finansów przedsiębiorcy). W takim wypadku uprawnieniem przetwarzającego będzie wynagrodzenie za świadczenie zasadnicze oraz dodatkowe świadczenie administratora. Jednakże w samej umowie powierzenia przetwarzania danych osobowych trudno jest wskazać korzyści odnoszące się do sfery uprawnień przetwarzającego.

Innym uprawnieniem przetwarzającego dającym się wyinterpretować z treści art. 28 RODO, a do tej pory stosowanym często na gruncie praktyki funkcjonowania umowy powierzenia przetwarzania danych osobowych pomimo braku oparcia w przepisach, jest możliwość korzystania z usług podmiotów trzecich przy przetwarzaniu danych osobowych na zlecenie administratora (tzw. podpowierzenie przetwarzania danych omówione już wcześniej). Jak wyżej stwierdzono, jest to bardzo powszechna praktyka i niezwykle istotna z perspektywy podmiotu przetwarzającego.

Kontrowersyjna jest treść art. 28 ust. 3 lit. h drugi akapit RODO, który stanowi, że podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia lub innych

przepisów Unii lub państwa członkowskiego o ochronie danych. Z uwagi na to, że ocena tego, czy polecenie administratora stanowi naruszenie, pozostaje w gestii przetwarzającego, to *de facto* decyzja o poinformowaniu o tym administratora również leży po stronie przetwarzającego. Dlatego też przepis ten należy traktować jako względnie obowiązujący, z którego wywodzić należy uprawnienie przetwarzającego bardziej niż obowiązek.

4.4. Obowiązki podmiotu przetwarzającego

W odróżnieniu od sfery uprawnień przetwarzającego, które nie wynikają bezpośrednio z przepisów prawa, obowiązki przetwarzającego opierają się bezpośrednio na treści przepisów. Na wstępie należy wyjaśnić, że aktualne pozostają rozważania prowadzone wcześniej w zakresie uprawnień administratora jako korelatów z obowiązkami przetwarzającego.

Do dnia 25 maja 2018 roku obowiązki przetwarzającego określone były w treści art. 31 ust. 3 UODO w sposób bardzo ogólny[598]. Uzupełnienie stanowiły przepisy Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r.[599].

Natomiast od dnia 25 maja 2018 roku, obowiązki przetwarzającego są wymienione literalnie w ośmiu punktach w treści art. 28 ust. 3 RODO, ale również wynikają z treści innych przepisów RODO.

Warto zaproponować podział obowiązków wynikających z powołanego przepisu na trzy grupy. W pierwszej z nich znajdują się te, które ściśle związane z pozycją administratora i w treści których wymaga się od przetwarzającego podlegania poleceniom administratora. W grupie tej umieścić można wymóg przetwarzania danych osobowych wyłącznie na udokumentowane polecenie administratora (art. 28 ust. 3 lit. a RODO) oraz wymóg usunięcia lub zwrotu wszelkich danych osobowych i ich istniejących kopii po zakończeniu umowy zależnie od decyzji administratora (art. 28 ust. 3 lit. g RODO). Druga

[598] Zgodnie z treścią przepisu, podmiot, o którym mowa w ust. 1, jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art.39a.
[599] Dz.U. z 2004, Nr 100, poz. 1024.

grupa to obowiązki zapewnienia bezpieczeństwa przetwarzanych danych, stanowiące pierwotnie obowiązki administratora, ale ze względu na dokonanie powierzenia będące pochodną obowiązków administratora. Wśród nich jest zapewnienie, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy (art. 28 ust. 3 lit. b RODO), podejmowanie wszelkich środków wymaganych na mocy art. 32 RODO (art. 28 ust. 3 lit. c RODO), jak również przestrzeganie warunków korzystania z usług innego podmiotu przetwarzającego (art. 28 ust. 3 lit. d RODO). Trzecią grupę stanowią obowiązki wspierające administratora w realizacji jego zobowiązań wynikających z przepisów prawa, w tym: pomoc administratorowi w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw, poprzez odpowiednie środki techniczne i organizacyjne (art. 28 ust. 3 lit. e RODO), pomoc administratorowi w wywiązywaniu się z obowiązków określonych w art. 32–36 (art. 28 ust. 3 lit. f RODO), jak również udzielanie administratorowi wszelkich informacji niezbędnych do wykazania spełnienia obowiązków, w tym umożliwianie administratorowi przeprowadzanie audytów, w tym inspekcji i przyczynianie się do nich.

Powyższy podział pozwala wyciągnąć wniosek, że pozycja przetwarzającego jest bardzo ściśle związana z administratorem danych i *de facto* wszystkie jego działania są nakierowane na zaspokajanie interesów administratora – przetwarzający nie realizuje zadań w interesie własnym. Wskazuje to również na zależność przetwarzającego od administratora.

Ponadto część obowiązków przetwarzającego wynikająca z przepisów RODO, ujęta jest w poszczególnych przepisach poza uregulowaniem stosunku powierzenia danych. Dla przykładu będzie to obowiązek przetwarzania danych wyłącznie na polecenie administratora (art. 29 RODO), prowadzenie rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora (art. 30 ust. 2 RODO), wdrażanie odpowiednich środków technicznych i organizacyjnych zabezpieczających przetwarzane dane (art. 32 RODO), zgłoszenie administratorowi naruszenia ochrony danych osobowych bez zbędnej zwłoki po jego stwierdzeniu (art. 33 RODO). Ten zbiór obowiązków przetwarzającego również nie występuje w oderwaniu od administratora. Powyższe uwagi potwierdzają też sformułowaną na wstępie tezę o kluczowym i niepodważalnie istotnym znaczeniu administratora danych w procesie przetwarzania danych osobowych.

Pamiętać należy, że regulacje prawne stanowią minimum zabezpieczeń interesów administratora, który podejmuje decyzję o powierzeniu przetwarzania innemu podmiotowi. W treści umowy administrator (jako strona odpowiedzialna za przetwarzanie danych osobowych w najszerszym zakresie, w tym wobec osób, których dane dotyczą, powinien zawrzeć jak najwięcej klauzul, które umożliwią mu egzekwowanie wypełniania obowiązków przez podmiot przetwarzający. Jednakże prawodawca wychodzi w tym aspekcie naprzeciw potrzebom administratorów, poprzez stosunkowo szczegółowe uregulowanie w RODO obowiązków przetwarzającego, co w rezultacie sprawia, że w treściach umów nie należy powielać treści przepisów art. 28 RODO, gdyż automatycznie wchodzą one w miejsce postanowień umownych, jeśli strony nie zastrzegą zgodnie innego sformułowania obowiązków przetwarzającego.

Z analizy treści dostępnych umów powierzenia przetwarzania danych osobowych wynika, że stosunkowo częstym działaniem stron przy konstruowaniu umowy jest przenoszenie obowiązków, którymi przepisy prawa obciążają administratora, na podmiot przetwarzający. Oprócz praktyki, pewne kontrowersyjne poglądy można również odnaleźć na gruncie nauki prawa. Przykładem dostrzeżonym zarówno w praktyce stosowania przedmiotowych umów, jak i w literaturze przedmiotu jest zawieranie postanowienia w umowie powierzenia, zgodnie z którym administrator zobowiązuje przetwarzającego do zrealizowania obowiązku informacyjnego wobec osoby, której dane dotyczą (art. 13-14 RODO). Zgodnie z wyrażonym w nauce prawa poglądem, nie ma przeszkód, aby administrator powierzył przetwarzającemu w treści umowy wykonywanie obowiązków informacyjnych wynikających z art. 13-14 RODO (wcześniej art. 24 i 25 UODO)[600]. Jednakże przepisy te wyraźnie stanowią, że administrator podczas pozyskiwania danych osobowych podaje osobie wszystkie informacje (art. 13 ust. 1 RODO). Z uwagi na to, że powołane przepisy mają charakter bezwzględnie obowiązujący (a świadczy o tym cel regulacji i sposób jej sformułowania, a także przewidziana odpowiedzialność), trudno jednoznacznie zgodzić się z powyższymi twierdzeniami. Jest to rozwiązanie, które wzbudza szereg wątpliwości. Rozważenia wymagałoby to, czy zapisy w umowie przenoszące obowiązki na drugą stronę są w ogóle zgodne z prawem (literalnie wskazano, że to administrator jest zobowiązany do poinformowania osoby). Tak samo jak w przypadku obowiązku informacyjnego, kształtuje się również obowiązek np. zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu (art. 33 RODO), czy też

[600] A. Drozd, *Ustawa..., op. cit.,* s. 212.

obowiązek dokonania oceny skutków dla ochrony danych (art. 35) – prawodawca literalnie wskazuje, że to administrator wykonuje te obowiązki. Jeżeli obowiązek dotyczy przetwarzającego, to prawodawca wyraźnie to zaznacza, np. art. 33 ust. 2 RODO, zgodnie z którym podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi; art. 32 ust. 1 RODO, stanowiący, że administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne. Ponadto, argumentem przemawiającym przeciwko zasadności przenoszenia na przetwarzającego realizacji obowiązku informacyjnego, czy też np. dokonania oceny skutków dla ochrony danych, jest moment realizacji obowiązku. Dla przykładu wskazać można fragment przepisu art. 35 RODO, który stanowi, że administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, czy też 13 RODO, zgodnie z który administrator podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje. W takim układzie, jeżeli realizacja obowiązków jest wymagana jeszcze przed bądź na samym początku dokonywania operacji na danych, technicznie utrudnione (o ile w ogóle możliwe) byłoby przeniesienie ich na podmiot przetwarzający (bo na tym etapie może jeszcze nie być nawet planu powierzenia przetwarzania danych), co jest kolejnym argumentem skłaniającym do negatywnego ustosunkowania się do zagadnienia przenoszenia uprawnień administratora na powierzającego.

ROZDZIAŁ IV

Zastosowanie i funkcje umowy powierzenia przetwarzania danych osobowych w obrocie gospodarczym

1. Umowy powierzenia przetwarzania danych osobowych w kontekście outsourcingu usług

Nie ulega kwestii, że powierzenie przetwarzania danych jest najczęściej integralną częścią procesów polegających na outsourcowaniu usług przez jeden podmiot innym podmiotom. Stosunek prawny outsourcingu jest przykładem zastosowania umowy powierzenia przetwarzania danych osobowych. Przy takim założeniu w prowadzonych w tej części rozważaniach, należy poświęcić kilka uwag samemu pojęciu outsourcingu. Ogólnie rzecz ujmując, podstawą kreowania relacji outsourcingowych jest to, że przedsiębiorca decyduje o tym czy będzie prowadzić przedsiębiorstwo własnymi siłami, czyli poprzez pracowników powiązanych z przedsiębiorcą stosunkiem podwładności, albo też siłami zewnętrznymi, bez formalnego podporządkowania przez podmioty znajdujące się na zewnątrz struktury, na zasadzie równorzędności podmiotów[601]. Decyzja o wyborze sposobu prowadzenia działalności gospodarczej opiera się najczęściej na następujących motywach: organizacyjnym, ekonomicznym, rynkowym, społecznym[602]. Aspekt organizacyjny przejawia się m.in. w uproszczeniu struktury organizacyjnej, uelastycznieniu przedsiębiorstwa w wyniku zmian organizacyjnych, wspomaganiu zarządzania. Umotywowanie ekonomiczne decyzji outsourcingowych polega m.in. na redukowaniu kosztów działalności (gdy koszty działań dostawcy zewnętrznego są niższe), oszczędnościach wynikających z transferu aktywów od dostawców usług zewnętrznych. W aspekcie rynkowym uzasadnieniem wyboru skorzystania z usług zewnętrznych może być pozytywny wpływ na wizerunek przedsiębiorcy, który korzysta z doświadczonych i wyspecjalizowanych podmiotów, co w konsekwencji powoduje wzrost konkurencyjności i wiarygodności przedsiębiorcy, a ponadto dzięki outsourcingowi przedsiębiorca ma większe możliwości zwiększenia skali swojej działalności. Natomiast społeczne motywy

[601] W. Włodyka, M. Spyra [w:] M. Stec (red.), *Prawo..., op. cit.*,. 24-25.
[602] J. Mróz, *Outsourcing w sektorze małych i średnich przedsiębiorstw*, [w:] S. Wawak, M. Sołtysik (red.), *Współczesne trendy outsourcingu*, Kraków 2015, s. 24.

wyboru opcji outsourcingu przejawiają się we wzroście motywacji i zaangażowania pracowników w główny zakres działalności przedsiębiorcy, wzroście satysfakcji klienta[603].

Pojęcie outsourcingu nie doczekało się jeszcze polskiego określenia, mimo to w obcym brzmieniu coraz bardziej ugruntowuje się zarówno w praktyce, jak i w nauce. Termin ten jest zaczerpnięty z języka angielskiego i pochodzi od zwrotu „*outside resource using*", który oznacza wykorzystywanie zasobów zewnętrznych[604]. Można powiedzieć, że zagadnienie to znajduje się na pograniczu prawa i ekonomii (a także zarządzania), ponieważ dotyczy dziedziny zarządzania przedsiębiorstwem, ale jednocześnie ma znaczenie prawne, bo wywołuje skutki na gruncie prawa. Z drugiej strony, wyrażono w nauce prawa pogląd, że o ile termin umowa outsourcingowa jest w powszechnym użyciu, to trudno określić ramy prawne outsourcingu jako metody organizowania działalności gospodarczej[605]. Można więc przyjąć, że outsourcing jest zjawiskiem mieszczącym się w sferze prawa, ekonomii i zarzadzania przedsiębiorstwem (lub innymi jednostkami organizacyjnymi).

Nie ma jednolitej i powszechnie przyjętej definicji pojęcia outsourcing. Dokonując przeglądu opracowań naukowych z różnych dziedzin nauki dotyczących tego zagadnienia, można przytoczyć przykładowe definicje outsourcingu. Przez to pojęcie rozumiane jest przedsięwzięcie polegające na wydzieleniu ze struktury organizacyjnej przedsiębiorstwa macierzystego realizowanych przez nie funkcji i przekazanie ich do realizacji innym podmiotom gospodarczym[606]. Wskazuje się też, że outsourcing to wyprowadzenie na zewnątrz firmy funkcji i działań, które nie należą do głównego trzonu działalności i mogą być taniej realizowane w wyspecjalizowanych podmiotach i zakupywane na zewnątrz w stosunkach rynkowych[607]. Można też powiedzieć, że chodzi o „oddelegowanie" na podstawie umowy kontraktowej całości lub części zasobów materialnych, zasobów ludzkich i odpowiedzialności zarządczej do dyspozycji zewnętrznego dostawcy[608]. Twierdzi się również, że outsourcing to przede wszystkim relacja biznesowa, której

[603] *Ibidem*, s.24.
[604] S. Włodyka [w:] S. Włodyka (red.) *System Prawa Handlowego,* tom V, 2014, Legalis.
[605] W. Robaczyński [w:] W. J. Katner (red.), *System…, op. cit*., s. 466 .
[606] M. Trocki, cyt. za M. Tyrańska, *Istota i znaczenie outsourcingu w działalności przedsiębiorstwa* [w:] S. Wawak M. Sołtysik (red.), *Współczesne..., op. cit.,* s. 13-14.
[607] T. Gruszecki, cyt. za M. Tyrańska, *Istota i znaczenie outsourcingu w działalności przedsiębiorstwa* [w:] S. Wawak M. Sołtysik (red.), *Współczesne..., op. cit.,* s. 13-14.
[608] M. Pańkowska, cyt. za M. Tyrańska, *Istota i znaczenie outsourcingu w działalności przedsiębiorstwa* [w:] S. Wawak M. Sołtysik (red.), *Współczesne..., op. cit.,* s. 13-14.

główną zasadą jest partnerstwo[609]. Warto zauważyć, że powyższe definicje łączy kilka cech charakteryzujących outsourcing. Jest to stosunek zobowiązaniowy co najmniej dwóch podmiotów. W stosunku tym jeden podmiot jest przedsiębiorcą, a drugi podmiot znajduje się poza strukturą wewnętrzną pierwszego. Oba podmioty łączy stosunek partnerstwa ze względu na wspólny cel – zrealizowanie określonego działania przedsiębiorcy. Ponadto następuje wydzielenie określonych zadań z całości działalności przedsiębiorcy (podmiot zewnętrzny działa na rzecz pierwszego) oraz przekazanie, „zlecenie" tych zadań podmiotowi zewnętrznemu. W ten sposób optymalnie można osiągnąć zakładane cele ekonomiczne i organizacyjne. Łączne spełnienie wymienionych cech pozwala zakwalifikować daną relację do kategorii outsourcingu.

Na gruncie literatury przedmiotu wyróżnia się szerokie i wąskie znaczenie outsourcingu. Znaczenie szerokie to outsourcing w ujęciu ekonomicznym, odnosi się do techniki zarządzania. Natomiast znaczenie wąskie odpowiada outsourcingowi w aspekcie prawnym: chodzi o wyodrębnienie organizacyjne funkcji realizowanych przez określony podmiot i powierzenie ich wyspecjalizowanym podmiotom zewnętrznym[610]. Z punktu widzenia prawa outsourcing postrzegany jest jako forma gospodarcza, w ramach której są kreowane stosunki umowne różnego rodzaju[611]. Rozróżnienie na węższe i szersze rozumienie outsourcingu bywa też widziane odmiennie. Sąd Apelacyjny w Katowicach stwierdził że outsourcing w znaczeniu węższym dotyczy obsługi w zakresie potrzeb wewnętrznych (np. umowa o prowadzenie ksiąg rachunkowych), natomiast w szerszym znaczeniu dotyczy także właściwej działalności przedsiębiorcy zlecającego adresowanej do jego odbiorców. Zlecający zamiast sam świadczyć usługi lub wytwarzać samemu produkty dostarczone odbiorcom powierza to osobom trzecim[612]. To szersze rozumienie jest istotniejsze z perspektywy prawa.

Co do znaczenia outsourcingu w sensie prawnym, zdecydowanie można przyjąć pogląd wyrażony w nauce prawa, zgodnie z którym outsourcing polega na zawarciu umowy, na podstawie której przedsiębiorca powierza wykonanie określonych czynności faktycznych lub prawnych związanych z prowadzeniem przedsiębiorstwa, albo przedmiotem swojej właściwej działalności, podmiotowi zewnętrznemu, zaś wykonujący

[609] J. Byrski, *Outsourcing w działalności dostawców usług płatniczych*, 2018, Legalis.
[610] J. Byrski, *Outsourcing…*, *op. cit.*, Legalis.
[611] S. Włodyka [w:] S. Włodyka (red.) *System…, op. cit.,* Legalis.
[612] Wyrok Sądu Apelacyjnego w Katowicach z dnia 28 października 2009 r., V ACa 418/09. Orzeczenie dostępne na stronie internetowej http://www.katowice.sa.gov.pl/container/biuletyny//orzeczenia//2010//1//C//V_ACa_418-09.pdf.

usługi outsourcingowe zobowiązuje się do ich realizacji w zamian za wynagrodzenie lub zapłatę ceny[613].

W opracowaniach naukowych dotyczących outsourcingu wymienia się obszary działalności przedsiębiorstw, w których najczęściej korzysta się z opcji zlecenia prowadzenia określonych usług podmiotowi zewnętrznemu. Są to m. in. finanse i rachunkowość, sprawy kadrowe, marketing, obsługa prawna, zaopatrzenie i logistyka, usługi IT, ochrona, reklama, szkolenia, audyty[614]. Uszczegóławiając ten wątek, można powiedzieć, że umową outsourcingową zawieraną przez przedsiębiorstwo będzie dla przykładu: „zlecenie" obsługi prawnej, umowa o świadczenie usług informatycznych, umowa o serwisowanie maszyn, umowa o świadczenie usług księgowych, umowa na stałe zaopatrzenie w artykuły biurowe, umowa o świadczenie usług kurierskich itp. Typowymi podmiotami kreującymi stosunek outsourcingu są również: podmioty świadczące usługi reklamowe, prowadzące badania marketingowe, jednostki świadczące usługi marketingu bezpośredniego, podmioty zajmujące się tworzeniem i analizą baz danych oraz przechowujące i niszczące dokumenty i nośniki informacji[615].

W prawie Unii Europejskiej outsourcing został zdefiniowany w treści art. 2 pkt 6 Dyrektywy Komisji 2006/73/WE z dnia 10 sierpnia 2006 r. wprowadzającej środki wykonawcze do Dyrektywy 2004/39/WE Parlamentu Europejskiego i Rady w odniesieniu do wymogów organizacyjnych i warunków prowadzenia działalności przez przedsiębiorstwa inwestycyjne oraz pojęć zdefiniowanych na potrzeby tejże Dyrektywy. Outsourcing wyjaśniono jako dowolnego rodzaju umowę między przedsiębiorstwem inwestycyjnym i dostawcą usług, na podstawie której dostawca wykonuje proces, usługę lub działalność, które w innym przypadku zostałyby wykonane przez samo przedsiębiorstwo inwestycyjne. W powyższej definicji legalnej również można wskazać wymienione wcześniej elementy stosunku outsourcingu[616].

---

[613] J. Wiak [w:] A. Kidyba (red.), *Pozakodeksowe umowy handlowe*, Warszawa 2018, s. 378.

[614] M. Tyrańska, *Istota i znaczenie outsourcingu w działalności przedsiębiorstwa,* [w:] S. Wawak, M. Sołtysik (red.), *Współczesne…, op. cit.,* s. 13.

[615] A. Bąkowska, *Outsourcing a ochrona danych osobowych – wybrane zagadnienia* [w:] Biuletyn Bankowy 2005, nr 7/8, s.61.

[616] 1) stosunek zobowiązaniowy co najmniej dwóch podmiotów (dowolnego rodzaju umowa); 2) jeden podmiot jest przedsiębiorcą, a drugi podmiot znajduje się poza strukturą wewnętrzną pierwszego (między przedsiębiorstwem inwestycyjnym i dostawcą usług); 3) oba podmioty łączy stosunek partnerstwa ze względu na wspólny cel – zrealizowanie określonego działania przedsiębiorcy; 4) wydzielenie określonych zadań z całości działalności przedsiębiorcy (podmiot zewnętrzny działa na rzecz pierwszego); 5) przekazanie, zlecenie tych zadań podmiotowi zewnętrznemu (punkty 3-5 zawierają się we fragmencie

Outsourcing występuje na gruncie polskiego języka prawnego i pomimo braku polskiego odpowiednika ma swoją definicję ustawową. Sformułowana jest w treści art. 3 ust. 1 pkt 27 ustawy z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej[617], który stanowi, że outsourcing rozumiany jest jako umowa między zakładem ubezpieczeń albo zakładem reasekuracji a dostawcą usług, na podstawie której dostawca usług wykonuje proces, usługę lub działanie, które w innym przypadku zostałyby wykonane przez zakład ubezpieczeń lub zakład reasekuracji, a także umowę, na podstawie której dostawca usług powierza wykonanie takiego procesu, usługi lub działania innym podmiotom, za pośrednictwem których wykonuje on dany proces, usługę lub działanie. Z samego brzmienia przepisu wynika, że definicja ta jest użyteczna tylko na gruncie powołanej ustawy, jednakże można z niej wyinterpretować pewne ogólne elementy, które mogłyby stanowić podstawę definicji outsourcingu w oderwaniu od tej konkretnej ustawy. Są to: umowa między podmiotem zlecającym a dostawcą usług; wykonywanie usługi znajdującej się w zakresie podmiotu zlecającego przez dostawcę usługi; umowa między dostawcą usługi a podmiotem trzecim, któremu dostawca podzleca wykonanie usługi lub jej części, która została mu powierzona przez podmiot zlecający. Ponadto przepisy tej ustawy formułują wprost uprawnienie zakładu ubezpieczeń i zakładu reasekuracji do powierzania w drodze outsourcingu wykonywania czynności (art.73 DziałUbezpReasU: Zakład ubezpieczeń może, w drodze outsourcingu, powierzyć, w formie pisemnej, wykonywanie czynności ubezpieczeniowych). Przewidziane zostały również zasady outsourcingu (art. 74 DziałUbezpReasU), czy też kwestie odpowiedzialności (art. 76 DziałUbezpReasU). Przepisy ustawy przewidują również prawa i obowiązki stron umowy outsourcingu czynności ubezpieczeniowych (art. 74 DziałUbezpReasU).

Drugim przykładem jest outsourcing w działalności bankowej, który uregulowany jest w treści art. 6a-6d ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe[618], co było już przedmiotem rozważań we wcześniejszych rozdziałach dysertacji. Podkreślić jednakże należy, że nie występuje na gruncie tej ustawy pojęcie outsourcingu, a zastępuje je pojęcie powierzenia. Natomiast przedstawiciele nauki prawa nazywają to zagadnienie

dostawca wykonuje proces, usługę lub działalność, które w innym przypadku zostałyby wykonane przez samo przedsiębiorstwo inwestycyjne).

[617] T.j. Dz.U. z 2017 r. poz. 1170. Dalej jako DziałUbezpReasU.

[618] T.j. Dz. U. z 2017 r. poz. 1876.

outsourcingiem bankowym[619]. Zgodnie z przepisami bank może w drodze umowy agencyjnej powierzyć przedsiębiorcy wykonywanie w imieniu i na rzecz banku szeregu wymienionych w treści art. 6a ustawy czynności. O ile jednak rozwiązanie polegające na outsourcingu pewnych czynności może stanowić dla banku możliwość obniżenia kosztów własnego działania, to należy brać pod uwagę istotne ograniczenia korzystania z outsourcingu, z uwagi na to, że powierzenie dokonywania niektórych czynności bankowych będzie wymuszać środki mające na celu zabezpieczenie interesów banku i jego klientów[620].

Działalność polegająca na outsourcingu usług, stanowi też przedmiot regulacji zawartej w art. 46 ustawy z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi[621]. Dotyczy on umowy, której przedmiotem jest zlecenie zarządzania portfelem inwestycyjnym funduszu lub jego częścią, w przypadku specjalistycznego funduszu inwestycyjnego otwartego i funduszu inwestycyjnego zamkniętego. Ponadto obowiązuje art. 170 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[622], stanowiący, że przedsiębiorca telekomunikacyjny jest uprawniony do udzielania informacji o numerach abonentów lub powierzenia tej czynności innemu podmiotowi z zachowaniem wszystkich warunków i ograniczeń. Jak widać termin outsourcing w powołanych przepisach nie występuje. Jedynie ustawa o działalności ubezpieczeniowej i reasekuracyjnej bezpośrednio używa nazwy outsourcing, a ponadto definiuje to pojęcie. Outsourcing na gruncie prawa, ale już nie rangi ustawowej, jest zdefiniowany w treści Rozporządzenia Rady Ministrów w sprawie Polskiej Klasyfikacji Działalności z dnia 24 grudnia 2007 r.[623], gdzie w punkcie 6 części I Załącznika pojęcie to rozumiane jest jako zlecenie wykonania usług na zewnątrz, kontrakt, zgodnie z którym zleceniodawca wymaga od zleceniobiorcy wykonania określonego zadania, np. części lub całego procesu produkcyjnego, usług związanych z zatrudnieniem lub usług pomocniczych. Przykładami części procesu produkcyjnego, które mogą być zlecane do wykonania na zewnątrz może być: działalność wytwórcza, usługi związane z zatrudnieniem, usługi pomocnicze itp.

[619] G. Sikorski (red.), *Prawo bankowe. Komentarz*, Warszawa 2015, Legalis.
[620] *Ibidem*.
[621] T.j. Dz.U. z 2018 r. poz. 56. Dalej jako ustawa o funduszach.
[622] T.j. Dz.U. z 2017 r. poz. 1907.
[623] Dz.U. 2007 Nr 251, poz. 1885. Dalej jako Rozporządzenie PKD.

Na stosunek prawny outsourcingu warto spojrzeć przez pryzmat analizy podstawowych elementów tej umowy, tj. strony podmiotowej, przedmiotu i treści umowy outsourcingowej. Zaczynając od zakresu podmiotowego umowy outsourcingu, już na wstępie należy zauważyć, że nie ma jednolitości co do określeń stron tego instrumentu prawnego. W samych aktach prawnych dostrzega się różnorodność terminologiczną (w treści Rozporządzenia PKD mówi się o zleceniodawcy i zleceniobiorcy, w treści DziałUbezpReasU jest nazwana tylko jedna strona - dostawca usług). W literaturze przedmiotu wspomniany jest też powierzający i przyjmujący, przedsiębiorca zlecający i przedsiębiorca wykonujący usługę, albo określenia zaczerpnięte z języka angielskiego – *outsourcer* i *insourcer*[624].

Umowy outsourcingu to umowy zawierane w obrocie profesjonalnym lub też półprofesjonalnym. Trudno byłoby znaleźć możliwość i praktyczne zastosowanie outsourcingu w relacjach między konsumentami. Z poglądów przedstawicieli nauki prawa wynika niejednolite podejście do charakteru stron umowy. Z jednej strony twierdzi się, że podmiot powierzający wykonywanie czynności podmiotowi zewnętrznemu musi być przedsiębiorcą, zaś od podmiotu wykonującego usługi outsourcingowe nie wymaga się konieczności prowadzenia przedsiębiorstwa, jednakże w praktyce najczęściej jest on również profesjonalistą[625]. Z drugiej strony można powołać się na pogląd, zgodnie z którym umowa outsourcingu jest umową gospodarczą sensu *stricto*, ponieważ obaj kontrahenci są przedsiębiorcami[626].To stwierdzenie zostało potwierdzone w wyroku Sądu Apelacyjnego w Katowicach z dnia 28 października 2009 roku, w którym stwierdzono, że istotą outsourcingu jest jego zewnętrzność i równorzędny charakter stosunków pomiędzy przedsiębiorcą zlecającym a przedsiębiorcą przyjmującym zlecenie[627]. Zakres podmiotowy umowy outsourcingu najczęściej nie wskazuje, jakie podmioty mogą być jej stronami, co do zasady mogą to być osoby fizyczne, prawne, jednostki organizacyjne nie posiadające osobowości prawnej. Jednakże zdarzają się w tej kwestii wyjątki, które wynikać mogą z przepisów prawa, bądź też z samych zapisów umownych. Pierwszy rodzaj wyjątków pojawił się już wcześniej – w ustawie o funduszach (art. 45a i 46) jest mowa o tym, że umowa outsourcingu czynności związanych z działalnością prowadzoną przez towarzystwo może być zawarta tylko z podmiotem prowadzącym działalność maklerską

[624] J. Wiak [w:] A. Kidyba (red.), *Pozakodeksowe…, op. cit*., s. 381.
[625] *Ibidem*, s. 383.
[626] W. Robaczyński [w:]. W. J. Katner (red.) *System…, op. cit*., s. 470.
[627] V ACa 418/09. Orzeczenie dostępne na stronie internetowej http://www.katowice.sa.gov.pl/container/biuletyny//orzeczenia//2010//1//C//V_ACa_418-09.pdf.

w zakresie zarządzania portfelami. Po drugie, ograniczenia mogą wynikać z przepisów prawa dotyczących działalności regulowanych prawnie jak np. czynności doradztwa podatkowego mogą wykonywać określone osoby: osoby fizyczne wpisane na listę doradców podatkowych, adwokaci i radcowie prawni, biegli rewidenci (art. 2 i 3 ustawy z dnia 5 lipca 1996 r. o doradztwie podatkowym[628]). Po trzecie jest też możliwość, że postanowienia umowne będą ograniczały możliwości outsourcowania pewnych działań, np. umowa przedsiębiorcy z danym kontrahentem może zastrzegać osobiste świadczenie przedsiębiorcy bez posługiwania się osobą trzecią[629].

Jeśli chodzi o zakres przedmiotowy umowy outsourcingu, najogólniej stwierdza się, że co do zasady przedmiotem outsourcingu jest dokonywanie czynności faktycznych lub prawnych związanych z prowadzonym przez powierzającego przedsiębiorstwem[630]. Każdorazowo zakres umowy jest konkretyzowany na etapie ustaleń stron, a finalnie w jej treści. Od generalnej zasady istnieją wyjątki polegające na określeniu w przepisach prawa czynności, które mogą być zlecane do wykonania podmiotom spoza struktury przedsiębiorcy. Takie przypadki wynikają z powoływanych w tym rozdziale przepisów ustawy Prawo bankowe oraz ustawy o działalności ubezpieczeniowej i reasekuracyjnej. Po pierwsze, przepis prawa wskazuje, które konkretnie działania mogą zostać zlecone zewnętrznemu podmiotowi, tak jak w treści art. 73 ust. 1 DziałUbezpReasU odniesiono się np. do składania oświadczeń woli w sprawach roszczeń o odszkodowania lub inne świadczenia należne z tytułu umów. Po drugie, przepis prawa może formułować katalog czynności, których outsourcowanie jest dopuszczalne (w znaczeniu, że powierzanie innych czynności nie jest dopuszczalne), jak w treści art. 6a ust. 1 Prawa bankowego. Sytuacje, kiedy przepis prawa ingeruje w zakres przedmiotowy umowy outsourcingu, są rzadkie. Ograniczenia wynikają najczęściej z prawnej reglamentacji określonych rodzajów działalności.

W nauce prawa wskazuje się, że umowa outsourcingu, jako umowa niejednorodna, niepodlegająca ani kategorii umów nazwanych, ani nienazwanych, jest umową konsensualną, dwustronnie zobowiązującą, odpłatną i wzajemną[631]. Zasadniczo jej treść jest kształtowana przez jej strony w granicach swobody umów (inaczej może być w przypadku outsourcingu bankowego i ubezpieczeniowego kształtowanego na podstawie

[628] T.j. Dz.U. z 2018 r. poz. 377.
[629] W. Włodyka, M. Spyra [w:] M. Stec (red.), *Prawo…, op. cit*., s. 28.
[630] J. Wiak, [w:] A. Kidyba (red.), *Pozakodeksowe…, op. cit*., s. 385.
[631] W. Robaczyński [w:]. W. J. Katner (red.) *System…, op. cit*., s. 470.

wyżej powoływanych przepisów). O ile trudno jest w sposób ogólny mówić o prawach i obowiązkach stron umowy outsourcingu z uwagi na różnorodność takich umów, w literaturze przedmiotu odnaleźć można sformułowanie generalnych obowiązków powierzającego (zapłata wynagrodzenia lub ceny, przekazanie niezbędnych dokumentów i informacji do wykonania umowy), generalnych obowiązków wykonującego usługi (wykonanie lub osobiste wykonanie powierzonych czynności, stosowanie się do wskazówek powierzającego, zachowanie tajemnicy przedsiębiorstwa)[632]. W odniesieniu do sfery praw przedsiębiorcy wykonującego usługi można powiedzieć, że jego prawa stanowią korelat obowiązków podmiotu zlecającego, zaś prawa przedsiębiorcy zlecającego działania na zewnątrz są odzwierciedleniem obowiązków podmioty przyjmującego zlecenie. Istotnym elementem treści umowy outsourcingu jest zagadnienie tzw. suboutsourcingu, czyli „zlecenie" przez przedsiębiorcę wykonującego usługę outsourcingową określonych działań osobie trzeciej. Zgodny w nauce prawa jest pogląd, że podmiot wykonujący usługę ma obowiązek osobistego działania w wykonywaniu umowy, jednakże dopuszczalne jest powierzenie czynności podmiotowi trzeciemu, gdy wynika to z umowy, zwyczaju, lub też wykonawca umowy jest zmuszony do powierzenia działań podmiotowi wykonującemu usługi suboutsourcingowe (prawo to w odniesieniu do outsourcingu bankowego regulują odrębne zasady)[633].

Umowa outsourcingu nie jest umową nazwaną w przepisach obowiązującego prawa i może być realizowana poprzez różne konstrukcje prawne, w tym umowy zlecenia, o dzieło, świadczenia usług, umowy agencyjnej, przewozu, spedycji, składu[634]. Cele, które ma zrealizować umowa outsourcingu mogą więc być realizowane na podstawie kilku różnych umów, jednak związanych ze sobą. W praktyce jednak, z uwagi na to, że wykonywanie „zleconych" czynności będzie rozpatrywane w kategoriach umowy starannego działania, a nie rezultatu, umowa outsourcingu najczęściej będzie umową o świadczenie usług.

Przenosząc dotychczasowe rozważania na grunt ochrony danych osobowych, można powiedzieć, że cały szereg umów outsourcingu powiązany jest z tym, że „zlecane" na zewnątrz usługi (czynności, zadania) mają w swoim zakresie bezpośrednio lub pośrednio działania polegające na dokonywaniu operacji na danych osobowych.

[632] *Ibidem*.
[633] J. Wiak, [w:] A. Kidyba (red.), *Pozakodeksowe…, op. cit*., s. 392.
[634] *Ibidem*, s. 390-392.

Na podstawie obserwacji praktyki w zakresie wspierania podmiotów sektora prywatnego w dostosowywaniu swoich działalności do wymogów wynikających z przepisów o ochronie danych osobowych, jak również bazując na literaturze przedmiotu, można wymienić szeroki katalog sytuacji przekazywania podmiotowi zewnętrznemu wykonywania zadań angażujących dokonywanie operacji na danych osobowych (czyli sytuacji wymagających powierzenia przetwarzania danych osobowych). Wśród nich znajduje się „zlecenie" czynności związanych z rekrutacją pracowników, czynności związanych z tworzeniem, organizacją i zarządzaniem dokumentacją pracowniczą, z niszczeniem dokumentów i urządzeń oraz czynności związanych z obsługą klienta (np. call center, wysyłanie korespondencji), „zlecenie" procesów zarządzania siecią telekomunikacyjną, „zlecenie" usług księgowych, „zlecenie" windykacji należności[635]. W związku z tym, należy przewidzieć, by zlecenie usług podmiotowi zewnętrznemu uwzględniało również zlecenie przetwarzania danych osobowych, zgodnie z wymogami prawnymi zawartymi w treści art. 28 RODO. W przeciwnym wypadku, o ile podstawą „zlecenia" określonych zadań na zewnątrz byłaby zgodna z przepisami prawa umowa, to nie zachodzi żadna przesłanka legalizująca przetwarzanie danych osobowych przez podmiot zewnętrzny (jako konieczny element realizacji tych zadań). W związku z tym dochodzić może do nieuprawnionego ujawnienia danych osobom niepowołanym i przetwarzanie danych, co zgodnie z przepisami o ochronie danych osobowych jest nielegalne.

Na podstawie wyżej poczynionych ustaleń można wysunąć wniosek, że umowa outsourcingu bardzo często nie jest wystarczająca, aby stanowić podstawę zgodnego z wymogami prawnymi i efektywnego biznesowo stosunku zlecenia czynności podmiotowi zewnętrznemu. Niejednokrotnie potrzebne są dodatkowe elementy, aby określone czynności mogły być realizowane w poszanowaniu przepisów prawa. Takim elementem jest umowa powierzenia przetwarzania danych osobowych, jako instrument stanowiący niezbędne uzupełnienie umowy outsourcingu, jeśli do wykonywania zleconych zadań angażowane są dane osobowe, a realizacja tej drugiej umowy nie może mieć miejsca bez dokonywania operacji na danych. Z doświadczeń na gruncie praktyki można wywieść, że bardzo wiele umów z zakresu działania przedsiębiorstwa będzie wymagało uzupełnienia postanowieniami odnoszącymi się do powierzenia przetwarzania danych osobowych.

[635] A. Krasuski, *Outsourcing danych osobowych w działalności przedsiębiorstw*, Warszawa 2010, s. 35-36.

Ponadto praktyka wskazuje, że są dwa sposoby na osiągnięcie celu, jakim jest działanie w sposób zgodny z prawem i w poszanowaniu prawa osób fizycznych do ochrony informacji na ich temat. Po pierwsze będzie to zawarcie obok umowy outsourcingu drugiej umowy (powierzenia przetwarzania danych osobowych), która stanowi jej integralną część, a po drugie, zawarcie jednej umowy outsourcingowej, która w swojej treści zawierać będzie klauzule odnoszące się do powierzenia przetwarzania danych osobowych. Wybór jednego z powyższych rozwiązań nie powinien być dowolny, ale musi opierać się na podstawach, które będą spełniały wymogi wynikające przede wszystkim z zasady rozliczalności w aspekcie przetwarzania danych. Każdorazowo należy przeanalizować treść i okoliczności umowy zasadniczej na usługę, która jest zlecana podmiotowi zewnętrznemu. Praktycznie rzecz ujmując, możliwe są trzy scenariusze działania.

Po pierwsze, przedsiębiorca może zawrzeć umowę outsourcingu, której wykonywanie nie będzie angażowało przetwarzania danych osobowych. Przykładem takiej sytuacji może być np. zlecenie firmie serwisowej dokonywania przeglądu i napraw maszyn produkcyjnych. W tym przypadku nie ma potrzeby uzupełniania umowy zasadniczej dodatkowymi postanowieniami odnoszącymi się do zagadnienia powierzenia przetwarzania danych osobowych (gdyż żadne dane osobowe nie będą tu powierzane przez zewnętrznego przedsiębiorcę). Dla zabezpieczenia interesów administratora można ewentualnie wprowadzić do treści umowy outsourcingu klauzulę wyłączającą np. Strony uzgadniają że „zlecane" na podstawie niniejszej umowy działania polegające na serwisowaniu maszyn produkcyjnych nie będą wymagały dokonywania jakichkolwiek operacji na danych osobowych. Dodatkowym zabezpieczeniem dla administratora może być w takim przypadku również zawarcie w umowie o outsourcing klauzuli z upoważnieniem serwisantów do przebywania w obszarze przetwarzania danych osobowych (jeśli np. serwis dotyczy drukarek czy kserokopiarek w miejscu, gdzie dane osobowe są przetwarzane).

Po drugie, zawierana przez przedsiębiorcę umowa outsourcingu może dotyczyć takiej usługi, której realizacja może pociągać za sobą konieczność dokonywania operacji na danych osobowych, ale skala przetwarzania danych jest stosunkowo niewielka i przetwarzanie danych stanowi tylko ewentualność lub uzupełnienie działań podmiotu przyjmującego zlecenie. Jako przykład wskazać można zlecenie firmie zewnętrznej usługi helpdesk. Z uwagi na fakt, że outsourcowana usługa jedynie potencjalnie

i w ograniczonym do niezbędnego minimum zakresie może obejmować czynności mieszczące się w ramach przetwarzania danych, można przewidzieć, że wystarczające będzie uzupełnienie treści umowy outsourcingu o klauzule dotyczące powierzenia danych (odpowiadające co najmniej minimalnym wymogom art. 28 RODO - przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora). Przykładowym rozwiązaniem jest dodanie do treści umowy outsourcingu paragrafu zatytułowanego Ochrona danych osobowych. Należałoby zawrzeć w nim przede wszystkim wskazanie, że realizacja zleconej usługi wymaga powierzenia danych osobowych zgodnie z treścią art. 28 RODO i ustalenie statusu stron: administratorem powierzanych danych jest podmiot zlecający, natomiast przetwarzającym jest podmiot przyjmujący zlecenie. Ponadto trzeba ukształtować sferę praw administratora (np. uprawnienia kontrolne, prawo do wyłączenia możliwości podpowierzania danych) oraz sferę praw przetwarzającego (np. prawo do podpowierzenia przetwarzania danych), jak również ustalić sferę obowiązków administratora (np. wydawanie poleceń przetwarzającemu, zapewnienie kontroli nad wprowadzaniem i przekazywaniem danych) oraz sferę obowiązków przetwarzającego (np. zobowiązanie do upoważnienia swoich pracowników do przetwarzania powierzonych danych). Następnie należy sformułować zapis dotyczący tego, jakie dane zostają powierzone (kategorie danych zwykłych lub wrażliwych, poszczególne rodzaje danych), jak również kategorie osób, których powierzone dane dotyczą (np. dłużnicy podmiotu zlecającego), jak również uszczegółowienie operacji, jakie może na powierzonych danych dokonywać podmiot przyjmujący zlecenie, a także określić, czy przetwarzanie ma mieć charakter czynności jednorazowej czy stałej, czy i jakie technologie angażuje. Wymagane jest też sformułowanie, w jakim celu następuje powierzenie – realizacja konkretnych zadań wynikających z umowy outsourcingu (np. windykacja należności podmiotu zlecającego) oraz ustalenie na jak długo dane osobowe są powierzane (najczęściej na czas zawarcia umowy outsourcingu) i co stanie się z danymi po zakończeniu umowy.

Po trzecie, możliwym działaniem jest też zawarcie odrębnej umowy powierzenia przetwarzania danych osobowych (czyli strony stosunku zlecenia prowadzenia usług przedsiębiorstwa na zewnątrz *de facto* zawierają dwie umowy). Z uwagi na jej akcesoryjny charakter, umowa powierzenia (co należy zaznaczyć w umowie zasadniczej) będzie integralną częścią zasadniczej umowy outsourcingowej, nie będzie stanowiła samoistnego stosunku prawnego, ale będzie uzupełniała zasadniczą relację między podmiotami outsourcingu. Wydaje się, że odrębnej umowy wymagać będzie zlecenie takiej usługi,

której realizacja w przeważającej części opierać się będzie na przetwarzaniu danych osobowych, bez dostępu do danych usługa ta nie będzie mogła być świadczona. Przykładem jest „zlecenie" przez przedsiębiorcę prowadzenia usług kadrowo-płacowych biuru rachunkowemu. Nie ma *de facto* możliwości realizacji tej usługi bez dostępu do danych osobowych, praktycznie rzecz biorąc każda czynność biura będzie mogła być dokonywana w oparciu o przetwarzanie danych osobowych. Dlatego dostrzega się tu potrzebę zawarcia umowy powierzenia przetwarzania danych osobowych odrębnej od umowy outsourcingu, że usługa w takim stopniu opierająca się na danych osobowych powierzanych przez administratora wymaga obwarowania szczegółowymi klauzulami w zakresie ochrony danych osobowych (w tym zobowiązania powierzającego, postanowienia o przestrzeganiu zasad poufności, szczegółowo określona odpowiedzialność stron), może stanowić zagrożenie dla bezpieczeństwa danych osób, których dane są powierzane. W odrębnej umowie stanowiącej integralną część umowy outsourcingu można na dużym poziomie szczegółowości określić zasady współpracy stron.

Umowa outsourcingu (w sensie ogólnym) oraz umowa powierzenia przetwarzania danych osobowych mają w swoich konstrukcjach kilka cech wspólnych. W przypadku obydwu rodzajów umów mamy do czynienia z uprawnieniem jednego podmiotu do zlecenia pewnych działań innemu podmiotowi. Zarówno w umowie outsourcingu, jak i umowie powierzenia dopuszczalne jest dalsze zlecenie wykonywania przedmiotu umowy podmiotowi trzeciemu (podzlecenie, podpowierzenie danych). Podobnie jest również rozwiązana kwestia odpowiedzialności – ani powierzenie przetwarzania danych ani powierzenie czynności w ramach outsourcingu nie powoduje, że podmiot zlecający działania przenosi swoją odpowiedzialność na kontrahenta. Ponadto przepisy prawa mogą ograniczać możliwość zlecania określonych czynności innemu podmiotowi - w przepisach szczególnych można znaleźć zakaz powierzania przewarzania danych osobowych przez detektywów. Istotna kwestia różniąca oba zagadnienia polega na tym, że umowa outsourcingu (w sensie ogólnym) polega na tym, że podmiot wykonuje powierzone czynności we własnym imieniu a na rzecz podmiotu zlecającego. Natomiast w przypadku stosunku prawnego powierzenia przetwarzania danych osobowych, przetwarzający działa w imieniu administratora danych i na rzecz administratora[636]. Nie wolno pominąć bardzo wyraźnej różnicy, polegającej na tym, że umowa outsourcingu jest umową samodzielną,

[636] M. Sakowska-Baryła, *Prawo…, op. cit*., s. 155.

realizuje cel założony przez przedsiębiorcę zlecającego usługę. Natomiast umowa powierzenia jest umową towarzyszącą umowie outsourcingu, której celem jest przede wszystkim zalegalizowanie przekazania danych innemu podmiotowi niż administrator i zabezpieczenie tych danych, nie jest jej celem to by dane były przetwarzane przez inny podmiot.

Dzisiejsze wymagania rynku usług są wysokie, co coraz częściej skłania podmioty do ukierunkowywania swoich usług, by podnieść poziom ich zaawansowania i jakości[637]. W przypadku podmiotów tak sektora prywatnego, jak i publicznego, przetwarzanie danych osobowych stanowi jeden z aspektów ich działalności, nie musi należeć do działalności głównej (innymi słowy przetwarzanie najczęściej nie stanowi głównego celu działalności przedsiębiorcy, ale jego główna działalność angażuje w większym bądź mniejszym stopniu operacje na danych). Jak wykazano już wcześniej, według przepisów o ochronie danych osobowych, administrator danych osobowych ma możliwość przekazania tych danych podmiotowi trzeciemu, który będzie je przetwarzał w imieniu administratora. Można też wyciągnąć wniosek, że coraz częściej przedsiębiorcy szukają na rynku wyspecjalizowanych partnerów, którym mogą „zlecić" część swojej działalności, która w sposób bezpośredni lub pośredni wiąże się z przetwarzaniem danych[638]. Umowa powierzenia przetwarzania danych osobowych jest instrumentem, który umożliwia outsourcing w poszanowaniu prawa. Niezastosowanie tego narzędzia przy zlecaniu określonych czynności podmiotom zewnętrznym może powodować naruszenie przepisów i związaną z tym odpowiedzialność cywilną, administracyjną i karną, a także inne konsekwencje jak utrata dobrej opinii i zaufania klientów, straty finansowe.

2. Zastosowanie umowy powierzenia przetwarzania danych osobowych w sferze usługi hostingu

W dobie szybkiego rozwoju nowoczesnych technologii, jak i funkcjonowania społeczeństwa informacyjnego, codziennością stało się to, że część usług świadczonych przez podmioty obrotu gospodarczego dostępnych jest za pomocą sieci Internet. Usługi te opierają się o udostępnianie informacji w sieci a jedną z nich jest usługa hostingu. Ma ona bardzo istotne znaczenie w obszarze prawa internetu, z uwagi na to, że twórcy

[637] A. Śleszyńska, *Instytucja…, op. cit*.
[638] *Ibidem.*

różnorodnych treści potrzebują przestrzeni by umieszczać te treści i udostępniać je innym użytkownikom[639]. Celem niniejszych rozważań jest potwierdzenie tezy, ze hosting stanowi jedno z zastosowań umowy powierzenia przetwarzania danych osobowych. Bez klauzul dotyczących powierzenia umowa hostingu jest niezupełna i może spotkać się z zarzutami dotyczącymi nieuprawnionego dostępu do danych osobowych podmiotu świadczącego usługę hostingu.

Rozważania należy rozpocząć od ustalenia znaczenia pojęcia hosting. Z uwagi na brak definicji legalnej pojęcia hosting na gruncie polskiego prawa, dla potrzeb prowadzonych analiz trzeba posiłkować się przede wszystkim poglądami przedstawicieli nauki prawa i autorów opracowań o charakterze publicystycznym, ale również orzeczeniami sądów (ponieważ zdarza się, że zagadnienie hostingu stanowi przedmiot rozstrzygnięć sądowych). W pierwszej kolejności analizy pod kątem wskazówek definicyjnych wymagają akty prawne, bezpośrednio lub pośrednio zawierające podstawy prawne umów hostingowych.

W 2000 roku weszła w życie Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym)[640]. Zgodnie z art. 14 Dyrektywy 2000/31/WE Państwa Członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę usługodawca nie był odpowiedzialny za informacje przechowywane na żądanie usługobiorcy, pod warunkiem wystąpienia dwóch wymienionych sytuacji[641]. Nie można stwierdzić, że powołany przepis stanowi legalną definicję hostingu, ale bez wątpienia zatytułowanie art. 14 Dyrektywy słowem „hosting" i opisanie zagadnienia jako usługi społeczeństwa informacyjnego polegającej na przechowywaniu informacji przekazanych przez usługobiorcę, przybliża pojęcie hostingu na gruncie prawa Unii Europejskiej.

---

[639] P. Polański, *Uwagi na temat odpowiedzialności usługodawcy hostingu w Intenecie*, [w:] J. Gołaczyński (red.), *Informatyzacja postępowania sądowego i administracji publicznej*, Warszawa 2010, s. 299.
[640] Dz.Urz.UE.L 2000 Nr 178, str. 1, dalej jako Dyrektywa 2000/31/WE.
[641] a) usługodawca nie ma wiarygodnych wiadomości o bezprawnym charakterze działalności lub informacji, a w odniesieniu do roszczeń odszkodowawczych - nie wie o stanie faktycznym lub okolicznościach, które w sposób oczywisty świadczą o tej bezprawności; lub b) usługodawca podejmuje niezwłocznie odpowiednie działania w celu usunięcia lub uniemożliwienia dostępu do informacji, gdy uzyska takie wiadomości lub zostanie o nich powiadomiony.

Do polskiego porządku prawnego przepisy Dyrektywy 2000/31/WE zaimplementowano poprzez ustawę z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2017 r. poz. 1219)[642]. Ustawodawca nie użył w niej słowa hosting, ale wyinterpretować można, że odpowiednikiem art. 14 Dyrektywy jest art. 14 UsługiElektrU. W porównaniu do przepisu Dyrektywy w jego treści, ustawodawca mniej szczegółowo określił ramy definicyjne hostingu, stanowiąc, że nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności. Z zacytowanego przepisu ustawy można wywnioskować, że hosting może być rozumiany jako udostępnianie zasobów systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę. Podkreślić warto, że z uwagi na fakt, iż hosting nie mieści się w definicji usługi telekomunikacyjnej[643], ponieważ jego zakres wykracza poza przekazywanie sygnałów w sieci telekomunikacyjnej, to nie można zakwalifikować go do umów o świadczenie usług telekomunikacyjnych, zatem nie będą stosowane do niego przepisy ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907).

W nauce prawa pojęcie hostingu jest różnie ujmowane. Analiza literatury przedmiotu pozwala oprzeć dalsze rozważania na kilku sposobach rozumienia hostingu. Jest to umowa o udostępnienie przestrzeni na serwerze i przechowywanie na nim danych, w które usługodawca przekazuje usługobiorcy przestrzeń na dysku, w calu zamieszczenia na nim informacji w Internecie, aby następnie udostępniać je osobom trzecim[644]. Zgodnie z innym poglądem hosting to zasadniczo odpłatne udostępnianie powierzchni dyskowych serwerów wraz ze stworzeniem możliwości utrzymywania na nich poczty elektronicznej usługobiorcy lub serwisów internetowych, na które mogą składać się strony internetowe, konta FTP lub bazy danych, narzędzia webowe itp[645], albo też oddanie do dyspozycji określonej przestrzeni dysków twardych[646]. W opracowaniach GIODO odnaleźć można

[642] Dalej jako UsługiElektrU.
[643] Art. 2 pkt 41 Ustawy Prawo telekomunikacyjne: świadczenie usług telekomunikacyjnych - wykonywanie usług za pomocą własnej sieci, z wykorzystaniem sieci innego operatora lub sprzedaż we własnym imieniu i na własny rachunek usługi telekomunikacyjnej wykonywanej przez innego dostawcę usług, art. 2 pkt 48: usługa telekomunikacyjna - usługę polegającą głównie na przekazywaniu sygnałów w sieci telekomunikacyjne.
[644] J. Gołaczyński [w:] W. J. Katner (red., System…, tom IX, op. cit., s. 491.
[645] P. Dynowski, I. Kowalczuk-Pakuła, G. Pacek, *Poradnik prawny dla e-biznesu*, Warszawa 2016, s. 272.
[646] J. Gołaczyński (red.), *Sporządzanie umów elektronicznych*, Warszawa 2017, s. 23.

wyjaśnienie hostingu jako dzierżawy miejsca na serwerze i świadczenia usług dostępu do tych serwisów z Internetu[647]. Serwery są zazwyczaj zasobem własnym dostawcy usług hostingowych i zlokalizowane są w określonych miejscach. Usługa hostingu prowadzona jest też z wykorzystaniem tzw. centrum danych (ang. *data center*, DC), które jest budynkiem lub jego częścią, składającą się z serwerowni (ang. *computer room*) oraz obszarów wspierających funkcjonalność całego centrum[648]. Niektórzy dostawcy usług hostingowych dysponują nawet kilkoma centrami danych, znajdującymi się w różnych lokalizacjach[649]. Podsumowując powyższe ustalenia można stwierdzić, że niezbędnymi elementami hostingu są: miejsce na serwerze w centrum danych, zamieszczenie tam informacji, udostępnienie tych informacji innym za pomocą Internetu. Brak któregokolwiek z wymienionych nie pozwala na kwalifikowanie danego działania jako usługę hostingu. Hosting w wielu publikacjach zestawiany jest z tzw. cachingiem. Obie usługi różni to, że hosting polega na przechowywaniu i udostępnianiu danych innym podmiotom w sposób nieograniczony w czasie, natomiast caching, najogólniej ujmując, to automatyczne, czasowe i pośrednie przechowywanie danych[650].

Hosting, jak wspomniano, stanowi również przedmiot orzeczeń sądowych. Dla przykładu przytoczyć można stanowisko Sądu Apelacyjnego w Warszawie z dnia 10 października 2013 roku, który uznał, że usługę hostingu należy raczej upatrywać w udostępnianiu zawartości systemu teleinformatycznego, oraz że Sąd I instancji nietrafnie utożsamił usługę hostingu jedynie z przechowywaniem danych usługobiorców (precyzyjniej udostępnieniem pamięci podłączonych do sieci serwerów w celu przechowywania na nich materiałów pochodzących od dostawców treści), bo jego istotę stanowi również ich udostępnianie w taki sposób, aby każdy mógł mieć do niego dostęp w miejscu i czasie przez siebie wybranym[651]. Jak widać, problemem natury praktycznej bywa rozpoznanie, co *de facto* wchodzi w zakres usługi hostingu. Z powyższego orzeczenia wynika, że hosting powinien być traktowany stosunkowo szeroko – jako udostępnienie przestrzeni do przechowywania danych, jak również udostępnianie tych danych osobom trzecim.

---

[647] A. Kaczmarek, *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Warszawa 2007, s. 48, opracowanie dostępne na stronie internetowej GIODO: https://giodo.gov.pl/data/filemanager_pl/1057.pdf.
[648] https://www.computerworld.pl/news/Czym-rozni-sie-serwerownia-od-centrum-danych,369934.html.
[649] Więcej informacji np. na stronie internetowej https://home.pl/firma/datacenter.
[650] G. Pacek, Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych, tekst dostępny na stronie internetowej http://www.bibliotekacyfrowa.pl/dlibra/doccontent?id=23622.
[651] I ACa 689/13, Legalis nr 775991.

W praktyce życia codziennego hosting najbardziej kojarzy się z funkcjonowaniem stron internetowych, umieszczonych w sieci na serwerach, które oferowane są serwisom internetowym w ramach usług hostingowych. Jednakże w literaturze przedmiotu wskazuje się wiele przykładów zastosowania tego typu usług. Uznaje się, że mianem usług hostingowych mogą być określane usługi należące do tak szerokiego spektrum stanów faktycznych, jak prowadzenie serwisu grup dyskusyjnych, prowadzenie systemu aukcji internetowych, prowadzenie serwisu społecznościowego, w którym użytkownicy zamieszczają informacje, czy prowadzenie serwisu umożliwiającego tworzenie tzw. blogów[652]. W czasopismach branżowych wskazuje się na różnorodność hostingu, wskazując ponadto jako przykład usługę współdzielenia plików w sieci – oferowaną przez przedsiębiorcę, którego odbiorca zwykle utożsamia z witryną sieciową umożliwiającą umieszczenie danych w sieci i następnie uzyskanie linku, pozwalającego na przeglądanie danych czy pobranie ich. W tym przypadku odbiorcą jest końcowy klient, natomiast przedsiębiorca nie musi sam dysponować serwerami, bo również może korzystać z usług hostingowych świadczonych przez inny podmiot[653]. Hosting definiują również sami dostawcy tych usług. Według home.pl hosting www (inaczej hosting internetowy, web hosting, serwer www) to przestrzeń, w której można umieścić dane – stronę WWW, sklep internetowy, prywatne pliki. To także miejsce, gdzie może znaleźć się poczta elektroniczna z adresem we własnej domenie[654]. Nazwa.pl określa hosting jako usługę serwera to usługa polegająca na oddaniu Klientowi do korzystania powierzchni dysku oraz uruchomieniu dostępnych usług wyspecyfikowanych na stronach WWW nazwa.pl oraz zgodnych z parametrami bezpieczeństwa[655]. Poza główną usługą hostingu (przestrzeń na serwerze, pojemność konta) niejednokrotnie oferowane są również usługi uboczne, w ramach których mieszczą się m.in. pomoc techniczna, kreator stron i aplikacje, nielimitowana liczba kont e-mail, ochrona przed spamem i wirusami, regularne kopie bezpieczeństwa[656] (dwie ostatnie opcje są bardzo istotne z perspektywy ochrony danych osobowych).

Strony umowy hostingu wskazuje w sposób bardzo ogólny treść art. 2 pkt 6 i 7 UsługiElektrU. Po jednej stronie występuje usługodawca - osoba fizyczna, osoba prawna

[652] P. Litwiński, *Hosting danych osobowych. Zagadnienia podstawowe,* w: Monitor Prawniczy 2008 nr 23, Legalis.
[653] http://www.komputerswiat.pl/jak-to-dziala/2015/06/hosting.aspx.
[654] https://home.pl/hosting
[655] https://www.nazwa.pl/fileadmin/nazwa/Regulaminy/Regulamin_uslugi_serwera.pdf
[656] https://www.cal.pl/hosting-serwery-shared

albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługi drogą elektroniczną. Po drugiej natomiast usługobiorca - osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która korzysta z usługi świadczonej drogą elektroniczną. Oznacza to, że stronami umów hostingowych mogą być podmioty, których forma organizacyjna nie ma znaczenia, chociaż usługa hostingu jest realizowana w ramach działalności gospodarczej[657]. Ten szeroki katalog podmiotów może potencjalnie zostać zawężony poprzez wyłączenie zawarte w art. 3 pkt 2 UsługiElektrU. Przepisów ustawy nie stosuje się do: używania poczty elektronicznej lub innego równorzędnego środka komunikacji elektronicznej między osobami fizycznymi, w celach osobistych niezwiązanych z prowadzoną przez te osoby, chociażby ubocznie, działalnością zarobkową lub wykonywanym przez nie zawodem. Można zatem wyciągnąć wniosek, że usługa hostingu nie będzie miała podstawy prawnej w UsługiElektrU w przypadku jej zawierania w obrocie konsumenckim (między konsumentami). Co najmniej usługodawca musi być przedsiębiorcą.

Przedmiot umowy hostingu to świadczenie, które polega generalnie na przechowywaniu danych osób trzecich[658]. Obejmuje on udostępnianie rodzajowo określonej przestrzeni na serwerze, którym dysponuje dostawca usługi i przechowywanie w niej określonych danych[659]. Pomimo braku świadomości, każdy użytkownik Internetu korzysta z usług hostingowych praktycznie codziennie. Najlepszym przykładem jest przechowywanie poczty email na przeznaczonych do tego serwerach zewnętrznych, dokonywanie zakupów w sklepach internetowych. Przedmiot umowy jest w aspekcie rynku usług hostingowych bardzo zróżnicowany. Z uwagi na rosnącą konkurencję, dostawcy usług oferują coraz to większe przestrzenie, nowe rodzaje usług (hosting współdzielony, VPS – wirtualny serwer prywatny, hosting dedykowany) i nowe rozwiązania (backup automatyczny, certyfikat SSL, pomoc techniczna, statystyki stron). Co należy koniecznie podkreślić, przedmiotem przechowywania i udostępniania w ramach usługi hostingu mogą być dane osobowe – potencjalny zakres sytuacji, w których będzie dochodziło do przechowywania i udostępniania danych osobowych na zasadzie hostingu jest bardzo szeroki[660]. Mieści się w nim hosting jako sposób działania tak podmiotów

[657] J. Gołaczyński [w:] W. J. Katner (red.), *System…*, tom IX, *op. cit.,* s. 497-498.
[658] J. Gołaczyński (red.), *Sporządzanie…, op. cit*., s. 23.
[659] J. Gołaczyński [w:] W. J. Katner (red.), *System…*, tom IX, *op. cit.,* s. 501.
[660] P. Litwiński, *Hosting…, op. cit*., Legalis.

sektora publicznego, jak i prywatnego, a nawet konsumentów. Dla przykładu wymienić można korzystanie z usług wyspecjalizowanych podmiotów zewnętrznych przez organy władzy publicznej celem udostępniania systemów teleinformatycznych do wpływu wniosków, w tym działanie Biuletynu Informacji Publicznej; prowadzenie internetowych stron o charakterze informacyjnym, które zawierają dane osobowe kontaktowe (np. dane osób wchodzących w skład organów osoby prawnej); udostępnianie w Internecie baz danych osobowych (np. internetowe książki telefoniczne), jak również portale społecznościowe[661].

Trzecim klasycznie wyodrębnianym elementem każdego stosunku prawnego jest treść, na którą składają się prawa i obowiązki stron. Jako pierwsze bardzo skrótowo wymienić można obowiązki dostawcy usług hostingowych. Są to przede wszystkim obowiązki o charakterze informacyjnym. Zgodnie z art. 6 UsługiElektrU jest to zapewnienie dostępu do aktualnej informacji o szczególnych zagrożeniach związanych z korzystaniem z usługi świadczonej drogą elektroniczną), ale też zawarte w art. 7 UsługiElektrU zapewnienie działanie systemu teleinformatycznego, albo w art. 8 UsługiElektrU: określenie regulaminu świadczenia usług drogą elektroniczną. Z umowy wynikać może dużo więcej zobowiązań usługodawcy jak np. archiwizacja danych, okresowe tworzenie kopii zapasowych. Po stronie usługobiorcy znajduje się obowiązek wypłaty wynagrodzenia w umówionej kwocie i terminach (jest to jednocześnie uprawnienie usługodawcy). Natomiast w sferze uprawnień usługobiorcy wskazać można dla przykładu prawo do uzyskania zdalnego dostępu do serwera, prawo do uzyskania pomocy ze strony administratora serwera, prawo do korzystania z dodatkowych usług[662].

Co bardzo ważne z perspektywy przedmiotowej problematyki ochrony danych osobowych, w motywie 14 preambuły Dyrektywy 2000/31/WE, przewidziano, że zarówno przepisy Dyrektywy 95/46/WE, jak i pozostającej poza zakresem prowadzonych rozważań Dyrektywy 97/66/WE, mają pełne zastosowanie do usług społeczeństwa informacyjnego. Dyrektywy te stanowią już wspólnotowe ramy prawne w dziedzinie danych osobowych, dlatego nie jest konieczne obejmowanie tego zagadnienia dyrektywą 2000/31/WE w celu zapewnienia sprawnego funkcjonowania rynku wewnętrznego, w szczególności swobodnego przepływu danych osobowych między Państwami Członkowskimi. Wykonywanie i stosowanie niniejszej dyrektywy 2000/31/WE powinny być całkowicie

[661] *Ibidem*.
[662] J. Gołaczyński [w:] W. J. Katner (red.), *System*…, tom IX, *op. cit*., s. 500.

zgodne z zasadami odnoszącymi się do ochrony danych osobowych. Oznacza to, że usługa społeczeństwa informacyjnego, do których zgodnie z treścią art. 14 Dyrektywy 2000/31/WE zaliczany jest hosting, należy stosować przepisy o ochronie danych osobowych. Na gruncie polskich przepisów powyższa regulacja funkcjonuje poprzez implementację w treści art. 16 UsługiElektrU, stanowiącego, że do przetwarzania danych osobowych w związku ze świadczeniem usług drogą elektroniczną, stosuje się przepisy tej ustawy o ochronie danych osobowych (aktualnie RODO). Dla prowadzonych rozważań jest to równoznaczne z tym, że jeśli hosting obejmuje również dane osobowe (a w zdecydowanej części przypadków właśnie tak jest), to umowa hostingu musi uwzględniać przepisy o ochronie danych osobowych, a w tym regulacje dotyczące powierzania danych osobowych przez administratora podmiotowi zewnętrznemu. Stanowi to argument potwierdzający tezę o zastosowaniu umowy powierzenia przetwarzania danych osobowych w świadczeniu usług hostingu. Należy przyjrzeć się przykładowej sytuacji, kiedy administrator danych osobowych (np. prowadzący sklep elektroniczny) podejmuje decyzję o zmianie dotychczasowego dostawcy usługi hostingu sklepu internetowego i jednocześnie warunków hostingu (decyzja o środkach przetwarzania danych osobowych). Umieszczenie witryny sklepu na serwerze dostawcy usługi hostingu oznacza jednocześnie, że dane osobowe klientów tego sklepu będą przechowywane w centrum danych, na serwerze dostawcy („zlecenie" przechowywania danych osobowych przez administratora podmiotowi zewnętrznemu). Przechowywanie jest czynnością mieszczącą się w zakresie definicji przetwarzania danych osobowych. Wszystko to prowadzi do wniosku, że hosting jako udostępnienie przestrzeni na serwerze i przechowywanie na nim danych pociąga za sobą konieczność powierzenia przetwarzania danych osobowych. Dzięki niej hostingodawca będzie mógł legalnie przechowywać dane, jak również (zgodnie z założeniami) zapewnione zostaną gwarancje bezpieczeństwa przetwarzanych danych przez dostawcę usługi hostingu, a administrator będzie upoważniony do kontroli kontrahenta. W związku z tym umowa powierzenia przetwarzania danych osobowych ma zastosowanie w przypadku świadczenia usług hostingowych.

Praktyka jest jednakże niejednolita i usługodawcy usług hostingowych różnie podchodzą do kwestii ochrony danych osobowych w ramach świadczonych usług hostingu. Jako przykład, w jaki sposób usługodawcy hostingu mogą kreować stosunek prawny z usługobiorcą w aspekcie dotyczącym ochrony danych osobowych,

przeanalizować można fragment treści regulaminu usługi hostingu dedykowanego[663] oferowanego przez jednego z kluczowych usługodawców usług hostingowych w Polsce – home.pl.

Uwagę przykuwa przede wszystkim punkt 1 w sekcji Ochrona danych osobowych, gdzie za podstawę legalizującą przetwarzanie danych osobowych przez dostawcę usługi hostingowej (tu operatora), uznaje się zgodę usługobiorcy (tu abonenta). Oświadcza on, że wyraża zgodę na przetwarzanie danych osobowych przez operatora w zakresie koniecznym do prawidłowego wykonania Usługi oraz wyraża zgodę na przekazanie i powierzenie ich przetwarzania innym podmiotom w celu i w zakresie koniecznym do prawidłowego i należytego wykonania Usługi, w tym Partnerom, rejestrom, podmiotom należącym do grupy kapitałowej do której należy operator[664]. Wydaje się, że zgodna nie jest tu właściwą podstawą prawną, skoro zgodnie z treścią art. 6 ust. 1 lit. a RODO aby przetwarzanie było zgodne z prawem, to osoba, której dane dotyczą ma wyrazić zgodę na przetwarzanie swoich danych osobowych. Usługobiorca nie może wyrazić zgody na przetwarzanie danych osobowych osób, które pozostawiają swoje dane osobowe np. za pośrednictwem formularza kontaktowego zawartego na stronie internetowej Usługobiorcy, na serwerze dostawcy usługi hostingowej. W związku z tym, spore wątpliwości budzi wyrażenie zgody przez abonenta, chyba że jest on osobą fizyczną i chodzi o umieszczenie jego danych osobowych na serwerze dostawcy usług hostingowych. Opierając się na doświadczeniu, intuicji i logice, wydaje się, że chodzi tu jednak o dane osobowe osób trzecich, które abonent jako administrator danych przechowywać będzie w ramach hostingu na serwerze. Dlatego też zgoda nie jest podstawą prawną, która legalizuje przetwarzanie danych osobowych przez dostawcę usługi hostingowej. Ponadto, w treści

[663] Całość Regulaminu dostępna na stronie https://home.pl/regulaminy/nowyhd. Fragment dotyczący ochrony danych osobowych: 1. Operator na podstawie zgody Abonenta, o której mowa w pkt II.5.c przetwarza dane osobowe w zakresie koniecznym do prawidłowego wykonania Usługi oraz przekazuje lub powierza ich przetwarzanie innym Podmiotom w celu i w zakresie koniecznym do prawidłowego i należytego wykonania Usługi. 2.Dane są przetwarzane zgodnie z zasadami wskazanymi w ustawie o ochronie danych osobowych i ustawie o świadczeniu usług drogą elektroniczną. 3.Operator przed rozpoczęciem przetwarzania danych podejmie środki zabezpieczające zbiór danych, o których mowa w art. 36-39 ustawy z dnia 29 sierpnia 1997 r o ochronie danych osobowych, oraz spełni wymagania określone w przepisach, o których mowa w art. 39a ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. 4. Operator oraz Podmioty, o których mowa w pkt IV. 1 są uprawnieni do przetwarzania danych przekazanych przez Abonenta wyłącznie w zakresie czynności podejmowanych w celu należytego wykonania Usługi. 5.Operator oraz podmioty, o których mowa w pkt IV. 1 zapewnią staranne zabezpieczenie danych przed dostępem osób nieuprawnionych oraz kontrole i nadzór przebiegu procesu przetwarzania na każdym jego etapie. 6. Operator nie ponosi odpowiedzialności za odpowiednie zabezpieczenie zbioru w systemie informatycznym Abonenta oraz w systemie informatycznym Abonenta w części zarządzanej przez Abonenta"

[664] *Ibidem.*

punktu 1 zapisano również, że operator na podstawie zgody abonenta przekazuje lub powierza przetwarzanie danych innym Podmiotom. Zaznaczyć należy, że powierzenie przetwarzania danych osobowych następuje nie na podstawie zgody, a w drodze umowy. Rozwiązaniem w takiej sytuacji wydaje się powierzenie przetwarzania danych osobowych w drodze umowy zawartej zgodnie z treścią art. 28 RODO. W takim układzie abonent jest administratorem danych osobowych (bo w sposób faktyczny decyduje o celach i sposobach przetwarzania danych – przechowywanie określonego zakresu danych na serwerze dostawcy usługi hostingowej w określonym celu i czasie), operator jest podmiotem przetwarzającym (bo na zlecenie administratora przetwarza dane osobowe uwzględniając określony przez niego zakres, cel, okres przetwarzania). Warte odnotowania jest również to, że w aspekcie art. 28 ust. 1 RODO, to czy i jak usługodawcy usług hostingowych gwarantują spełnianie wymogów określonych w przepisach o ochronie danych osobowych, powinno stanowić kryterium, które usługobiorca powinien rozpatrzyć niemalże w pierwszej kolejności w sytuacji gdy będą decydować o wyborze konkretnego usługodawcy.

Podsumowując, można powiedzieć, że zawarcie umowy powierzenia przetwarzania danych osobowych z dostawcą usług hostingowych jest *de facto* obowiązkiem usługobiorcy (administratora danych), który wywodzi się z przepisów o ochronie danych osobowych (art. 28 RODO), a nie z przepisów UsługiElektrU. Faktycznie nie w każdym przypadku obowiązek ten będzie aktualny. Podobnie jak w kontekście umów o outsourcing, w aspekcie umów hostingowych również możliwe są trzy scenariusze działania. Może się zdarzyć, że przedmiotem hostingu będzie udostępnienie przestrzeni na serwerze dedykowanej stronie internetowej, która w żadnym stopniu nie będzie dotyczyła danych osobowych osób fizycznych (np. witryna przedsiębiorstwa zajmującego się sprzedażą artykułów budowlanych jedynie dużym podmiotom gospodarczym (spółkom). Drugą potencjalną możliwością jest sytuacja, kiedy dostawca usługi hostingu nie ma wiedzy na temat tego, jakie konkretnie treści będą umieszczane na serwerze w ramach usługi (w tym czy będą tam dane osobowe), zaś usługobiorca nie ma intencji co do zawarcia umowy powierzenia przetwarzania danych osobowych. Nad tą kwestią pochylono się w opracowaniu GIODO, wskazując, że „jeżeli podmiot udostępniający system (serwer) nie posiada wiedzy co do rodzaju danych przetwarzanych w tym systemie i nie powierzono mu danych w myśl art. 31 UODO, to podlega on postanowieniom art.

14[665] ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną i jego odpowiedzialność za przetwarzane dane jest ograniczona zgodnie z art. 12–15 tej ustawy"[666]. Ponadto możliwe są sytuacje, kiedy w umowie hostingu będzie trzeba zawrzeć klauzule dotyczące powierzenia przetwarzania danych osobowych, ponieważ dla przykładu, hosting dotyczyć będzie strony internetowej zawierającej zakładkę z formularzem kontaktowym, gdzie osoby fizyczne będą miały możliwość pozostawienia swoich danych osobowych na serwerze usługodawcy. Trzecią opcją jest hosting np. witryny apteki internetowej, gdzie zamówienia składają osoby fizyczne podając swoje dane osobowe w celu złożenia zamówienia, wystawienia faktury i wysyłki zamówionych towarów, albo też hosting poczty e-mail, w ramach której przesyłane i przechowywane mogą być duże ilości danych. W takim przypadku wskazane byłoby skrupulatne uregulowanie kwestii związanych z powierzeniem przetwarzania danych osobowych w ramach osobnej umowy powierzenia przetwarzania danych osobowych, stanowiącej integralną część umowy o hosting, zawierającą wszystkie podstawowe elementy przewidziane w przepisach art. 28 RODO, ale również dokładne określenie sfery praw i obowiązków stron oraz odpowiedzialności.

Ponadto w kwestii ochrony danych osobowych w przypadku hostingu, istotnym jest, że administrator danych, nawet jeśli dołożył należytych starań i zawarł umowę powierzenia przetwarzania danych osobowych z dostawcą usługi hostingowej, nadal pozostaje odpowiedzialny za przetwarzanie danych osobowych (też tych, które znajdują się na serwerze podmiotu świadczącego usługę hostingu). Mając to na uwadze, administrator wybierając dostawcę hostingu powinien przeanalizować wiele kwestii, w tym bezpieczeństwo danych, poziom jakości usług, wiarygodność kontrahenta. W szczególności zbadać należy kwestie tego jakie zabezpieczenia fizyczne i techniczne wdrożył dostawca usługi hostingu, przede wszystkim czy dostęp do danych obsługi technicznej jest nadzorowany i monitorowany. Weryfikacji wymaga to, jaki jest zakres usług dodatkowych (np. jak często robione są aktualizacje, kopie zapasowe) a także jak kształtuje się odpowiedzialność dostawcy usługi hostingu i jej wyłączenia oraz jakie są

[665] Zgodnie z treścią art. 14 ust. 1 UsługiElektrU: Nie ponosi odpowiedzialności za przechowywane dane ten, kto udostępniając zasoby systemu teleinformatycznego w celu przechowywania danych przez usługobiorcę nie wie o bezprawnym charakterze danych lub związanej z nimi działalności, a w razie otrzymania urzędowego zawiadomienia lub uzyskania wiarygodnej wiadomości o bezprawnym charakterze danych lub związanej z nimi działalności niezwłocznie uniemożliwi dostęp do tych danych.

[666] A. Kaczmarek, *ABC ..., op. cit.*, s. 48, opracowanie dostępne na stronie internetowej GIODO: https://giodo.gov.pl/data/filemanager_pl/1057.pdf.

ograniczenia serwera (np. procentowa dostępność w określonym czasie, obciążenie dostępu, wykorzystanie czasu procesora)[667].

Aktualnie, dostrzega się przygotowania podmiotów świadczących usługi hostingowe do spełniania wymogów wynikających z przepisów o ochronie danych osobowych. Coraz więcej dostawców usług oferuje tzw. hosting zgodny z RODO, co oznacza hosting rozszerzony o nowe funkcjonalności. Analiza ofert zamieszczanych na stronach internetowych usługodawców pozwala wyciągnąć wniosek, że głównym aspektem dostosowania usługi hostingu do nowych przepisów jest zawieranie umowy powierzenia przetwarzania danych osobowych pomiędzy usługodawcą a usługobiorcą. Dostawcy usług bardzo niechętnie udostępniają wzór takiej umowy, jednakże podjęte próby dotarcia do treści umów, których najważniejsze postanowienia mogą stanowić przedmiot niniejszych rozważań, zakończyły się sukcesem.

Jeden z głównych dostawców oferujących hosting w Polsce uwzględniający przepisy o ochronie danych osobowych zamieścił na swojej stronie internetowej[668] informacje o trybie zawierania umów powierzenia przetwarzania danych osobowych. Już na wstępie określono, że zawartość umowy została określona przez home.pl i zawarcie jej jest możliwe tylko w takiej formie (podpisanie umowy powierzenia przetwarzania danych osobowych odbywa się tylko na ustandaryzowanej formie określonej przez home.pl., zgodnie ze szczegółowo opracowaną instrukcją wypełniania formularza generowania umowy powierzenia). Niestety bez przejścia całej procedury i wypełnienia formularza wraz z podaniem wymaganych danych nie jest możliwe uzyskanie wzoru umowy. Jednakże w innym miejscu na stronie home.pl[669] jest możliwość pobrania treści umowy i to ona będzie stanowiła przedmiot analizy. Umowa ta ma charakter adhezyjny, klient ma do wyboru tylko dwie opcje: Zawieram umowę / Nie zawieram umowy. Jednakże usługodawca daje możliwość modyfikacji jej treści w aspekcie rodzaju i zakresu powierzanych danych[670]. Strony umowy powierzenia są określone poprawnie –

[667] M. Engelmann [w:] P. Karwatka (red.) *Technologia w ecommerce. Teoria i praktyka. Poradnik menedżera*, Gliwice 2013, s. 161-162.
[668] https://pomoc.home.pl/baza-wiedzy/umowy-o-powierzeniu-danych-do-przetwarzania#2
[669] https://regulaminy.home.pl/umowa-powierzenia-przetwarzania-danych-osobowych.pdf
[670] Pod oświadczeniem co do zawarcia bądź niezawarcia umowy powierzenia widnieje oświadczenie o następującej treści: „Mam świadomość, iż w przypadku, gdy w związku z korzystaniem przeze Mnie z usług home.pl dojdzie do przetwarzania przez home.pl danych osobowych, których jestem Administratorem mam obowiązek zawrzeć z home.pl umowę powierzenia przetwarzania danych osobowych. W związku z powyższym oświadczam, iż zawieram w trybie art. 384 Kc z home.pl umowę o powierzenie przetwarzania danych o treści jak w załączniku. W przypadku, gdy rodzaj i zakres danych osobowych, które rzeczywiście

administratorem jest usługobiorca hostingu, zaś podmiotem przetwarzającym jest home.pl S.A. jako dostawca usług hostingowych. Wątpliwość budzi jeden z początkowych zapisów, zgodnie z którym Podmiot przetwarzający uzyskał stosowną certyfikację w zakresie ochrony danych osobowych ISO/IEC 27001. Należy wyjaśnić, że zgodnie z poglądami wyrażonymi w nauce prawa, certyfikacja przewidziana w przepisach RODO nie może być zrównywana z certyfikacją zgodności z określoną normą czy grupą norm ISO. Jest pojęciem odrębnym, w którym jedynie pomocniczo można sięgać po poszczególne normy jako źródła wymagań dotyczących np. bezpieczeństwa informacji dotyczy grupa norm z serii 27000 (przede wszystkim ISO ISO/IEC 27001)[671]. Zapis ten należy zatem uznać za niepoprawny i wprowadzający w błąd, gdyż nie mamy do czynienia z podmiotem certyfikowanym na podstawie RODO. Zbyt ogólnie określono cel zawarcia umowy powierzenia jako wykonanie umowy głównej zawartej drogą elektroniczną (nie określono o jaką umowę chodzi). W treści §3 umowy powierzenia wymieniono zobowiązania podmiotu przetwarzającego, jak np. dokładanie należytej staranności przy przetwarzaniu, upoważnienie osób mających dostęp do danych i zobowiązanie ich do zachowania tajemnicy, usunięcie danych po zakończeniu umowy, pomoc w realizacji obowiązków administratora. Następnie postanowienia dotyczą zobowiązań administratora, jak przestrzeganie zasady minimalizmu czy też dysponowanie podstawą prawną do przetwarzania danych powierzanych, oraz standardowe zapisy dotyczące podpowierzenia przetwarzania danych. Wątpliwości wzbudzają zapisy dotyczące odpowiedzialności podmiotu przetwarzającego. Nie jest zrozumiałe w kontekście przepisów RODO sformułowanie: „Podmiot przetwarzający nie ponosi odpowiedzialności za brak zgodności zastosowanych środków technicznych i organizacyjnych do rodzaju powierzonych mu na podstawie niniejszej Umowy Powierzenia danych osobowych, jeśli środki te są zgodne z rodzajem danych osobowych zadeklarowanym przez Administratora", ponadto odpowiedzialność jest ograniczona do kwoty„(…) równej całkowitej kwocie zapłaconej za usługi świadczone w ramach Umowy Głównej za okres dwunastu miesięcy poprzedzających zdarzenie, które pociąga za sobą odpowiedzialność"[672]. Należy uznać, że jest to umowa jednostronnie zabezpieczająca interesy usługodawcy hostingu i nie spełnia

powierzam home.pl do przetwarzania odbiega od zakresu i rodzaju danych osobowych określonego w wyżej wymienionej Umowie, zobowiązuje się do powiadomienia o tym home.pl w formie elektronicznej za pośrednictwem formularza kontaktowego dostępnego na stronie www.home.pl w terminie 7 dni od dnia złożenia niniejszego oświadczenia.

[671] B. Fischer [w:] M. Sakowska-Baryła (red.), *Ogólne..., op. cit*., Legalis.

[672] https://regulaminy.home.pl/umowa-powierzenia-przetwarzania-danych-osobowych.pdf

wszystkich wymogów wynikających z treści art. 28 RODO, jak choćby umożliwienie przeprowadzania przez administratora audytów bezpieczeństwa.

Drugi z dostawców oferujących usługi hostingowe uwzględniające przepisy RODO, po pierwsze stworzył nową opcję w ofercie (Plan taryfowy Hosting z ochroną danych osobowych), jak również zamieścił na stronie wzór umowy powierzenia przetwarzania danych osobowych[673]. Z udostępnionego na stronie internetowej zestawienia dotychczasowej usługi oraz nowej uwzględniającej wymogi RODO wynika, że hosting uwzględniający przepisy o ochronie danych osobowych został rozszerzony o następujące kwestie: obowiązek zawarcia umowy powierzającej operatorowi usługi przetwarzanie danych osobowych w zakresie niezbędnym do udostępnienia zasobów w sieci Internet; informowanie o potrzebie systematycznej zmiany haseł na kontach użytkowników i usług; oraz dostęp do plików (FTP) i bazy danych MS SQL Server tylko w kanale szyfrowanym[674]. Można powiedzieć, że wymienione opcje stanowią przykładowe zabezpieczenia organizacyjne (umowa) i informatyczne (systematyczna zmiana haseł i szyfrowanie), których stosowanie wymagają od administratorów przepisy prawa, pomimo, że RODO nie wymienia konkretnie żadnych (poza pseudonimizacją) rodzajów zabezpieczeń przetwarzania danych osobowych. Natomiast jeśli chodzi o udostępniony wzór umowy powierzenia przetwarzania danych osobowych w związku z usługą hostingu zgodną z RODO[675], interesującym, ale jednocześnie wykazującym na stosunkowo niewielkie rozeznanie w temacie powierzania przetwarzania danych osobowych podmiotów, które *de facto* zajmują się tym profesjonalnie, jest fakt, że wzór umowy nie jest dostosowany do nowych przepisów (które są stosowane od dnia 25 maja 2018 roku), a opiera się na dotychczasowych. Mimo to, drugi z analizowanych wzorów dużo precyzyjniej określa zakres przetwarzania, co potwierdza treść następujących postanowień: „Zleceniodawca powierza Zleceniobiorcy przetwarzanie danych osobowych objętych zbiorem danych osobowych przechowywanych na koncie hostingowym" oraz „Poprzez przetwarzanie danych rozumie się: zbieranie, zapisywanie, modyfikację, przechowywanie (także w formie kopii zapasowych) oraz utrwalanie danych osobowych". Cel sformułowany jest trafnie: „Dane osobowe będą przetwarzane przez Zleceniobiorcę tylko i wyłącznie w celu realizacji umowy zawartej pomiędzy stronami (tj. udostępnienia Zleceniodawcy usługi udostępniania strony WWW w ramach

[673] http://hostedwindows.pl/pl/hosting/hosting-ochrona-danych-osobowych-rodo/.
[674] *Ibidem*.
[675] http://hostedwindows.pl/pl/regulaminy/wzor-umowy-na-powierzenie-przetwarzania-danych-osobowych/

Shared Hosting)". Analizując przedmiotowy wzór umowy powierzenia pod kątem RODO, można powiedzieć, że nie zostaje spełniony praktycznie żaden wymóg z wymienionych w treści art. 28 ust. 3 RODO: określenie przedmiotu i czasu trwania przetwarzania, charakteru przetwarzania, rodzaju danych osobowych oraz kategorii osób, których dane dotyczą, obowiązków i praw administratora. Wyjątek stanowi wskazanie w tej umowie okresu przetwarzania: „Zakończenie niniejszej umowy następuje wraz z zakończeniem opłaconego abonamentu usługi Shared Hosting". Brak we wzorze umowy powierzenia podstawowych i niezbędnych elementów umowy wynikających z treści przepisu RODO, poddają w wątpliwość deklarowaną zgodność hostingu z RODO, choć zdecydowanie pozytywnie należy ocenić pozostałe z wymienionych funkcjonalności uzupełniające standardową usługę hostingu.

Zdarza się również, że kluczowi usługodawcy w branży IT stosują zaskakujące rozwiązania w aspekcie wypełniania obowiązków w związku z powierzaniem przetwarzania danych osobowych. Z korespondencji mailowej z przedstawicielami Spółki nazwa.pl (określającej się jako największy polski rejestrator domen i dostawca usług internetowych dla firm) wynika konieczność zawarcia umowy powierzenia przetwarzania danych na zasadach przyjętych przez usługodawcę. Niestety usługodawca nie informuje nowych klientów o takich zasadach przed rozpoczęciem świadczenia usług, a w jego trakcie usługobiorca otrzymuje informację, że przed podpisaniem umowy powierzenia przetwarzania danych osobowych konieczne będzie przeprowadzenie procesu audytu tych danych. Na podstawie tego audytu, zostanie podjęta decyzja, czy zakres przetwarzanych przez Państwa danych pozwala na podpisanie umowy powierzenia przetwarzania danych osobowych. Usługa audytu jest podyktowana koniecznością dochowania należytej staranności w ocenie przetwarzania danych i wiąże się z koniecznością uiszczenia jednorazowej opłaty w wysokości 2 000 zł + 23% podatku VAT. Natomiast miesięczny koszt usługi powierzenia przetwarzania danych osobowych wynosi 500 zł + 23% podatku VAT. Należy zauważyć, że zostają tu odwrócone role administratora i podmiotu przetwarzającego. Przeprowadzanie audytu jest przecież uprawnieniem administratora wobec przetwarzającego, a nie na odwrót. Wątpliwości co do zasadności budzą również wymienione kwoty oraz sytuacja, kiedy administrator chce spełnić swój obowiązek i zawrzeć umowę powierzenia, ale nie zgadza się na audyt (co do którego trudno wskazać podstawę prawną), ani na tak wysokie koszty. Wydaje się, że sprawami tego typu powinien zająć się Urząd Ochrony Danych Osobowych.

Na podstawie analizy udostępnianych w Internecie ofert usług hostingowych, można odnieść wrażenie, że spełnianie jednego z wymogów prawnych, czyli powierzanie przetwarzania danych osobowych w drodze umowy, nie jest powszechnie funkcjonujące w tym obszarze usług. Można powiedzieć, że usługodawcy traktują to jako swój atut, wyróżnienie na tle innych usługodawców i podniesienie konkurencyjności na rynku usług hostingowych. Ten atut powinien jednakże być standardem. Ponadto okazuje się, że niejednokrotnie deklarowane tzw. „hostingi zgodne z RODO" są tylko chwytliwymi sloganami i wymagają jeszcze dostosowania do nowych przepisów. Usługodawcy, którzy przestrzegają wymogów wynikających z przepisów RODO, umożliwiają usługobiorcom zawieranie umów powierzenia, jednakże najczęściej jako umowy adhezyjne z niewielkimi (jeśli w ogóle) możliwościami ich indywidualnych modyfikacji. Powyższe uwagi podsumować można również stwierdzeniem, że nawet wśród wyspecjalizowanych usługodawców świadomość i wiedza z zakresu ochrony danych osobowych jest jeszcze wciąż niska. Brak świadomości jest jednym z podstawowych i głównych zagrożeń dla ogólnie rozumianej prywatności, w tym ochrony danych osobowych.

3. Zastosowanie umowy powierzenia przetwarzania danych osobowych w kontekście przetwarzania danych w chmurze (Cloud Computing)

Zagadnienie, które nazywane i określane bywa w różny sposób (przetwarzanie danych w chmurze, usługi chmurowe, chmura obliczeniowa, *cloud computing*), to tematyka przede wszystkim z obszaru nauk informatycznych a jedynie w niewielkim aspekcie nauk prawnych. Potwierdza to chociażby rodzaj źródeł wykorzystanych w prowadzonych rozważaniach –w dużo większym stopniu można oprzeć się na publikacjach branżowych, czy też artykułach publicystycznych i stronach internetowych, niż na literaturze prawniczej. Nie zmienia to jednak faktu, że usługi związane z przetwarzaniem danych w chmurze obliczeniowej mają wiele aspektów prawnych, które są bardzo istotne zarówno dla użytkowników chmury, jak i dostawców tej usługi, ale i podmiotów danych osobowych. Po drugie, są one bardzo skomplikowane ze względu na złożoność tematu chmury, brak kompleksowych opracowań o charakterze prawniczym, czy też brak regulacji prawnych bezpośrednio regulujących to zagadnienie. Ze względu na temat niniejszej rozprawy, prawny kontekst tzw. chmury należy ograniczyć do zagadnienia powierzenia przetwarzania danych osobowych w związku z korzystaniem z usług

chmurowych, pozostawiając poza zakresem rozważań m.in. kwestie związane z prawem własności intelektualnej.

Próby zdefiniowania chmury podejmowane do tej pory nie doprowadziły do wypracowania jednolitego sposobu rozumienia tego pojęcia, a tym bardziej do sformułowania definicji legalnej chmury obliczeniowej. Nie jest to pozytywnie oceniane szczególnie z uwagi na fakt, że z rozwiązań chmurowych korzystamy obecnie na coraz większą skalę i problemów prawnych w tej sferze będzie coraz więcej. W ten sposób funkcjonuje poczta e-mail, aplikacje do połączeń głosowych i wideo, platformy zakupów online, bankowość online, przeglądanie i przesyłanie dokumentów, prezentacji lub arkuszy kalkulacyjnych z różnych urządzeń podłączonych do Internetu, magazynowanie plików i tworzenie ich kopii zapasowych, media społecznościowe.

Większość autorów publikacji poświęconych tematyce *cloud computingu* (tłumaczonego jako chmura obliczeniowa, przetwarzanie w chmurze), powołuje się na definicję wypracowaną przez Narodowy Instytut Standaryzacji i Technologii (NIST) w dokumencie SP-800-145, zgodnie z którą jest to model usługi umożliwiający powszechny, szybki i wygodny dostęp na żądanie za pomocą sieci do współdzielonych zasobów teleinformatycznych (serwerów, masowych pamięci, aplikacji, platform, sieci) oraz ich szybkie pozyskanie i wydanie przy minimalnym wysiłku i interakcji z dostawcą modelu[676]. Oprócz ogólnej definicji przez NIST sformułowane zostały również główne cechy chmury, które pozwalają wyjaśnić skomplikowaną definicję. Istotną właściwością chmury jest szeroki dostęp do zasobów informatycznych przez powszechne mechanizmy jak komputer stacjonarny, laptop, smartfon, aplikacje. Chmurę cechuje błyskawiczna elastyczność, co oznacza, że zasoby w chmurze powinny być możliwe do wykorzystania w dowolnej ilości i w dowolnym czasie. Ponadto jedną z właściwości usług chmurowych jest też samoobsługa na żądanie, co przejawia się w tym, że klient korzysta z zasobów w sposób zautomatyzowany wedle swoich potrzeb, bez konieczności interakcji z dostawcą[677].

Najbardziej widoczną i podstawową różnicą pomiędzy usługami hostingowymi a usługami chmurowymi jest kwestia ograniczeń i dostępności. W przypadku tzw.

[676] P. Mell, T. Grace, SP-800-145 The NIST definition of cloud computing, 2011, dostępne na: https://csrc.nist.gov/publications/detail/sp/800-145/final.
[677] A. Rot, *Wybrane zagadnienia bezpieczeństwa danych i usług w modelu cloud computing* [w:] A. Gąsiorkiewicz, K. Sitarski, O. Sobolewska, M. Wiśniewski (red.), *Gospodarka cyfrowa 2016. Zarządzanie, innowacje, społeczeństwo i technologie*, Warszawa 2017, s. 98-99.

dzierżawy miejsca na serwerze, usługobiorcy hostingu niejednokrotnie spotykają się z trudnościami w zakresie wydajności. Przy usługach hostingu niejednokrotnie zdarza się, że usługobiorca nie ma wiedzy dotyczącej tego, z kim współdzieli serwer, jakie dane są na serwerze przechowywane przez innych usługobiorców, a w przypadku zajęcia przestrzeni serwera przez inny podmiot i wykorzystaniu jego zasobów fizycznych, trudno jest szybko sprawnie i bezproblemowo przenieść dane na inny serwer. Specjaliści w branży IT twierdzą, że serwery działające w chmurze nie są w żaden sposób ograniczane przez aktualną dostępność zasobów, w sytuacji braku pamięci lub mocy procesora, serwer w chmurze zostaje przesunięty na inną fizyczną maszynę z wolnymi zasobami, w sposób niezauważalny dla użytkowników[678]. Różnica przejawia się również w dostosowaniu do potrzeb usługobiorcy, skalowalności. Innymi słowy, serwery dostawców usług hostingowych mają przypisane pule zasobów, w niektórych opcjach można je zwiększyć poprzez działanie usługodawcy, ale raczej nie jest to dostosowanie wielkości pamięci czy mocy procesora adekwatnie do bieżących potrzeb usługobiorcy. Wynika to przede wszystkim z faktu, że dostawcy usług hostingowych nie opłaca się zachowywać zapas miejsca niewykorzystanego na serwerze na wypadek gdyby usługobiorca potrzebował dodatkowej przestrzeni[679]. Natomiast technologia chmury pozwala każdorazowo i automatycznie zapewnić taką ilość zasobów, jaka jest aktualnie potrzebna usługobiorcy, ma on do dyspozycji zapasy, na wypadek zwiększenia zapotrzebowania w przyszłości. Kolejna istotna różnica to ograniczenia techniczne związane z funkcjonowaniem fizycznych serwerów. W przypadku ich awarii najczęściej oznacza to po prostu przerwę w ich działaniu, a niejednokrotnie nawet zagrożenie utraty danych i konieczności przywracania ich z kopii zapasowych. Poglądy specjalistów z branży IT przekonują, że w przypadku awarii w usłudze chmurowej, zasadniczo nie ma przestoju w funkcjonowaniu chmury, a w razie awarii dane przenoszone są na inny dowolny serwer wirtualny[680]. Inny jest aspekt finansowy obu usług. W przypadku usług hostingowych poza ustaloną miesięczną opłatą stałą za konto o określonych zasobach, bez względu na to, czy zasoby to zostały w danym okresie rozliczeniowym wykorzystane czy nie, często uiszcza się również opłatę aktywacyjną. W przypadku chmury natomiast użytkownik płaci za faktycznie wykorzystane zasoby, zgodnie z modelem *pay-per-use* (płatność zgodnie z zużyciem), co niejednokrotnie okazuje się rozwiązaniem bardziej opłacalnym. Jednakże

[678] https://www.spidersweb.pl/2012/12/maciej-kuzniar-chmurach-niechmurach-czyli-czym-sie-rozni-cloud-computing-od-zwyklego-hostingu.html.
[679] *Ibidem*.
[680] *Ibidem*.

z punktu widzenia prawa istotna będzie kolejna różnica pomiędzy hostingiem a przetwarzaniem chmurowym. Hosting na serwerze fizycznym jest *de facto* równoznaczny z umieszczeniem danych na jednej maszynie zlokalizowanej w określonym centrum danych zarządzanym przez określony podmiot. Natomiast przetwarzanie danych w chmurze może być obsługiwany przez wiele maszyn, które mogą przesyłać dane między sobą oraz między usługodawcą, który może posiadać różne centra obliczeniowe, a użytkownikami oraz podwykonawcami (np. podmiotami wykonującymi kopie zapasowe)[681]. Na każdym etapie przetwarzania dane mogą być w innej lokalizacji (np. serwery umieszczone w centrach obliczeniowych mogą być umiejscowione na terenie Unii Europejskiej, ale np. podwykonawcy mogą znajdować się poza Europejskim Obszarem Gospodarczym). Natomiast geograficzne określenie obszaru przetwarzania danych osobowych ma decydujący wpływ na to, jakie przepisy prawa znajdą zastosowanie. Z punktu widzenia prawa zagadnienie terytorialności chmury determinuje szereg kwestii w zakresie usług chmurowych, jak przekazywanie danych poza EOG, prawo właściwe do rozstrzygania sporów, kwestie umów z dostawcami usług chmurowych[682]. Z uwagi na ograniczenie rozważań prowadzonych na kanwie rozprawy doktorskiej do terytorium Unii Europejskiej, zagadnienia te nie są omawiane.

Najczęściej w publikacjach książkowych i źródłach internetowych wyróżnia się cztery rodzaje chmury. Jako kryterium tego podziału wskazać można kwestię ograniczenia dostępności zasobów. Pierwszy rodzaj to chmura publiczna, którą rozumieć można jako usługi obliczeniowe oferowane przez dostawców z innych firm za pośrednictwem publicznego Internetu, dla praktycznie nieograniczonego spektrum użytkowników. Zasoby mogą należeć do różnych dostawców i współdzielone są z różnymi użytkownikami na zasadzie samoobsługi[683]. Usługi te mogą być albo bezpłatne albo sprzedawane odpłatnie, dzięki czemu chmury publiczne pozwalają firmom na zaoszczędzenie na wysokich kosztach zakupu i konserwacji sprzętu i infrastruktury aplikacji oraz zarządzania nimi[684]. Co więcej, chmura publiczna jest najpopularniejszym rozwiązaniem spośród innych

[681] M. Kępiński, K. Klafkowska-Waśniowska, R. Sikorski, *Własność intelektualna w obrocie elektronicznym* tom V 2015, Legalis.
[682] A. Romaszewski, W. Trąbka, M. Kielar, *Perspektywy wprowadzenia modelu chmury obliczeniowej w ochronie zdrowia w świetle istniejących rozwiązań prawnych i organizacyjnych,* Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie, s. 2, tekst dostępny na stronie internetowej http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fef88407-fd08-4113-8803-22dc9c7586d8
[683] J. Zawiła Niedźwiedzki, S. Dyrda, L. Wisłowski, [w:] A. Stabryła, S. Wawak (red.), *Metody, badania i modele rozwoju organizacji*, Kraków 2012, s. 100.
[684] https://azure.microsoft.com/pl-pl/overview/what-is-a-public-cloud/.

modeli, ale też uważa się, że jest technicznie mniej bezpieczna niż chmura prywatna, choć może być to jedynie kwestią czasu i zastosowania odpowiednich zabezpieczeń[685]. Infrastrukturą chmury publicznej zarządza dostawca usługi, który udostępnia ją użytkownikom indywidualnym, przedsiębiorstwom, organom administracji publicznej. Rozważania prowadzone w tej części dysertacji w największym stopniu są poświęcone chmurze publicznej.

Drugim rodzajem usług c*loud computingu* jest chmura prywatna. Jeden z głównych dostawców, nazywając ją również chmurą wewnętrzną lub korporacyjną, definiuje ją jako usługi obliczeniowe oferowane za pośrednictwem Internetu lub prywatnej sieci wewnętrznej, wyłącznie wybranym użytkownikom, a nie ogółowi społeczeństwa[686]. Jest to zatem infrastruktura przeznaczona dla określonej organizacji, najczęściej zlokalizowana jest w jej ramach i podlegająca kontroli organizacji, ale zarządzana najczęściej zewnętrznie. Łączy się z tym, że dana organizacja posiada we własnym zakresie swój system teleinformatyczny własne zabezpieczone serwery i pomieszczenia. Inny dostawca wskazuje, że chmura prywatna pozwala na dostosowanie środowiska do unikalnych potrzeb oraz wymagań w zakresie bezpieczeństwa zapewnia organizacji, większą kontrolę nad środowiskiem, przewidywalność kosztów, a także jeszcze bardziej rygorystyczne zabezpieczenia i elastyczne opcje zarządzania[687].

Natomiast trzecia forma usługi chmurowej, tzw. chmura hybrydowa, polega na połączeniu dwóch poprzednich: publicznej i prywatnej. Ich współdziałanie polega na tym, że dane i aplikacje mogą być przenoszone między chmurami prywatnymi i publicznymi, w zależności od bieżącej potrzeby. Organizacja może korzystać z chmury prywatnej, dokonując wrażliwych i krytycznych operacji, a w krótkim czasie przenieść ruch do chmury publicznej w celu skorzystania z dodatkowych zasobów obliczeniowych[688].

Nie zawsze wyróżnianym, ale funkcjonującym w praktyce rodzajem chmury jest tzw. chmura współdzielona (lub wspólnotowa). Rozwiązanie to polega na współdzieleniu infrastruktury informatycznej przez kilka organizacji dla określonych kategorii użytkowników[689]. Dla chmury wspólnotowej charakterystyczne jest to, że jest ona

[685] https://www.intel.pl/content/www/pl/pl/it-managers/jaka-chmure-wybrac.html.
[686] https://azure.microsoft.com/pl-pl/overview/what-is-a-private-cloud/.
[687] https://www.ibm.com/cloud-computing/pl-pl/learn-more/what-is-private-cloud/
[688] https://azure.microsoft.com/pl-pl/overview/what-are-private-public-hybrid-clouds/.
[689] X. Konarski, *Przetwarzanie danych osobowych w chmurze obliczeniowej* [w:] Dodatek do Monitora Prawniczego 2013 nr 8, Legalis.

udostępniana podmiotom spełniającym te same standardy (np. co do bezpieczeństwa) i wykorzystywana przez użytkowników z kręgu organizacji o wspólnych cechach, jak np. wymagania bezpieczeństwa[690]. W ten sposób często działają chmury wykorzystywane przez organy administracji publicznej.

Faktycznie świadomość społeczna dotycząca użytkowania chmury jest jeszcze stosunkowo niewielka. W 2012 roku zostało przeprowadzone badanie przez firmę Wakefield Research pod nadzorem Citrix na grupie ponad 1000 dorosłych Amerykanów. Wyniki pokazują, że większość respondentów wierzy, iż *cloud computing* jest zjawiskiem związanym z pogodą, a 95% osób deklarujących, że nigdy nie korzystali z usług w chmurze, w rzeczywistości używa tego typu rozwiązań poprzez internetową bankowość, zakupy online, portale społecznościowe czy przechowywanie zdjęć i muzyki w wirtualnych lokalizacjach[691]. Zatem bardzo często błędnie wydaje się, że nie korzystamy z tego typu rozwiązań, podczas gdy nawet powszechnie stosowane narzędzie komunikacji, jakim jest poczta email polega na przetwarzaniu danych w chmurze.

Za najbardziej znane usługi IT opierające się na wykorzystywaniu *cloud computingu* uznawany jest Dysk Google, Dysk Onet, Dropbox, Apple Cloud, Google Apps, iCloud, ale użytkownicy często intuicyjnie opierając się jedynie na funkcjonalności tych narzędzi, nie wgłębiają się w sposób ich działania, przez co nie są w stanie przewidzieć zagrożeń związanych z korzystaniem z usług chmurowych.

Kwestii zagrożeń dla bezpieczeństwa danych osobowych poświęcono sporo uwagi w treści Opinii 5/2012 Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych[692]. Podzielono je na dwie kategorie. Pierwszą stanowi brak kontroli nad danymi będący konsekwencją umieszczenia danych w systemach informatycznych dostawcy (chmura publiczna). Mieści się w tym zakresie przede wszystkim problem braku wyłącznego dostępu klienta usługi do danych i możliwe uzależnienie od dostawcy, np. w aspekcie stosowanych przez niego technologii. Ponadto zidentyfikowano tu zagrożenie jakim jest brak integralności danych ze względu na współdzielenie zasobów i pochodzenie danych z różnych źródeł, jak też trudności co do podejmowania interwencji w proces przetwarzania informacji zarówno przez klienta jak i osoby, których dane dotyczą. Drugą

[690] K. Biczysko-Pudełko, *Administrator danych osobowych i przetwarzający dane na zlecenie a chmura obliczeniowa – problemy interpretacyjne* [w:] Prawo Mediów Elektronicznych 2016 nr 1, Legalis.
[691] http://computingcloud.pl/pl/cloud-przewodnik/ciekawostki/228-co-amerykanie-wiedza-o-chmurze.
[692] Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej przyjęta w dniu 1 lipca 2012, tekst dostępny na stronie internetowej https://giodo.gov.pl/pl/1520111/4760.

kategorię zagrożeń według przedstawicieli Grupy Roboczej stanowi brak przejrzystości, czyli niewystarczające informacje dotyczące przetwarzania danych w chmurze. W tym zakresie wskazano głównie brak informacji o licznych podmiotach łańcucha przetwarzania danych w chmurze, czy też o geograficznych lokalizacjach przetwarzania danych. Należy podkreślić, że zidentyfikowanie zagrożeń, jakie niesie za sobą korzystanie z usług przetwarzania danych w chmurze, jest niezwykle istotnym krokiem na etapie kształtowania stosunku prawnego między klientem a dostawcą usług chmurowych. Zagrożenia te powinny znaleźć odzwierciedlenie w postanowieniach umownych, tak aby uniknąć w przyszłości sporów i wzajemnego przerzucania odpowiedzialności. Podobnie jest z podziałem ról stron takiej umowy.

Uczestnicy rynku usług chmurowych dążą do tego, by negatywny aspekt przetwarzania danych w chmurze był balansowany korzyściami płynącymi z decyzji o przeniesieniu procesów przetwarzania danych do chmury. Wśród korzyści wymienia się najczęściej ograniczenie kosztów, z uwagi na to, że organizacja nie musi inwestować we własną infrastrukturę IT bo korzysta z zasobów zewnętrznych, posiadanie praktycznie nieograniczonych przestrzeni dyskowych i mocy obliczeniowych za optymalną cenę (płatność za faktyczne wykorzystanie, brak konieczności ponoszenia kosztów archiwów czy niszczenia dokumentów), wysoki poziom zabezpieczeń IT, dostęp do zasobów z każdego miejsca połączonego z siecią umożliwiające większą mobilność użytkowników, oszczędność czasu i zwiększenie możliwości rozwoju podmiotów korzystających z tego typu usług[693]. Poza korzyściami ekonomicznymi są jeszcze społeczne, takie jak dostęp do nowych technologii podnoszących standard życia.

Istotne jest dostrzeżenie, że świadczenie i korzystanie z usług w chmurze w zdecydowanej większości przypadków nierozłącznie powiązane jest z przetwarzaniem danych osobowych. Zauważyć należy, że zgodnie z definicją danych osobowych sformułowaną w treści art. 4 pkt 1 RODO, już sam login pracownika wykonującego obowiązki pracownicze w środowisku chmury, który stanowi identyfikator internetowy, jest daną osobową. W zależności od funkcjonalności chmury, zapotrzebowania klientów i możliwości technologicznych dostawców, w chmurze mogą być prowadzone różne operacje na danych osobowych. Odwołując się do definicji przetwarzania ujętej w treści art. 4 pkt 2 RODO, wydaje się, że najczęściej dostawca usługi chmurowej przechowuje

[693] A. Rot, *Wybrane..., op. cit.*, s. 101-102 i powołana tam literatura.

dane osobowe oraz dokonuje ich kopii zapasowych. Nawet bez opcji fizycznego dostępu do treści danych osobowych, są to bez wątpienia operacje mieszczące się w kategorii przetwarzania. Ponadto nie wymaga argumentacji fakt, że relacja klienta oraz podmiotu świadczącego usługi chmurowe będzie stanowiła stosunek powierzenia – dane będą przetwarzane w imieniu administratora przez podmiot zewnętrzny, na jego polecenie (zlecenie usługi). Większość wątpliwości co do przypisania właściwej roli podmiotom uczestniczącym w tym stosunku rozwiewa treść Opinii 5/2012 Grupy Roboczej Art. 29 ds. Ochrony Danych Osobowych[694]. Stwierdzono w niej, że klient, z uwagi na to, że określa ostateczny cel przetwarzania i decyduje o powierzeniu tego przetwarzania zewnętrznej organizacji, działa jako administrator danych. Według przedstawicieli Grupy, klient ma prawo powierzyć dostawcy usługi chmurowej wybór metod i środków technicznych lub organizacyjnych wykorzystywanych do celów administratora. Natomiast dostawca świadczący usługi *cloud computingu* w różnych formach, co do zasady działa w imieniu klienta, dostarczając środki i platformę. Wtedy działa on w roli wykonawcy klienta i jest uznawany za podmiot przetwarzający. W tym przypadku, który można przyjąć jako regułę, wymagane jest zawarcie umowy powierzenia przetwarzania danych osobowych między klientem a dostawcą usług chmurowych. Jednakże w środowisku chmury nie zawsze istnieje czysty podział ról, w treści Opinii zaznaczono, że zdarza się, iż dostawca usług w chmurze może być uznany za administratora lub współadministratora, gdy przetwarza dane do celów własnych[695].

Korzystanie z usług przetwarzania w chmurze w dużej mierze utrudnia fakt, że do chwili obecnej nie ma przepisów prawa stanowionego, które bezpośrednio regulowałyby obszar *cloud computingu*. Taki stan rzeczy może sprzyjać nadużyciom ze strony dostawców usług chmurowych, rozmyciu odpowiedzialności, utrudnieniom w realizacji praw osób, których dotyczą dane przetwarzane w środowisku chmury. Z drugiej jednak strony daje to pole do działania regulacjom *soft law*, przez co rozumiane są zalecenia, opinie, deklaracje, rezolucje, komunikaty, raporty, memoranda, wytyczne i dobre praktyki. O ile nie mają one mocy wiążącej, są *de facto* jedynymi regulacjami, które wyznaczają kierunek działań dostawców usług, jak i wymagań klientów.

[694] Opinia 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej przyjęta w dniu 1 lipca 2012, tekst dostępny na stronie internetowej https://giodo.gov.pl/pl/1520111/4760.
[695] *Ibidem*.

Poza treścią powołanej wcześniej Opinii 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej, funkcjonują jeszcze inne dokumenty, z których wywieść można kwestie istotne przy rozważaniach dotyczących ram prawnych przetwarzania danych w chmurze. Jednym z nich jest Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie chmur obliczeniowych[696], której celem było zgromadzenie praktycznych doświadczeń na temat rynku *cloud computing* oraz zachęcenie Europy do zajęcia czołowej pozycji w tej dziedzinie. Komitet wskazał katalog podstawowych zagrożeń i słabości związanych z modelem chmury, wymieniając wśród nich brak europejskiego organu nadzoru, który czuwałby nad przestrzeganiem standardów użytkowania i kontroli chmury, słabości techniczne Internetu jak przerwy w połączeniu, zatory, cyberataki, przeciążenie serwerów, trudności w zakresie lokalizacji danych i ich przepływu do państw niegwarantujących odpowiedniego stopnia ochrony, czy też niedostateczny poziom wiedzy i niejasności co do praw i obowiązków stron bardzo złożonych umów o świadczenie usług chmurowych. Ponadto Komitet, upatrując dla Europy szansy wejścia na obiecujący, duży i strategiczny rynek *cloud computing,* sformułował zalecenia działań dla Komisji Europejskiej wspieranej przez państwa członkowskie[697]. Jako priorytetowe potraktowane zostały badania (koordynacja działań przez europejskie ośrodki badawcze), szkolenia (rozwijanie umiejętności informatyków, zatwierdzanie specjalistycznych świadectw i dyplomów), inwestycje (rozbudowa światłowodów, subwencjonowanie inwestorów), a także tworzenie ram prawnych dla obszaru chmury (utworzenie przepisów, zachęcanie do wspólnych pac nad zasadami relacji pomiędzy dostawcami usług chmurowych, przedsiębiorcami korzystającymi z tych usług i osobami, których dane dotyczą, jak też powołanie agencji odpowiedzialnej za przestrzeganie tych zasad). Komitet odniósł się też do kwestii umów o usługi *cloud computingu*. Zalecił, by przedsiębiorcy wnikliwie analizowali ich treść przy pomocy specjalistów z tego zakresu i nie poprzestawali na podpisaniu standardowego formularza umowy. O ile najczęściej umowy o świadczenie usług chmurowych nie podlegają negocjacjom, to warto zachęcać dostawcę do wyrażenia zgody na indywidualne warunki umowy[698]. Niestety, w treści Opinii Europejskiego Komitetu Ekonomiczno-Społecznego nie poświęcono uwagi na kwestie spełniania przez podmioty uczestniczące

[696] Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie chmur obliczeniowych (cloud computing) w Europie (opinia z inicjatywy własnej) z dnia 26 października 2011 r. (2012/C 24/08), dostępna na stronie https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:024:0040:0047:PL:PDF
[697] *Ibidem*.
[698] *Ibidem.*

w przetwarzaniu danych w chmurze obowiązujących przepisów o ochronie danych osobowych (w momencie opracowywania dokumentu były to przepisy Dyrektywy 95/46/WE). Nie odniesiono się do kwestii podziału ról dostawcy i klienta w procesie przetwarzania danych oraz do zawierania umów powierzenia przetwarzania danych osobowych.

Kolejnym znaczącym aktem *soft law* poświęconym przetwarzaniu danych osobowych w chmurze obliczeniowej jest „Dokument roboczy w sprawie przetwarzania danych w chmurze obliczeniowej – kwestii ochrony danych i prywatności – Memorandum z Sopotu"[699]. Jest to dokument opracowany przez Międzynarodową Grupę Roboczą ds. Ochrony Danych w Telekomunikacji (nazywanej Grupą Berlińską) w trakcie 51. spotkania w Sopocie w 2012 roku. Zawiera on wspólne stanowisko Grupy na temat zasad ochrony prywatności w przypadku przetwarzania danych przy użyciu chmury obliczeniowej. Grupa Robocza zwraca uwagę na ciągłą niepewność związaną z funkcjonowaniem usług chmurowych w aspekcie ochrony prywatności, powodowaną m.in. brakiem międzynarodowego porozumienia ustalającego wspólną terminologię, brak przejrzystości w procesach, procedurach i praktykach dostawców usług w chmurze, powodowane przez to utrudnienia prowadzenia oceny ryzyka i utrudnienia w egzekwowaniu przepisów regulujących obszar ochrony danych osobowych, oraz nacisk na dostawców co do zmniejszenia kosztów usług z jednoczesnym podniesieniem poziomu bezpieczeństwa danych. Taki stan rzeczy powoduje zwiększenie ryzyka wystąpienia negatywnych skutków dla prywatności osób fizycznych, w tym przyznawaniu dostawcom zbyt szerokiej swobody działania poprzez akceptowanie standardowych warunków umów, utratę kontroli administratora nad danymi, rozmycie odpowiedzialności w łańcuchu podpowiedzeń, uniemożliwienie organom ochrony danych osobowych właściwego nadzorowania przetwarzania[700]. Grupa Robocza identyfikując powyższe okoliczności, zaproponowała również zalecenia w formie dobrych praktyk adresowanych zarówno do administratorów danych (klientów), jak i podmiotów przetwarzających (dostawców usług w chmurze). W odniesieniu do pierwszej kategorii podmiotów zalecono, by administrator zadbał o przeprowadzenie analizy ryzyka przed zastosowaniem technologii chmurowych, w treści umowy przewidział zasadę przejrzystości lokalizacji oraz zobowiązanie do niewykorzystywania powierzonych danych do celów podmiotu przetwarzającego

[699] Treść Memorandum dostępna na stronie https://giodo.gov.pl/pl/1520129/4646.
[700] *Ibidem*.

i podprzetwarzających, zabezpieczył realną możliwość zakończenia współpracy z dostawcą by uniknąć uzależnienia, jak też zobligował dostawcę do wdrożenia procedur umożliwiających realizację praw osób, których dane dotyczą[701]. Następnie Grupa Robocza skierowała zalecenia do podmiotu przetwarzającego. Przede wszystkim zarekomendowano zapewnienie przejrzystości co do miejsc przetwarzania danych oraz podmiotów uczestniczących w procesach jako podprzetwarzający, powstrzymywanie się od oferowania usług na bazie standardowych warunków oraz umożliwianie administratorom monitorowania swoich działań za pomocą audytów.

Zainteresowanie problematyką *cloud computingu* wyraził Generalny Inspektor Ochrony Danych Osobowych (GIODO)[702] oraz Urząd Komisji Nadzoru Finansowego (UKNF)[703] wydając opracowania i komunikat zawierające zasady korzystania z *cloud computingu.* Na podstawie lektury stanowisk GIODO i UKNF odnośnie zagadnienia przetwarzania danych w chmurze zaprezentowanych przez oba organy, można sformułować wniosek, że Generalny Inspektor Ochrony Danych Osobowych (aktualnie Prezes Urzędu Ochrony Danych Osobowych) bardzo lakonicznie potraktował problematykę *cloud computingu.* Można stwierdzić, że w odniesieniu do organu, który od 1998 roku pełnił kluczową rolę w zakresie ochrony danych osobowych w Polsce, oczekiwania społeczne co do wskazywania pożądanych zachowań jak i zagrożeń wynikających z upowszechniania usług przetwarzania w chmurze, są największe.

[701] *Ibidem.*

[702] https://www.giodo.gov.pl/259/id_art/6271/j/pl. Opracowanie opublikowane przez GIODO nosi nazwę „Dekalog chmuroluba. Dziesięć zasad stosowania usług chmurowych przez administrację publiczną". Nie należy traktować go jako *soft law* ani też jako oficjalne stanowisko organu. Jest bardzo krótkie (zawiera 10 punktów), jego adresatem są podmioty administracji publicznej (występujące tu jako podmioty publiczne). Przypisano role poszczególnym uczestnikom procesu przetwarzania w chmurze. Określono, że podmiot publiczny powinien pozostawać wyłącznym administratorem danych osobowych, a każdy z podwykonawców jest traktowany jako podprzetwarzający dane osobowe i jest związany takimi samymi klauzulami umownymi jak dostarczyciel usług chmurowych. Sformułowano katalog zobowiązań dostarczyciela usługi chmurowej, zaznaczono też, że podmiot administracji publicznej nie może stać się stroną umowy adhezyjnej.

[703] Komunikat z dnia 23 października 2017 r., dostępny na stronie https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_dot_korzystania_przez_podmioty_nadzorowane_z_uslug_przetwarzania_danych_w_chmurze_obliczeniowej_59626.pdf. Urząd stanął na stanowisku, że usługa przetwarzania danych w chmurze ma charakter powierzenia wykonywania czynności i skrupulatnie określił wymogi umowy podmiotu nadzorowanego z dostawcą usługi. Stwierdzono, że umowa na usługę chmurową w szczególności powinna zawierać zapisy określające obowiązek zapewnienia odpowiedniego poziomu bezpieczeństwa i ochrony powierzonych danych, określenia lokalizacji centrów, w których dane będą przechowywane i przetwarzane, ze szczególnym uwzględnieniem obsługi danych przez podwykonawców. Ponadto zdaniem Urzędu w treści umowy powinien znaleźć się zakres informacji i dokumentacji przekazywanych przez dostawcę w związku ze świadczeniem usługi, procedury zarządzania incydentami i współpracy w tym zakresie, prawo do przeprowadzenia audytu lub certyfikacji przez podmiot nadzorowany. Nietrudno zauważyć, że wymagane przez organ elementy umowy w dużej mierze pokrywają się z elementami umowy powierzenia przetwarzania danych osobowych wynikającymi z treści art. 28 RODO.

Do chwili obecnej jednak organ nie opublikował oficjalnego stanowiska z wytycznymi w przedmiotowym zakresie. Uczynił to Urząd Komisji Nadzoru Finansowego, wydając powołany Komunikat w odpowiedzi na zgłaszane potrzeby ze strony podmiotów nadzorowanych. Z treści Komunikatu można wywnioskować, że UKNF nie wszedł w obszar działania GIODO (aktualnie PUODO), ponieważ dokument ten nie ma charakteru ogólnego, a raczej sektorowy - kierowany jest do podmiotów sektora usług finansowych (podmioty nadzorowane).

Interesująca okazała się analiza charakterystycznych postanowień dla umów o świadczenie usług w chmurze[704]. Przede wszystkim wskazuje się, że bardzo często stosowane są zapisy o maksymalnym ograniczeniu odpowiedzialności dostawcy usług chmurowych za szkody wyrządzone przez błędy systemu informatycznego, jak np. przerwy w dostępie. Dostawcy usług chmurowych niejednokrotnie nie gwarantują również naprawy wszelkich wad w działaniu systemu lub też podejmowania wszelkich kroków w celu przeciwdziałania przestojom. O ile teoretycznie takie działanie dopuszcza zasada swobody umów, to można mieć wątpliwości co do jego uzasadnienia w kontekście zasad współżycia społecznego i słuszności. W powyższym aspekcie uwidacznia się znaczenie tzw. *Service Level Agreement* (SLA), znanej też jako Gwarancja Jakości Świadczonych Usług. Jest to umowa pomiędzy dostawcą usługi i jej użytkownikiem, w której dostawca zobowiązuje się do zapewnienia określonego poziomu jakości usługi, opisanego poprzez uzgodnione z użytkownikiem cechy (parametry jakościowe dotyczące np. dostępności usługi, czasu na reakcję) i na wypadek świadczenia usługi poniżej tego poziomu przyznaje użytkownikowi określone uprawnienia[705]. W postanowieniach tych zawiera się również m.in. uzgodnienia co do udziału osób trzecich w świadczeniu usługi, odzyskiwania danych po awarii. Są to bardzo istotne, przede wszystkim z perspektywy klienta, elementy stosunku prawnego świadczenia usług w chmurze.

Niejednokrotnie zdarza się, że w treści umowy o świadczenie usług w chmurze dostawca usługi zapewnia sobie prawo do zmiany zakresu świadczenia usługi bądź wysokości opłat. Wynika to z dominującej pozycji dostawców usług chmurowych. Kształtują oni sobie daleko idące prawo, pozwalające na podniesienie opłat za korzystanie z usług chmurowych w trakcie trwania nawet wieloletnich umów, jedynie po

[704] E. Molenda-Kropielnicka, *Cloud compting – zagadnienia prawne*, Zeszyty Naukowe Uniwersytetu Jagiellońskiego 2013 nr 1, LEX nr 167346.
[705] J.Gołaczyński, Prawo Mediów Elektronicznych 2/2005, Dodatek do Monitora Prawniczego Nr 3/2005, Legalis.

poinformowaniu o tym klienta z krótkim wyprzedzeniem. Z perspektywy klienta taka klauzula rodzi problemy, ponieważ nie ma on gwarancji niezmienności warunków korzystania z usług w trakcie obowiązywania umowy i pewności co do działania w uzgodniony sposób przez ustalony czas (podwyżki cen lub zmiany innych warunków mogą zmuszać klientów do zmiany dostawcy). Natomiast z punktu widzenia dostawcy istotne jest zapewnienie możliwości rozwoju i podnoszenia jakości usługi w oparciu o nowe technologie, co generuje koszty, a odbieranie od każdego klienta zgody na zmianę warunków może stanowić nadmierną trudność. Dlatego też klient powinien dołożyć staranności, by w umowie zostało przewidziane w jakim zakresie mogą następować modyfikacje w świadczeniu usług *cloud computingu*[706].

Ostatnim z wymienianych elementów charakterystycznych dla umów o świadczenie usług w chmurze są postanowienia dotyczące wypowiedzenia umowy. Z treści umów będących przedmiotem prowadzonych badań wynika, że bardzo często możliwość rozwiązania umowy jest kształtowana na korzyść dostawcy chmury, tak by uzależnić klienta od dostawcy i ograniczyć interoperacyjność danych (ta tendencja określana jest w literaturze przedmiotu jako *vendor-lock-in*)[707]. Najczęściej możliwość wypowiedzenia umowy przez klienta jest ograniczana do wystąpienia istotnych naruszeń ze strony dostawcy, do których nie zaliczają się powtarzające się problemy w działaniu systemu. Na etapie zawierania umowy należy zadbać o prawo klienta do przeniesienia danych (tzw. przenoszalność). W kontekście usług chmurowych przenoszalność to możliwość przenoszenia przez klienta aplikacji i danych pomiędzy swoimi własnymi systemami i usługami chmurowymi, usługami różnych dostawców, a także pomiędzy różnymi modelami usług[708]. Zdarza się jednakże, że dostawca usługi chmurowej nie związuje klienta i nie wprowadza do umowy zapisów utrudniających wypowiedzenie umowy[709].

---

[706] E. Molenda-Kropielnicka, *Cloud..., op. cit*., LEX.

[707] Byrski J., *Outsourcing w działalności dostawców usług płatniczych*, Warszawa 2018, Legalis.

[708] https://zaufanatrzeciastrona.pl/post/interoperacyjnosc-i-przenaszalnosc-jak-uniezaleznic-sie-od-dostawcy/.

[709] W treści paragrafu 7 Regulaminu Usług Comarch ERP Optima w modelu usługowym postanowiono, że: „Każdej ze stron przysługuje prawo wypowiedzenia umowy z zachowaniem dwumiesięcznego okresu wypowiedzenia ze skutkiem na koniec miesiąca kalendarzowego. (...) Klientowi przysługuje prawo rezygnacji z poszczególnych Usług Comarch ERP Optima w modelu usługowym ze skutkiem na koniec następnego miesiąca kalendarzowego po złożeniu stosownego oświadczenia. W celu wypowiedzenia umowy Klient powinien wysłać do Comarch stosowne oświadczenie w formie pisemnej pod rygorem nieważności. Wzór wypowiedzenia można otrzymać po przesłaniu informacji na adres optima.chmura@comarch.pl". Regulamin dostępny na stronie https://www.comarch-

Bez wątpienia wymienione powyżej rodzaje klauzul przedstawiane jako najczęściej występujące w obrocie powinny być uzupełnione o klauzule dotyczące powierzenia przetwarzania danych. Możliwe jest albo zawarcie odrębnej umowy powierzenia pomiędzy klientem (administratorem) a dostawcą usługi chmurowej (podmiotem przetwarzającym), albo umieszczenie postanowień realizujących wymogi określone w art. 28 RODO w treści umowy o świadczenie usługi w chmurze. W przeciwnym wypadku kontrahenci narażają się na zarzut przetwarzania danych osobowych bez podstawy prawnej) w przypadku podmiotu przetwarzającego) oraz udostępnienia danych podmiotowi nieuprawnionemu (w przypadku administratora). Należy pamiętać, że z akcesoryjnego charakteru umowy powierzenia wynika, że obowiązuje ona tak długo, jak umowa zasadnicza o świadczenie usług w chmurze.

Na bazie dostępnych w Internecie wzorów umów warto przeanalizować w jaki sposób do przetwarzania danych w chmurze podchodzą kluczowi dostawcy usług cloud computingu. Jednym z takich podmiotów jest IBM Corporation z siedzibą w Nowym Jorku, w Polsce występujący jako IBM Polska Sp. z o.o., uznający się za światowego lidera w kreowaniu, rozwijaniu i produkcji najbardziej zaawansowanych technologii informatycznych obejmujących systemy komputerowe, oprogramowanie, systemy sieciowe, pamięci masowe i rozwiązania z zakresu mikroelektroniki[710]. Treść Umowy o usługi przetwarzania w chmurze przez IBM[711] ma charakter bardzo ramowy. Umowa ta zawiera ogólne zapisy dotyczące samej usługi (w tym wymagania leżące po stronie dostawcy, zobowiązania klienta), gwarancji, płatności, odpowiedzialności i zakończenia umowy. Istotny jest zapis dotyczący tzw. zawartości, czyli wszelkich danych udostępnianych przez klienta w usłudze przetwarzania w chmurze, do której IBM ma dostęp i korzysta z niej wyłącznie w celu udostępnienia usługi chmurowej i zarządzania nią, a którą traktuje jako poufną i może udostępniać jedynie wymienionym podmiotom (w tym pracownikom i wykonawcom IBM). Natomiast bardziej szczegółowe rozwiązania są zawarte w treści załączników, do których umowa odsyła. Są to przede wszystkim „Zasady ochrony danych i prywatności dla usług przetwarzania w chmurze IBM”[712], gdzie zawarto opis środków technicznych i organizacyjnych stosowanych przez dostawcę. Jest

cloud.pl/public/userfiles/ERP/Optima%20dla%20firm/Regulamin_Comarch_ERP_Optima_w_modelu_uslugowym.pdf.

[710] https://www.ibm.com/ibm/pl/pl/?lnk=fab_plpl.

[711] https://www.ibm.com/support/customer/pdf/csa_pl_pl.pdf.

[712] https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW3/$file/Z126-7745-WW-3_05-2018_pl_PL.pdf

to szereg zobowiązań IBM, jak np. stosowanie strategii reagowania na incydenty związane z cyberbezpieczeństwem, szkolenie kadry z zakresu bezpieczeństwa danych, szyfrowanie przesyłanych danych, kontrola fizycznego dostępu. Dopiero kolejny załącznik, do którego odsyła umowa, zatytułowany „Dodatek dotyczący przetwarzania danych”[713] (czyli *de facto* stanowiący załącznik do powołanych Zasad ochrony danych i prywatności) zawiera postanowienia, których treść odpowiada w pewnym zakresie wymogom umowy powierzenia przetwarzania danych osobowych. Na wstępie następuje określenie ról podmiotów, tj. klient jest administratorem danych osobowych, a IBM jest podmiotem przetwarzającym. Co należy ocenić jako niewłaściwe rozwiązanie, w treści Dodatku zawarto odesłanie do kolejnego załącznika, w którym określone są kategorie osób, których przetwarzanie dane dotyczą oraz zakres operacji na danych. Wydaje się, że informacje te mają na tyle podstawowe znaczenie dla stosunku powierzenia danych, że nie powinny być odseparowane do kolejnego załącznika.

Analizowana umowa o świadczenie usług w chmurze przez IBM zawierająca szereg dodatkowych dokumentów wydaje się mieć złożoną i skomplikowaną konstrukcję. Wysoko należy ocenić skrupulatność i szczegółowość zapisów dotyczących powierzenia przetwarzania danych. Można powiedzieć, że IBM dokłada starań, by umowy zawierane z klientami decydującymi się skorzystać z usług chmurowych, spełniają wymogi RODO co do elementów umowy powierzenia. Nie ma tu jednakże odrębnej umowy powierzenia przetwarzania danych osobowych kompleksowo regulującej sferę zlecenia przetwarzania danych dostawcy. Postanowienia istotne z punktu widzenia ochrony danych osobowych i wymogów RODO są rozproszone po wielu dokumentach, często powielane (jak np. sekcja „Środki organizacyjne i techniczne”, która występuje w obu powołanych załącznikach i przewiduje się ją również w załączniku do załącznika), czy też umieszczane poza głównymi regulacjami powierzenia danych (jak lista podmiotów podprzetwarzających). Treść analizowanych postanowień formułowanych przez IBM daje do zrozumienia, że klient nie ma realnych możliwości kształtowania zapisów zawieranej umowy, a jedynie może modyfikować i precyzować treść poszczególnych załączników. Oznacza to *de facto* brak kontroli nad sferą powierzonych danych, jaką powinien mieć administrator zlecający określone działania podmiotowi zewnętrznemu, jak również brak przejrzystości zasad współpracy stron. Po drugie, jako zbyt daleko idące można ocenić poszczególne zapisy dotyczące przerzucenia odpowiedzialności na klienta. Widoczne jest

[713] https://www.ibm.com/support/customer/pdf/dpa_pl.pdf

to m.in. w zapisie, że klient potwierdza, że środki organizacyjne i techniczne (które stosuje dostawca) zapewniają odpowiedni poziom ochrony danych osobowych. W kontekście art. 28 ust. 1 RODO, który stanowi, że administrator korzysta wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi rozporządzenia, wydaje się, że to dostawca powinien udzielić rzeczonego potwierdzenia. Po trzecie, wątpliwości budzić może lakoniczne odniesienie się do odpowiedzialności IBM jako podmiotu przetwarzającego. Jedynym postanowieniem dotyczącym odpowiedzialności dostawcy jest pkt 6 Umowy o usługi przetwarzania w chmurze, gdzie została ona ograniczona do wartości rzeczywistych szkód bezpośrednich poniesionych przez klienta do wysokości kwoty opłat. Zapis ten nie koresponduje z zakresem odpowiedzialności podmiotu przetwarzającego wynikającym z treści art. 82 RODO.

Drugim powszechnie dostępnym do analizy przykładem uregulowania stosunku prawnego dotyczącego korzystania z usług przetwarzania danych w chmurze jest umowa Oracle Polska Sp. z o.o. z siedzibą w Warszawie[714]. Do całokształtu analizy treść umowy powinna być rozpatrywana wraz z zamówieniem klienta, jednakże jego wzór nie jest dostępny w sieci.

Zgodnie z treścią umowy o świadczenie usług w chmurze Oracle, dostawca Oracle udziela klientowi prawa do korzystania z usług wymienionych w zamówieniu klienta, natomiast klient udziela Oracle prawa do hostowania, używania, przetwarzania, prezentowania i przesyłania treści klienta w celu świadczenia usług zgodnie z umową i zamówieniem klienta[715]. Wśród postanowień tej umowy uwagę zwraca przede wszystkim kwestia ograniczenia odpowiedzialności dostawcy i przerzucenia jej na klienta. W umowie stwierdza się między innymi, że: „klient ponosi odpowiedzialność za wszelkie luki w zabezpieczeniach oraz za ich skutki, w tym między innymi jakiekolwiek wirusy, konie trojańskie, robaki czy inne szkodliwe programy zawarte w treściach, które wynikają z treści klienta lub ze sprzecznego z warunkami niniejszej umowy sposobu korzystania z usług". Za charakterystyczne należy uznać także postanowienie, że „klient zachowuje wyłączną odpowiedzialność za przestrzeganie przepisów w związku z korzystaniem

[714] Wzór umowy dostępny jest na stronie http://www.oracle.com/us/corporate/contracts/cloud-csa-pl-pl-2653554.pdf.
[715] Punkt 1 oraz 3 powołanej umowy.

z usług". Nie ma natomiast mowy o obowiązkach dostawcy co do zapewnienia bezpieczeństwa przetwarzania danych. Ponadto w umowie postanawia się, że „w żadnym przypadku całkowita odpowiedzialność Oracle i podmiotów stowarzyszonych Oracle wynikająca z niniejszej umowy lub z nią związana, niezależnie od tego czy kontraktowa, deliktowa, czy jakakolwiek inna, nie przekroczy łącznej kwoty wpłaconej za usługi świadczone na podstawie zamówienia będącego podstawą roszczenia, w ciągu dwunastu miesięcy bezpośrednio poprzedzających wydarzenie będące podstawą roszczenia z tytułu takiego zamówienia".

Należy przewidzieć, że w aspekcie zagrożeń związanych z przetwarzaniem chmurowym, bardzo możliwym jest wystąpienie szkód po stronie klienta, których wysokość znacznie przekroczy kwotę określonego powyżej odszkodowania. W kontekście ochrony danych osobowych, w treści umowy o świadczenie usług w chmurze Oracle, podobnie jak w przypadku usług IBM, mamy do czynienia z odniesieniami do szeregu innych dokumentów, w tym do Zasad ochrony prywatności Oracle[716], Specyfikacji Usług[717], czy Umowy powierzenia przetwarzania danych osobowych[718]. Należy też stwierdzić, że trudno określić, by Oracle przedstawiała transparentne zasady przetwarzania danych w chmurze, co uwidacznia się w ogólnym zapisie „Oracle oraz podmioty stowarzyszone Oracle mogą świadczyć pewne aspekty usług (na przykład administrację, utrzymanie, asystę techniczną, awaryjne odtwarzanie danych, przetwarzanie danych, etc.) z lokalizacji, i/lub za pośrednictwem podwykonawców, na całym świecie". Podwykonawcy ci najprawdopodobniej powinni być traktowani jako podprzetwarzający, przy czym nie ma informacji co to za podmioty i gdzie prowadzą działalność, na jakich zasadach współpracują z Oracle. Ponadto poważną wątpliwość budzi zapis o treści: „na mocy niniejszej umowy, strony mogą ujawniać poufne informacje. Informacje poufne ograniczone są do warunków i cen wynikających z niniejszej umowy, treści klienta umieszczonych w usługach oraz wszelkich informacji jasno określonych jako poufne w chwili ujawnienia"[719].

[716] Dostępne w wersji angielskiej na stronie https://www.oracle.com/legal/privacy/.
[717] Określają one administracyjne, fizyczne, techniczne i inne zabezpieczenia Treści Klienta umieszczonych w usługach i opisują inne aspekty zarządzania systemem mające zastosowanie do świadczonych usług, ale nie zostały udostępnione.
[718] Dostępna w wersji angielskiej na stronie https://www.oracle.com/assets/data-processing-agreement-072718-5029569.pdf.
[719] Wydaje się, że mógł tu nastąpić błąd w tłumaczeniu z języka angielskiego, ponieważ standardem wśród dostawców usług chmurowych jest zachowywanie poufności co do zawartości umieszczanych w chmurze przez klientów.

To co odróżnia podejście Oracle od IBM, to stosowanie odrębnej umowy powierzenia przetwarzania danych osobowych[720], stanowiącej integralną część omawianej umowy o świadczenie usług w chmurze Oracle. W treści umowy powierzenia prawidłowo przydzielono rolę administratora klientowi i rolę podmiotu przetwarzającego – dostawcy[721]. Skrupulatnie określono, jakie rodzaje danych osobowych mogą być przedmiotem powierzenia, jak również kategorie osób, których dane mogą dotyczyć. W treści umowy powierzenia wyraźnie zaznaczono, że o ile umowa o świadczenie usług w chmurze nie stanowi inaczej, zawartość zamieszczana przez klienta w chmurze nie może zawierać szczególnych kategorii danych, które wymagają ze strony Oracle dodatkowych zabezpieczeń[722]. Interesującym i niestandardowym postanowieniem jest zapis stanowiący, że możliwe jest nałożenie dodatkowych opłat nieobjętych umową o świadczenie usług w chmurze, jeśli okaże się, że polecenie administratora wymaga zaangażowania dodatkowego kontrahenta zewnętrznego (czyli podprzetwarzającego). Administrator zostanie o tym poinformowany, a podmiot przetwarzający zobowiązuje się do negocjowania wysokości opłat w interesie administratora[723]. Takie rozwiązanie nie jest często spotykanym na gruncie praktyki stosowania umów powierzenia przetwarzania danych osobowych w polskich realiach. W kontekście realizacji praw osób, których dane dotyczą, można powiedzieć, że Oracle spełnia przypisaną podmiotowi przetwarzającemu rolę wsparcia dla administratora. Stanowi o tym treść punktu 6 umowy powierzenia, zgodnie z którym Oracle zapewnia klientowi dostęp do środowiska usług chmurowych, aby umożliwić odpowiadanie na żądania podmiotów danych w zakresie realizacji ich praw. Ponadto Oracle umożliwia zastosowanie narzędzia polegającego na dokonaniu zgłoszenia serwisowego przez klienta oraz podania stosownych instrukcji, by to dostawca udzielił odpowiedzi osobie, której dane dotyczą. Istnieje też możliwość, że Oracle niezwłocznie przekaże klientowi otrzymane bezpośrednio od podmiotu danych żądanie. Ogólnie można powiedzieć, że w powyższy sposób realizowany jest wymóg zawarty

[720] Dostępna w wersji angielskiej na stronie https://www.oracle.com/assets/data-processing-agreement-072718-5029569.pdf.

[721] "3.1 You are and will at all times remain the Controller of the Personal Data Processed by Oracle under the Cloud Services Agreement. (…) 3.2 Oracle is and will at all times remain a Processor with regard to the Personal Data provided by You to Oracle under the Cloud Services Agreement".

[722] "Unless otherwise specified in the Cloud Services Agreement, Your Content may not include any sensitive or special personal data that imposes specific data security or data protection obligations on Oracle in addition to or different from those specified in the Service Specifications".

[723] "To the extent, Oracle expects to incur additional charges or fees not covered by the fees for Cloud Services payable under the Cloud Services Agreement, such as additional license or third party contractor fees, it will promptly inform You thereof upon receiving Your instructions. Without prejudice to Oracle's obligation to comply with Your instructions, the parties will then negotiate in good faith with respect to any such charges or fees".

w art. 28 ust. 3 lit. e RODO, polegający na pomaganiu administratorowi w zakresie obowiązku odpowiadania na żądania osoby, której dane dotyczą.

Na podstawie analizy dostępnych materiałów źródłowych, jakimi są wzory umów dotyczących usług przetwarzania danych w chmurze można sformułować wniosek, że pomiędzy klientem a dostawcą usług chmurowych brak jest równorzędności podmiotów i pozycję dominującą w tej relacji zajmuje dostawca. Klient pomimo tego, że ma rolę administratora, czyli podmiotu zlecającego usługę i wydającego polecenia co do przetwarzania danych osobowych, jest *de facto* ograniczony do wyboru opcji zaakceptowania warunków oferowanych przez dostawcę bądź opcji niewyrażenia zgody skutkującej odmową współpracy.

Podsumowując, należy powiedzieć, że przetwarzanie danych osobowych w chmurze cechuje się dynamicznością, zautomatyzowaniem procesów przetwarzania i skomplikowaniem zasad działania przy jednoczesnym ułatwieniu dokonywania operacji na danych przez użytkowników. Wskazywane w dokumentach przyjmowanych na przestrzeni praktycznie dekady zagrożenia wynikające z użytkowania rozwiązań chmurowych podzielić można na trzy grupy. W pierwszej znajdują się słabości techniczne systemów, w tym m.in. przeciążenie i zatory w sieci, przerwy w połączeniu internetowym, przeciążenie serwerów. W drugiej grupie są ryzyka związane z brakiem kontroli nad danymi przetwarzanymi w chmurze, do których zaliczają się łańcuchy podwykonawców, delokalizacja danych, przepływ danych do państw z systemem prawnym, który nie zapewnia właściwej ochrony danych. W trzeciej grupie znaleźć się mogą zagrożenia związane z brakiem transparentności i informacji co do przetwarzania danych w chmurze. Wśród nich wskazać można niejasność co do praw i obowiązków klientów i dostawców usług chmurowych, rozmycie odpowiedzialności, skomplikowanie treści umów o świadczenie usług *cloud computingu*. Ponadto usługi chmurowe stanowią wciąż na tyle nowy paradygmat przetwarzania danych, że trudno jest nadać im ramy prawne, ekonomiczne, terytorialne i czasowe, wydaje się zatem, że chmura jest nieograniczona i nieprzewidywalna. Trudność z wyznaczeniem jakiegokolwiek zakresu tego zagadnienia sprawia, że do chwili obecnej nie wprowadzono powszechnie obowiązujących regulacji prawnych zapewniających globalną kontrolę nad chmurą, pozostając na poziomie regulacji *soft law*. Opracowane dokumenty z pewnością wnoszą cenne zalecenia, wskazują kierunki działania i kształcą świadomość pożądanych zachowań zarówno administratorów danych, jak i podmiotów przetwarzających. Biorąc pod uwagę dynamikę, globalizm i złożoność

cloud computingu można dojść do wniosku, że prace nad twardymi regulacjami będą od początku skazane na niepowodzenie, z uwagi na to, że procedury legislacyjne są zbyt długotrwałe w stosunku do tempa rozwoju technologii chmurowych. Przepisy zwykle nie nadążają za tempem rozwoju nowoczesnych technologii, a od momentu ich ustanowienia do momentu rozpoczęcia stosowania mogą nie spełniać zakładanych celów. Dlatego wydaje się, że w najbliższej perspektywie główne podstawy kształtowania stosunków prawnych pomiędzy dostawcami usług chmurowych a klientami będą stanowiły przepisy RODO (a przede wszystkim zasady przetwarzania danych, przepisy dotyczące praw podmiotów danych oraz obowiązków administratorów i podmiotów przetwarzających) wraz z kierunkami wyznaczonymi w aktach prawa miękkiego (przede wszystkim Opinii 5/2012 czy tzw. Memorandum z Sopotu) oraz postanowieniami umów zawieranych przez strony. Wydaje się, że z biegiem czasu i adekwatnie do stopnia zaawansowania rozwoju i upowszechniania usług i rynku *cloud computing,* zaistnieje potrzeba wprowadzenia globalnego systemu zarządzania obszarem chmury oraz powołania organu nadzoru nad obszarem przetwarzania danych w chmurze. Możliwym rozwiązaniem byłaby umowa międzynarodowa ratyfikowana globalnie przez państwa, co obligowałoby do podjęcia działań bardziej efektywnych niż obecne.

4. Funkcje umowy powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych jest instrumentem ochrony danych, w którym uwidacznia się powiązanie i wzajemne przenikanie sfery publicznoprawnej i prywatnoprawnej. Ma ona istotne funkcje zarówno dla stron stosunku prawnego, jak i dla organu nadzoru, a pośrednio także dla podmiotów danych. Na gruncie nauk społecznych sporo uwagi zostało poświęcone pojęciu funkcji. Termin funkcja jest pojęciem wieloznacznym i może być odnoszony do pojęcia funkcji jako relacji, funkcji jako roli i funkcji jako celu[724]. Najczęściej wyróżnia się znaczenie funkcji jako skutku, ogółu następstw określonego zachowania, albo też jako cel, założony rezultat zachowania[725]. Podkreślenia wymaga, że funkcja i cel powinny być od siebie

[724] J. Helios, W. Jedlecka, *Podstawowe pojęcia prawa i prawoznawstwa dla ekonomistów*, Wrocław 2015, s. 20, http://www.bibliotekacyfrowa.pl/Content/65987/Podstawowe_pojecia_prawa_i_prawoznawstwa_dla_ekonomistow.pdf.

[725] Szerzej na temat pojęcia funkcji: M. Tenenbaum, *Instytucja zadatku w polskim prawie cywilnym*, Warszawa 2008, s. 32 i n. oraz powołana tam literatura autorstwa Z. Ziembińskiego, I. Boguckiej, A. Kędzierskiej-Cieślakowej.

odróżniane[726], wynika to m.in. z zaproponowanego na gruncie nauki prawa wyjaśnienia pojęcia funkcji prawa. Wyróżniono aż cztery jego znaczenia: jako podstawowe kierunki działalności określonej instytucji, jako cele działania, jako sposoby, metody i środki realizacji założonych celów oraz jako następstwa, skutki społeczne wywołane działaniem podmiotu[727]. Funkcja rozumiana jako rola jest społecznym oczekiwaniem co do stanu rzeczy, który ma być osiągnięty za sprawą kogoś lub czegoś, podczas gdy cel ma charakter subiektywny i jest stanem rzeczy, który ma być osiągnięty zgodnie z czyimś zamierzeniem[728]. Na gruncie wyżej przytoczonych definicji funkcji można przyjąć, że przez funkcje umowy powierzenia przetwarzania danych osobowych należy rozumieć role jakie pełni ten instrument, realizowane zadania i oddziaływania zarówno na relację stron umowy, sytuację podmiotów danych oraz organu nadzorczego. W pierwszej kolejności wymagają rozważenia funkcje tej umowy istotne dla stron umowy.

Pierwsza z funkcji umowy powierzenia przetwarzania danych osobowych nie wynika z bezpośrednich uregulowań zawartych w RODO, choć wydaje się, że powinna być z punktu widzenia prawodawcy najistotniejszą funkcją tego instrumentu. Można ją określić jako funkcję legalizacyjną. Umowa powierzenia stanowi *de facto* jedyną podstawę prawną przetwarzania danych osobowych przez podmiot niebędący administratorem. Innymi słowy, umowa powierzenia legalizuje operacje przetwarzania danych dokonywane przez zewnętrzny podmiot przetwarzający. Jak zwrócono uwagę już we wcześniejszych rozważaniach, podstawy przetwarzania danych osobowych zostały wymienione enumeratywnie w treści art. 6 RODO (w odniesieniu do danych zwykłych) oraz w art. 9 RODO (w przypadku szczególnych kategorii danych). W żadnym z wymienionych artykułów nie wspomniano o umowie powierzenia przetwarzania danych osobowych. Podmiot przetwarzający nie dysponuje zazwyczaj sformułowanymi tam przesłankami dopuszczalności przetwarzania, przykładowo- zgodę odbiera administrator, umowę z podmiotem danych zawiera administrator, obowiązek prawny obciąża administratora itd. Natomiast gdyby podmiot przetwarzający został zapytany o podstawę przetwarzania

[726] Twierdzi w tak również A. Marek [w:] *System Prawa Karnego*, Tom I, Warszawa 2010, Legalis: „Należy jednak zwrócić uwagę, iż pojęć „celu" i „funkcji" nie można utożsamiać. O ile przez cele prawa karnego (także cele kary) rozumie się oczekiwane efekty, które według przyjętych założeń prawo to powinno realizować, o tyle pojęcie funkcji odnosi się zwykle do rzeczywistych, faktycznych efektów, jakie prawo to wywołuje. Między zamierzonymi celami a rzeczywistymi efektami może występować daleko idąca rozbieżność".

[727] M. Borucka-Arctowa (red.), *Społeczne poglądy na funkcje prawa*, Wrocław-Warszawa-Kraków-Gdańsk-Łódź 1982, s. 7-8.

[728] Z. Ziembiński, *O pojmowaniu celu, zadania, roli i funkcji*, [w:] Państwo i Prawo 1987 z. 12, s. 20 i 25.

danych w imieniu i na polecenie administratora, wskazana może być *de facto* tylko zawarta przez niego umowa powierzenia. Co więcej, gdyby administrator i podmiot przetwarzający nie zawarli umowy powierzenia w wymaganej przepisami formie (pisemnej w tym elektronicznej), narażają się na zarzut przetwarzania danych bez podstawy prawnej tj. złamania zasady legalności, jak też udostępnienia danych osobom nieuprawnionym. Umowa służy tu jako zabezpieczenie interesów stron przed zarzutami dokonywania niezgodnych z prawem operacji na danych osobowych. Dlatego uzasadnionym wydaje się postulat *de lege ferenda* dodania umowy powierzenia przetwarzania danych osobowych do katalogu przesłanek dopuszczalności przetwarzania danych osobowych w art. 6 i 9 RODO.

Wśród podstawowych funkcji umowy powierzenia przetwarzania danych osobowych należy wskazać umożliwienie administratorom korzystania z usług świadczonych przez wyspecjalizowane podmioty. Administrator nie musi więc samodzielnie przetwarzać danych osobowych. Pozwala to w dużej mierze, aby przedsiębiorcy skupili się na przedmiocie swojej działalności, a kwestie związane z jej obsługą zostały przesunięte na podmioty zewnętrzne, co ma na celu usprawnienie procesów biznesowych. Funkcję tę można określić jako dynamizującą bądź kreacyjną. Przykład stanowić może podjęcie decyzji o korzystaniu z zewnętrznej obsługi księgowej czy prawnej. Odnosi się to również do jednostek sektora publicznego, które mogą sprawniej realizować swoje zadania, korzystając z pomocnych rozwiązań oferowanych przez podmioty zewnętrzne (np. specjalistyczne oprogramowanie). Konsekwencją tej funkcji jest kształtowanie się rynku usług outsourcingowych, w tym usług z zakresu przetwarzania danych osobowych, oraz specjalizowanie się podmiotów w wąskich dziedzinach i podnoszenie jakości usług.

Kolejną funkcją umowy powierzenia przetwarzania danych osobowych istotną z punktu widzenia jej stron jest funkcja organizacyjna. Postanowienia stron respektujące odpowiednie przepisy RODO tworzą ramy prawne i organizują współpracę administratora i podmiotu przetwarzającego. Funkcja ta uwidacznia się m.in. poprzez skonkretyzowanie, w jakiej formie mają być komunikowane polecenia administratora, z jakim wyprzedzeniem podmiot przetwarzający jest powiadamiany o audycie przetwarzania danych, co ma się stać z powierzonymi danymi po zakończeniu stosunku prawnego między administratorem a podmiotem przetwarzającym, czy też jak dalej powierzać dane podwykonawcom przetwarzającego. Takich ustaleń nie przewidują przepisy art. 28

RODO, a są one istotne dla obu stron w trakcie realizowania umowy powierzenia, dlatego faktycznie obopólnie korzystnym rozwiązaniem jest ujęcie tego typu kwestii w postanowieniach umowy. Ponadto należy stwierdzić, że umowne określenie zasad współpracy administratora i podmiotu przetwarzającego, w tym ustalenie pomiędzy stronami celów i sposobów przetwarzania danych, pozwala zabezpieczyć interesy stron. Powoduje uniknięcie zarzutu, że podmiot przetwarzający sam określa cele i sposoby przetwarzania, przez co naraża się na uznanie go za administratora w odniesieniu do tego przetwarzania i wynikającą z tego odpowiedzialność.

Oprócz funkcji kształtowania współpracy administratora z podmiotem zewnętrznym przetwarzającym dane osobowe na jego polecenie, umowa powierzenia pełni również funkcję zabezpieczającą. Stanowi zabezpieczenie dla administratora, w sytuacji gdy podmiot przetwarzający nie wykonuje poleceń samodzielnie, a korzysta z podwykonawców (tzw. podpowierzenie przetwarzania danych). Dzięki odpowiednim postanowieniom umownym konkretyzującym przepisy art. 28 ust. 2 i 28 ust. 4 RODO, po pierwsze administrator może mieć wpływ, kto poza podmiotem przetwarzającym ma dostęp do powierzanych danych osobowych (w tym może wyrazić swój sprzeciw lub brak zgody na obecność określonego podwykonawcy w procesie przetwarzania). Po drugie, umowa powierzenia przewiduje obowiązki podmiotów przetwarzających wobec podwykonawców, jak wybór podwykonawcy zapewniającego odpowiednie gwarancje, zawarcie umowy podpowierzenia, ponoszenie odpowiedzialności za podwykonawców. Ponadto jak stanowi treść art. 28 ust. 4 RODO, obowiązki nałożone w drodze umowy administratora z przetwarzającym są odzwierciedlone w umowie podmiotu przetwarzającego z podprzetwarzającym. Takie regulacje pozwalają zapewnić te same wymogi co do poziomu ochrony danych bez względu na to, kto faktycznie zajmuje się ich przetwarzaniem. Innymi słowy umowa powierzenia daje administratorowi wiedzę i wpływ na uczestników procesu przetwarzania danych, które zostają powierzone.

Jako odrębną można wyróżnić funkcję przymuszającą. Postanowienia umowne dotyczące „zlecenia" przetwarzania danych osobowych zawarte albo w umowie zasadniczej albo w treści odrębnej umowy, będą wymagały od podmiotu przetwarzającego i podprzetwarzającego dostosowania swojej działalności do wymogów RODO, utrzymywania jej na odpowiednim poziomie bezpieczeństwa i tym samym gwarantowania odpowiedniego (do okoliczności przetwarzania) poziomu ochrony danych osobowych.

Jednocześnie będzie to oznaczało ochronę ich interesów własnych (uniknięcie odpowiedzialności), administratora oraz osób, których powierzone dane dotyczą.

Umowa powierzenia przetwarzania danych osobowych pełni również funkcję kontrolną, zarówno wobec podmiotów przetwarzających i podprzetwarzających, jak i administratorów. Realizowane jest to w kilku aspektach. Po pierwsze, w treści umowy administrator może zobowiązać podmiot przetwarzający do zgłaszania mu w ustalonym czasie wszelkich naruszeń ochrony danych osobowych przetwarzanych na polecenie administratora. Dzięki temu administrator jest na bieżąco informowany o zaistniałych naruszeniach i ma możliwość podejmowania natychmiastowych reakcji. Po drugie, funkcja kontrolna wiąże się z omówionymi już możliwościami podejmowania działań na skutek informowania o podwykonawcach podmiotu przetwarzającego (zgoda, brak zgody, sprzeciw). Kolejny aspekt funkcji kontrolnej to możliwość przeprowadzania audytów i inspekcji dotyczących przetwarzania danych przez podmiot przetwarzający. Ten aspekt jest ważny nie tylko dla administratora – również interes podmiotu przetwarzającego jest chroniony jeśli postanowienia umowy będą przewidywać np. częstotliwość audytów, termin uprzedzenia strony, zakres audytu. Można więc powiedzieć, że funkcja kontrolna umowy powierzenia przetwarzania danych osobowych zabezpiecza interesy obu stron umowy.

Powiązana z powyższymi funkcjami jest kolejna funkcja umowy powierzenia przetwarzania danych osobowych, którą można określić jako funkcję regulacyjno-represyjną. Umowa stanowi określenie odpowiedzialności stron umowy za działania bądź zaniechania niezgodne z treścią umowy lub przepisami prawa. Co za tym idzie, przedmiotowa umowa umożliwia dochodzenie roszczeń z tytułu odpowiedzialności kontraktowej stron. W przypadku gdy mamy do czynienia z łańcuchem powierzeń, umowa powierzenia umożliwia pociągnięcie do odpowiedzialności podmiotów uczestniczących w procesie przetwarzania. Należy też pamiętać o odpowiedzialności podmiotu przetwarzającego wobec administratora, wynikającej z art. 28 ust. 4 RODO, który stanowi, że jeżeli 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. Oczywiście można kwestie odpowiedzialności potraktować w treści umowy bardzo lakonicznie bądź w ogóle pominąć, co w razie zaistniałej potrzeby będzie skutkowało zastosowaniem przepisów RODO (w tym art. 82

i 83 RODO) oraz odpowiednich przepisów Kodeksu cywilnego. Pomimo kontrowersji co do tego zagadnienia, w nauce wyrażane są stanowiska o dopuszczalności ograniczania odpowiedzialności podmiotu przetwarzającego względem administratora. Negatywnie postrzegane są natomiast działania prowadzące do obciążenia podmiotów przetwarzających potencjalnymi kosztami kar nałożonych na administratorów, co dość często jest spotykane w praktyce stosowania umów powierzenia[729]. W zakresie funkcji związanej z przypisywaniem odpowiedzialności umowa powierzenia ma jeszcze inną istotną kwestię. Jeśli podmiot przetwarzający działa wbrew poleceniom administratora bądź wykracza poza granice poleceń, czyli nie realizuje postanowień umowy, a także naruszy wymogi RODO, uznaje się go za administratora w odniesieniu do tego przetwarzania. W konsekwencji tego, to on pozostaje w pełni odpowiedzialny za niezgodne z przepisami prawa przetwarzanie danych osobowych, co skutkować może nałożeniem przez organ nadzorczy kary pieniężnej. Ponadto umowa powierzenia przetwarzania danych osobowych może znacznie ułatwiać dochodzenie prawa do odszkodowania przez osobę, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia RODO, zgodnie z treścią art. 82 RODO.

Dotychczasowe rozważania nad funkcjami umowy powierzenia przetwarzania danych osobowych dotyczyły perspektywy stron umowy, tj. administratora i podmiotu przetwarzającego, ewentualnie podmiotów powiązanych- podprzetwarzających. Warto spojrzeć na to zagadnienie również z innych punktów widzenia. Przede wszystkim podkreślenia wymaga, że umowa powierzenia pełni funkcję dowodową, ponieważ wspomaga realizację zasady rozliczalności (zgodnie z treścią art. 5 ust. 2 administrator jest odpowiedzialny za przestrzeganie zasad wynikających z RODO i musi być w stanie wykazać ich przestrzeganie). Umowa zawarta w wymaganej formie może stanowić dowód podczas kontroli Prezesa Urzędu Ochrony Danych Osobowych. Dzięki niej administrator będzie mógł wykazywać, że spełnia wymogi art. 28 RODO, że nie udostępnia danych podmiotowi nieuprawnionemu oraz generalnie dokłada należytej staranności w procesie przetwarzania danych osobowych. Należy tu pamiętać, że ciężar dowodu leży po stronie kontrolowanego, który musi wykazać, że dopełnił obowiązków, co wynika wprost z art. 5 ust. 2 RODO – administrator musi być w stanie wykazać przestrzeganie przepisów RODO. Z perspektywy organu nadzoru właściwie zawarta umowa powierzenia przetwarzania

[729] Tak m.in. A. P. Czarnowski, M. Gawroński, P. Naklicka [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018, s. 389-390.

danych osobowych będzie mogła stanowić dowód pozwalający nie zastosować sankcji wobec kontrolowanego.

Warto tu podkreślić, że umowa powierzenia może mieć też istotną funkcję informacyjną i zabezpieczającą dla podmiotów danych. Po pierwsze, dzięki temu instrumentowi osoba, której dane dotyczą może dowiedzieć się kto przetwarza jej dane w imieniu administratora (choć niebezpośrednio, bo prawo do takiej informacji wynika z innego instrumentu - zgodnie z art. 13 RODO osobę należy poinformować o odbiorcach jej danych, a w myśl przepisów RODO podmiot przetwarzający należy do kategorii odbiorców). Po drugie umowa powierzenia może okazać się pomocnym instrumentem dla osoby, której dane dotyczą i która poniosła szkodę w wyniku przetwarzania danych niezgodnie z RODO. Postanowienia umowy, przede wszystkim dotyczące podpowierzenia mogą być istotne dla ustalenia odpowiedzialności za powstałą szkodę. Należy przy tym pamiętać, że podmioty danych bezpośrednio nie dysponują umową powierzenia jako dowodem w dochodzeniu swoich roszczeń, a przepisy RODO właściwie nie przewidują takich rozwiązań jak udostępnienie przez administratora treści umowy osobie, której powierzone dane dotyczą. Jednakże w ramach prawa dostępu do swoich danych wynikającego z treści art. 15 RODO, osoba ma możliwość uzyskania od administratora informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione. W zakresie pojęcia odbiorcy mieszczą się również podmioty przetwarzające, co oznacza, że podmiot danych korzystając na wniosek z prawa dostępu do danych ma prawo wiedzieć, komu administrator powierzył jego dane w drodze umowy. Faktycznie możliwe jest, że gdyby takiej umowy nie było, osoba fizyczna nie dowiedziałaby się, że jej dane są przetwarzane przez inny podmiot poza administratorem.

Reasumując można powiedzieć, że główną funkcją umowy powierzenia przetwarzania danych osobowych jest szeroko rozumiane zabezpieczanie interesów stron, zarówno wzajemnie wobec siebie, jak i w odniesieniu do organu nadzoru (Urzędu Ochrony Danych Osobowych). Może się zdarzyć, że umowa powierzenia okaże się też instrumentem pomocnym dla osoby, której dane dotyczą, w przypadku wyrządzenia jej szkody. Tu jednak trzeba pamiętać, że podmiot danych raczej nie będzie miał realnej możliwości wglądu w treść umowy łączącej administratora z podmiotem przetwarzającym. W takim przypadku można polegać na prawie dostępu do danych osobowych, a następnie na przepisach dotyczących odpowiedzialności podmiotu przetwarzającego głównie na treści art. 82 RODO stanowiącego, że każda osoba, która poniosła szkodę majątkową lub

niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

ROZDZIAŁ V

Odpowiedzialność stron umowy powierzenia przetwarzania danych osobowych jako przejaw realizacji funkcji ochronnej

1. Odpowiedzialność prywatnoprawna, odpowiedzialność publicznoprawna – uwagi ogólne

Dociekania dotyczące umowy powierzenia przetwarzania danych osobowych byłyby niepełne bez uwzględnienia kwestii odpowiedzialności zarówno na gruncie prawa prywatnego, jak i publicznego. Najwięcej uwagi należy poświecić odpowiedzialności na gruncie prawa prywatnego, co uzasadnione jest charakterem tego instrumentu ochrony danych osobowych, będącego stosunkiem umownym pomiędzy administratorem a podmiotem przetwarzającym. Dlatego też odpowiedzialność administracyjna oraz karna zostanie tu przedstawiona tylko w podstawowym zakresie.

Według klasycznego ujęcia odpowiedzialności prawnej, jest to ponoszenie przez podmiot przewidzianych prawem ujemnych konsekwencji za zdarzenia lub stany rzeczy podlegające ujemnej kwalifikacji normatywnej i przypisywalne prawnie określonemu podmiotowi w danym porządku prawnym[730]. Ogólnie przyjęty jest podział odpowiedzialności ze względu na metodę regulacji prawnej, czyli na odpowiedzialność cywilną, administracyjną i karną. W obszarze przetwarzania danych osobowych możliwe jest ponoszenie każdego z wymienionych rodzajów odpowiedzialności.

Zarówno na gruncie prawa prywatnego jak i prawa publicznego odpowiedzialność jest ważnym uzupełnieniem każdej konstrukcji prawnej. Jej istnienie wzmacnia, a czasem wręcz umożliwia realizację podstawowych funkcji prawa. Bez odpowiedzialności często trudno byłoby osiągnąć rzeczywisty, obiektywny skutek, rezultat istnienia jakiejś instytucji czy normy prawnej. W literaturze zwykle wymienia się funkcję ochronną, organizacyjną, represyjną, wychowawczą, kontrolną, dystrybutywną i szereg innych funkcji prawa[731]. Trzeba tu podkreślić, że na różnych obszarach prawa różnie układa się nasilenie realizacji określonych funkcji. Dla przykładu w prawie karnym zdecydowanie widoczna jest funkcja represyjna, a w prawie prywatnym chodzi głównie o ochronę interesów majątkowych

[730] W. Lang, *Struktura odpowiedzialności prawnej* [w:] „Prawo" 1968 nr 8 s.12.
[731] T. Chauvin, T. Stawecki, P. Winczorek, *Wstęp do prawoznawstwa,* Warszawa 2016, s. 179 i n.

(oraz niektórych wartości niemajątkowych, takich jak np. dobra osobiste). Rzecz jasna, że instrumenty prawne dotyczące odpowiedzialności mogą być wykorzystywane jako narzędzie do osiągania założonych celów, jednakże tylko z uwzględnieniem społecznie akceptowalnych wartości. W przeciwnym razie może dojść do instrumentalizacji prawa, które przestanie być gwarantem sprawiedliwości czy pewności w stosunkach między ludźmi. Wychodząc z takiego założenia należy przede wszystkim odnieść się do problematyki odpowiedzialności odszkodowawczej, administracyjnej i karnej stron umowy powierzenia przetwarzania danych osobowych w przypadku naruszenia przepisów prawa ze sfery ochrony danych osobowych. Należy podkreślić, że funkcja ochronna prawa ma podstawowe znaczenie zarówno w samym procesie przetwarzania danych osobowych jak i w przypadku naruszenia zasad przetwarzania.

Prawodawca unijny uregulował zagadnienie odpowiedzialności na gruncie prawa prywatnego w sposób rozproszony, częściowo w treści art. 28 RODO i częściowo w art. 82 i 83 RODO. W przepisach tych zawiera się szereg kwestii, które muszą być uzupełnione w drodze wyinterpretowania z przepisów prawa krajowego, np. zasady odpowiedzialności czy też zasady naprawienia szkody. Należy zauważyć, że o ile prawodawca uwzględnił kwestię odpowiedzialności cywilnej administratora i podmiotu przetwarzającego wobec osób, których dane dotyczą, jak również odpowiedzialności podmiotu przetwarzającego za podprzetwarzających, to nie poświęcił uwagi na podstawową relację podmiotu przetwarzającego z administratorem.

2. Odpowiedzialność odszkodowawcza z tytułu wyrządzenia szkody przy przetwarzaniu danych osobowych

Pojęcie odpowiedzialności na gruncie prawa cywilnego, które jest trzonem prawa prywatnego najogólniej wyjaśnia się jako ponoszenie przez podmiot stosunków cywilnoprawnych ujemnych konsekwencji przewidzianych przez przepisy prawa cywilnego, za fakty ocenione ujemnie z punktu widzenia porządku prawnego oraz przypisane temu podmiotowi przez prawo cywilne[732]. Sankcje cywilne nie mają na celu wymierzenia dolegliwości podmiotowi bezprawnego zachowania, a raczej przywrócenie naruszonego stanu prawnego, przy czym nadaje się odpowiedzialności cywilnej

[732] W. Lang, *Struktura...*, op. cit., s. 22, A. Stelmachowski, *Wstęp do teorii prawa cywilnego*, Warszawa 1984, s. 22 i n.

kompleksowy charakter poprzez jednoczesną realizację funkcji kompensacyjnej, penalnej i wychowawczo-prewencyjnej[733].

Odpowiedzialność cywilna może przybierać różną postać (w jej zakres wchodzić mogą konsekwencje prawne o różnorodnym charakterze, jak np. nieważność czynności prawnej, przymusowe wykonanie zobowiązania czy też odstąpienie od umowy, rozwiązanie lub przekształcenie stosunku prawnego[734]), ale najdonioślejszą rolę odgrywa odpowiedzialność odszkodowawcza. Uzasadnia się to faktem, że o ile strony dążą do realnego wykonania zobowiązania, to odpowiedzialność odszkodowawcza jest stosowana bardzo często z uwagi na trudności w wymuszeniu spełnienia świadczenia *in natura*[735]. W nauce prawa ustalono, że istotą odpowiedzialności odszkodowawczej jest możliwość zaspokajania roszczeń wierzyciela z tytułu wyrządzonej mu szkody, w drodze egzekucji z majątku osoby, której przypisano tę szkodę[736]. Ma ona zastosowanie do wszystkich stosunków zobowiązaniowych, których treścią jest obowiązek naprawienia szkody, w reżimie deliktowym i kontraktowym. Podkreślić należy, że przypadki, kiedy odszkodowanie jest przedmiotem świadczenia zostały podzielone na trzy grupy[737]. W pierwszej znajdują się sytuacje, gdy szkoda rodzi samoistny stosunek zobowiązaniowy, bo zostaje wyrządzona niezależnie od istniejącego wcześniej stosunku prawnego między wyrządzającym i odnoszącym szkodę. Takie przypadki mają miejsce, w odniesieniu do relacji administratora danych (bądź podmiotu przetwarzającego) z osobami, których przetwarzane dane dotyczą – pierwotnie nie ma między nimi żadnego stosunku zobowiązaniowego, powstaje on dopiero na skutek wyrządzenia szkody podmiotowy danych. Drugą grupą są przypadki, kiedy szkoda jest wyrządzona przez niewykonanie lub nienależyte wykonanie zobowiązania przez dłużnika. Ma to miejsce w sytuacji, kiedy administrator „zleca" przetwarzanie danych osobowych innemu podmiotowi w drodze umowy powierzenia. Powstaje tu stosunek zobowiązaniowy w postaci umowy, w którym wierzycielem jest administrator danych, a dłużnikiem podmiot przetwarzający i niewykonanie bądź nienależyte wykonanie umowy spowoduje szkodę po stronie administratora lub osoby, której dane dotyczą. Natomiast do trzeciej grupy zalicza się przypadki, gdy dany podmiot zobowiązuje się do spełnienia świadczenia

[733] S. Prutis, *Instytucje..., op. cit*., s. 378. Dodatkowo, w nauce prawa wyróżnia się też funkcję prewencyjną, represyjną i repartycyjną – tak M. Kaliński, *Szkoda na mieniu i jej naprawienie*, Warszawa 2008, s. 160-169.
[734] A. Stelmachowski, *Zarys..., op. cit.*, s. 212.
[735] S. Prutis, *Instytucje..., op. cit*., s. 377.
[736] T. Dybowski [w:] Z. Radwański (red.), *System Prawa Cywilnego.* Tom III, Wrocław, Warszawa, Kraków, Gdańsk, Łódź 1981, s. 167.
[737] S. Prutis, *Instytucje..., op. cit*., s. 388.

odszkodowawczego na rzecz kontrahenta, gdy wyrządzona zostanie mu szkoda. Chodzi tu przede wszystkim o umowy ubezpieczeniowe, gdzie świadczenie odszkodowawcze staje się głównym świadczeniem. Do tej grupy przypadków przepisy RODO nie odnoszą się.

Tradycyjnie w doktrynie prawa cywilnego wskazywane są dwa reżimy odpowiedzialności odszkodowawczej. Chodzi tu o odpowiedzialność z tytułu czynów niedozwolonych, zwaną odpowiedzialnością *ex delicto,* i odpowiedzialność kontraktową, czyli z tytułu niewykonania bądź nienależytego wykonania zobowiązania nazywaną odpowiedzialnością *ex contractu*. Dualizm ten został zachowany w konstrukcji Kodeksu cywilnego (odpowiedzialności z czynów niedozwolonych dotyczą art. 415 KC i n., a kontraktowej art. 471 KC i n.), choć znajdują się w niej również wspólne dla obu podstaw przepisy, jak te dotyczące naprawienia szkody (art. 361-363 KC) czy zbiegu podstaw odpowiedzialności deliktowej i kontraktowej (art. 443 KC). Z biegiem czasu okazało się, że po pierwsze, nieuzasadnione jest ostre rozgraniczanie i przeciwstawianie obu klasycznych podstaw odpowiedzialności, a po drugie dualizm jest niewystarczający[738]. Przede wszystkim zaproponowano rozszerzenie systematyki reżimów odpowiedzialności również o odpowiedzialność z tytułu szkód przy wykonywaniu funkcji publicznych[739], odpowiedzialność z tytułu szkód przy wykonywaniu praw podmiotowych, odpowiedzialność gwarancyjną, odpowiedzialność z tytułu szkód poniesionych w cudzym lub wspólnym interesie[740]. Prowadzone w tej części dysertacji rozważania skupiają się na klasycznych reżimach odpowiedzialności: *ex delicto* i *ex contractu*.

Odpowiedzialność z tytułu niewykonania lub nienależytego wykonania zobowiązania uregulowana jest w treści art. 471 i n. Kodeksu cywilnego. Zgodnie z treścią art. 471 KC dłużnik obowiązany jest do naprawienia szkody wynikłej z niewykonania lub nienależytego wykonania zobowiązania, chyba że niewykonanie lub nienależyte wykonanie jest następstwem okoliczności, za które dłużnik odpowiedzialności nie ponosi.

Rozpocząć należy od tego, że podstawowym i oczekiwanym sposobem wykonania zobowiązania jest spełnienie świadczenia, czyli takie zachowanie dłużnika, które odpowiada treści zobowiązania. Przenosząc to na grunt zobowiązania, jakim jest przetwarzanie danych osobowych na polecenie administratora, można powiedzieć,

[738] O tym wspominał już T. Dybowski [w:] Z. Radwański (red.), *System..., op. cit.*, s. 182 i n.
[739] Szerzej na ten temat Z. Banaszczyk, *Odpowiedzialność za szkody wyrządzone przy wykonywaniu władzy publicznej*, Warszawa 2012.
[740] M. Kaliński [w:] A. Olejniczak (red.), *System Prawa Prywatnego.* Tom VI, Warszawa 2018, Legalis.

że spełnieniem świadczenia będzie zachowanie podmiotu przetwarzającego, które spełnia wymogi art. 28 RODO (realizuje nałożone w tym przepisie obowiązki np. odpowiednie zabezpieczenie danych czy też wspieranie administratora), jak również spełnia wymogi ustalone przez strony w treści umowy powierzenia przetwarzania danych osobowych. Na gruncie przedmiotowej umowy, z uwagi na jej skomplikowaną treść, bardzo złożoną sferę obowiązków podmiotu przetwarzającego, a także akcesoryjny charakter umowy powierzenia i zaliczenie jej do umów starannego działania a nie rezultatu, bardzo trudno byłoby rozgraniczyć sytuacje, kiedy podmiot przetwarzający nie wykonuje zobowiązania, a kiedy wykonuje zobowiązanie nienależycie. Należy zauważyć, że w praktyce dla samego ponoszenia odpowiedzialności *ex contractu* nie ma znaczenia, czy zobowiązanie nie zostało wykonane czy zostało wykonane nienależycie. Co do zasady z obydwoma stanami łączy się ten sam skutek – pełna odpowiedzialność dłużnika, niezależna od stopnia naruszenia zobowiązania[741]. Rozgraniczenie to istotne jest dla mechanizmu przyczynienia się poszkodowanego do powstania szkody (art. 362 KC), obliczania wysokości odszkodowania, gdy wynika ona z częściowo wykonanego zobowiązania oraz gdy zobowiązanie w całości nie zostało spełnione[742].

W zakresie stosunku prawnego, jakim jest powierzenie przetwarzania danych osobowych, odpowiedzialność *ex contractu* ponosić może podmiot przetwarzający wobec administratora, albo też podmiot podprzetwarzający wobec podmiotu przetwarzającego. Przykładów nienależytego wykonania umowy powierzenia, które mogą spowodować szkodę jest dużo. Przede wszystkim podmiot przetwarzający naraża się na odpowiedzialność poprzez spowodowanie szkody, nie realizując poleceń administratora lub wychodząc poza ich zakres, nie stosując lub stosując niewłaściwe środki zabezpieczania danych osobowych, wybierając podmiot podprzetwarzający niezapewniający stosownych gwarancji lub podpowierzając przetwarzanie danych osobowych bez zgody administratora. Zaznaczyć trzeba, że świadczenie odszkodowawcze ma w przypadku reżimu odpowiedzialności kontraktowej charakter zastępujący lub uzupełniający świadczenie główne[743].

W kontekście przepisów RODO odpowiedzialność kontraktowa pojawia się w treści art. 28 ust. 4 RODO. Dotyczy on możliwości korzystania przez podmiot

[741] W. J. Katner [w:] M. Stec (red.), *System ..., op. cit.*, s. 397.
[742] M. Gutowski (red.), *Kodeks cywilny. Tom II. Komentarz. Art. 353–626*. Warszawa 2019, Legalis.
[743] T. Dybowski [w:] Z. Radwański (red.), *System..., op. cit.*, s. 184.

przetwarzający z podwykonawców (podpowierzenie przetwarzania danych osobowych) i nakłada obowiązek zawarcia umowy pomiędzy podmiotem przetwarzającym a podprzetwarzającym. Jest to stosunek prawny w którym zachodzi trójstopniowy łańcuch powierzenia (administrator danych powierza przetwarzanie danych osobowych podmiotowi przetwarzającemu, a ten „podzleca" przetwarzanie podmiotowi podprzetwarzającemu). W sytuacji gdy administrator poniósłby szkodę, prawodawca postanowił, że jeżeli podmiot podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, to pełna odpowiedzialność wobec administratora za wypełnienie obowiązków kolejnego podmiotu przetwarzającego (nazywanego podprzetwarzającym) będzie spoczywać na pierwotnym podmiocie przetwarzającym. Z uwagi na fakt, że podmioty w łańcuchu powierzeń łączą umowy, będzie miał tu zastosowanie reżim odpowiedzialności kontraktowej. W związku z tym mamy do czynienia z odpowiedzialnością za inne osoby i odnieść się należy do treści art. 474 KC, który stanowi, że dłużnik odpowiedzialny jest jak za własne działanie lub zaniechanie za działania i zaniechania osób, z których pomocą zobowiązanie wykonywa, jak również osób, którym wykonanie zobowiązania powierza. Gdyby natomiast podmiotu przetwarzającego z podprzetwarzającym nie łączyło zobowiązanie ze stosunku umownego (co byłoby *de facto* niezgodne z treścią art. 28 ust. 4 RODO), podstawą prawną naprawienia szkody poniesionej przez administratora byłby art. 429 KC, stanowiący, że kto powierza wykonanie czynności drugiemu, ten jest odpowiedzialny za szkodę wyrządzoną przez sprawcę przy wykonywaniu powierzonej mu czynności, chyba że nie ponosi winy w wyborze albo że wykonanie czynności powierzył osobie, przedsiębiorstwu lub zakładowi, które w zakresie swej działalności zawodowej trudnią się wykonywaniem takich czynności. Wina w wyborze i zawarte w tym przepisie domniemanie winy powierzającego zmienia klasyczny rozkład ciężaru dowodu, czyli jest odstępstwem od art. 6 KC, co ułatwia sytuację osoby poszkodowanej. Można więc powiedzieć, że art. 429 KC zawiera konstrukcję odpowiedzialności na zasadzie winy lecz jest ona ostrzejsza w stosunku do sprawcy szkody (z uwagi na domniemanie winy), niż odpowiedzialność na podstawie art. 415 KC. Warto też zauważyć, że art. 429 KC nie zwalnia z odpowiedzialności bezpośredniego sprawcę szkody, bowiem może on odpowiadać na zasadzie przewidzianej w art. 415 KC. Tak wiec nie można ty wyłączyć konstrukcji odpowiedzialności solidarnej na podstawie art. 441 KC.

Współcześnie przez czyn niedozwolony rozumie się różne zdarzenia kreujące odpowiedzialność odszkodowawczą, w tym także zdarzenia generalnie dozwolone przez prawo lub całkowicie oderwane od zachowania człowieka (czyn niedozwolony w znaczeniu techniczno-prawnym)[744]. Nie ma zamkniętego katalogu czynów niedozwolonych, są to to fakty przewidziane nie tylko w art. 415–449 KC, lecz także w innych przepisach Kodeksu Cywilnego (np. art. 449^1 i n. KC) oraz w pozakodeksowych aktach prawnych[745]. Charakterystyczne dla tego reżimu odpowiedzialności jest to, że w odróżnieniu od odpowiedzialności kontraktowej, szkoda zostaje wyrządzona niezależnie od istniejącego uprzednio stosunku zobowiązaniowego. Wyrządzenie szkody staje się samoistnym źródłem zobowiązania, prawo czyni kogoś za tę szkodę odpowiedzialnym, a naprawienie szkody jest głównym świadczeniem dłużnika[746]. Czyn niedozwolony może popełnić każdy i polega to na naruszeniu powszechnie obowiązujących norm prawnych, z wyłączeniem norm dotyczących wykonania zobowiązań. W nauce prawa i judykaturze, na gruncie Kodeksu Cywilnego wyróżnia się kilka podstaw odpowiedzialności deliktowej: odpowiedzialność za własne czyny, odpowiedzialność za cudze czyny, odpowiedzialność za rzeczy i zwierzęta oraz odpowiedzialność wynikającą z posługiwania się elementarnymi siłami przyrody.

Na gruncie przepisów RODO i zagadnienia powierzenia przetwarzania danych osobowych, odpowiedzialność *ex delicto* wynika z treści art. 82 ust. 1 RODO. Stanowi on, że każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę. Przepis ten należy zestawić z wyróżnianymi w nauce prawa czterema cechami charakterystycznymi dla czynu niedozwolonego. Jako podstawową wskazuje się, że musi być to fakt, z którym ustawa wiąże obowiązek naprawienia szkody. Z treści powołanego przepisu wynika, że za zachowanie naruszające rozporządzenie i powodujące szkodę należne jest odszkodowanie (forma odpowiedzialności). Ponadto można dodać, że obowiązek naprawienia szkody powstaje przy zaistnieniu normalnego związku przyczynowego między szkodą a zachowaniem się sprawcy. Drugą cechą wskazywaną w nauce prawa jest to, że

[744] P. Machnikowski, A. Śmieja [w:] A. Olejniczak (red.), *System..., op. cit*., Legalis. Autorzy wskazują, że „współczesne rozumienie czynu niedozwolonego jest bez porównania szersze niż tradycyjne pojmowanie deliktu, ponieważ obejmuje także odpowiedzialność uniezależnioną od winy osoby odpowiadającej za szkodę, a nawet odpowiedzialność za zdarzenia niewiele mające wspólnego – przynajmniej z normatywnego punktu widzenia – z zachowaniem się człowieka".
[745] *Ibidem*.
[746] T. Dybowski [w:] Z. Radwański (red.), *System..., op. cit.*, s. 182.

powstanie tego obowiązku nie może być uzależnione od uprzedniego istnienia więzi prawnej między zobowiązanym do naprawienia szkody a podmiotem, który doznał szkody. Samo przetwarzanie danych osobowych nie jest stosunkiem prawnym pomiędzy osobą fizyczną a administratorem. Przetwarzanie może się opierać o podstawę legalizującą to działanie, która jest więzią prawną (np. przetwarzanie danych osobowych pracowników jako realizacja umowy o pracę), ale powstanie obowiązku odszkodowawczego nie jest związane z tym stosunkiem, jest obowiązkiem samoistnym. Ponadto przepis wskazuje, że prawo do odszkodowania ma każda osoba, nie ma tu mowy o osobach połączonych więzią prawną z administratorem lub podmiotem przetwarzającym. Po trzecie wskazywane jest, że zdarzenie powodujące szkodę wywołuje skutki prawne *ex lege*. W kontekście analizowanego przepisu art. 82 ust. 1 RODO, zachowanie naruszające rozporządzenie i powodujące szkodę skutkuje obowiązkiem odszkodowawczym, co wprost wynika z treści przepisu. Ostatnią z wymienianych w nauce prawa cech czynu niedozwolonego jest to, że świadczenie odszkodowawcze ma mieć charakter świadczenia głównego i pierwotnego. Jest to połączenie z samoistnym charakterem obowiązku odszkodowawczego, który wynika z treści art. 82 ust. 1 RODO, odszkodowanie nie będzie uzupełniało ani zastępowało innego świadczenia między stronami jak w odpowiedzialności *ex contractu* (bo nie ma między nimi innego zobowiązania), tylko będzie świadczeniem pierwotnym i głównym. Reasumując, przepis art. 82 ust. 1 RODO przewiduje deliktową odpowiedzialność administratora lub podmiotu przetwarzającego za spowodowanie szkody przetwarzaniem danych naruszającym RODO.

Bez względu na reżim odpowiedzialności do zaistnienia obowiązku naprawienia szkody potrzebne są trzy klasycznie wymieniane przesłanki odpowiedzialności odszkodowawczej. Są to zaistnienie szkody, zaistnienie zdarzenia, z którym ustawa wiąże obowiązek naprawienia szkody oraz zaistnienie normalnego (adekwatnego) związku przyczynowego pomiędzy zdarzeniem a wystąpieniem szkody (art. 361 KC). Łączne wystąpienie w stanie faktycznym tych trzech elementów warunkuje powstanie odpowiedzialności odszkodowawczej.

Szkoda ma znaczenie prawne, o ile przepisy prawa przewidują obowiązek jej naprawienia, w pozostałym zakresie jest to kategoria głównie ekonomiczna. Ma ona charakter podstawowy wśród przesłanek odpowiedzialności, ponieważ dopiero wtedy, gdy ustalone zostanie, czy szkoda miała miejsce, można analizować pozostałe przesłanki by

dojść do wniosku czy i kto będzie ponosił odpowiedzialność[747]. O ile normatywnej definicji szkody nie sformułowano, to w doktrynie wypracowano rozumienie szkody jako uszczerbku w prawnie chronionych dobrach (interesach), który wyraża się w różnicy pomiędzy istniejącym stanem dóbr i mogącym się wytworzyć w normalnej kolei rzeczy oraz stanem dóbr powstałym na skutek zdarzenia, z którym związana jest odpowiedzialność odszkodowawcza[748].

W nauce prawa ustalone zostało, że dla powstania odpowiedzialności szkoda ma być bezprawna. Oznacza skutki naruszenia prawnie chronionego interesu. O ile interes jest chroniony prawnie, to jego naruszenie prowadzi do powstania szkody bezprawnej, innymi słowy irrelewantne dla odpowiedzialności są zachowania sprzeczne z obowiązującym porządkiem prawnym, ale niepowodujące naruszenia prawnie chronionych interesów[749]. Już na tym etapie można powiedzieć, że szkoda wyrządzona przy przetwarzaniu danych osobowych może być rozpatrywana w kategorii szkody bezprawnej, w kilku aspektach. Po pierwsze, jak stwierdzono w pierwszym rozdziale rozprawy, dane osobowe są szczególnym rodzajem dóbr, blisko związanych z osobą, której dotyczą. Mogą być postrzegane w kategorii dóbr osobistych lub też w kategorii informacji, obie kategorie podlegają prawnej ochronie. Prawo do ochrony danych osobowych jest emanacją prawa do prywatności[750]. Istnieją regulacje prawa krajowego, unijnego i międzynarodowego, które gwarantują ochronę danych osobowych oraz prawa do ochrony danych osobowych i prywatności. W związku z tym bez wątpienia szkoda związana z przetwarzaniem danych będzie skutkiem naruszenia prawnie chronionego interesu, zatem będzie szkodą bezprawną.

Najwyższy szczebel klasyfikacji pojęcia szkody według kryterium przedmiotu oddziaływania zdarzenia szkodzącego na sferę dóbr poszkodowanego stanowi podział na szkodę majątkową i szkodę niemajątkową[751]. Szkoda majątkowa ma miejsce, gdy przedmiotem uszczerbku stają się dobra i interesy, których wartość da się ustalić w ekonomicznym mierniku wartości – w pieniądzu, a szkoda niemajątkowa dotyczy uszczerbku w dobrach i interesach, których wartość nie daje się adekwatnie wyrazić

[747] S. Prutis, *Instytucje..., op. cit.*, s. 397-398.
[748] M. Kaliński, *Szkoda..., op. cit.*, s. 172-175.
[749] *Ibidem*, s. 68-70.
[750] Na temat prywatności zob. szerzej np. A. Kopff, *Ochrona sfery życia prywatnego jednostki w świetle doktryny i orzecznictwa*, ZNUJ 1982, nr 100, s. 35; Uchwała 7 sędziów SN z 16.07.1993 r., I PZP 28/93 OSCCP 1994, nr 1, poz. 2; Wyrok SN z 18.01.1984 r., I CR 400/83, OSNC 1984, nr 11, poz. 195.
[751] M. Kaliński [w:] A. Olejniczak (red.), *System..., op. cit.*, Legalis.

i ocenić w pieniądzu[752]. Podkreślić natomiast trzeba, że użycie przez ustawodawcę przy określaniu zakresu obowiązku odszkodowawczego pojęcia szkody bez dalszego określenia nawiązującego do charakteru naruszonych dóbr, oznacza, że indemnizacja (w postaci odszkodowania i zadośćuczynienia) obejmuje zarówno szkodę majątkową, jak i niemajątkową. Regulacja art. 361 § 2 KC generalnie ustala zakres obowiązku odszkodowawczego do normalnych następstw działania lub zaniechania. Zasadniczo tak zakreślony obowiązek naprawienia szkody obejmuje straty i utracone korzyści. Roszczenie o zadośćuczynienie musi być uzasadnione przepisem szczególnym (448 i 445 KC)[753]. Pomijając w tym miejscu inne klasyfikacje szkody występujące w literaturze i judykaturze[754], należy stwierdzić, że szkoda związana z przetwarzaniem danych osobowych może być zarówno szkodą majątkową (w przeważającym zakresie), jak i szkodą niemajątkową (w rzadszych przypadkach). W przypadku szkód wyrządzonych administratorom danych przez podmioty przetwarzające i podprzetwarzające, będą to dla przykładu straty finansowe, utrata wiarygodności, utrata pozycji na rynku, utrata klientów, zmniejszenie lub utrata dochodów, zasobów własnych. W zakresie szkód wyrządzonych na skutek przetwarzania danych, w dobrach osób, których przetwarzane dane dotyczą, mogą częściej niż w poprzednim przypadku wystąpić szkody niemajątkowe. Może to być np. ciężki uszczerbek na zdrowiu (wywołany np. długotrwałym stresem i poczuciem braku bezpieczeństwa z powodu wycieku danych z systemu bankowości elektronicznej) czy też utrata dobrego imienia (np. na skutek popełnionych oszustw w związku z kradzieżą tożsamości).

W dalszej klasyfikacji pojęcia szkoda dokonuje się rozróżnienia w ramach szkody majątkowej na szkodę na mieniu i szkodę na osobie. Szkoda na mieniu to negatywne reperkusje naruszenia własności i innych praw majątkowych poszkodowanego. Szkoda na osobie to powstające w sferze majątkowej skutki naruszenia dóbr osobistych poszkodowanego[755]. Na gruncie ochrony danych osobowych mogą wystąpić oba rodzaje szkody majątkowej, co potwierdzają wskazane wyżej przykłady możliwych szkód związanych z przetwarzaniem danych. W obu przypadkach będzie chodziło o straty

[752] T. Dybowski [w:] Z. Radwański (red.), *System..., op. cit.,* s. 221;
[753] M. Kaliński [w:] A. Olejniczak (red.), *System..., op. cit.,* Legalis.
[754] M. Kaliński, *Szkoda..., op. cit*., s. 474-475, także uchwała SN z 12.10.2001 r., III CZP 57/01, OSNC 2002, nr 5, poz. 57 dotycząca pojęcia szkody handlowej; Wyrok z 17.01.2001 r. SA w Katowicach, I ACa 1094/00, Legalis nr 52338 odnoszący się do szkody ewentualnej.
[755] M. Kaliński, *Szkoda..., op. cit*., s. 241.

i utracone korzyści (*damnum emergens i lucrum cessans*), bowiem ustawodawca nie ograniczył tu zakresu naprawienia szkody.

W doktrynie prawa cywilnego wyróżniana jest też szkoda obecna i szkoda przyszła, które łączą się z chwilą ustalenia rozmiaru szkody. Przyjęto, że szkoda obecna to uszczerbek istniejący w chwili orzekania stwierdzony na podstawie faktów, które już zaistniały, a szkoda przyszła to uszczerbek, który może powstać po wydaniu wyroku zasądzającego odszkodowanie[756]. Co do zasady uwzględniana przez sądy jest szkoda istniejąca w chwili orzekania, co wyrażone zostało m.in. w wyroku Sądu Najwyższego z dnia 12 lutego 2016 r., zgodnie z którym zakresem szkody wynikającym z art. 361 § 1 KC nie jest szkoda przyszła. Te uszczerbki, których w chwili wyrokowania poszkodowany jeszcze nie doznał, nie są objęte obowiązkiem odszkodowawczym, gdyż obowiązek naprawienia szkody nie jest związany ze stanem zagrożenia, ale dopiero z zaistnieniem szkody. Ustawodawca kreuje obowiązek naprawienia szkody przyszłej w szczególnych wypadkach, np. art. 444 § 2 i 3 oraz art. 446 § 2 i 3 KC[757]. Do uwzględnienia szkody przyszłej wymaga się, by była ona oceniona według doświadczenia życiowego jako konieczna konsekwencja zaistniałego stanu. Ma charakter hipotetyczny, ale musi istnieć duże prawdopodobieństwo jej wystąpienia[758]. Wydaje się, że w zakresie szkód wyrządzonych przy przetwarzaniu danych osobowych, szkody przyszłe mogą wystąpić w każdym obszarze tj. mogą dotknąć podmiot przetwarzający na skutek naruszenia ochrony danych osobowych przez podmiot podporzetwarzający, mogą dotknąć administratora, który odniósł szkodę wyrządzoną przez podmiot przetwarzający, ale również mogą one dotyczyć osób fizycznych, których dane byłby przetwarzane. Jako szkodę przyszłą potencjalnie można by określić upadłość przedsiębiorcy jako konsekwencję rozwiązania z nim współpracy przez kontrahentów, czy też odroczone w czasie uszczerbki majątkowe osoby fizycznej na skutek wycieku danych z banku. Można nawet przewidywać, że szkoda spowodowana przetwarzaniem danych osobowych naruszającym przepisy o ochronie danych osobowych będzie miała najczęściej charakter szkody przyszłej. Taką hipotezę można uzasadnić tym, że skutki naruszenia bezpieczeństwa, poufności i integralności danych osobowych (np. poprzez ich utracenie lub udostępnienie nieuprawnionemu podmiotowi), może wywołać długofalowe skutki, których ilość, rozmiar i waga nie będą znane przez długi okres od wystąpienia zdarzenia.

[756] T. Dybowski [w:] Z. Radwański (red.), *System..., op. cit.,* s. 278.
[757] Wyrok Sądu Najwyższego - Izba Cywilna z dnia 12 lutego 2016 r., II CSK 172/15, Legalis nr 1461030.
[758] T. Dybowski [w:] Z. Radwański (red.), *System..., op. cit.,* s. 279.

Drugą z przesłanek odpowiedzialności jest wystąpienie zdarzenia, z którym ustawa wiąże powstanie odpowiedzialności. Jeśli chodzi o opis normatywny zdarzenia powodującego zaistnienie obowiązku odszkodowawczego, jest to kategoria zróżnicowana, ponieważ może być nim i czyn niedozwolony i niewykonanie bądź nienależyte wykonanie zobowiązania[759]. W odniesieniu do zagadnienia powierzenia przetwarzania danych osobowych, przykładem zdarzenia, z którym wiąże się odpowiedzialność są np. ujawnienie danych o stanie zdrowia osobom nieuprawnionym poprzez nieszyfrowanie danych przesyłanych za pomocą chmury. Faktem jest tu naruszenie przepisów RODO poprzez naruszenie poufności danych i ujawnienie ich podmiotom bez podstawy prawnej. Zdarzeniem może być również niewłaściwe wykonywanie umowy zawartej między administratorem a podmiotem przetwarzającym, np. poprzez wykraczanie poza zakres poleceń administratora i wykorzystywanie danych do własnych celów, skutkujące utratą klientów przez przedsiębiorcę.

Związek przyczynowy pomiędzy szkodą a zdarzeniem nie budzi kontrowersji w doktrynie prawa cywilnego. Przyjęta została teoria adekwatnej przyczynowości, wyrażona w treści art. 361 §1 Kodeksu Cywilnego, stanowiącego, że zobowiązany do odszkodowania ponosi odpowiedzialność tylko za normalne następstwa działania lub zaniechania, z którego szkoda wynikła. W doktrynie prawa cywilnego wypracowano sposób ustalania, czy związek przyczynowo-skutkowy jest adekwatny, tzn. czy odpowiedzialność ograniczona będzie tylko do skutków zdarzenia powodującego szkodę, które będą ocenione jako normalne następstwa. Pierwszym etapem jest tzw. test *sine qua non*, polegający na odpowiedzi na pytanie, czy szkoda powstałaby, gdyby nie nastąpiło zdarzenie, z którym łączy się odpowiedzialność. Po potwierdzeniu drugi etap polega na odpowiedzi, czy wśród zwykłych następstw zdarzenia ocenianych obiektywnie, znalazłby się skutek w postaci tej szkody[760]. Odzwierciedlenie adekwatnego związku przyczynowego w przepisach dotyczących odpowiedzialności na gruncie RODO można odnaleźć w treści art. 82 ust. 2 zd. 2, stanowiącej, że podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. W przypadku tego przepisu RODO (choć nie wszystko wydaje się w nim oczywiste jak

[759] S. Prutis, *Instytucje..., op. cit*., s. 404.
[760] W. J. Katner [w:] M. Stec (red.), *System ..., op. cit.*, s. 388.

np. obowiązki nakładane na podmioty przetwarzające „bezpośrednio"), ułatwione wydaje się przypisywanie odpowiedzialności odszkodowawczej podmiotowi przetwarzającemu i badanie związku przyczynowego między szkodą a faktem ją wyrządzającym. W nauce prawa zebrano w trzy grupy okoliczności, w których przetwarzający odpowiada za szkody spowodowane przetwarzaniem. Pierwszą stanowią naruszenia jego obowiązków określonych w RODO. Druga grupa to działanie wbrew warunkom przetwarzania określonym w umowie z administratorem (wbrew instrukcjom). Do trzeciej należy działanie w sferze własnej dyskrecji, poza zakresem ustaleń z administratorem i poza instrukcjami[761]. Niestety nie można tego samego powiedzieć w stosunku do odpowiedzialności odszkodowawczej administratora, której dotyczy art. 82 ust. 2 zd. 1 RODO, przy przypisywaniu której związek przyczynowy będzie musiał być wnikliwiej analizowany, o czym świadczy ogólność przepisu (Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie). Podobnie jest z odpowiedzialnością podmiotów podprzetwarzających (art. 28 ust. 4 RODO).

Istotną kwestią w ramach szerokiego zagadnienia odpowiedzialności odszkodowawczej są zasady odpowiedzialności. Rozumieć je należy jako założenia determinujące wyróżnienie faktów uzasadniających obciążenie odpowiedzialnością za szkodę, w celu wyjaśnienia społecznego sensu i mechanizmu działania przepisów dotyczących odpowiedzialności[762]. Z klasycznie sformułowanej triady zasad winy, ryzyka i słuszności, aktualnie (choć nie powszechnie) przyjmuje się rozszerzony katalog zasad: winy, bezprawności, ryzyka, absolutną i słuszności[763].

Dominującą zarówno w reżimie odpowiedzialności z tytułu czynów niedozwolonych, jak i odpowiedzialności z tytułu niewykonania lub nienależytego wykonania zobowiązania jest zasada winy[764]. W nauce prawa wyjaśniono, że naczelny charakter winy przejawia się w tym, że wina stanowi główną zasadę odpowiedzialności, pozostałe zaś zasady znajdują zastosowanie w szczególnych okolicznościach wskazanych w hipotezie normy ustanawiającej tę odpowiedzialność[765]. Zgodnie też przyjmuje się, że

[761] M. Sakowska-Baryła (red.), *Ogólne..., op. cit.*, Legalis.
[762] M. Kaliński, *Szkoda... op. cit.*, s. 94.
[763] *Ibidem*.
[764] Co do rozumienia pojęcia winy zob. szerzej literaturę powoływaną w tej części rozprawy.
[765] M. Kaliński [w:] A. Olejniczak (red.), *System..., op. cit., Legalis.*

zasada winy oznacza, że szkodę powinien naprawić ten, kto ją wyrządził w sposób zawiniony, a uprzednio należy stwierdzić przesłankę bezprawności[766].

Na gruncie przepisów RODO odpowiedzialność na zasadzie winy wynika z treści art. 82 ust. 2 i 3[767]. Można z tych przepisów interpretować, że generalną zasadą jest ponoszenie odpowiedzialności za naruszenie RODO przez administratora, chyba że udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody. Odpowiedzialność może również ponosić podmiot przetwarzający (o ile nastąpiło powierzenie danych do przetwarzania w imieniu i na polecenie administratora podmiotowi zewnętrznemu). Podmiot przetwarzający zwolni się od odpowiedzialności, jeśli udowodni, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody. Należy w konstrukcji odpowiedzialności za szkody spowodowane przetwarzaniem danych, na relatywną obiektywizację odpowiedzialności. Zastosowano tu mechanizm przesunięcia ciężaru dowodowego na zobowiązanego, który musi wykazać, że w żaden sposób nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody[768]. Można powiedzieć, że taki rozkład ciężaru dowodzenia ułatwia poszkodowanemu dochodzenie roszczeń.

Druga z powszechnie uznawanych zasad odpowiedzialności - zasada ryzyka polega na nałożeniu odpowiedzialności odszkodowawczej na dłużnika niezależnie od istnienia po jego stronie winy i bezprawności[769]. Jest to zaostrzony rodzaj odpowiedzialności, w którym udowodnienie braku winy nie zwalnia z ponoszenia odpowiedzialności, co umotywowane jest szczególnym ryzykiem działalności. Nie oznacza to jednak, że nie da się od niej uwolnić (co charakteryzuje odpowiedzialność absolutną). Przepisy prawa wskazują przypadki wyłączające odpowiedzialność, nazywane okolicznościami egzoneracyjnymi. Nie ma jednego katalogu takich przesłanek, który byłby możliwy do zastosowania w każdym przypadku, jednak najczęściej wskazuje się triadę okoliczności egzoneracyjnych wymienioną w art. 435 § 1 KC: działania siły wyższej, wyłącznie z winy

[766] Nie można postawić osobie zarzutu winy, jeśli zachowanie nie miało znamion bezprawności, ale możliwe jest bezprawne zachowanie osoby, które jest niezawinione – T. Dybowski, *System..., op. cit.*, s. 199.

[767] 2. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. 3. Administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

[768] M. Sakowska-Baryła, *Ogólne..., op. cit*., Legalis.

[769] M. Kaliński, *Szkoda... op. cit.,* s. 125.

poszkodowanego, wyłącznie z winy osoby trzeciej. Odpowiedzialność na zasadzie ryzyka występuje zarówno w ramach regulacji odpowiedzialności z tytułu czynów niedozwolonych (art. 425 § 2, art. 433–436 § 1, art. 449^1 i n. KC), jak i odpowiedzialności z tytułu niewykonania lub nienależytego wykonania zobowiązania (art. 474 KC) oraz w innych ustawach.

W odniesieniu do analizowanego obszaru RODO, odpowiedzialność na zasadzie ryzyka pojawia się w aspekcie odpowiedzialności podmiotu przetwarzającego za zachowania podmiotu podprzetwarzającego tj. niewywiązanie się ze spoczywających na nim obowiązków ochrony danych (art. 28 ust. 4 RODO). Będzie to odpowiedzialność dłużnika za osoby trzecie na podstawie art. 474 KC. Warto podkreślić, że przepis art. 474 KC dotyczy sytuacji, w której dłużnik jest uprawniony do posłużenia się osobami trzecimi, ale jeśli mimo obowiązku osobistego świadczenia, powierzył wykonanie świadczenia osobie trzeciej, to ponosi odpowiedzialność za działanie własne, bo już samo powierzenie wykonania innej osobie jest naruszeniem zobowiązania[770]. Będzie to sytuacja, w której podmiot przetwarzający nie uzyska zgody administratora na podpowierzenie przetwarzania danych, a mimo to będzie korzystał z usług podwykonawców w procesach przetwarzania danych. Zmianie ulegnie wtedy zasada odpowiedzialności na zasadę winy. Wątpliwość w zakresie przepisu o odpowiedzialności podmiotu przetwarzającego za zachowania podprzetwarzających budzi to, że przepis ogranicza się jedynie do odpowiedzialności wobec administratora. Nie odnosi się do sytuacji gdy wyrządzono szkodę działaniem podmiotów podprzetwarzających osobom, których dane dotyczą.

Trzecią z klasycznie wyróżnianych zasad odpowiedzialności jest zasada słuszności, opierająca się na zasadach współżycia społecznego i występująca w nielicznych i ściśle oznaczonych wypadkach[771]. Należy podzielić pogląd, że praktyczne znaczenie tej zasady odpowiedzialności jest niewielkie, występuje jako wyjątek od pozostałych zasad (w zakresie odpowiedzialności deliktowej są to regulacje art. 417^2, 428, 431 § 2 KC, a w reżimie kontraktowym – art. 826 i 827 § 1 KC)[772]. Zasada ta polega na uzależnieniu powstania odpowiedzialności odszkodowawczej od zgodności z zasadami współżycia społecznego, ale nie istnieje ogólna kompetencja sądu do orzekania na podstawie słuszności, podstawa musi wynikać z normy prawa pisanego. W bardzo nielicznych

[770] W. Popiołek [w:] K. Pietrzykowski (red.), *Kodeks cywilny. T II. Komentarz. Art. 450–1088. Przepisy wprowadzające*, Warszawa 2018, Legalis.
[771] Zob. szersze uwagi na temat tej zasady w: Z. Banaszczyk, *Odpowiedzialność..., op. cit.*
[772] T. Dybowski, *System..., op. cit*., s. 206-207.

przypadkach sędzia ma możliwość dokonania samodzielnej oceny i zasądzenia odszkodowania biorąc pod uwagę szczególne okoliczności towarzyszące wyrządzeniu szkody[773]. Jeśli chodzi o odpowiedzialność administratora i podmiotu przetwarzającego za szkody wyrządzone przy przetwarzaniu danych osobowych, można stwierdzić, że zasada słuszności nie ma zastosowania.

Należy poświęcić uwagę jeszcze jednemu zagadnieniu dotyczącemu prywatnoprawnej odpowiedzialności w obszarze powierzenia przetwarzania danych osobowych, a jest to odpowiedzialność solidarna, która zgodnie z treścią art. 369 KC może wynikać z ustawy lub z czynności prawnej[774]. Może ona zaistnieć od chwili powstania zobowiązania, jak również może zostać wprowadzona w wyniku modyfikacji istniejącego już zobowiązania, przy czym nie może być domniemana[775]. Solidarność może występować zarówno po stronie dłużników, jak i wierzycieli, jednakże w kontekście przedmiotu rozważań prowadzonych w dysertacji należy skupić się na tzw. solidarności biernej (dłużników), ponieważ drugi rodzaj raczej na tym gruncie nie występuje. Solidarność bierną reguluje treść art. 366 KC, zgodnie z którym dłużnikami solidarnymi są dłużnicy zobowiązani w ten sposób, że wierzyciel może żądać całości lub części świadczenia od wszystkich dłużników łącznie, od kilku z nich lub od każdego z osobna, a zaspokojenie wierzyciela przez któregokolwiek z dłużników zwalnia pozostałych. Dopóki jednak wierzytelność wynikająca z zobowiązania solidarnego nie zostanie zaspokojona w całości, wszyscy dłużnicy pozostają zobowiązani. Dla przykładu wskazać można również inne przepisy wskazujące na ukształtowanie zobowiązania jako solidarne, które zawarto w treści art. 289, 370, 380, 614, 1044, 1055 KC. W przypadku odpowiedzialności za szkody wyrządzone przy przetwarzaniu danych osobowych, wierzycielem będzie podmiot poszkodowany, a dłużnikiem będzie sprawca szkody. W sytuacji szkody, która wystąpiła w okolicznościach powierzenia przetwarzania danych osobowych dłużników zarówno wobec poszkodowanego administratora, jak i poszkodowanej osoby fizycznej, może być kilku (z uwagi na łańcuch powierzeń i podpowierzeń, w tym dłużnikiem jest administrator).

[773] M. Kaliński, *Szkoda... op. cit.*, s. 135-136.
[774] Zob. uwagi M. Frasa w glosie aprobującej do wyroku Sądu Najwyższego z dnia 19 października 2011 r. (II CSK 86/11, LEX nr 1096037) - Rozprawy Ubezpieczeniowe nr 12 (1/2012), dostępnej na stronie internetowej https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Mariusz_Fras___Glosa_aprobujaca_do_wyroku_Sadu_Najwyzszego_z_dnia_19_pazdziernika_2011_r___II_CSK_86_11__LEX_nr_1096037___21397#_ftn8.
[775] B. Lackoroński [w:] K. Osajda (red.), *Kodeks cywilny. Komentarz*, Warszawa 2018, Legalis.

Kluczową kwestią w praktyce funkcjonowania solidarności dłużników jest problem ich wzajemnych rozliczeń. Zagadnienie to reguluje art. 376 KC, zgodnie z którym jeżeli jeden z dłużników solidarnych spełnił świadczenie, treść istniejącego między współdłużnikami stosunku prawnego rozstrzyga o tym, czy i w jakich częściach może on żądać zwrotu od współdłużników. Jeżeli z treści tego stosunku nie wynika nic innego, dłużnik, który świadczenie spełnił, może żądać zwrotu w częściach równych. Dodatkowo ustawodawca zastrzegł, że część przypadająca na dłużnika niewypłacalnego rozkłada się między współdłużników. Żądanie zwrotu spełnionego świadczenia od pozostałych współdłużników nazywa się regresem i stanowi ułatwienie dla wierzyciela w uzyskaniu zaspokojenia, przez przerzucenie ciężaru rozliczeń między dłużnikami na nich samych[776].

Prawodawca unijny konstrukcję solidarnej odpowiedzialności przewidział w treści art. 82 ust. 4 RODO, stanowiąc, że jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający, lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i odpowiadają oni za szkodę spowodowaną przetwarzaniem, ponoszą odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. W regulacji tej wyraźnie został wskazany cel, dla którego ustanawia się solidarną odpowiedzialność administratora i podmiotu przetwarzającego. Jest on tożsamy z przyjętym w nauce prawa cywilnego uzasadnieniem dla stosowania konstrukcji solidarności. Chodzi przede wszystkim o ochronę poszkodowanego, ponieważ podmioty zobowiązane ponoszą pełną odpowiedzialność wobec poszkodowanego (a częściową dopiero po rozliczeniach regresowych), nawet jeżeli *de facto* nie spowodowały całej szkody[777]. Tym samym prawodawca ustanowił jako priorytet interes poszkodowanego. Można powiedzieć, że poprzez treść art. 82 ust. 4 RODO dotyczącego solidarnej odpowiedzialności i podkreślenia jej celu, realizuje się najistotniejsza wartość umowy powierzenia przetwarzania danych osobowych. Jest ona instrumentem pozwalającym zapewnić realność uzyskania odszkodowania przez podmiot, który zostaje na skutek niewłaściwego przetwarzania danych poszkodowany. Może to być zarówno osoba fizyczna, której dane dotyczą, jak i administrator danych. Dużo trudniej (o ile w ogóle

[776] W Dubis [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, Warszawa 2017, Legalis.
[777] E. Bagińska, *Teoria odpowiedzialności częściowej (proportional liability) jako koncepcja sprawiedliwego rozłożenia ciężaru odpowiedzialności deliktowej – wprowadzenie do problematyki* [w:] Gdańskie Studia Prawnicze 2016, tom XXXV, s. 58, tekst dostępny na stronie internetowej: https://prawo.ug.edu.pl/sites/default/files/_nodes/strona-pia/33461/files/35baginska.pdf.

byłoby to realnie możliwe) wyglądałoby dochodzenie naprawienia szkody gdyby podmioty uczestniczące w procesie przetwarzania danych osobowych nie były związane stosunkiem umowy powierzenia. W nauce prawa wyrażono pogląd, że koncepcja solidarności nie rozwiązuje całkowicie problemu sprawiedliwego rozłożenia ciężaru szkody, a przesuwa go tylko na płaszczyznę rozliczeń między sprawcami. Jeżeli pozwany jedynie przyczynił się do stworzenia ryzyka powstania szkody, można kwestionować słuszność przyjęcia solidarnego obowiązku kompensacji przez tych wszystkich, którzy istotnie przyczyniają się do powstania zagrożenia[778].

Wewnętrzny stosunek między współdłużnikami solidarnymi jasno określa treść art. 82 ust. 5 RODO. Administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2. Należy się zgodzić z poglądem, iż zakres przyczynienia się do powstania szkody jest bez znaczenia dla odpowiedzialności solidarnej, ale będzie miał znaczenie dla ustalenia roszczeń regresowych pomiędzy zobowiązanymi[779]. Nie rodzi też problemów interpretacyjnych określenie przez prawodawcę reguł rozliczeń – co do zasady odpowiedzialny jest administrator, podmiot przetwarzający (i podprzetwarzający) odpowiada we wskazanych wyżej trzech przypadkach.

3. Odpowiedzialność administracyjna za naruszenie przepisów dotyczących powierzania przetwarzania danych osobowych

W doktrynie prawa administracyjnego rzadko podejmowane jest ogólne zagadnienie odpowiedzialności administracyjnej, odnosi się ją najczęściej do poszczególnych dziedzin, jak np. prawo ochrony środowiska. Zaproponowana w nauce prawa definicja o charakterze uniwersalnym ujmuje odpowiedzialność administracyjną jako zasadę ponoszenia przez osoby fizyczne, prawne i jednostki organizacyjne posiadające zdolność prawną, przewidzianych w prawie ujemnych konsekwencji, realizowanych w swoistych dla administracji formach i procedurze, za działania lub

[778] *Ibidem*, s. 59
[779] M. Sakowska-Baryła (red.), *Ogólne..., op. cit*., Legalis.

zaniechania stanowiące naruszenie nakazów lub zakazów ustanowionych w przepisach prawa lub aktach administracyjnych o charakterze indywidualnym[780]. Wymienia się też cechy odpowiedzialności administracyjnej, a wśród nich obiektywny charakter – przesłanką jest sam fakt naruszenia obowiązków, bez znaczenia czy było ono zawinione (bezprawność jako działanie niezgodne z przepisami prawa lub decyzją administracyjną jest kluczową przesłanką). Z pojęciem odpowiedzialności administracyjnej wiążą się sankcje administracyjne, rozumiane jako nakładane przez organy administracji publicznej w drodze aktu stosowania prawa i wynikające ze stosunku administracyjnoprawnego niekorzystne skutki dla podmiotów prawa, które nie stosują się do obowiązków wynikających z norm prawnych lub aktów stosowania prawa[781]. W ramach tego rodzaju odpowiedzialności występują sankcje o dużym zróżnicowaniu, np. kara pieniężna, cofnięcie zezwolenia, sankcje karne[782]. W poglądach przedstawicieli nauki prawa[783] wskazuje się wiele cech sankcji administracyjnych, jak to, że stosowanie sankcji musi mieć podstawę prawną w ustawie, sankcja jest konsekwencją niezgodnego z prawem działania bądź zaniechania. Wskazuje się też na prewencyjno-represyjny charakter sankcji i formę – akt władczy administrującego. Ponadto sankcja ma respektować zasadę proporcjonalności – musi być konieczna, odpowiednia i racjonalnie dolegliwa, a jej nałożenie podlega sądowej kontroli[784]. Podkreślenia wymaga również to, że na gruncie orzecznictwa wyjaśniono, że obiektywna koncepcja odpowiedzialności administracyjnej nie jest odpowiedzialnością absolutną, co oznacza, że można się od niej zwolnić, wykazując, że uczyniono wszystko, czego można było od podmiotu wymagać, aby nie doszło do naruszenia przepisów[785]. Chodzi zatem o wykazanie należytej staranności w wykonywaniu obowiązków i braku możliwości innego zachowania się.

Odpowiedzialności administracyjnej na gruncie przepisów RODO dotyczy przede wszystkim treść art. 58 ust. 2 oraz art. 82. Można na ich podstawie powiedzieć, że sankcjami administracyjnymi wynikającymi z przepisów RODO są środki naprawcze

[780] P. Wojciechowski, *Model odpowiedzialności administracyjnej w prawie żywnościowym*, Warszawa 2015, s. 222-223.
[781] M. Wincenciak, *Sankcje w prawie administracyjnym i procedura ich wymierzania*, Warszawa 2008, s. 73.
[782] S. Prutis, *Instytucje..., op. cit*., s. 348 i 368.
[783] M. Stahl (red.), *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie,* Warszawa 2015, *s. 88 i n.*
[784] *Ibidem*.
[785] Wyrok Wojewódzkiego Sądu Administracyjnego w Białymstoku z dnia 25 lipca 2007 r., II SA/Bk 276/07, Legalis nr 827104.

nazwane uprawnieniami naprawczymi[786] organu nadzoru i wymienione w art. 58 ust. 2 RODO, w postaci zakazów i nakazów określonego działania wydawanych administratorom i podmiotom przetwarzającym dane, jak również administracyjne kary finansowe nakładane oprócz lub zamiast środków naprawczych[787]. Celem przyznanych organowi kompetencji jest przywrócenie stanu zgodnego z prawem, naprawienie naruszeń stwierdzonych przez organ. Wątpliwości budzi fakt, że do zakresu uprawnień naprawczych wymienionych w art. 58 ust. 2 RODO zaliczono również administracyjną karę pieniężną, która nie ma charakteru naprawczego, a raczej represyjny. W przepisie tym znalazły się również inne uprawnienia organu niebędące sankcjami, jak ostrzeżenia kierowane w przypadku zaistnienia możliwości naruszenia przez planowane operacje przetwarzania, oraz upomnienia, nie mające charakteru wiążącego.

Na tej podstawie można powiedzieć, że sankcje administracyjne za naruszenie przepisów o ochronie danych osobowych wymienione zostały w art. 58 ust. 2 lit. c-j RODO. Dyskusyjna jest kwestia kto jest adresatem sankcji. Wątpliwości nie budzi nakazanie spełnienia żądania osoby, której dane dotyczą oraz nakazanie dostosowania operacji przetwarzania do przepisów rozporządzenia. Prawodawca wprost wskazuje tu administratora oraz podmiot przetwarzający. Jeśli chodzi o nakazanie zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych, adresatem jest administrator danych. Natomiast jeśli chodzi o pozostałe sankcje (wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania, nakazanie sprostowania lub usunięcia danych osobowych lub ograniczenia ich przetwarzania oraz powiadomienia o tych czynnościach odbiorców, cofnięcie certyfikacji, zastosowanie administracyjnej kary pieniężnej, jak też nakazanie zawieszenia przepływu danych do odbiorcy w państwie trzecim lub do organizacji międzynarodowej), pomimo braku sformułowania tego w przepisie, na gruncie nauki istnieje pogląd, że adresatami tych kompetencji organu nadzoru są administrator i podmiot przetwarzający[788].

O ile przepis w art. 58 RODO nie rozstrzyga, w jakiej formie prawnej organ nadzorczy korzysta z wymienionych w ust. 2 kompetencji (kwestię tę pozostawiono do regulacji państwom członkowskim), to analizując przepisy ustawy o ochronie danych

[786] Należy zgodzić się z poglądem wyrażonym w nauce prawa, że pojęcie "uprawnienia naprawcze" nie jest fortunne, bardziej adekwatne byłoby użycie terminu "kompetencje" lub "środki", co bardziej odpowiadałoby angielskiemu *corrective powers.* Tak M. Sakowska-Baryła, *Ogólne..., op. cit*., Legalis.
[787] D. Krajewska-Kekusz, *Rola Prezesa UODO w świetle ustawy o ochronie danych osobowyc*h [w:] Informacja w administracji publicznej 2018, nr 4, str. 29.
[788] P. Litwiński (red.), *Rozporządzenie..., op. cit*., Legalis.

osobowych z 10 maja 2018 r.[789], można przewidzieć, że chodzi o formę decyzji, ale nie jest to jednoznacznie przesądzone[790]. Ponadto wskazuje się, że katalog kompetencji przyznanych organowi nadzorczemu ma charakter zamknięty, ale państwa członkowskie mogą go rozszerzyć na podstawie upoważnienia, przewidzianego w art. 58 ust. 6 RODO. Pod rządami ustawy o ochronie danych osobowych z 1997 roku Generalny Inspektor Ochrony Danych Osobowych podejmował kroki dążące do stwierdzenie naruszeń art. 31 UODO z 1997 r. w formie decyzji. Na podstawie badań decyzji organu można sformułować wniosek, że najczęstszymi rozstrzygnięciami było nakazanie zawarcia umowy powierzenia, usunięcie uchybień poprzez określenie w treści umowy zakresu i celu powierzenia danych[791], czy też nakazanie zaprzestania powierzania przetwarzania danych osobowych bez zawarcia pisemnych umów powierzenia[792]. Aktualnie Urząd Ochrony Danych Osobowych nie publikuje wydawanych decyzji na oficjalnej stronie internetowej organu, decyzji brak też w uznanych na rynku prawniczym systemach informacji prawnej (LEX, Legalis).

Przechodząc do zagadnienia odpowiedzialności administracyjnej w postaci administracyjnych kar pieniężnych, należy podkreślić ich związek z innymi sankcjami wynikającymi z treści art. 58 ust. 2 RODO. Z treści przepisu wynika, że kary mogą być nakładane zarówno na administratora, jak i na podmiot przetwarzający. Pozwala to sformułować wniosek, że obie strony umowy powierzenia przetwarzania danych osobowych mogą ponosić odpowiedzialność administracyjną za naruszenie przepisów o ochronie danych osobowych. Adresatami kar mogą być również podmioty certyfikujące i podmioty monitorujące, ale wątek ten pozostaje poza nurtem prowadzonych rozważań. Swobodę państwom członkowskim pozostawiono co do rozstrzygnięcia stosowania administracyjnych kar pieniężnych wobec podmiotów sektora publicznego. Polski ustawodawca zdecydował się w treści art. 103 UODO z 2018 r. ograniczyć maksymalną kwotę kary do 100 tysięcy złotych w stosunku do jednostek sektora finansów publicznych[793], instytutów badawczych i Narodowego Banku Polskiego. Zróżnicowanie

[789] T.j. Dz. U. 2018 poz. 1000 ze zm., dalej jako UODO z 2018 r.
[790] Dla przykładu w drodze decyzji następuje cofnięcie akredytacji (art. 22 ust. 3 UODO), decyzję o stwierdzeniu naruszenia udostępnia się w Biuletynie Informacji Publicznej (art. 73 UODO).
[791] Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dnia 31 maja 2012, DIS/DEC-492/12/34095, dostępna na stronie internetowej https://giodo.gov.pl/pl/306/4985.
[792] Decyzja Generalnego Inspektora Ochrony Danych Osobowych z dnia 28 października 2014, DIS/DEC-1022/14/84106, dostępna na stronie internetowej https://giodo.gov.pl/pl/293/8218.
[793] Chodzi tu o podmioty, o których mowa w art. 9 pkt 1-12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2017 r. poz. 2077 ze zm.), czyli organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; jednostki

maksymalnych wysokości kar nakładanych na podmioty sektora prywatnego i publicznego tłumaczone jest na gruncie nauki prawa tym, że o ile w odniesieniu do podmiotów spoza administracji publicznej administracyjna kara pieniężna jest dotkliwą sankcją, o tyle nie można się zgodzić, iż taki sam skutek odniesie ona w stosunku do podmiotów publicznych i zachwiany zostanie represyjny cel kary[794]. Można powiedzieć, że bardziej przekonuje argument co do ograniczenia wysokości kary związany z faktem, że zgodnie z treścią art. 104 UODO z 2018 r. środki z administracyjnej kary pieniężnej stanowią dochód budżetu państwa. W związku z tym uiszczenie kary przez podmioty sektora publicznego, a przede wszystkim organy administracji publicznej, oznacza *de facto* przepływ środków publicznych między podmiotami finansowanymi z budżetu państwa z powrotem do budżetu państwa. Mniej zrozumiałe jest odrębne potraktowanie w treści art. 102 ust. 2 UODO z 2018 r. państwowych i samorządowych instytucji kultury (w tym muzeów, domów kultury, teatrów, bibliotek), dla których górną granicę kary ustalono w wysokości 10 tysięcy złotych. Rodzi to wątpliwość przede wszystkim w aspekcie zasady równości podmiotów wobec prawa.

Prawodawca unijny w art. 83 RODO poświęconym karom stanowi, że administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków naprawczych omówionych wyżej. Można w związku z tym stwierdzić, że kary mają charakter samoistny i autonomiczny lub wspomagający inne sankcje administracyjne. Rolę kar prawodawca sformułował w treści motywu 148 i 150 preambuły RODO, stanowiąc, że aby egzekwowanie przepisów niniejszego rozporządzenia było skuteczniejsze, należy za jego naruszenie nakładać sankcje, w tym administracyjne kary pieniężne; ponadto w celu wzmocnienia i zharmonizowania sankcji administracyjnych za naruszenie rozporządzenia każdy organ nadzorczy powinien być uprawniony do nakładania administracyjnych kar pieniężnych. Jest jeszcze za wcześnie na formułowanie ocen, czy kary wynikające

samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; państwowe fundusze celowe; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasa Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; samodzielne publiczne zakłady opieki zdrowotnej; uczelnie publiczne; Polska Akademia Nauk i tworzone przez nią jednostki organizacyjne; państwowe i samorządowe instytucje kultury; 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.

[794] A. Dmochowska, A. Piotrowska, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Legalis.

z przepisów RODO spełniają funkcje przypisywane ogólnie administracyjnym karom pieniężnym, tj. funkcję prewencyjną, restytucyjną, represyjną i ochronną[795].

Prawodawca sformułował otwarty katalog okoliczności, które organ nadzorczy (w Polsce Prezes Urzędu Ochrony Danych Osobowych) powinien brać pod uwagę, decydując indywidualnie w każdym przypadku o nałożeniu administracyjnej kary pieniężnej oraz o jej wysokości. Wśród nich wskazać można skutki naruszenia czy też zachowanie administratora lub podmiotu przetwarzającego zarówno przed jak i po naruszeniu[796]. Ponadto ustanowiono dwie wysokości kar. Kwota wyższa (granica 20 milionów euro, a w przypadku przedsiębiorstw do 4 % całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego) dotyczy przypadku stwierdzenia, że administrator lub podmiot przetwarzający nie wykonał nakazów z art. 58 ust. 2 RODO, albo też dotyczy naruszeń wymienionych w treści art. 83 ust. 5 lit. a-e RODO (jak np. naruszenie zasad przetwarzania lub praw podmiotów danych). Kwota niższa (granica 10 milionów euro, a w przypadku przedsiębiorstw do 2 % całkowitego rocznego światowego obrotu) stosowana jest w przypadku naruszeń, które wskazane są w art. 83 ust. 4 lit. a–c RODO (jak np. naruszenie przez administratora lub podmiot przetwarzający obowiązku uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrona danych).

Jeśli chodzi o sytuacje, gdy dane osobowe w imieniu administratora przetwarza podmiot przetwarzający, konsekwencją naruszenia przepisów związanych z powierzaniem przetwarzania danych osobowych może być kara administracyjna w niższej kwocie, o czym stanowi treść art. 83 ust. 4 lit. a – chodzi tu o obowiązki administratora i podmiotu przetwarzającego wynikające z art. 28 RODO. Teoretycznie administracyjna kara pieniężna do 10 milionów euro lub do 2% obrotu może grozić za brak umowy powierzenia między administratorem a podmiotem przetwarzającym, niewłaściwy wybór podmiotu przetwarzającego i niesprawdzenie czy zapewnia on wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, nieprzestrzeganie wymogów co do podpowierzenia przetwarzania danych osobowych, nierealizowanie obowiązków podmiotu przetwarzającego wymienionych w art. 28 ust. 3 lit. a-h RODO. Nie jest jednakże przesądzone, że wymienione uchybienia w realizacji wymogów określonych w RODO będą skutkowały nałożeniem kary. Pamiętać należy, że zgodnie z motywem 148

[795] Funkcje te wskazano w pozycji M. Wierzbowski, R. Hauser (red.), *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2018, Legalis.
[796] Szerzej na ten temat J. Łuczak [w:] E. Bielak-Jomaa (red.), *RODO. Ogólne...., op. cit.*, LEX.

preambuły RODO, jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia.

Warto zwrócić uwagę na treść przepisu zawartego w art. 83 ust. 1 RODO, stanowiącego, że każdy organ nadzorczy zapewnia, by administracyjne kary pieniężne stosowane za naruszenia rozporządzenia, były w każdym indywidualnym przypadku skuteczne, proporcjonalne i odstraszające. Trudno tak sformułowane zobowiązanie organu odnieść do praktyki. Nie wiadomo bowiem, w jaki sposób organ ma udzielić takiego zapewnienia. Nie wynika z treści przepisu kogo należy zapewnić i w jakiej formie. Trzeba podkreślić, że zapewnienie to odnosi się do teraźniejszości (że nakładana kara jest proporcjonalna do stopnia naruszenia), ale przede wszystkim do przyszłości (że kara będzie skuteczna – przez co rozumieć można, że osiągnięte zostaną funkcje kar administracyjnych jak prewencyjna, restytucyjna, represyjna i ochronna, oraz że kara będzie odstraszająca przed dokonywaniem kolejnych naruszeń, tak przez podmiot ukarany, jak i inne podmioty). Wydaje się, że udzielenie takiego zapewnienia jest praktycznie niemożliwe, a przepis zawierający takie zobowiązanie organu pozostanie przepisem martwym.

Na chwilę obecną w Polsce nie zastosowano jeszcze administracyjnej kary pieniężnej. Natomiast francuski organ ochrony danych osobowych nałożył karę w wysokości 50 mln euro na korporację Google. Podmiotowi zarzucono m.in. brak pozyskiwania zgód użytkowników na przesyłanie spersonalizowanych reklam, inwazyjne metody zbierania informacji oraz niespełniające wymogów informowanie użytkowników na temat przetwarzania ich danych osobowych[797]. Prezes Urzędu Ochrony Danych Osobowych zapowiedział, że w niedługim czasie przystąpi do nakładania pierwszych kar na administratorów w Polsce.

Na podstawie doświadczeń na gruncie praktycznym można stanąć na stanowisku, że kary pieniężne są sankcją administracyjną, która z punktu widzenia podmiotów uczestniczących w procesach przetwarzania danych osobowych powoduje największe obawy. Tym samym wydaje się być najefektywniejszą motywacją do podjęcia tematu ochrony danych osobowych w organizacji. Należy jednak zwrócić uwagę na fakt, że

[797] https://businessinsider.com.pl/technologie/nowe-technologie/francja-ukarala-google-50-mln-euro-za-naruszenie-rodo/m419et9.

niebagatelna wysokość kar wskazywana w treści art. 83 RODO jest maksymalną granicą ich wymierzenia, ogólnie w odniesieniu do administratorów z Unii Europejskiej. Nakładając kary organ ma zapewnić, by były one skuteczne, proporcjonalne i odstraszające, dlatego też w każdym indywidualnym przypadku należy wziąć pod uwagę szereg okoliczności wymienionych w treści art. 83 ust. 2 lit. a-k. Wydaje się, że w odniesieniu do realiów polskich przedsiębiorców, wymóg dotyczący proporcjonalności kary do wagi naruszenia ochrony danych osobowych będzie stanowił granicę racjonalności w określaniu kwot kar. Wydaje się, że nie w pełni dostrzegana przez administratorów i podmioty przetwarzające jest sankcja wskazana w treści art. 58 ust. 2 lit. f RODO w postaci wprowadzenia czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania. Jej dolegliwość może być porównywana z dolegliwością kar finansowych, a może je też przewyższyć. Niejednokrotnie nawet czasowy zakaz przetwarzania danych osobowych może doprowadzić do całkowitego paraliżu działania organizacji. Trudno sobie wyobrazić dalsze funkcjonowanie sklepu internetowego czy hotelu po nałożeniu takiego zakazu.

Na podstawie doświadczeń na gruncie praktyki można też powiedzieć, że w odbiorze społecznym kary administracyjne są głównym czynnikiem motywującym do zajęcia się tematyką ochrony danych osobowych, zarówno w przedsiębiorstwach, jak i innych podmiotach jak szkoły czy szpitale. Co do pozostałych sankcji administracyjnych najprawdopodobniej zawodzi stopień świadomości i niski poziom wiedzy z zakresu zagadnień uregulowanych w RODO. Ogólnie rzecz ujmując, można powiedzieć, że odpowiedzialność administracyjna z tytułu naruszania przepisów o ochronie danych osobowych uregulowana jest w sposób umożliwiający efektywną ochronę danych osobowych. Ich realizacja pozostaje w gestii organu nadzorczego.

4. Odpowiedzialność karna związana z niezgodnym z prawem przetwarzaniem danych osobowych

W nauce prawa utrwalono pogląd, że odpowiedzialność karna polega na ponoszeniu ujemnych konsekwencji w postaci sankcji karnych za przypisany określonemu podmiotowi czyn podlegający kwalifikacji normatywnej. W odróżnieniu od odpowiedzialności administracyjnej, podstawą odpowiedzialności karnej jest indywidualna wina sprawcy, przy czym możliwość przypisania sprawcy winy za

popełnienie czynu zabronionego pod groźbą kary, a tym samym pociągnięcia go do odpowiedzialności karnej, zależy od tego, czy miał on możliwość wyboru zachowania innego niż przestępne[798]. W dodatku pamiętać należy, że odpowiedzialność karną może ponosić tylko osoba fizyczna zdolna do ponoszenia winy, co w przypadku przetwarzania danych osobowych przekładać się może dla przykładu na pracownika przedsiębiorstwa albo też członka kierownictwa.

Przepisy dotyczące sankcji karnych zostały umieszczone poza RODO, w przepisach krajowych – zgodnie z sugestią prawodawcy wynikającą z motywu 152 preambuły RODO, stanowiącą, że w sytuacjach, w których rozporządzenie nie harmonizuje sankcji administracyjnych, lub w razie potrzeby w innych przypadkach, na przykład w razie poważnego naruszenia niniejszego rozporządzenia, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające sankcje. Charakter takich sankcji (karny lub administracyjny) powinno określać prawo państwa członkowskiego. Polski ustawodawca skorzystał z kompetencji wynikającej z treści art. 84 ust. 1 RODO[799] i uregulował odpowiedzialność karną w treści UODO z 2018 r., w art. 107 i 108. Bardzo istotnym jest fakt, że określonych w tych przepisach przestępstw można dokonać bez względu na to, czy w odniesieniu do danego przetwarzania RODO będzie miało zastosowanie, czy nie. Oznacza to, iż pomimo, że przepisy RODO nie odnoszą się np. do kradzieży danych osobowych, to nielegalne wejście w posiadanie lub nielegalne wykorzystanie danych jest objęte definicją przetwarzania i będzie stanowiło przestępstwo na mocy przepisów UODO z 2018 r. [800].

Już na wstępie należy zauważyć, że regulacja odpowiedzialności karnej została znacznie ograniczona w stosunku do przepisów nieobowiązującej już ustawy o ochronie danych osobowych z 1997 r.[801]. Na podstawie poprzedniego stanu prawnego wyróżniano odpowiedzialność za przetwarzanie danych osobowych w sytuacji, gdy takie przetwarzanie było niedopuszczalne bądź gdy podmiot nie miał uprawnienia do przetwarzania danych (art. 49 UODO z 1997r.), odpowiedzialność za udostępnianie

[798] A. Krajewski [w:] A. Marek (red.), *System Prawa Karnego*, Tom 1, Warszawa 2010, Legalis.
[799] Zgodnie z tym przepisem państwa członkowskie przyjmują przepisy określające inne sankcje za naruszenia niniejszego rozporządzenia, w szczególności za naruszenia niepodlegające administracyjnym karom pieniężnym na mocy art. 83, oraz podejmują wszelkie środki niezbędne do ich wykonania. Sankcje te muszą być skuteczne, proporcjonalne i odstraszające.
[800] M. Gawroński, K. Kloc [w:] M. Gawroński (red.), *Ochrona danych osobowych. Przewodnik po ustawie i RODO z wzorami*, Warszawa 2018, s. 674.
[801] Ustawa z dnia 29 sierpnia 1997 r., t.j. Dz. U. z 2016 r., poz. 922 ze zm.

danych podmiotom nieuprawnionym (art. 51 UODO z 1997r.), odpowiedzialność za naruszenie obowiązku zabezpieczenia danych (art. 52 UODO z 1997r.), odpowiedzialność za brak zgłoszenia zbiorów danych do rejestracji (art. 53 UODO z 1997r.) oraz odpowiedzialność za niepoinformowanie osoby, której dane dotyczą o przetwarzaniu jej danych i przysługujących jej prawach (art. 54 UODO z 1997r.) i odpowiedzialność za udaremnianie lub utrudnianie wykonanie czynności kontrolnej (art. 54a UODO z 1997r.). Należy stwierdzić, że zakres odpowiedzialności karnej z tytułu naruszenia przepisów o ochronie danych osobowych był szeroki, ale nie można powiedzieć, że efektywny. W literaturze przedmiotu zwraca się uwagę, że ochrona miała charakter raczej iluzoryczny, co wynikało np. z konstrukcji przestępstw stypizowanych w art. 53 i 54 UODO z 1997r. jako typów wyłącznie umyślnych[802]. Słabość karnoprawnej ochrony danych osobowych gwarantowanej przepisami sprzed rozpoczęcia stosowania RODO widoczna jest w statystykach[803]. Po pierwsze, wynika z nich niewielka (choć rosnąca) liczba zawiadomień o popełnieniu przestępstwa (10 w roku 2014, 24 w roku 2015, 36 w roku 2016, 45 w roku 2017). Również liczba prawomocnych wyroków skazujących wydanych w oparciu o przepisy UODO z 1997r. wydaje się nieznacząca (9 w roku 2011, 16 w roku 2012, 9 w roku 2013, 20 w roku 2014, 9 w roku 2015)[804]. Jeśli chodzi o rodzaj wymierzanych kar, dominowała kara grzywny. Ponadto zgodzić się należy z poglądem, że przepisy dotyczące niezgłoszenia zbioru danych osobowych do rejestracji czy naruszenia obowiązków informacyjnych względem osób, których dane dotyczą stanowiły nieuzasadnioną kryminalizację zachowań, które nie powinny mieć rangi przestępstwa[805].

Od 25 maja 2018 roku odpowiedzialność karna za naruszanie przepisów o ochronie danych osobowych kształtuje się inaczej. Poświęcono jej tylko dwa artykuły w UODO z 2018 r.[806]. W treści art. 107 ust. 1 ujęto odpowiedzialność za przetwarzanie danych osobowych choć ich przetwarzanie nie jest dopuszczalne albo osoba nie jest uprawniona do ich przetwarzania. Za to zachowanie przewidziana została kara grzywny, ograniczenia

[802] P. Barta [w:] P. Litwiński (red.), *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018, Legalis.
[803] Dla przykładu https://www.giodo.gov.pl/pl/1520114/9175, https://www.giodo.gov.pl/pl/1520114/4583.
[804] Opracowanie dostępne na stronie internetowej https://gdpr.pl/przeciw-utrzymaniu-penalizacji-ochronie-danych-osobowych#_ftn4.
[805] P. Barta [w:] P. Litwiński (red.), *Ustawa..., op. cit.*, Legalis.
[806] Szerzej przestępstwa wynikające z ustawy o ochronie danych osobowych analizuje A. Błachnio-Parzych, *Przepisy karne w ustawie z 10.5.2018 r. o ochronie danych osobowych*, dodatek do Monitora Prawniczego 2018 nr 22, Legalis oraz M. Gawroński, K. Kloc [w:] *Ochrona..., op. cit.*, s. 670-683. Zob. też E. Hruniewicz-Lach [w:] R. Zawłocki (red.), *System Prawa Handlowego*, tom X, Warszawa 2018, Legalis.

wolności albo pozbawienia wolności do lat dwóch. W ustępie drugim zaostrzono karę pozbawienia wolności do lat 3, jeżeli niedopuszczalne przetwarzanie danych bądź przetwarzanie przez osobę nieuprawnioną dotyczy szczególnej kategorii danych[807]. W myśl przepisu odpowiedzialność karna powinna zostać przypisana tej osobie, która podjęła faktycznie decyzję o przetwarzaniu danych osobowych, albo jako administrator (gdy działa we własnym imieniu), albo jako podmiot przetwarzający (gdy działa w imieniu administratora)[808].

Odpowiedzialność wynikająca z art. 108 UODO z 2018 r. dotyczy zachowania osoby udaremniającej kontrolę np. poprzez niedopuszczenie kontrolującego do miejsca prowadzenia kontroli, bądź osoby utrudniającej kontrolę. Podlega ono grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch, przy czym zaznaczyć trzeba, że zmoże za nie zostać nałożona również administracyjna kara pieniężna na administratora lub podmiot przetwarzający zgodnie z art. 83 ust. 5 lit. e RODO.

Odnosząc zagadnienie odpowiedzialności karnej do przedmiotu rozważań w dysertacji, czyli umowy powierzenia przetwarzania danych osobowych, można powiedzieć, że strony umowy mogą potencjalnie być sprawcami obu uregulowanych przestępstw. W kontekście art. 107 UODO z 2018 r., na zastosowanie tej regulacji do wielu stanów faktycznych pozwala przede wszystkim szeroki zakres definicji przetwarzania danych osobowych (zgodnie z treścią art. 4 pkt 5 RODO jest nim operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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). Można przewidzieć, że przestępstwo z art. 107 UODO z 2018 r. może popełnić administrator danych, w sytuacji gdy sam nie legitymuje się przesłanką legalizującą przetwarzanie danych z art. 6 RODO lub też naruszy zasady minimalizacji czy ograniczonego przechowywania (niedopuszczalność przetwarzania), a ponadto udostępni dane do przetwarzania innemu podmiotowi bez

[807] Tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej.
[808] P. Barta [w:] P. Litwiński (red.), *Ustawa..., op. cit.,* Legalis.

podstawy prawnej (w tym bez umowy powierzenia przetwarzania danych osobowych co jest sprzeczne z prawem). Określony w przepisie karnym czyn może zostać również popełniony przez podmiot przetwarzający, który dostał polecenie przetwarzania od administratora, ale nie ma ono formy umowy i nie są przez ten podmiot realizowane wymogi wynikające z art. 28 RODO (przetwarzanie przez nieuprawnionego), albo też podpowierzy przetwarzanie danych osobowych podmiotowi podprzetwarzającemu bez zgody administratora i bez umowy podpowierzenia (niedopuszczalność przetwarzania). Należy się przy tym zgodzić, z poglądem wyrażonym w nauce prawa, że uchybienia w zakresie staranności wyboru podmiotu przetwarzającego nie prowadzą do stwierdzenia, że dane są przetwarzane przez osobę nieuprawnioną[809]. Drugie z przestępstw wynikające z ustawy o ochronie danych osobowych i uregulowane w treści art. 108 UODO z 2018 r. także może dotyczyć obu stron stosunku powierzenia przetwarzania danych osobowych, ponieważ zarówno administrator, jak i podmiot przetwarzający mogą podlegać kontroli przestrzegania przepisów o ochronie danych osobowych. Należy jednak pamiętać przy tym, że kontrolującym, zgodnie z art. 79 ust. 1 UODO z 2018 r., jest upoważniony pracownik Urzędu Ochrony Danych Osobowych lub członek lub pracownik organu nadzorczego państwa członkowskiego Unii Europejskiej. Podkreślenia wymaga, że regulacja zawarta w art. 108 UODO z 2018 r. nie będzie miała odniesienia do sytuacji kontroli (audytu, inspekcji), do której uprawniony jest administrator wobec podmiotu, któremu powierza przetwarzanie danych osobowych zgodnie z wymogami art. 28 RODO.

Wskazane w treści art. 107 i 108 UODO z 2018 r. achowania stanowią aktualnie jedyne, za które na gruncie UODO z 2018 r. ponosi się odpowiedzialność karną, oba stanowiły przestępstwa na gruncie UODO z 1997 r. Należy mieć jednakże na uwadze przepisy zawarte w rozdziale XXXIII Kodeksu Karnego[810], dotyczące przestępstw przeciwko ochronie informacji. Ograniczenie liczby przestępstw w nowych przepisach oznacza zdepenalizowanie takich zachowań jak niezgłoszenie zbioru danych osobowych do rejestracji czy naruszenia obowiązków informacyjnych, co należy ocenić pozytywnie z uwagi na wątpliwości co do proporcjonalności kary do szkodliwości społecznej tych czynów. Można to interpretować w ten sposób, że odpowiedzialność karna pełni rolę dodatkową, wzmacniającą odpowiedzialność administracyjną oraz cywilną, innymi słowy odpowiedzialność karna ma być wyjątkiem przewidzianym wyłącznie dla najcięższych

[809] A. Błachnio-Parzych, *Przepisy..., op. cit.,* Legalis.
[810] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny, tj. Dz. U. z 2018 r., poz. 1600 ze zm.

naruszeń przepisów[811]. Odpowiedzialność karna ukierunkowana jest przede wszystkim na realizację funkcji represyjnej, wychowawczej i odstraszającej.

[811] A. Dmochowska, A. Piotrowska, *Ustawa...*, *op. cit*., Legalis.

ZAKOŃCZENIE

Podsumowując przeprowadzoną analizę normatywno-dogmatyczną dotycząca problematyki umowy powierzenia przetwarzania danych osobowych, należy potwierdzić postawioną we wstępie hipotezę, że dane osobowe, jako kategoria informacji, są szczególnym rodzajem dóbr prawnie chronionych. Umowa powierzenia przetwarzania danych osobowych jest istotnym instrumentem prywatnoprawnej ochrony danych osobowych. Warto podkreślić, że jej celem jest też realizacja ustawowych zasad dotyczących przetwarzania danych osobowych. Można ją więc nazwać umową szczególnego zaufania.

Problematyka umowy powierzenia przetwarzania danych osobowych wymaga analizy takich pojęć jak przede wszystkim informacja i dane osobowe. O tym, czy należy przyznać informacji status danych osobowych i w konsekwencji tego odpowiednią ochronę, nie decydują inne czynniki poza spełnieniem przesłanek wynikających z przepisu prawa – ma to być informacja dotycząca osoby fizycznej zidentyfikowanej lub możliwej do zidentyfikowania. Bez znaczenia dla takiej kwalifikacji pozostaje m.in. to, czy informacja jest prawdziwa. Dla ustalenia, że mamy do czynienia z danymi osobowymi nie ma znaczenia forma przedmiotowej informacji, choć istotne jest, by informacja była zapisana na nośniku. Najbardziej problematycznym elementem definicji i zarazem najważniejszym kryterium umożliwiającym nadanie informacji statusu danych osobowych jest to, że informacja ma dotyczyć zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. W przepisach wskazano narzędzia umożliwiające identyfikację osoby, jednakże tylko ogólnie poprzez otwarty katalog sposobów identyfikacji.

Na podstawie poczynionych tu ustaleń teoretycznych oraz analizy przykładów informacji najbardziej wątpliwych i problematycznych w kwalifikowaniu jako dane osobowe (w tym numer IP, VIN, adres email), należy wywnioskować, że brak jest realnej możliwości sformułowania generalnego i abstrakcyjnego katalogu informacji, które mogą być standardowo kwalifikowane jako dane osobowe. W praktyce określona informacja dla jednego podmiotu stanowi dane osobowe, a jednocześnie dla drugiego takiego charakteru nie ma. Decyduje o tym zespół różnorodnych okoliczności jak kontekst działalności, posiadanie zasobów i innych informacji oraz możliwość prowadzenia operacji ich łączenia

i wyciągania wniosków, dostępne możliwości pozyskiwania informacji i używana technologia. Należy jednak zauważyć, że nie jesteśmy w stanie przewidzieć wszelkich możliwości, ani też stopnia wiedzy jaki posiada podmiot, który przetwarza dane. Wobec tego nierealne jest dzielenie informacji dwubiegunowo, czyli na takie, które na pewno są danymi i takie, które na pewno danymi osobowymi nie są.

Rozważania na poziomie bardziej ogólnym, dotyczące informacji i danych osobowych jako dobra chronionego prawnie wykazały, że informacja nie stanowi wyraźnie wyodrębnionego przedmiotu ochrony prawa prywatnego, bardziej wyodrębnia się na gruncie prawa publicznego. Informacja i dane osobowe to niestandardowy przedmiot ochrony w obrocie prawnym, podobnie jak np. energia czy domeny internetowe. Ich wartość ekonomiczna oraz poziom zagrożenia stale rosną, co rodzi potrzebę poszukiwania nowych środków ochrony prawnej tych dóbr. Wydaje się, że informacje, a w tym dane osobowe, należy postrzegać jako dobra niematerialne, które na gruncie obecnych regulacji prawnych w Polsce nie stanowią standardowego przedmiotu ochrony prawa. Pokazuje to, że przepisy prawa nie zawsze nadążają za tempem postępu technologicznego i naukowego.

Jeśli chodzi o normatywne ujęcie przetwarzania danych osobowych, należy stwierdzić, że nie jest możliwe określenie z góry wszystkich czynności, które wchodzą lub ewentualnie mogą wchodzić w zakres pojęcia przetwarzania danych osobowych. Można powiedzieć, że sformułowanie otwartego katalogu operacji na danych osobowych w definicji przetwarzania danych jest racjonalnym sposobem na zapewnienie ochrony prawnej danym osobowym. Jednocześnie pozytywnie należy ocenić elastyczność pojęcia przetwarzania, ponieważ pozostawiono możliwość dostosowywania się przepisów do zmieniającej się rzeczywistości i nadążania za postępem technologicznym. Trudno jednak uzasadnić, dlaczego prawodawca nie uwzględnił w zakresie normatywnym definicji przetwarzania danych osobowych operacji polegającej na powierzeniu przetwarzania danych w drodze umowy. Mimo tego nie ulega wątpliwości, że w powierzenie mieści się w zakresie przetwarzania danych osobowych.

Na podstawie prowadzonych rozważań można ocenić, że „powierzenie" na gruncie przepisów o ochronie danych osobowych jest w znacznym stopniu spójne z jego znaczeniem wynikającym z przepisów prawa z różnych dziedzin (np. prawo cywilne, prawo pracy, prawo bankowe). W porównaniu z przepisami UODO z 1997 r., w aspekcie

przetwarzania danych w imieniu administratora przez podmiot przetwarzający, nowe regulacje RODO są zdecydowanie bardziej szczegółowe. Prawodawca dostrzegł potrzebę efektywniejszej regulacji tego obszaru ze względu na to, że tendencja do korzystania z usług innych podmiotów zamiast samodzielnego przetwarzania danych przez administratora, aktualnie już nie jest wyjątkiem, a coraz częściej regułą. Stwierdzić jednak należy, że uszczegółowione przepisy ujęte w treści art. 28 RODO nie są w pełni oczywiste i budzą szereg wątpliwości w praktyce ich stosowania. Można powiedzieć, że pomocne w odczytywaniu celów i wartości chronionych tymi przepisami są zasady przetwarzania danych osobowych wynikające z treści art. 5 RODO, które mogą być odnoszone również do kwestii związanych z powierzeniem przetwarzania danych osobowych.

We wstępie sformułowano hipotezę, że przepisy prawa regulujące umowę powierzenia przetwarzania danych osobowych i skonstruowana w ich oparciu umowa powierzenia mają gwarantować, aby przetwarzanie danych respektowało ustawowe zasady przetwarzania danych osobowych. Należy podkreślić, że w tym procesie duże znaczenie ma również praktyka,, szczególnie w aspekcie zasady legalności przetwarzania. Należy zauważyć, że w aktualnym brzmieniu przepisów RODO żadna z przesłanek legalizujących prowadzenie operacji na danych osobowych (art. 6 i 9 RODO) nie odnosi się wprost do sytuacji, w której dane przetwarzane są na „zlecenie" administratora danych. Nie jest więc jasne, która z przesłanek dopuszczalności przetwarzania zachodzi w przypadku powierzenia przetwarzania danych. Dlatego sformułowany został wniosek *de lege ferenda,* by wśród przesłanek legalizujących przetwarzanie danych osobowych umieścić również działanie polegające na „zlecaniu" przetwarzania danych osobowych innym podmiotom. Mogłoby to zostać ujęte w treści art. 6 ust. 1 RODO poprzez dodanie lit. „g", np. w sformułowaniu: „administrator danych powierzył przetwarzanie danych podmiotowi przetwarzającemu w drodze umowy na mocy art. 28 RODO". Dla zapewnienia spójności przepisów podobne sformułowanie mogłoby znaleźć się również w treści art. 9 ust. 2 RODO poprzez dodanie litery „k" o powyższej treści.

Ponadto w świetle zasad przetwarzania danych wątpliwości budziła kwestia rzetelności i przejrzystości przetwarzania. Faktycznie rozważania wykazały, że osoba fizyczna nie została wyposażona w możliwość decydowania o tym, czy i komu jej dane mogą zostać powierzone (powierzenie nie jest zależne od zgody podmiotu danych). Natomiast zasadę rzetelności i ochronę praw jednostki realizuje instrument umowy powierzenia niesamodzielnie, a razem z innym instrumentem – tzw. obowiązkiem

informacyjnym (wymóg poinformowania podmiotu danych w treści klauzuli informacyjnej o odbiorcach danych, w tym o podmiotach przetwarzających dane na zlecenie administratora w drodze umowy). Można zatem powiedzieć, że umowa powierzenia przetwarzania danych osobowych realizuje zasadę rzetelności i przejrzystości w sposób pośredni. Dla wzmocnienia gwarancji ochrony, zapewnienia spójności przepisów i podkreślenia wagi informacji o dokonywanym powierzeniu, zaproponowano wniosek *de lege ferenda* by w treści art. 28 RODO dodać ustęp 11, który stanowiłby, że w przypadku, gdy dane osobowe są lub będą przetwarzane w imieniu administratora przez podmiot przetwarzający, administrator danych informuje o tym osobę, której dane dotyczą. Są też zasady (takie jak zasada prawidłowości czy rozliczalności), do których prawodawca nie odnosi się, regulując powierzenie przetwarzania danych, a pozostawia ich realizację stronom umowy w praktyce. W odniesieniu do innych zasad przetwarzania danych osobowych wymienionych w treści art. 5 RODO, oceniono że regulacja prawna dotycząca umowy powierzenia i konstruowana na jej podstawie umowa spełniają pozostałe zasady, dzięki czemu umowa stanowi gwarancje bezpieczeństwa ochrony danych osobowych.

Analiza zasad przetwarzania danych osobowych pozwoliła sformułować wniosek, że zasad przetwarzania jest za dużo w stosunku do wąskiego obszaru prawa, jakim jest ochrona danych osobowych, by efektywnie pełniły swoje funkcje. Ponadto są one zbyt szczegółowe w odniesieniu do istoty i funkcji pełnionych przez zasady w prawie. W konsekwencji wydaje się, że może to prowadzić do ich deprecjacji i utraty nadrzędnego charakteru, jako zapisów podstawowych, naczelnych i szczególnie doniosłych. W związku z tym zaproponowano ujęcie zasad ochrony danych osobowych w następujący katalog: 1) zasada staranności przetwarzania danych (do której zaliczone mogą być zasady: rzetelności i przejrzystości, legalności, prawidłowości danych); 2) zasada niezbędności danych (w jej ramach znalazłaby się zasada ograniczenia celu, zasada minimalizacji i zasada ograniczenia przechowywania); 3) zasada bezpieczeństwa danych (w zakresie której umieścić można zasadę integralności i poufności, zasadę rozliczalności przetwarzania danych i zasadę uwzględniania ochrony danych w fazie projektowania (*privacy by design*) i domyślnej ochrony danych (*privacy by default*)). Zaproponowany katalog zasad uwzględnia wszystkie zasady wymienione i nazwane przez prawodawcę w treści art. 5 RODO. Ponadto rozszerzony został o wprowadzone w treści RODO

regulacje, które nie zostały literalnie określone mianem zasad przez prawodawcę, ale na gruncie nauki prawa uznawane są za zasady.

Podsumowując, z prowadzonych rozważań wynika, że modyfikacji wymaga sformułowana we wstępie do rozważań hipoteza, że przepisy prawa regulujące umowę powierzenia przetwarzania danych osobowych i skonstruowana w ich oparciu umowa powierzenia z założenia gwarantują, by przetwarzanie danych respektowało ustanowione przez prawodawcę zasady przetwarzania danych osobowych, co nie zawsze udaje się w praktyce.

Celem rozważań prowadzonych w kolejnej części dysertacji było dokonanie charakterystyki prawnej umowy powierzenia przetwarzania danych osobowych. Należy potwierdzić, że specyfika umowy powierzenia przetwarzania danych osobowych, w tym jej akcesoryjny charakter, nie pozwalają na jednoznaczne umiejscowienie jej w klasycznych systematyzacjach umów, co wskazuje na niejednolity charakter prawny umów tego typu. Powoduje to konieczność indywidualnej oceny okoliczności, w jakich ma funkcjonować umowa. W oparciu o przyjęty w nauce prawa prywatnego katalog przesłanek stanowiących warunki prawne umowy nienazwanej[812] należy uznać, że umowa powierzenia ma pewne cechy umowy nazwanej, ale w kontekście aktualnej regulacji zawartej w treści art. 28 RODO należy zakwalifikować ją do kategorii umów nienazwanych. Ponadto zgodnie z klasycznymi na gruncie prawa cywilnego podziałami umów, umowa powierzenia przetwarzania danych osobowych została zakwalifikowana jako zobowiązująca (kształtuje zobowiązanie na mocy art. 353 §1 KC i nie stanowi rozporządzenia), dwustronnie zobowiązująca (a dokładniej wzajemna), w pewnych okolicznościach może mieć charakter umowy konsensualnej, a w innych realnej. Jest też umową odpłatną, ponadto może być umową swobodnie negocjowaną i adhezyjną. W praktyce doniosłym jest akcesoryjny charakter umowy – jest ona zawsze umową związaną z umową zasadniczą, nie występuje w obrocie samodzielnie.

Trzeba zauważyć, że na gruncie nauki prawa przyjęto pogląd, zgodnie z którym umowa powierzenia przetwarzania jest umową o świadczenie usług. Jednakże jednocześnie warto zaznaczyć wewnętrzną niejednolitość w ramach umów tego typu, ponieważ część z nich będzie miała charakter umowy o świadczenie usług z wyraźnymi elementami umowy zlecenia, a część (choć zdecydowanie mniejsza) – charakter umowy o świadczenie usług z wyraźnymi elementami umowy o dzieło. Podkreślenia wymaga,

[812] W. J. Katner [w:] W. J. Katner (red.) *System…, op. cit.,* s. 16-17.

że przetwarzanie to nie tylko czynności faktyczne, ale również czynności prawne, np. podpowierzenie (dalsze powierzenie) przetwarzania danych. Można powiedzieć, że do oceny tego, czy do konkretnej umowy powierzenia przetwarzania danych osobowych należy stosować odpowiednio przepisy o zleceniu, czy też dana umowa jest jednak bardziej podobna do umowy o dzieło, każdorazowej analizy wymaga przedmiot umowy, a dokładniej jakie operacje wchodzące w zakres przetwarzania danych osobowych będzie obejmowała umowa. Charakter prawny umowy jest *de facto* uzależniony od rodzaju czynności przetwarzania, których dotyczy konkretna umowa.

W rozważaniach podjęto również zagadnienie regulacji prawnej umowy powierzenia przetwarzania danych osobowych w kontekście zasady swobody umów. Z prowadzonych rozważań wynika, że zasada swobody umów nie ma zastosowania w zakresie swobody zawarcia umowy, ponieważ samo nawiązywanie tego stosunku zobowiązaniowego jest obowiązkiem wynikającym z RODO i podlegającym sankcjom administracyjnym, jeśli administrator decyduje się nie przetwarzać danych samodzielnie. Jeśli chodzi o swobodę wyboru kontrahenta, stosunek powierzenia może być nawiązany jedynie z tym podmiotem, z którym administrator zawarł umowę zasadniczą (np. na określoną usługę). Ponadto RODO wprowadza dodatkowe ograniczenie, że administrator może korzystać wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich zabezpieczeń. Elementy, które ma zawierać umowa prawodawca narzucił w treści art. 28 ust. 3 RODO. Są więc wyraźne ograniczenia w kształtowaniu treści umowy przez jej strony. Co do wyboru formy zawarcia umowy, prawodawca w przypadku umowy powierzenia przetwarzania danych osobowych nie zwolnił stron z formalizmu prawnego, stanowiąc w treści art. 28 ust. 9 RODO że umowa ma formę pisemną, w tym formę elektroniczną. Swoboda umów jest znacznie ograniczona w przypadku umów powierzenia przetwarzania danych osobowych, znajduje zastosowanie dopiero wtedy, gdy minimalne wymogi zawarte w treści art. 28 RODO i stanowiące przepisy o charakterze imperatywnym, zostają spełnione. Wydaje się, że ograniczenia swobody umów są tu uzasadnione, z uwagi na to że wynikają ze swoistego rodzaju dóbr, jakimi są dane osobowe. Ograniczenie zasady swobody umów jest tu sposobem na ich szczególną, podwyższoną ochronę. Swoboda umów nie jest wartością absolutną, w niektórych przypadkach jej ograniczenia są uzasadnione, co nie deprecjonuje samej idei swobody umów.

Podsumowując zagadnienie stron umowy powierzenia przetwarzania danych osobowych, należy stwierdzić, że właściwe przypisanie ról uczestnikom procesów przetwarzania danych osobowych bywa w praktyce trudnym zadaniem, pomimo faktu, że prawodawca sformułował definicje legalne administratora i podmiotu przetwarzającego. Z rozważań nad kwestią wzajemnej relacji administratora i podmiotu przetwarzającego wynika brak równorzędności stron umowy powierzenia, w większości przypadków z przewagą administratora, choć bywa też odwrotnie. Można powiedzieć, że w oparciu o inne ustalenia będą identyfikowani administratorzy danych w przypadku podmiotów sektora publicznego i prywatnego. Bywa, że administratora danych wskazują literalnie przepisy prawa, albo na ich podstawie należy przypisać tę rolę (np. poprzez analizę zakresu kompetencji). Wskazywanie administratorów przez ustawodawcę stanowiłoby znaczne ułatwienie, przede wszystkim z perspektywy osób, których dane są przetwarzane, ale również innych podmiotów procesu przetwarzania. Istnieje zatem potrzeba, by *de lege ferenda* ustawodawca określał, kto pełni funkcję administratora danych osobowych np. na uczelni wyższej, w przedszkolu, szpitalu, jednostkach samorządu terytorialnego i ich organach, policji, spółce skarbu państwa, itd. Interesujące okazały się również sposoby identyfikacji administratora w sytuacjach, w których z przepisów prawa nie wynika bezpośrednio, kto jest administratorem danych w odniesieniu do konkretnego procesu przetwarzania (kryterium formalne), przy czym każdy z nich ma wady i zalety. Charakterystyczny jest przede wszystkim umowny podział ról administratora i podmiotu przetwarzającego, jak również kryterium faktyczne - kto faktycznie ustala cele i sposoby przetwarzania danych, czy też kryterium tzw. dorozumianej kompetencji – odwołanie się do utrwalonych praktyk, tradycyjnych ról i związanej z nimi odpowiedzialności.

Systematyzując obowiązki administratora warto zaproponować ich podział na trzy grupy (obowiązki związane z legalnością przetwarzania, obowiązki związane z prawami osób, których dane dotyczą, obowiązki związane z zabezpieczaniem danych). Można sformułować wniosek, że znaczną część przepisów RODO stanowią obowiązki administratora danych, co potwierdza tezę, że odgrywa on kluczową rolę w procesie przetwarzania danych.

W rozprawie znalazła się również analiza nowej kategorii wprowadzonej przepisami RODO, jaką jest współadministrowanie danymi osobowymi oraz jego odmienności od powierzenia. Współadministrowanie opiera się na równorzędności

podmiotów i braku pomiędzy nimi stosunku zobowiązaniowego (nie ma wśród nich podmiotu uprawnionego i podmiotu zobowiązanego), natomiast w przypadku powierzenia wyinterpretować można zależność podmiotów tej relacji mającą cechy podległości, zobowiązanie jednej strony i uprawnienie drugiej strony. Jeśli chodzi o pozycję prawną podmiotu przetwarzającego, to należało jej dokonać na zasadzie kontrastu z pozycją administratora. Trzeba więc zauważyć, że kluczowym kryterium rozróżniającym administratora i przetwarzającego jest to, jak samodzielny, niezależny i decyzyjny jest określony podmiot w stosunku do danych osobowych.

Obowiązki podmiotu przetwarzającego, zgodnie z poglądami wyrażanymi w nauce prawa, można podzielić na dwie grupy, z których pierwsza dotyczy obowiązków z zakresu umowy powierzenia, a druga to obowiązki wynikające z przepisów RODO w oderwaniu od umowy. Można przyjąć, że istotnym i nowym aspektem dotyczącym podmiotu przetwarzającego jest zbliżenie jego pozycji prawnej w przepisach RODO do pozycji administratora danych. Uzasadnia to fakt, że podmiot przetwarzający jest często adresatem przepisów RODO obok administratora. Ponadto w odróżnieniu od regulacji obowiązujących przed dniem 25 maja 2018 roku, prawodawca unijny w treści RODO dokonał szczegółowej i kompleksowej regulacji podpowierzenia przetwarzania danych osobowych. Można pozytywnie ocenić regulację tego stosunku prawnego. Jest ona dużo bardziej szczegółowa od przepisów obowiązujących przed 25 maja 2018 r. i w przeciwieństwie do nich pozwala na ustanowienie przejrzystych ram współpracy podmiotów w łańcuchu powierzeń. Dodatkowo regulacje dotyczące odpowiedzialności podmiotu przetwarzającego za działania i zaniechania podmiotów podprzetwarzających, zabezpieczają interesy administratora, a pośrednio również podmiotu danych.

Odnosząc się do rozważań prowadzonych w czwartym rozdziale dysertacji niewątpliwie należy potwierdzić hipotezę ujętą we wstępie, iż umowa powierzenia przetwarzania danych osobowych ma szerokie zastosowanie w obrocie gospodarczym, a jej znaczenie prawne, ekonomiczne i społeczne jest istotne i szczególne z uwagi na wielość funkcji, jakie może pełnić ta umowa. Co do pierwszego z wskazanych w rozdziale czwartym obszarów zastosowania w praktyce umowy powierzenia przetwarzania danych osobowych, należy stwierdzić, że potrzeba powierzenia przetwarzania danych zachodzić będzie zawsze wtedy, gdy outsourcowane czynności wymagają prowadzenia jakichkolwiek operacji na danych osobowych. Ponadto umowa powierzenia będzie

stanowiła swego rodzaju legitymację dla podmiotu zewnętrznego (przekazanie mu danych nie będzie stanowiło nieuprawionego dostępu do danych zagrożonego sankcją karną). Można więc sformułować wniosek, że umowa powierzenia przetwarzania danych osobowych jest instrumentem, który umożliwia outsourcing w poszanowaniu prawa. Niezastosowanie tego narzędzia przy zlecaniu określonych czynności podmiotom zewnętrznym może powodować naruszenie przepisów i związaną z tym odpowiedzialność cywilną, administracyjną i karną, a także inne konsekwencje jak utrata dobrej opinii i zaufania klientów, straty finansowe. Następnie udało się ustalić, że hosting stanowi przechowywanie informacji na serwerze dostawcy i udostępnienie ich innym za pomocą internetu, a jeśli informacje te mają charakter danych osobowych, to hosting wchodzi w zakres definicji przetwarzania danych. W związku z tym umowa hostingu bez klauzul dotyczących powierzenia danych jest niekompletna, a jej strony mogą spotkać się z zarzutami dotyczącymi nieuprawnionego dostępu do danych osobowych podmiotu świadczącego usługę hostingu. Podobny wniosek wypływa z rozważań dotyczących usług chmurowych. Ponadto można sformułować wniosek, że pomiędzy usługobiorcą a dostawcą usług chmurowych brak jest równorzędności podmiotów i pozycję dominującą w tej relacji zajmuje dostawca. Podmiot korzystający z usług chmurowych pomimo tego, że pełni rolę administratora, czyli podmiotu zlecającego usługę i wydającego polecenia co do przetwarzania danych osobowych, jest *de facto* ograniczony do wyboru opcji zaakceptowania warunków oferowanych przez dostawcę bądź opcji niewyrażenia zgody skutkującej odmową współpracy. Nie należy uznawać tego za dobrą praktykę. Ogólnie można stwierdzić, że w założeniach umowa powierzenia przetwarzania danych osobowych ma stanowić nie tylko instrument ochrony danych osobowych, ale również pomagać osiągnąć wysoki standard bezpieczeństwa usług outsourcingu, usług chmurowych i hostingowych. Ogólnie w odniesieniu do zastosowania umów powierzenia można powiedzieć, że każdorazowo należy przeanalizować treść i okoliczności umowy zasadniczej na usługę, która jest zlecana podmiotowi zewnętrznemu, by podjąć decyzję o konieczności powierzenia przetwarzania danych zgodnego z przepisami art. 28 RODO.

Niewątpliwie potwierdzić trzeba również hipotezę o wielości funkcji umowy powierzenia przetwarzania danych osobowych. Funkcja legalizująca polega na tym, że umowa powierzenia stanowi *de facto* jedyną podstawę prawną przetwarzania danych osobowych przez podmiot niebędący administratorem. Innymi słowy, umowa powierzenia legalizuje operacje przetwarzania danych dokonywane przez zewnętrzny podmiot

przetwarzający. Dlatego, jak wspomniano, uzasadnionym wydaje się postulat *de lege ferenda* dodania umowy powierzenia przetwarzania danych osobowych do katalogu przesłanek dopuszczalności przetwarzania danych osobowych w art. 6 i 9 RODO. Funkcja kreacyjna (dynamizująca) przejawia się w tym, że umożliwiono administratorom korzystanie z usług świadczonych przez wyspecjalizowane podmioty. Administrator nie musi więc samodzielnie przetwarzać danych osobowych, umożliwiono mu podjęcie decyzji o korzystaniu z zewnętrznej obsługi. Funkcja organizacyjna polega na tworzeniu ram prawnych i organizowaniu współpracy administratora i podmiotu przetwarzającego w drodze postanowień stron respektujących odpowiednie przepisy RODO (chodzi o kształtowanie współpracy administratora z zewnętrznym podmiotem przetwarzającym). Funkcja zabezpieczająca przejawia się w kilku aspektach. Umowa stanowi zabezpieczenie dla administratora, przede wszystkim w sytuacji gdy podmiot przetwarzający nie wykonuje poleceń samodzielnie, a korzysta z podwykonawców (tzw. podpowierzenie przetwarzania danych). Jej treść przewiduje obowiązki podmiotów przetwarzających związanych z udziałem podwykonawców, jak wybór podwykonawcy zapewniającego odpowiednie gwarancje. Obowiązki nałożone w drodze umowy administratora z przetwarzającym są odzwierciedlone w umowie podmiotu przetwarzającego z podprzetwarzającym. Takie regulacje pozwalają zapewnić te same wymogi co do poziomu ochrony danych bez względu na to, kto faktycznie zajmuje się ich przetwarzaniem. Innymi słowy, umowa powierzenia daje administratorowi wiedzę i wpływ na uczestników procesu przetwarzania danych, które zostają powierzone. Podobnie jak funkcja zabezpieczająca, kilka aspektów ma też funkcja kontrolna przemiotowej umowy. Administrator może zobowiązać podmiot przetwarzający do zgłaszania mu w ustalonym czasie wszelkich naruszeń ochrony danych osobowych przetwarzanych na polecenie administratora. Administrator ma też możliwość podejmowania działań na skutek poinformowania go o podwykonawcach podmiotu przetwarzającego (zgoda, brak zgody, sprzeciw) oraz możliwość przeprowadzania audytów i inspekcji dotyczących przetwarzania danych przez podmiot przetwarzający. Następnie funkcja regulacyjno-represyjna polega na określeniu odpowiedzialności stron umowy za działania bądź zaniechania niezgodne z treścią umowy lub przepisami prawa, umożliwia dochodzenie roszczeń z tytułu odpowiedzialności kontraktowej stron oraz pociągnięcie do odpowiedzialności podmiotów uczestniczących w procesie przetwarzania. Funkcja przymuszająca polega na tym, że postanowienia umowne dotyczące „zlecenia" przetwarzania danych osobowych zawarte albo w umowie zasadniczej albo w treści

odrębnej umowy, będą wymagały od podmiotu przetwarzającego i podprzetwarzającego dostosowania swojej działalności do wymogów RODO, utrzymywania jej na odpowiednim poziomie bezpieczeństwa i tym samym gwarantowania odpowiedniego (do okoliczności przetwarzania) poziomu ochrony danych osobowych. Jednocześnie będzie to oznaczało ochronę ich interesów własnych (uniknięcie odpowiedzialności przetwarzającego i podprzetwarzającego), interesów administratora oraz osób, których powierzone dane dotyczą. Umowa powierzenia przetwarzania danych osobowych pełni również funkcję dowodową, ponieważ wspomaga realizację zasady rozliczalności, może stanowić dowód podczas kontroli Prezesa Urzędu Ochrony Danych Osobowych. Administrator będzie mógł wykazywać, że spełnia wymogi art. 28 RODO, że nie udostępnia danych podmiotowi nieuprawnionemu oraz generalnie dokłada należytej staranności w procesie przetwarzania danych osobowych. Bardzo istotna jest funkcja informacyjna i zabezpieczająca dla podmiotów danych. Polega ona na tym że osoba, której dane dotyczą może dowiedzieć się kto przetwarza jej dane w imieniu administratora zgodnie z art. 13 RODO. Ponadto umowa może okazać się pomocnym instrumentem dla osoby, której dane dotyczą i która poniosła szkodę w wyniku przetwarzania danych niezgodnie z RODO. Postanowienia umowy, przede wszystkim dotyczące podpowierzenia mogą być istotne dla ustalenia odpowiedzialności za powstałą szkodę. Reasumując wszystkie wymienione funkcje, można powiedzieć, że generalną funkcją umowy powierzenia przetwarzania danych osobowych jest ochrona zarówno podmiotów danych, jak i podmiotów dokonujących przetwarzania. Istnienie odpowiedzialności prawnej w obszarze przetwarzania danych osobowych (w tym jego powierzania) wzmacnia, a niekiedy wręcz umożliwia realizację podstawowych funkcji umowy powierzenia przetwarzania danych osobowych.

Reasumując, sformułowana na wstępie rozważań główna hipoteza badawcza wymaga niewielkiej modyfikacji. Początkowo twierdzono, że umowa powierzenia przetwarzania danych osobowych jest instrumentem ochrony danych osobowych, który ma gwarantować ochronę interesów zarówno podmiotów, które uczestniczą w procesie przetwarzania danych, jak i osób, których dane dotyczą. Po dokonaniu szeregu analiz można powiedzieć, że umowa powierzenia przetwarzania danych osobowych zdecydowanie jest instrumentem ochrony danych osobowych, jednakże na pierwszy plan wysuwa się jej funkcja ochrony interesów stron umowy, a następnie ochrona praw osoby, której powierzone dane dotyczą. Nie zmienia to faktu, że założenia prawodawcy co do roli

i znaczenia tego instrumentu prawnego należy ocenić pozytywnie, natomiast zapewnienie skuteczności i rzeczywistego spełniania funkcji umowy powierzenia przetwarzania danych osobowych leży po stronie podmiotów stosujących tę umowę w praktyce.

Poziom skomplikowania przepisów RODO nie ułatwia podmiotom zastosowania się do wymogów tego aktu. Efektem znacznego uszczegółowienia przepisów jest konieczność zweryfikowania zawartych dotąd umów powierzenia, pod kątem ich treści i ewentualnego uzupełnienia o nowe wymogi, ponieważ dotychczasowe umowy (zawarte przed 25 maja 2018 r.) nie w pełni gwarantują poziom ochrony danych osobowych przewidziany w przepisach RODO.

BIBLIOGRAFIA

Wykaz aktów prawnych

Europejska Konwencja Praw Człowieka i Podstawowych Wolności, RE, CETS nr 005, 1950;

Międzynarodowy pakt praw obywatelskich i politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r., Dz.U. 1977 nr 38 poz. 167;

Konwencja Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z 28 stycznia 1981 roku, Dz. U. z 2003 r., nr 3, poz. 25;

Traktat o Funkcjonowaniu Unii Europejskiej z 26 października 2012 roku (Dz. Urz. UE C nr 326, s. 47);

Karta Praw Podstawowych Unii Europejskiej (Dz. Urz. UE C 326 z 26.10.2012, s. 391);

Rozporządzenie 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, tzw. „RODO", Dz. Urz. UE.L 2016 Nr 119, str. 1);

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.Urz.UE.L 1995 Nr 281, str. 31;

Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym), Dz.Urz.UE.L 2000 Nr 178, str. 1;

Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz.U. 1997 Nr 78, poz. 483;

Kodeks cywilny z dnia 23 kwietnia 1964 r., t.j. Dz.U. z 2018 r. poz. 1025;

Kodeks karny z dnia 6 czerwca 1997 r., t.j. Dz.U. z 2018 r. poz. 1600 ze zm.;

Kodeksu postępowania cywilnego z dnia 17 listopada 1964 r., t.j. Dz.U. z 2018 r. poz. 155;

Kodeks rodzinny i opiekuńczy z dnia 25 lutego 1964 r., t.j. Dz.U. z 2017 r. poz. 682;

Kodeks pracy z dnia 26 czerwca 1974 r., t.j. Dz.U. z 2018 r. poz. 917;

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, (Dz. U. z 2018 r. poz. 1000 ze zm.);

Ustawa z dnia 6 marca 2018 r. Prawo przedsiębiorców (Dz.U. z 2018 r. poz. 646 ze zm.);

Ustawa z dnia 8 grudnia 2017 r. o Służbie Ochrony Państwa (Dz.U. z 2018 r. poz. 138 ze zm.)

Ustawa z dnia z dnia 28 stycznia 2016 r. Prawo o prokuraturze (t.j. Dz.U. z 2017 r. poz. 1767 ze zm.);

Ustawa z dnia 30 listopada 2016 r. o organizacji i trybie postępowania przed Trybunałem Konstytucyjnym (Dz. U. z 2016, poz. 2072 ze zm.);

Ustawa z dnia 11 lutego 2016 r. o pomocy państwa w wychowywaniu dzieci (Dz.U. z 2016 r. poz. 195 ze zm.);

Ustawa z dnia 11 września 2015 r. o działalności ubezpieczeniowej i reasekuracyjnej (t.j. Dz.U. z 2017 r. poz. 1170 ze zm.);

Ustawa z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny (t.j. Dz.U. z 2017 r. poz. 1832 ze zm.):

Ustawa z dnia 22 listopada 2013 r. o systemie powiadamiania ratunkowego (Dz.U. z 2013 r. poz. 1635, ze zm.);

Ustawa z dnia z dnia 23 listopada 2012 r. Prawo Pocztowe, (t.j. Dz.U. z 2017 r. poz. 1481, ze zm.)

Ustawa z dnia 16 września 2011 r. o wymianie informacji z organami ścigania państw członkowskich Unii Europejskiej (Dz. U. 2011 Nr 230, poz. 1371 ze zm.);

Ustawa z dnia 9 czerwca 2011 roku Prawo geologiczne i górnicze, (t.j. Dz.U. z 2017 r. poz. 2126 ze zm.);

Ustawa z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia, (t.j. Dz.U. z 2017 r. poz. 1845 ze zm.);

Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych, (t.j. Dz.U. z 2018 r. poz. 412 ze zm);

Ustawa z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym (t.j Dz.U. z 2017 r. poz. 2136);

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (t.j. Dz. U. z 2017 r. poz. 2077 ze zm.);

Ustawa z dnia 3 października 2008 roku o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko, (t.j. Dz.U. z 2017 r. poz. 1405 ze zm.);

Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j. Dz.U. z 2017 r. poz. 1993);

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2017 r. poz. 570 ze zm.);

Ustawa z dnia z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz.U. z 2017 r. poz. 1907 ze zm.);

Ustawa z dnia 2 lipca 2004 roku o swobodzie działalności gospodarczej, (Dz. U. nr 173, poz. 1807 ze zm.);

Ustawa z dnia 27 maja 2004 r. o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (t.j. Dz.U. z 2018 r. poz. 56);

Ustawa z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz.U. z 2017 r. poz. 1221 ze zm.);

Ustawa z dnia 27 maja 2004 roku o funduszach inwestycyjnych i zarządzaniu alternatywnymi funduszami inwestycyjnymi (t.j. Dz. U. z 2016 r. poz. 1896 ze zm.)

Ustawa z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną (t.j. Dz.U. z 2017 r. poz. 1219 ze zm.);

Ustawa z dnia 23 listopada 2002 r. o Sądzie Najwyższym (Dz. U. z 2016 r. poz. 1254, 2103, 2261 oraz z 2017 r. poz. 38 ze zm.);

Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej, (t.j. Dz.U. z 2016 r. poz. 1764 ze zm.);

Ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz. U. nr 100 poz. 1087 ze zm.);

Ustawa z dnia 27 lipca 2001 r. o ochronie baz danych, (Dz.U. 2001 Nr 128, poz. 1402 ze zm.);

Ustawa z dnia 24 maja 2000 r. o Krajowym Rejestrze Karnym (Dz. U. z 2017 r. poz. 678 ze zm.);

Ustawa z dnia 19 listopada 1999 roku Prawo działalności gospodarczej (Dz.U. 1999 Nr 101, poz. 1178 ze zm.);

Ustawa z 29 sierpnia 1997 roku o ochronie danych osobowych (t.j. Dz. U. z 2016r. poz. 922 ze zm.);

Ustawa z dnia 24 czerwca 1997 roku Prawo o ruchu drogowym (t.j. Dz. U. z 2017r. poz. 1260 ze zm.);

Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. z 2017 r. poz. 1876 ze zm.);

Ustawa z dnia 5 lipca 1996 r. o doradztwie podatkowym (t.j. Dz.U. z 2018 r. poz. 377 ze zm.);

Rządowy projekt ustawy o ochronie danych osobowych (druk nr 1928 z dn. 1996-10-03),

Ustawa z dnia z dnia 29 czerwca 1995 r. o statystyce publicznej, (T.j. Dz. U. 2016, poz. 1061 ze zm);

Ustawa z dnia 24 czerwca 1994 r. o własności lokali (Dz. U. z 2015 r., poz. 1892 ze zm.);

Ustawa z dnia 29 września 1994 roku o rachunkowości (t.j. Dz.U. z 2016 r. poz. 1047 ze zm.);

Ustawa z dnia 14 lipca 1983 roku o narodowym zasobie archiwalnym i archiwach, (t.j. Dz.U. z 2016 r. poz. 1506 ze zm.);

Rozporządzenie Rady Ministrów w sprawie Polskiej Klasyfikacji Działalności z dnia 24 grudnia 2007 r. (Dz.U. 2007, Nr 251, poz. 1885);

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 roku, (Dz.U. 2004 Nr 100, poz. 1024);

Rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 roku w sprawie „Zasad techniki prawodawczej", (t.j. Dz. U. 2016, poz. 283);

Projekt ustawy Przepisy wprowadzające ustawę o ochronie danych osobowych wraz z dokumentami towarzyszącymi dostępny jest na stronie internetowej https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-przepisy-wprowadzajace-ustawe-o-ochronie-danych-osobowych.html.

Wykaz orzeczeń

Wyrok Trybunału Sprawiedliwości (wielka izba) z dnia 16 grudnia 2008 r. Heinz Huber przeciwko Bundesrepublik Deutschland. Wniosek o wydanie orzeczenia w trybie prejudycjalnym: Oberverwaltungsgericht für das Land Nordrhein-Westfalen - Niemcy. Ochrona danych osobowych - Obywatelstwo europejskie - Zasada niedyskryminacji ze względu na przynależność państwową - Dyrektywa 95/46/WE - Pojęcie konieczności - Ogólne przetwarzanie danych osobowych dotyczących obywateli Unii będących obywatelami innego państwa członkowskiego - Centralny

rejestr cudzoziemców. Sprawa C-524/06, http://curia.europa.eu/juris/liste.jsf?language=pl&num=C-524/06;

Wyrok Trybunału Sprawiedliwości z dnia 6 listopada 2003 r. Postępowanie karne przeciwko Bodil Lindqvist. Wniosek o wydanie orzeczenia w trybie prejudycjalnym: Göta hovrätt - Szwecja. Dyrektywa 95/46/CE. Sprawa C-101/01. http://curia.europa.eu/juris/liste.jsf?language=pl&jur=C,T,F&num=C-101/01&td=ALL;

Wyrok Trybunału Sprawiedliwości, z dnia 20 maja 2003 r. Rechnungshof (C-465/00) przeciwko Österreichischer Rundfunk i innym oraz Christa Neukomm (C-138/01) i Joseph Lauermann (C-139/01) przeciwko Österreichischer Rundfunk. Wnioski o wydanie orzeczenia w trybie prejudycjalnym: Verfassungsgerichtshof (C-465/00) i Oberster Gerichtshof (C-138/01 i C-139/01) - Austria. Dyrektywa 95/46/CE. Sprawy połączone C-465/00, C-138/01 oraz C-139/01 http://curia.europa.eu/juris/liste.jsf?num=C-465/00&language=pl;

Wyrok Trybunału Sprawiedliwości z dnia 20 maja 2003r. – Neukomm, Sprawa C-138/01 (Sprawy połączone C-465/00, C-138/01, C-139/01), http://curia.europa.eu/juris/liste.jsf?language=pl&jur=C,T,F&num=C-138/01&td=ALL;

Wyrok Trybunału Konstytucyjnego z dnia 12 grudnia 2005 roku, K 32/04, Legalis nr 71527;

wyrok Trybunału Konstytucyjnego z 24 czerwca 1997 roku, K 21/96, OTK 1997, Nr 2, poz. 23, Legalis nr 10365;

Wyrok Trybunału Konstytucyjnego z dnia 19 maja 1998 r., U 5/97, Legalis nr 10436;

Wyrok Trybunału Konstytucyjnego z dnia 17 czerwca 2008, K 8/04, http://trybunal.gov.pl/fileadmin/content/omowienia/K_8_04_PL.pdf;

Trybunał Konstytucyjny w wyroku z dnia 20 listopada 2002 roku, K 41/02, Legalis nr 55361;

Orzeczenie Trybunału Konstytucyjnego z dnia 29 października 1986 r., U 2/86, Legalis nr 35959.

Uchwała Pełnego Składu Izby Cywilnej Sądu Najwyższego z dnia 28 kwietnia 1995 r., III CZP 166/94, nr Legalis 29265;

Wyrok Sądu Apelacyjnego w Warszawie z dnia 10 października 2013 roku, I ACa 689/13, Legalis nr 775991;

Wyrok NSA z dnia 18 sierpnia 2016 roku, I OSK 864/16, dostępny na stronie internetowej http://orzeczenia.nsa.gov.pl/doc/CA1E71D70A;

Wyrok Naczelnego Sądu Administracyjnego z dnia 30 listopada 2011 roku, I OSK 2118/10, http://orzeczenia.nsa.gov.pl/doc/6A2A1D2737;

Wyrok Naczelnego Sądu Administracyjnego z dnia 19 maja 2011r., I OSK 1086/10, Legalis nr 378897;

Wyrok Naczelnego Sądu Administracyjnego z dnia 19 stycznia 2010 r., I OSK 491/09, Legalis nr 222666;

Wyrok Naczelnego Sądu Administracyjnego z dnia 28 listopada 2002 roku, II SA 3389/01, Legalis nr 99136;

Wyrok Sądu Apelacyjnego w Lublinie z dnia 11 maja 2016 r., I ACa 874/15, Legalis nr 1470120;

Wyrok Sądu Apelacyjnego w Katowicach z dnia 13 stycznia 2016 r., V ACa 874/15, Legalis nr 1408581;

Wyrok Wojewódzkiego Sądu Administracyjnego siedziba w Warszawie z dnia 9 października 2015r., II SA/Wa 40/15, Legalis nr 1364248;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 9 kwietnia 2013 r. II SA/Wa 211/13, Legalis nr 1186854;

Wyrok Sądu Najwyższego - Izba Cywilna z dnia 13 grudnia 2012 r., V CSK 30/12, Legalis nr 667433;

Wyrok Sądu Najwyższego z dnia 13 kwietnia 2017 roku, I CSK 289/16

Wyrok Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 4 listopada 2011 r., II SA/Wa 1002/11, Legalis nr 400297;

Wyrok Naczelnego Sądu Administracyjnego z dnia 6 września 2011 r., I OSK 1476/10, Legalis nr 369758;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 5 listopada 2010 roku, II SA/Wa 964/10, Legalis nr 379532;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 26 sierpnia 2010 r. II SA/Wa 923/10 LEX nr 456399;

Wyrok Wojewódzkiego Sądu Administracyjnego z siedzibą w Warszawie z dnia 7 grudnia 2009 r., II SA/Wa 1094/09, Legalis nr 213824;

Wyrok Naczelnego Sądu Administracyjnego z dnia 1 grudnia 2009 r. I OSK 249/09, Legalis nr 332309;

Wyrok Sądu Apelacyjnego w Katowicach z dnia 28 października 2009 r., V ACa 418/09, Legalis nr 227145;

Wyrok Sądu Najwyższego - Izba Cywilna z dnia 12 lutego 2016 r., II CSK 172/15, Legalis nr 1461030;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 3 marca 2009 r., II SA/Wa 1495/08, Legalis nr 837761;

Wyrok SN z 18.01.1984 r., I CR 400/83, OSNC 1984, nr 11, poz. 195;

Wyrok z 17.01.2001 r. SA w Katowicach, I ACa 1094/00, Legalis nr 52338;

Uchwała 7 sędziów SN z 16.07.1993 r., I PZP 28/93 OSCCP 1994, nr 1, poz. 2;

Wyrok Sądu Najwyższego z dnia 23 stycznia 2008 r., V CSK 377/07, Legalis nr 140220;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia z dnia 2 kwietnia 2007 r., II SA/Wa 2328/06, Legalis nr 840404;

Uchwała SN z 12.10.2001 r., III CZP 57/01, OSNC 2002, nr 5, poz. 57;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 23 marca 2006 roku, II SA/Wa 2047/05, Legalis nr 280899;

Wyrok Wojewódzkiego Sądu Administracyjnego siedziba w Warszawie z dnia 15 lutego 2006 r., II SA/Wa 2055/05, Legalis nr 334989;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 1 grudnia 2005 r., II SA/Wa 917/05, Legalis nr 293064;

Wyrok Wojewódzkiego Sądu Administracyjnego w Białymstoku z dnia 25 lipca 2007 r., II SA/Bk 276/07, Legalis nr 827104;

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z dnia 22 lutego 2005 r., II SA/Wa 2030/04, Legalis nr 75127.

Wykaz decyzji Generalnego Inspektora Ochrony Danych Osobowych

Decyzja GIODO z dnia 15 lipca 2015 roku, DIS/DEC 594/15/62961, Legalis nr 1336609;

Decyzja GIODO z dnia 1 grudnia 2014r., 1215/14/102796, Legalis nr 133656;

Decyzja GIODO z dnia 9 stycznia 2013 roku, DOLiS/DEC-18/13/1245, Legalis nr 813845;

Decyzja GIODO z dnia 22 października 2013r., DOLiS/DEC 1113/13/69461, Legalis nr 1336564;

Decyzja GIODO z dnia 17 września 2013 r., DOLiS/DEC-982/13/60210, Legalis nr 831157;

Decyzja GIODO z dnia 22 maja 2012 r. DOLiS/DEC-458/12/31753, Legalis nr 804426;

Decyzja GIODO z dnia 1 czerwca 2011 r. DOLiS/DEC-442/11, Legalis nr 464291;

Decyzja GIODO z dnia 15 kwietnia 2011 r., DOLiS/DEC-304/11, Legalis nr 1348599;

Decyzja GIODO z dnia 14 września 2010 r. DOLiS/DEC-1103/10, Legalis nr 464232;

Decyzja GIODO z dnia 22 lipca 2010 roku DOLiS/DEC-957/10/29459/10, https://giodo.gov.pl/pl/1520058/3636;

Decyzja GIODO z dnia 22 stycznia 2008 roku DIS-DEC-42/1511, 1515, 1520/08/08 dot. GI-DIS-K-411/22/07;

Decyzja GIODO z dnia 14 grudnia 2007 r., DOLIS/DES-2/440/07, Legalis nr 465536;

Decyzja GIODO z dnia 2 sierpnia 2005 r., GI-DEC-DS-233/05, dostępna na stronie internetowej https://giodo.gov.pl/pl/307/1505;

Decyzja GIODO z dnia 29 kwietnia 2005 r., GI-DEC-DS.-93/05, Legalis nr 465547;

Decyzja GIODO z dnia 23 listopada 2001 r., GI-DEC-DS-178/01, Legalis nr 464277;

Decyzja GIODO z dnia 31 maja 2012, DIS/DEC-492/12/34095, dostępna na stronie internetowej https://giodo.gov.pl/pl/306/4985;

Decyzja GIODO z dnia 28 października 2014, DIS/DEC-1022/14/84106, dostępna na stronie internetowej https://giodo.gov.pl/pl/293/8218.

Wykaz literatury

Adamski A., *Prawo karne komputerowe*, Warszawa 2000;

Bagińska E., *Teoria odpowiedzialności częściowej (proportional liability) jako koncepcja sprawiedliwego rozłożenia ciężaru odpowiedzialności deliktowej – wprowadzenie do problematyki* [w:] Gdańskie Studia Prawnicze 2016, tom XXXV;

Banaszak B., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2012;

Banaszczyk Z., *Odpowiedzialność za szkody wyrządzone przy wykonywaniu władzy publicznej*, Warszawa 2012;

Banyś T., Bielak-Jomaa E., Kuba M., Łuczak J., *Prawo ochrony danych osobowych. Podręcznik dla studentów i praktyków*, Warszawa 2016;

Barta P., P. Litwiński, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2015;

Barta J., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2016;

Bąkowski T., Bielski P., Kaszubowski K., Kokoszczyński M., Stelina J., Warylewski J.K., Wierczyński G., *Zasady techniki prawodawczej. Komentarz do rozporządzenia*, LEX nr 65753;

Bąkowska A., *Outsourcing a ochrona danych osobowych – wybrane zagadnienia* [w:] Biuletyn Bankowy 2005, nr 7/8;

Bielak-Jomaa E., Lubasz D. (red.) *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018;

Bierć A., *Zarys prawa prywatnego*, Warszawa 2015;

Bierć A., *Ochrona prawna danych osobowych w sferze działalności gospodarczej w Polsce – aspekty cywilnoprawne*, [w:] M. Wyrzykowski (red.), *Ochrona danych osobowych*, Warszawa 1999;

Biczysko-Pudełko K., *Administrator danych osobowych i przetwarzający dane na zlecenie a chmura obliczeniowa – problemy interpretacyjne* [w:] Prawo Mediów Elektronicznych 2016 nr 1, Legalis;

Błachnio-Parzych A., *Przepisy karne w ustawie z 10.5.2018 r. o ochronie danych osobowych*, dodatek do Monitora Prawniczego 2018 nr 22, Legalis;

Błachut J., *Dokument jako przedmiot ochrony prawno karnej*, Warszawa 2011;

Boillat P., Kjaerum M., *Podręcznik europejskiego prawa o ochronie danych osobowych*, Luksemburg 2014;

Borucka-Arctowa M. (red.), *Społeczne poglądy na funkcje prawa*, Wrocław-Warszawa-Kraków-Gdańsk-Łódź 1982;

Bosek L., *Gwarancje godności ludzkiej*, Warszawa 2012;

Brzozowski A., J. Jastrzębski, M. Kaliński, E. Skowrońska-Bocian, *Zobowiązania. Część ogólna*, Warszawa 2016;

Byrski J., *Umowne powierzenie do przetwarzania danych osobowych ustawie o ochronie danych osobowych, dyrektywie 95/46 i w ogólnym rozporządzeniu o ochronie danych*, [w:] Dodatek do Monitora Prawniczego 2016 nr 20, Legalis;

Byrski J., *Outsourcing w działalności dostawców usług płatniczych*, 2018, Legalis;

Chauvin T., Stawecki T., Winczorek P., *Wstęp do prawoznawstwa,* Warszawa 2016;

Cieślak Z., *Porozumienie administracyjne*, Warszawa 1985;

Cygan T., *Podręcznik Administratora Bezpieczeństwa Informacji*, Wrocław 2016;

Czachórski W., *Zobowiązania. Zarys wykładu*, Warszawa 2009;

Czaplińska M., *Informacje z CEIDG jako dane osobowe* [w:] ABI-EXPERT 1/2018;

Dmochowska A., M. Zadrożny (red.), *Unijna reforma ochrony danych osobowych. Analiza zmian*, Warszawa 2016;

Dmochowska A., Piotrowska A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018;

Dörre- Kolasa D. (red.), *Ochrona danych osobowych pracowników w świetle rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679*, Warszawa 2017;

P. Drobek [w:] E. Bielak-Jomaa, D. Lubasz (red.), *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018;

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy.* Warszawa 2008;

Dubis W. [w:] E. Gniewek, P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, Warszawa 2017;

Dybowski T. [w:] Z. Radwański (red.), *System Prawa Cywilnego.* Tom III, Wrocław, Warszawa, Kraków, Gdańsk, Łódź 1981;

Dynowski P., Kowalczuk-Pakuła I., Pacek G., *Poradnik prawny dla e-biznesu,* Warszawa 2016;

Engelmann M. [w:] P. Karwatka (red.) *Technologia w ecommerce. Teoria i praktyka. Poradnik menedżera*, Gliwice 2013;

Erechemla A., *Rola wybranych instrumentów prawa ochrony środowiska w zapewnieniu bezpieczeństwa walorów przyrodniczych i turystycznych obszarów przyrodniczo-cennych*, 2007, http://www.pogorzedynowskie.pl/data/referaty/IVBS/ref_13_IVBS.pdf;

Fajgielski P., *Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007;

Fajgielski P. (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008;

Fras M. glosa aprobująca do wyroku Sądu Najwyższego z dnia 19 października 2011 r. (II CSK 86/11, LEX nr 1096037) - Rozprawy Ubezpieczeniowe nr 12 (1/2012), dostępnej na stronie internetowej https://rf.gov.pl/publikacje/artykuly-pracownikow-i-wspolpracownikow/Mariusz_Fras___Glosa_aprobujaca_do_wyroku_Sadu_Najwyzszego_z_dnia_19_pazdziernika_2011_r___II_CSK_86_11__LEX_nr_1096037___21397#_ftn8;

Fuchs B. [w:] M. Habdas, M. Fras (red.) *Kodeks cywilny. Komentarz*, tom III, Warszawa 2018;

Gałach A., Hoc S., Jędruszczak A., Kędzierka K., Kowalik P., Kuszel A., Kuźma M., Marek R., Nowakowski B., *Ochrona danych osobowych i informacji niejawnych w sektorze publicznym*, Warszawa 2015;

Gałaj-Emiliańczyk K., *Tworzenie systemu ochrony danych osobowych krok po kroku*, Warszawa 2016;

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

Gizbert-Studnicki T., *Zasady i reguły prawne*, „Państwo i Prawo" 1988, nr 3;

Gnela B., *Ustawowe ograniczenia swobody umów. Zagadnienia wybrane*, Warszawa 2010;

Gniewek E. (red.) *System Prawa Prywatnego tom 3, Prawo rzeczowe*, Warszawa 2013, Legalis;

Gniewek E., P. Machnikowski (red.), *Kodeks cywilny. Komentarz*, 2017, Legalis;

Gołaczyński J., *Informacja jako przedmiot ochrony*, Prawo Mediów Elektronicznych 1/2004, Legalis 2004;

Gołaczyński J. (red.), *Sporządzanie umów elektronicznych*, Warszawa 2017;

Greniewski H., *Cybernetyka niema tematyczna*, Warszawa 1982;

Grabowski M., Zając A., *Dane, informacja, wiedza – próba definicji*, www.uci.agh.edu.pl;

Greniewski H., *Cybernetyka niema tematyczna*, Warszawa 1982;

Grochowski M., *„Nieuregulowane" umowy o świadczenie usług na gruncie art. 750 KC*, Monitor Prawniczy 2016 nr 23, Legalis;

Gutowski M. (red.), *Prawo cywilne. Komentarz*, T. I, Warszawa 2016, Legalis;

Gutowski M. (red.), *Kodeks cywilny. Tom II. Komentarz*, Warszawa 2019;

Habdas M., Fras M. (red.) *Kodeks cywilny. Komentarz*, tom III, Warszawa 2018;

Helios J., Jedlecka W., *Podstawowe pojęcia prawa i prawoznawstwa dla ekonomistów*, Wrocław 2015, s. 20, http://www.bibliotekacyfrowa.pl/Content/65987/Podstawowe_pojecia_prawa_i_prawoznawstwa_dla_ekonomistow.pdf;

Hruniewicz-Lach E. [w:] R. Zawłocki (red.), *System Prawa Handlowego*, tom X, Warszawa 2018;

Ignaczewski J., *Umowy nienazwane*, Warszawa 2004;

Jagielski M., *Prawo do ochrony danych osobowych. Standardy europejskie*, Warszawa 2010;

Jankowska-Galińska A., Sawicka K., *RODO: Zmiany w zasadach przetwarzania danych osobowych*, https://www2.deloitte.com/pl/pl/pages/doradztwo-prawne/articles/ochrona-danych-osobowych/RODO-zmiany-w-zasadach-przetwarzania-danych-osobowych.html;

Janowski J., *Informatyka prawnicza*, Warszawa 2011;

Janowski J., *Technologia informacyjna dla prawników i administratywistów*, Warszawa 2009;

Jemielniak D., *Koźmiński A.K., Zarządzanie wiedzą*, Warszawa 2012;

Jezioro J., w: E. Gniewek, P. Machnikowski (red.), *Zarys prawa cywilnego*, Warszawa 2016;

Kaczmarek A., *ABC bezpieczeństwa danych osobowych przetwarzanych przy użyciu systemów informatycznych*, Warszawa 2007, s. 48, opracowanie dostępne na stronie internetowej GIODO: https://giodo.gov.pl/data/filemanager_pl/1057.pdf;

Kalina P. [w:] P. Walczak (red.), *Dokumentacja wewnętrzna w jednostkach sektora finansów publicznych*, 2018, Legalis;

Kaliński M., *Szkoda na mieniu i jej naprawienie*, Warszawa 2008;

Kaliński M., [w:] A. Olejniczak (red.), *System Prawa Prywatnego.* Tom VI, Warszawa 2018;

Katner W. J. (red.), *Prawo gospodarcze i handlowe*, Warszawa 2016;

Katner W. J. [w:] M. Stec (red.), *System Prawa Handlowego*, Tom V, Warszawa 2017;

Katner W. J. (red.), *System Prawa Prywatnego T. 9 – Prawo zobowiązań – umowy nienazwane*, Warszawa 2015;

Kędzierska K., [w:] A. Brzezińska, S. Gajewski, A. Gawrońska-Baran, B. Jakacka, K. Kędzierska, Ł. Kudelski, W. Mende, P. Mrozek, E. Pawka-Nowak, B. Pietrzak, M. Rączka, M. Sroczyński, A. Wicik, M. Zając*, Vademecum dyrektora jednostki pomocy społecznej*, Warszawa 2017, Legalis;

Kępa L., *Reforma ochrony danych osobowych w UE. 24 kluczowe zmiany*, Warszawa 2016, s. 10, https://odo24.pl;

Kępiński M., Klafkowska-Waśniowska K., Sikorski R., *Własność intelektualna w obrocie elektronicznym tom V* 2015, Legalis;

Kidyba A. (red.), *Pozakodeksowe umowy handlowe*, Warszawa 2018;

Kluska M. [w:] Kołodziej M. (red.), *Vademecum administratora bezpieczeństwa informacji*, Warszawa 2016;

Kluska M. [w:] M. Kołodziej (red.), *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, 2017, Legalis;

Kłodawski M., *Pojęcie informacji w naukach teoretyczno prawnych*, s. 1, http://depot.ceon.pl/bitstream/handle/123456789/316/Maciej_Klodawski_-_Pojecie_informacji_w_naukach_teoretycznoprawnych.pdf;

Konarski X., *Przetwarzanie danych osobowych w chmurze obliczeniowej* [w:] Dodatek do Monitora Prawniczego 2013 nr 8, Legalis;

Kołodziej M. (red.), *Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych*, Warszawa 2017;

Kopff A., *Ochrona sfery życia prywatnego jednostki w świetle doktryny i orzecznictwa,* ZNUJ 1982, nr 100;

Kowalik P., Wociór D. [w:] D. Wociór (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa 2016;

Krajewska-Kekusz D., *Rola Prezesa UODO w świetle ustawy o ochronie danych osobowyc*h [w:] Informacja w administracji publicznej 2018, nr 4;

Krajewski A. [w:] A. Marek (red.), *System Prawa Karnego*, Tom 1, Warszawa 2010;

Krasińska M., Mizerek S., *ABC wybranych zagadnień z ustawy o ochronie danych osobowych*, Warszawa 2007;

Krasuski A., *Dane osobowe w obrocie tradycyjnym i elektronicznym*, Warszawa 2012;

Krasuski A., *Outsourcing danych osobowych w działalności przedsiębiorstw*, Warszawa 2010;

Krasuski A., Skolimowska D., *Dane osobowe w przedsiębiorstwie*, Warszawa 2007;

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

Kuraś M., System informacyjny - system informatyczny. Co poza nazwą różni te dwa obiekty?, oraz powołana tam literatura, dostępne na: uci.agh.edu.pl/uczelnia/tad/PSI9/3.rtf;

Kwiatkowska-Cylke M. [w:] D. Lubasz (red.), RODO w e-commerce, Warszawa 2018;

Lackoroński B. [w:] K. Osajda (red.), *Kodeks cywilny. Komentarz*, Warszawa 2018;

Lang W., *Struktura odpowiedzialności prawnej* [w:] „Prawo" 1968 nr 8;

Litwiński P., *Pojęcie danych osobowych w rozporządzeniu ogólnym o ochronie danych osobowych*, [w:] *Informacja w administracji publicznej* 2017 nr 3;

Litwiński P., *Hosting danych osobowych. Zagadnienia podstawowe*, w: Monitor Prawniczy 2008 nr 23, Legalis;

Litwiński P., *Administrator danych osobowych w sektorze publicznym po zmianach w ustawie o ochronie danych osobowych wprowadzonych ustawą „500+"* [w:] Informacja w Administracji Publicznej 2016, Nr 2;

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

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

Litwiński P. [w:] D. Szostek (red.), *Bezpieczeństwo danych i IT w kancelarii prawnej radcowskiej/ adwokackiej/ notarialnej/ komorniczej. Czyli jak bezpiecznie przechowywać dane w kancelarii prawnej*, Warszawa 2018, Legalis;

Litwiński P. [w:] M. Jagielski, M. Krasińska, P. Litwiński, P. Kawczyński, K. Wojsyk, A. Sieradzka, E. Bielak-Jomaa, K. Andres, *Ochrona danych osobowych medycznych*, Warszawa 2013;

Lubański M., *Filozoficzne zagadnienia teorii informacji*, Warszawa 1975;

Łętowska E. (red.), *System Prawa Prywatnego Tom V Prawo zobowiązań – część ogólna*, Warszawa 2012;

Łętowska E., Woleński J., *Czy prawo zatruwa wolność?* [w:] Przegląd Filozoficzny – Nowa Seria R. 22: 2013, Nr 3;

Machnikowski P., *Swoboda umów według art. 353[1] KC. Konstrukcja prawna*, Warszawa 2005;

Machnikowski P., A. Śmieja [w:] A. Olejniczak (red.), *System Prawa Prywatnego.* Tom VI, Warszawa 2018;

Malinowska K., *Umowa ubezpieczenia w Europie bez granic*, Warszawa 2008;

Marek A., *System Prawa Karnego*, Tom I, Warszawa 2010;

Maroń G., *Zasady prawa. Pojmowanie i typologie a rola w wykładni prawa i orzecznictwie konstytucyjnym*, Poznań 2011;

Maryniarczyk A. (red.), *Powszechna Encyklopedia Filozofii*, www.ptta.pl/pef;

Mazur M., *Jakościowa teoria informacji*, http://www.autonom.edu.pl/publikacje/mazur_marian/jakosciowa_teoria_informacji-tiff.pdf;

Mednis A., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2001;

Mednis A. (red.), *Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016, Legalis;

Mell P., Grace T., SP-800-145 The NIST definition of cloud computing, 2011, https://csrc.nist.gov/publications/detail/sp/800-145/final;

Michalski D., *RODO: przetwarzanie danych pod kątem adekwatności*, Rzeczpospolita, 6 października 2017 roku, http://www.rp.pl/Firma/310069981-RODO-przetwarzanie-danych-pod-katem-adekwatnosci.html;

Molenda-Kropielnicka E., *Cloud compting – zagadnienia prawne*, Zeszyty Naukowe Uniwersytetu Jagiellońskiego 2013 nr 1;

Motyka K., *Prawo do prywatności*, Zeszyty Naukowe Akademii Podlaskiej w Siedlcach 2010, Nr 85;

Mróz T. (red.), *Zobowiązania*, Warszawa 2016;

Mróz T., *Dekompozycja zasady swobody umów? Próba klasyfikacji i oceny niektórych czynników kształtujących tę zasadę*, [w:] B. Gnela (red.), *Ustawowe ograniczenia zasady swobody umów. Zagadnienia wybrane*, Warszawa 2010;

Mróz J., *Outsourcing w sektorze małych i średnich przedsiębiorstw*, [w:] S. Wawak, M. Sołtysik (red.), *Współczesne trendy outsourcingu*, Kraków 2015;

Nadolna B., *Informacja i komunikacja jako element kontroli zarządczej w jednostkach sektora finansów publicznych, Zeszyty Naukowe Uniwersytetu Szczecińskiego* 2011 nr 669, Finanse, Rynki Finansowe, Ubezpieczenia nr 42, s. 85, dostępne na: http://www.wneiz.pl/nauka_wneiz/frfu/42-2011/FRFU-42-81.pdf;

Napierała K., *Prawne aspekty ochrony danych osobowych, przetwarzanych w systemach informatycznych*, Warszawa 1997;

Niewiadomski Z. (red.), *Prawo administracyjne*, Warszawa 2013;

Osajda K. (red.), *Kodeks cywilny. Komentarz*, 2018, Legalis;

Ossowska-Salamonowicz D., *Ochrona danych osobowych w działalności dziennikarskiej*, Olsztyn 2015;

Pacek G., *Wybrane zagadnienia związane z odpowiedzialnością dostawców usług hostingowych*, http://www.bibliotekacyfrowa.pl/dlibra/doccontent?id=23622;

Pietrzykowski K. (red.), *Kodeks cywilny. T. I. Komentarz*, Warszawa 2015, Legalis;

Piotrowska A., *Wiedza jawna i niejawna jako zasób decyzyjny w zarządzaniu personelem* [w:] A. Grzegorczyk (red.) *Procesy decyzyjne w warunkach niepewności*, Warszawa 2012, wsp.pl/file/1064_490624587.pdf;

Płowiec W., *Koncepcja aktu prawa wewnętrznego w Konstytucji RP*, Poznań 2006, https://repozytorium.amu.edu.pl/bitstream/10593/19276/3/Koncepcja%20aktu%20prawa%20wewn%C4%99trznego.pdf;

Polański P., *Uwagi na temat odpowiedzialności usługodawcy hostingu w Internecie*, [w:] J. Gołączyński (red.), *Informatyzacja postępowania sądowego i administracji publicznej*, Warszawa 2010;

Popiołek W. [w:] K. Pietrzykowski (red.), *Kodeks cywilny. T II. Komentarz. Art. 450–1088. Przepisy wprowadzające*, Warszawa 2018;

Prutis S., *Instytucje podstawowe prawa prywatnego (w opozycji do regulacji prawa publicznego)*, Białystok 2018;

Pulka Z. [w:] A. Bator (red.), *Wprowadzenie do nauk prawnych : leksykon tematyczny*, Warszawa 2016;

Radwański Z., *Teoria umów*, Warszawa 1977;

Radwański Z. (red.) *System Prawa Prywatnego, Tom 2 – Prawo cywilne część ogólna*, Warszawa 2008;

Radwański Z., Olejniczak A., *Prawo cywilne – część ogólna*, Warszawa 2015;

Radwański Z., Olejniczak A., *Zobowiązania - część ogólna*, Warszawa 2016;

Radwański Z., Panowicz-Lipska J., *Zobowiązania –część szczegółowa*, Warszawa 2015;

Rajski J., *Prawo o kontraktach w obrocie gospodarczym*, Warszawa 2002;

Romaszewski A., Trąbka W., Kielar M., *Perspektywy wprowadzenia modelu chmury obliczeniowej w ochronie zdrowia w świetle istniejących rozwiązań prawnych i organizacyjnych,* Zeszyt Naukowy Wyższej Szkoły Zarządzania i Bankowości w Krakowie, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fef88407-fd08-4113-8803-22dc9c7586d8;

Rot A., *Wybrane zagadnienia bezpieczeństwa danych i usług w modelu cloud computing* [w:] A. Gąsiorkiewicz, K. Sitarski, O. Sobolewska, M. Wiśniewski (red.), *Gospodarka cyfrowa 2016. Zarządzanie, innowacje, społeczeństwo i technologie*, Warszawa 2017;

Rzucidło J., *Prawo do prywatności i ochrona danych osobowych*, http://www.repozytorium.uni.wroc.pl/Content/52920/09_Jakub_Rzucidlo.pdf;

Rzymowski J., *Zasada rozliczalności w RODO*, [w:] ABI EXPERT 2018 nr 1;

Safjan M. (red.), *System Prawa Prywatnego, Tom I, Prawo cywilne- część ogólna*, Warszawa 2012, Legalis;

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

Sakowska-Baryła M. (red.), *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2018;

Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003;

Sibiga G., *Podpowierzenie przetwarzania danych osobowych*, [w:] Dodatek do Monitora Prawniczego 2012 nr 7;

Sieńczyło-Chlabicz J., *Naruszenie prywatności osób publicznych przez prasę. Analiza cywilnoprawna*, Zakamycze 2006;

Sikorski G. (red.), *Prawo bankowe. Komentarz*, Warszawa 2015;

Skrodzka M. J., Skrodzki K., *Źródła zasady swobody umów oraz wybrane aspekty jej granic – w świetle orzecznictwa*, Białostockie Studia Prawnicze 2008 z. 3;

Sobczak J., *Ochrona danych osobowych - standardy unijne i rzeczywistość polska* [w:] J. Jaskiernia (red.), *Wpływ standardów międzynarodowych na rozwój demokracji i ochronę praw człowieka*, Warszawa 2013;

Sobczak J. [w:] A. Wróbel (red.), *Karta Praw Podstawowych Unii Europejskiej. Komentarz*, Warszawa 2013;

Stahl M. (red.), *Prawo administracyjne. Pojęcia, instytucje, zasady w teorii i orzecznictwie,* Warszawa 2015;

Stec M. (red.), *System Prawa Handlowego tom V, Prawo umów handlowych*, Warszawa 2017;

Stelmachowski A., *Wstęp do teorii prawa cywilnego*, Warszawa 1984;

Stelmachowski A., *Zarys teorii prawa cywilnego*, Warszawa 1998;

Szafrański D., Białończyk W., Bielecki A., Kasiak Ł., Piecha J. (red.), *Zasady techniki prawodawczej w zakresie aktów prawa miejscowego. Komentarz praktyczny z wzorami oraz przykładami*, 2016, Legalis;

Szaraniec M., *Działalność ubezpieczeniowa pośredników ubezpieczeniowych. Studium publicznoprawne*, Warszawa 2017;

Szaraniec M., *Publicznoprawne ograniczenia swobody kontraktowej w działalności krajowego zakładu ubezpieczeń – zagadnienia wybrane,* [w:] B. Gnela (red.), *Ustawowe ograniczenia zasady swobody umów. Zagadnienia wybrane,* Warszawa 2010;

Szewc T. [w:] S. Hoc, T. Szewc, *Ochrona danych osobowych i informacji niejawnych*, Warszawa 2014;

Szmit M., *Wybrane zagadnienia opiniowania sądowo-informatycznego*, Warszawa 2014;

Szpor G., *Jawność i jej ograniczenia, Tom I, Idee i pojęcia*, 2016, Legalis;

Szpor G., *Pojęcie informacji a zakres ochrony danych*, [w:] P. Fajgielski (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008;

Szumiło-Kulczycka D., *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012;

Szymczak M. (red.), *Słownik języka polskiego, tom II*, Warszawa 1993;

Śleszyńska A., *Instytucja powierzenia przetwarzania danych osobowych* [w:] Temidium.pl -Portal Okręgowej Izby Radców Prawnych w Warszawie, https://www.temidium.pl/artykul/instytucja_powierzenia_przetwarzania_danych_osobowych-2172.html;

Świętochowska E., *Dane nieosobowe mogą płynąć ponad granicami UE,* [w:] Gazeta Prawna z dnia 19 września 2017 roku, http://prawo.gazetaprawna.pl/artykuly/1071970,transgraniczny-transfer-danych-nieosobowych.html;

Tenenbaum M., *Instytucja zadatku w polskim prawie cywilnym*, Warszawa 2008;

Ura E., *Prawo administracyjne*, Warszawa 2015;

Walaszek-Pyzioł A., *Regulacja – innowacja w sektorze energetycznym*, Legalis 2013;

Wanio G. [w:] M. Kołodziej (red.), *Vademecum administratora bezpieczeństwa informacji*, Warszawa 2016;

Wawszczak W., *Wprowadzenie do filozofii informacji*, chfpn.pl/files/?id_plik=413;

Wierzbicki T., *System informacji gospodarczej*, Warszawa 1981;

Wierzbowski M., Hauser R. (red.), *Kodeks postępowania administracyjnego. Komentarz*, Warszawa 2018;

Wiącek M. [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP. Tom II. Komentarz do art. 87–243*, Warszawa 2016, Legalis;

Wierczyński G., *Redagowanie i ogłaszanie aktów normatywnych. Komentarz*, 2016, LEX nr 500982;

Wikariak S., *SN: Przedsiębiorca może ponosić odpowiedzialność za wyciek danych, do którego doszło w innej firmie, Gazeta Prawna*, 13.11.2017, http://prawo.gazetaprawna.pl/artykuly/1084457,odpowiedzialnosc-przedsiebiorcy-za-wyciek-danych-w-innej-firmie.html;

Wild, [w:] M. Safjan, L. Bosek (red.), *Konstytucja RP. Tom I. Komentarz do art. 1–86*, Warszawa 2016, Legalis;

Wincenciak M., *Sankcje w prawie administracyjnym i procedura ich wymierzania*, Warszawa 2008;

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

Włodyka S. (red.), *Prawo umów w obrocie gospodarczym*, Kraków 2001;

Wociór D. (red.), *Ochrona danych osobowych i informacji niejawnych z uwzględnieniem ogólnego rozporządzenia unijnego*, Warszawa 2016;

Wojciechowski P., *Model odpowiedzialności administracyjnej w prawie żywnościowym*, Warszawa 2015;

Wronkowska S., *Podstawowe pojęcia prawa i prawoznawstwa*, Poznań 2005;

Wronkowska S., Ziembiński Z., *Zarys teorii prawa*, Poznań 2001;

Wronkowska S., Zieliński Z., Ziembiński Z., *Zasady prawa. Zagadnienia podstawowe*, Warszawa 1974;

Zakrzewski P. [w:] M. Habdas, M. Fras (red.), *Kodeks cywilny. Komentarz. Tom IV. Zobowiązania. Część szczegółowa (art. 535-764*(1) Warszawa 2018;

Zawiła-Niedźwiedzki J., Dyrda S., Wisłowski L., [w:] A. Stabryła, S. Wawak (red.), *Metody, badania i modele rozwoju organizacji*, Kraków 2012;

Zawłocki R. (red.), *System Prawa Handlowego*, tom X, Warszawa 2018;

Ziembiński Z., *O pojmowaniu celu, zadania, roli i funkcji*, [w:] Państwo i Prawo 1987 z. 12.

Wykaz innych materiałów źródłowych

Norma PN-ISO/IEC 27000:2014: Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Przegląd i terminologia.

Publikacja GIODO materiał „Czy jesteś gotowy na RODO?" dostępny na stronie internetowej https://www.giodo.gov.pl/pl/1520281/10255;

Publikacja Narodowego Instytutu Wolności oraz GIODO, *Gotowi na RODO;*.

Publikacja Biura Generalnego Inspektora Ochrony Danych Osobowych *Jak rozumieć podejście oparte na ryzyku*, 2017, dostępna na https://giodo.gov.pl/pl/1520282/10294;

Opracowanie *Data controllers and data processors: what the difference is and what the governance implications are*, dostępne na stronie internetowej https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf;

Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający" przyjętej w dniu 16 lutego 2010 roku przez Grupę Roboczą ds. ochrony danych powołaną na mocy art. 29 Dyrektywy 95/46/WE;

Opinia Grupy Roboczej ds. Ochrony Danych Osobowych w sprawie zasady rozliczalności (WP 173) nr 3/2010;

Opinia 4/2007 Grupy Roboczej art. 29 ds. Ochrony Danych Osobowych w sprawie pojęcia danych osobowych WP 136;

Opinia Grupy Roboczej ds. Ochrony Danych Osobowych nr 5/2012 w sprawie przetwarzania danych w chmurze obliczeniowej WP 196;

Rekomendacja Organizacji Współpracy Gospodarczej i Rozwoju (OECD) z dnia 23 września 1980 r., w sprawie wytycznych dotyczących ochrony prywatności i przekazywania danych osobowych pomiędzy krajami;

Rezolucja w sprawie Prywatności w Fazie Projektowania przyjętej przez Rzeczników Ochrony Danych Osobowych i Prywatności w 2010 roku w Jerozolimie;

Opinia Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie chmur obliczeniowych (cloud computing) w Europie (opinia z inicjatywy własnej) z dnia 26 października 2011 r. (2012/C 24/08), dostępna na stronie https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:024:0040:0047:PL:PDF;

Komunikat Urzędu Komisji Nadzoru Finansowego dotyczącego korzystania przez podmioty nadzorowane z usług przetwarzania danych w chmurze obliczeniowej z dnia 23 października 2017 r., dostępny na stronie internetowej: https://www.knf.gov.pl/knf/pl/komponenty/img/Komunikat_dot_korzystania_przez_podmioty_nadzorowane_z_uslug_przetwarzania_danych_w_chmurze_obliczeniowej_59626.pdf.

Wykaz stron internetowych

http://sjp.pwn.pl/szukaj/informacja.html

http://www.wsjp.pl/index.php?id_hasla=22125&id_znaczenia=3976450&l=10&ind=0

https://www.synonimy.pl/synonim/informacja/

http://encyklopedia.pwn.pl/szukaj/cybernetyka.html

http://sjp.pwn.pl/szukaj/niejawny.html

https://www.synonimy.pl/synonim/niejawny/

www.sn.pl/sites/orzecznictwo/orzeczenia3/i%20csk%20289-16-1.pdf

http://www.giodo.gov.pl/pl/1520286/9964

http://www.giodo.gov.pl/568/j/pl/

http://www.giodo.gov.pl/568/id_art/603/j/pl/

http://www.abi-expert.pl/wydania/styczen-marzec-2018/art,1969,zasady-informowania.html

http://orka.sejm.gov.pl/proc2.nsf/projekty/1928_p.htm

http://orka.sejm.gov.pl/Rejestrd.nsf/wgdruku/3171/$file/3171.pdf

http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm.

http://www.giodo.gov.pl/pl/306/2329

https://accounts.google.com/SignUp?service=mail&continue=https%3A%2F%2Fmail.google.com%2Fmail%2Fu%2F0%2F&ltmpl=default

https://support.google.com/accounts/answer/1733224?hl=pl

https://pl.wikipedia.org/wiki/Newsletter

https://slownik.intensys.pl/definicja/adres-ip/

http://www.giodo.gov.pl/pl/319/2258

https://pl.wikipedia.org/wiki/Business_Intelligence

http://www.giodo.gov.pl/pl/319/2836

http://www.giodo.gov.pl/317/id_art/3512/j/p

https://pl.wikipedia.org/wiki/Nick.

https://finanse.wp.pl/sony-stracilo-ponad-170-mln-dolarow-przez-hakerow-6114319048091777a

http://www.katowice.sa.gov.pl/container/biuletyny//orzeczenia//2010//1//C//V_ACa_418-09.pdf.

http://sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=2051

http://www.giodo.gov.pl/560/id_art/3637/j/pl

https://giodo.gov.pl/305/id_art/1469/j/pl

http://www.giodo.gov.pl/pl/1520301/10243

https://edugiodo.giodo.gov.pl/file.php/1/UST/UST_03_02.htm

https://edugiodo.giodo.gov.pl/file.php/1/UST/UST_03.htm

http://www.giodo.gov.pl/pl/147/713

https://sjp.pwn.pl/slowniki/nick.html

https://www.giodo.gov.pl/259/id_art/6271/j/pl

https://edugiodo.giodo.gov.pl/file.php/1/ODO/ODO_R02_07.htm

https://edugiodo.giodo.gov.pl/file.php/1/UST/UST_03_05.htm

https://www.giodo.gov.pl/pl/1520281/10255

https://ico.org.uk/media/for-organisations/documents/1546/data-controllers-and-data-processors-dp-guidance.pdf

https://ec.europa.eu/info/strategy/justice-and-fundamental-rights/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_en

https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-przepisy-wprowadzajace-ustawe-o-ochronie-danych-osobowych.html

https://www.gov.pl/cyfryzacja/projekt-ustawy-o-ochronie-danych-osobowych-skierowany-na-komitet-do-spraw-europejskich-rady-ministrow

https://www.poradyodo.pl/odpowiedzialnosc-abiado/czy-podmiot-przetwarzajacy-moze-odrzucic-zapisy-umowy-dotyczace-kontroli-jego-dzialania-8306.html

https://giodo.gov.pl/317/id_art/3254/j/pl.

https://giodo.gov.pl/pl/1520111/4760

http://www.giodo.gov.pl/pl/1520057/3595

https://edugiodo.giodo.gov.pl/file.php/1/REJ/REJ_R06_03.html
http://www.giodo.gov.pl/pl/1520281/10023

http://www.giodo.gov.pl/pl/1520084/3830

https://edugiodo.giodo.gov.pl/pluginfile.php/36/mod_resource/content/5/KON/KON_R03.html#8

https://edugiodo.giodo.gov.pl/pluginfile.php/36/mod_resource/content/5/KON/KON_R03.html#8

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

https://www.computerworld.pl/news/Czym-rozni-sie-serwerownia-od-centrum-danych,369934.html.

https://giodo.gov.pl/data/filemanager_pl/1057.pdf

https://home.pl/firma/datacenter

http://www.komputerswiat.pl/jak-to-dziala/2015/06/hosting.aspx.

https://home.pl/hosting

https://www.nazwa.pl/fileadmin/nazwa/Regulaminy/Regulamin_uslugi_serwera.pdf

https://www.cal.pl/hosting-serwery-shared

https://home.pl/regulaminy/nowyhd.

http://www.bibliotekacyfrowa.pl/dlibra/doccontent?id=23622

https://pomoc.home.pl/baza-wiedzy/umowa-na-hosting-wirtualny-z-zapisami-giodo

http://hostedwindows.pl/pl/hosting/hosting-ochrona-danych-osobowych-rodo/

http://hostedwindows.pl/pl/regulaminy/wzor-umowy-na-powierzenie-przetwarzania-danych-osobowych/

https://www.spidersweb.pl/2012/12/maciej-kuzniar-chmurach-niechmurach-czyli-czym-sie-rozni-cloud-computing-od-zwyklego-hostingu.html

http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-fef88407-fd08-4113-8803-22dc9c7586d8,

https://azure.microsoft.com/pl-pl/overview/what-is-a-public-cloud/

https://www.intel.pl/content/www/pl/pl/it-managers/jaka-chmure-wybrac.html

https://azure.microsoft.com/pl-pl/overview/what-is-a-private-cloud/.

https://www.ibm.com/cloud-computing/pl-pl/learn-more/what-is-private-cloud/

https://azure.microsoft.com/pl-pl/overview/what-are-private-public-hybrid-clouds/

http://computingcloud.pl/pl/cloud-przewodnik/ciekawostki/228-co-amerykanie-wiedza-o-chmurze

https://www.ibm.com/support/customer/pdf/csa_pl_pl.pdf

https://www-03.ibm.com/software/sla/sladb.nsf/pdf/7745WW3/$file/Z126-7745-WW-3_05-2018_pl_PL.pdf

https://www.ibm.com/support/customer/pdf/dpa_pl.pdf

http://computingcloud.pl/pl/cloud-przewodnik/ciekawostki/228-co-amerykanie-wiedza-o-chmurze

https://giodo.gov.pl/pl/1520129/4646

https://www.oracle.com/legal/privacy/

https://www.oracle.com/assets/data-processing-agreement-072718-5029569.pdf

https://www.oracle.com/assets/data-processing-agreement-072718-5029569.pdf.

https://www.comarch-cloud.pl/public/userfiles/ERP/Optima%20dla%20firm/Regulamin_Comarch_ERP_Optima_w_modelu_uslugowym.pdf

https://zaufanatrzeciastrona.pl/post/interoperacyjnosc-i-przenaszalnosc-jak-uniezaleznic-sie-od-dostawcy/

https://businessinsider.com.pl/technologie/nowe-technologie/francja-ukarala-google-50-mln-euro-za-naruszenie-rodo/m419et9

https://gdpr.pl/przeciw-utrzymaniu-penalizacji-ochronie-danych-osobowych#_ftn4