REFORMA
OCHRONY DANYCH OSOBOWYCH
– CEL, NARZĘDZIA, SKUTKI

REFORMA OCHRONY DANYCH OSOBOWYCH – CEL, NARZĘDZIA, SKUTKI

red. naukowa
J. Taczkowska-Olszewska
M. Nowikowska
A. Brzostek

Wydawnictwo Naukowe
SILVA RERUM

Akademia Sztuki Wojennej
Wydział Bezpieczeństwa Narodowego

Poznań 2018

Recenzja
prof. dr hab. Grzegorz Tylec
prof. dr hab. Michał Domagała

Redaktor prowadzący
Paulina Wiśniewska

Korekta
Anna Surendra, Sebastian Surendra

Projekt okładki
Studio Graficzne SILVA RERUM

Skład komputerowy
Munda Maciej Torz

Zdjęcie na okładce
Depositphotos

Prawa autorskie
Yakobchuk

ISBN
978-83-65697-30-1 /druk/
978-83-65697-31-8 /e-book/

Wydanie I: Wydawnictwo Naukowe SILVA RERUM
www.wydawnictwo-silvarerum.eu
Poznań 2018

Druk i oprawa - Zakład Poligraficzny Moś i Łuczak spółka jawna
ul. Piwna 1, 61-065 Poznań
tel./fax 0-61 6337165
www.mos.pl

Skład ukończono w maju 2018

SPIS TREŚCI

Wstęp

Oddawana do rąk czytelników praca zbiorowa „Reforma ochrony danych osobowych – cel, narzędzia skutki" należy do cyklu monografii, których tematyka dotyczy nowych rozwiązań prawnych przyjętych na płaszczyźnie działalności prawodawczej UE i obejmujących analizę zakresu, skutków oraz trybu wdrażania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U.L 119 z 4.5.2016, s. 1 – dalej jako RODO). RODO zastąpiło dotychczas obowiązującą dyrektywę 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, a jego przepisy zaczną być stosowane od 25 maja 2018 r.

W ocenie autorów niniejszej pracy zbiorowej uchylenie dyrektywy 95/46/WE i zastąpienie jej rozporządzeniem RODO powinno być analizowane nie tylko w wymiarze formalnym wskazującym na zmianę charakteru aktu prawnego regulującego zasady ochrony danych osobowych i ich transgraniczny przepływ pomiędzy państwami członkowskimi UE, ale także w wymiarze materialno-prawnym, tj. poprzez kształt, jaki został nadany przez prawodawcę europejskiego nowym instytucjom prawnym. Za celowe Autorzy tej publikacji uznają także definiowanie zmian wprowadzonych w wyniku wejścia w życie RODO w ujęciu systemowym wymagającym uwzględnienia rangi i charakteru aktów prawych oraz analizy norm prawnych, niekiedy rozproszonych w przepisach prawa i zawartych w wielu dokumentach. Ponadto konieczne jest dostrzeżenie aspektów funkcjonalnych i celowościowych towarzyszących zarówno pracom nad ostatecznym kształtem przepisów zawartych w RODO, jak i zawartym w 178 motywach tworzących preambułę zasadniczego tekstu RODO.

Autorzy niniejszej pracy, w przeciwieństwie do wielu powstałych na przełomie 2017 i 2018 r. publikacji, zrezygnowali, w sposób świadomy i celowy, z podejmowania analizy nowych regulacji z perspektywy odpowiadającej potrzebom podmiotów prawa prywatnego, w tym w szczególności przedsiębiorców, na których RODO nakłada nowe obowiązki oraz na nowo definiuje ich status jako administratorów danych osobowych. Autorzy przyjmują bowiem, że centralnym problemem, jaki jawi się w związku z zachodzącymi zmianami, jest modyfikacja samej natury prawa do ochrony danych osobowych, które nabiera charakteru majątkowego, co w konsekwencji nakłada na organy władzy publicznej nowe obowiązki związane z potrzebą zagwarantowania bezpieczeństwa przepływu danych osobowych oraz regulowania do nich dostępu nie tylko w celu wzmocnienia zaufania obywateli do środowiska cyfrowego, ale przede wszystkim ze względu na potrzebę zapewnienia bezpieczeństwa państwa, którego składnikiem jest bezpieczeństwo informacyjne, w tym zwłaszcza ochrona danych osobowych obywateli jako uczestników Jednolitego Rynku Cyfrowego.

Tematyce tej poświęcony został w szczególności artykuł dr hab. Joanny Taczkowskiej-Olszewskiej, prof. ASzWoj, który stanowi wprowadzenie do opracowania, a zarazem zawiera uwagi dotyczące zakresu oraz charakteru zmian dokonanych wprowadzeniem RODO oraz odniesienia do problematyki ochrony majątkowych aspektów prawa do ochrony danych osobowych. Artykuł dr hab. Lucyny Szot, prof. UWr, zawiera analizę problematyki prawa do bycia zapomnianym przez pryzmat regulacji dotyczących ochrony danych osobowych. Dr Maria Łoszewska-Ołowska omawia natomiast podstawowe zasady związane z ochroną danych osobowych w działalności prasowej, w tym w szczególności w związku z postanowieniami zawartymi w art. 13 prawa prasowego ustanawiającego zakaz wypowiadania tzw. przedsądów. Artykuł zawiera zwięzłe streszczenie poglądów przedstawicieli nauki prawa oraz orzecznictwa sądowego dotyczące opisywanego problemu.

Drugą część książki otwiera artykuł dr. Konrada Walczuka poświęcony korelacji istniejącej, zdaniem Autora, pomiędzy zakresem ochrony danych osobowych przewidywanym w nowych rozwiązaniach prawnych a dostępem do informacji publicznej. Zagadnienie dotyczące bezpieczeństwa informacyjnego PNR w lotnictwie cywilnym omówiła w swym artykule dr hab. Małgorzata Polkowska. W opracowaniu omówiony został projekt ustawy autorstwa Ministerstwa Spraw Wewnętrznych i Administracji (MSWiA) w sprawie przetwarzania danych dotyczących przelotów pasażerskich oraz regulacje UE dotyczące wykorzystywania danych dotyczących takich przelotów (danych PNR).

W kolejnej części monografii znalazły się artykuły autorstwa dr. Piotra Milika, dr Moniki Nowikowskiej, dr. Mariusza Kamińskiego, dr. Dariusza Nowaka oraz dr Agnieszki Brzostek i dr. Filipa Radoniewicza. Autorzy odnoszą się w nich do szczegółowych problemów, jakie występują lub mogą wystąpić w związku z wejściem w życie RODO w tych sferach działania organów administracji publicznej, które obejmują pozyskiwanie i przetwarzanie danych osobowych. W nurt tych rozważań wpisuje się oparty na cennych spostrzeżeniach natury praktycznej artykuł dr Moniki Nowikowskiej, która omawia zasady ochrony danych osobowych w dokumentach kontrolnych a także opracowanie dr. Mariusza Kamińskiego dotyczące uprawnień służb specjalnych w zakresie dostępu do danych osobowych oraz przeprowadzona przez dr. Sławomira Chomoncika analiza problematyki obejmującej zasady ochrony danych osobowych osób zatrudnionych w ramach stosunku pracy. Natomiast dr D. Nowak dokonuje przeglądu aktów prawnych regulujących ochronę danych osobowych w Siłach Zbrojnych RP a dr Agnieszka Brzostek podejmuje próbę zarysowania zasad przetwarzania informacji, w tym danych osobowych i związanych z tym obowiązków ciążących na organach administracji publicznej. Aspekt prywatnoprawny ochrony danych pojawia się w artykułach dr. Piotra Milika i dr. Filipa Radoniewicza. Dr Piotr Milik analizuje zasady ochrony danych osobowych w działalności podmiotów prowadzących działalność gospodarczą w sferze obrotu specjalnego, a dr Filip Radoniewicz przeprowadza analizę krytyczną tych przepisów prawa karnego, które sankcjonują przestępstwo kradzieży tożsamości.

Zważywszy na szerokie ujęcie problematyki związanej z ochroną danych osobowych, należy mieć nadzieję, że zawarte w monografii materiały stanowić będą przyczynek do dyskusji nad skutecznością nowych rozwiązań prawnych, a zarazem – na co szczególnie liczą Autorzy monografii – staną się wskazówką w poszukiwaniu odpowiedzi na pytania rodzące się na tle stosowania przepisów RODO w działalności podmiotów prywatnych oraz praktyce organów administracji publicznej.

Część I

OCHRONA DANYCH OSOBOWYCH W UE – NOWE ROZWIĄZANIA PRAWNE

dr hab. Joanna Taczkowska-Olszewska[1]

MAJĄTKOWY I NIEMAJĄTKOWY CHARAKTER PRAWA DO (OCHRONY) DANYCH OSOBOWYCH W ŚWIETLE PRZEPISÓW REFORMUJĄCYCH SYSTEM OCHRONY DANYCH OSOBOWYCH W UE

1. Uwagi ogólne

Wejście w życie 24 maja 2016 r. rozporządzenia (UE) 2016/679 z 27 kwietnia 2016 r. (ogólne rozporządzenie o ochronie danych – dalej jako RODO)[2], które – zgodnie z treścią art. 99 ust. 2 – będzie stosowane we wszystkich państwach członkowskich UE począwszy od 25 maja 2018 r.[3], oznacza, że w miejsce 28 krajowych aktów prawnych znajdzie zastosowanie jeden ogólnoeuropejski zbiór przepisów regulujących zasady ochrony danych osobowych. Zwraca się uwagę, że przyjęcie RODO oznacza powierzenie nadzoru nad transgranicznymi[4] operacjami przetwa-

[1] Dr hab. prof. nadzw. ASzWoj Joanna Taczkowska-Olszewska – kierownik Katedry Administracji i Prawa Administracyjnego, Instytut Prawa i Administracji Obronnej, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej.

[2] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U.L 119 z 4.05.2016, s. 1) – dalej jako RODO.

[3] Parlament Europejski przyjął RODO 27 kwietnia 2016 r., a opublikowanie jego tekstu w Dzienniku Urzędowym Unii Europejskiej nastąpiło 4 maja 2016 r. Zgodnie z treścią art. 99 ust. 2 RODO weszło w życie dwudziestego dnia po publikacji w Dzienniku Urzędowym UE, tj. 24 maja 2016 r., a jego stosowanie rozpocznie się 25 maja 2018 r. (art. 99 ust. 2 RODO).

[4] Pojęcie „transgranicznego przetwarzania danych" zostało zdefiniowane w art. 4 pkt 23 RODO i oznacza a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach

rzania[5] danych jednemu organowi oraz zagwarantowanie jednolitej interpretacji zawartych w rozporządzeniu przepisów[6], co wynika z dostrzeżonej przez organy UE potrzeby zwiększenia zaufania względem usług cyfrowych i poprawy ich bezpieczeństwa[7] w związku z realizacją strategii Jednolitego Rynku Cyfrowego. Jednolity Rynek Cyfrowy (*digital single market*) definiowany jest jako „przestrzeń, w której zapewniony jest swobodny przepływ towarów, osób, usług i kapitału, a obywatele i przedsiębiorstwa mogą bez przeszkód i na zasadach uczciwej konkurencji uzyskać dostęp do usług *online* lub je świadczyć"[8].

---

działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim.

[5] Zgodnie z treścią art 4 pkt 2 RODO „przetwarzanie" oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie

[6] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Budowa europejskiej gospodarki opartej na danych" (COM/2017/09 final) z 10 stycznia 2017 r.,http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2017:9:FIN.

[7] Z ustaleń Komisji Europejskiej wynika, że konsumenci w UE mogliby co roku zaoszczędzić 11,7 mld euro, gdyby kupując w internecie, mieli dostęp do pełnej gamy produktów i usług oferowanych w UE. 61% konsumentów ma zaufanie do firm prowadzących sprzedaż w internecie, jeżeli mają one siedzibę w tym samym państwie członkowskim, ale tylko 38% ma zaufanie do sprzedawców internetowych z innych państw członkowskich UE. Jedynie 7% MŚP w UE prowadzi sprzedaż transgraniczną (Komunikat komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Strategia Jednolitego Rynku Cyfrowego dla Europy, COM(2015)192 final z 6 maja 2015 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52015DC0192).

[8] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu regionów, Strategia Jednolitego Rynku Cyfrowego dla Europy, COM(2015)192 final z 6 maja 2015 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex%3A52015DC0192). Wprowadzenie Jednolitego Rynku Cyfrowego w założeniu ma pomóc europejskim przedsiębiorstwom rozwijać działalność w skali globalnej, co zapewni Europie utrzymanie pozycji światowego lidera gospodarki cyfrowej. Likwidacja barier związanych z tworzeniem Jednolitego Rynku Cyfrowego jest przedmiotem zainteresowania również polskiego rządu. Zadania obejmujące analizę i ocenę bariera, a także opracowywanie kierunków rozwoju gospodarki elektronicznej, spójnej z zasadami Jednolitego Rynku Cyfrowego oraz projektowanie odpowiednich instytucji prawnych powierzono pełnomocnikowi Rządu do spraw Jednolitego Rynku Cyfrowego (Rozporządzenie Rady Ministrów z 14 marca 2017 r.

RODO zastąpiło dotychczas obowiązującą dyrektywę 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, która została uchylona na podstawie art. 94 ust. 1 i 2 rozporządzenia ze skutkiem od dnia 25 maja 2018 r. Uchylenie dyrektywy 95/46/WE i zastąpienie jej rozporządzeniem RODO wskazywać może na determinację ze strony prawodawcy unijnego, który nie poprzestał na uporządkowaniu i odświeżeniu zasad ochrony danych osobowych w państwach UE, ale zdecydował się przejąć rolę kreatora oraz koordynatora i kontrolera tej płaszczyzny działalności państw członkowskich, która wiąże się ze stanowieniem i stosowaniem prawa w zakresie ochrony danych osobowych.

2. Zakres i charakter zmian w systemie ochrony danych osobowych w UE

Zmiana charakteru aktu regulacyjnego polegająca na zastąpieniu dyrektywy rozporządzeniem oznacza objęcie sfery związanej z przetwarzaniem danych osobowych kompetencją ustawodawczą organów UE. Jeśli zatem ingerencja prawodawcy unijnego w ten zakres działalności państwa była ograniczona ze względu na rodzaj aktu prawnego o charakterze nieustawodawczym, jakim była dyrektywa, o tyle zastąpienie jej rozporządzeniem spowodowało, że przepisy rozporządzenia nie mogą być ani implementowane do prawa krajowego, ani nawet interpretowane przez ustawodawcę krajowego, a ewentualne doprecyzowanie lub zawężenie poszczególnych przepisów RODO przez prawodawcę krajowego możliwe jest wyłącznie w sytuacjach wskazanych w rozporządzeniu (motyw 8 RODO)[9]. Zgodnie z treścią art. 288 Traktatu o funkcjonowaniu UE[10]dyrektywa wiązała wyłącznie te państwa członkowskie, do których była adresowana, i jedynie w ograniczonym zakresie, tj. w odniesieniu do rezultatu, który ma być osiągnięty, pozostawiając organom krajowym swobodę wyboru formy i środków. Rozporządzenie ma tymczasem zasięg ogólny, wiąże w całości wszystkie państwa członkowskie i jest bezpośrednio

w sprawie ustanowienia Pełnomocnika Rządu do spraw Jednolitego Rynku Cyfrowego, Dz. U. z 2017 r., poz. 563).

[9] E. Bielak-Jomaa, *Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych*?, MOP 2017, nr 20, s. 3.

[10] Traktat o funkcjonowaniu Unii Europejskiej z 26 października 2012 r. (Dz. Urz.UE.C 2012 nr 326, s. 47)

stosowane w nich[11].Wraz z wejściem w życie RODO rola krajowego ustawodawcy została ograniczona i polega zasadniczo na udzieleniu gwarancji i staniu na straży dochowania postanowień zawartych w RODO[12]. Bezpośrednie stosowanie rozporządzenia wspólnotowego oznacza bowiem, że jego wejście w życie i stosowanie na korzyść lub przeciwko jego adresatom jest niezależne od jakichkolwiek środków adaptujących. Jest prawdą, że w przypadku trudności interpretacyjnych administracja państwowa może być zmuszona do przyjęcia szczegółowych przepisów dla stosowania wspólnotowego rozporządzenia, tak by jednocześnie wyjaśnić wszelkie podniesione wątpliwości, jednak może to czynić tak dalece, jak pozostaje to w zgodzie z przepisami prawa wspólnotowego, a organy krajowe nie mogą podejmować wiążących reguł w zakresie interpretacji[13].

Prawodawca unijny w sposób kategoryczny stanął zarazem na stanowisku, że państwa członkowskie UE nie mogą w wystarczającym stopniu samodzielnie osiągnąć celu realizacji RODO polegającego na zapewnieniu równoważnego stopnia

[11] Istotą rozporządzeń unijnych jest ich bezpośredni skutek, z czego wynika, że to normy zawarte w rozporządzeniu są podstawą prawną załatwiania sprawy zawisłej przed organem państwa członkowskiego, a nie przepis prawa wewnętrznego państwa członkowskiego (P. Litwiński, J. Barta, J. Kawecki, *Komentarz do art. 99 RODO*, [w:]*Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018). Bezpośredni skutek przepisu prawa unijnego oznacza, że jednostka odwołująca się do konkretnego przepisu zawartego w RODO ma prawo do powołania się na jego normę przed sądem państwa członkowskiego zarówno w stosunkach prywatnoprawnych, jak i w stosunkach z organami władzy publicznej (wyrok TSUE z 27 września 2001 r. w sprawie *Queen/Secretary of the State*, C-63/99, ECLI:EU:C:2001:488; wyrok TSUE z 27 września 2001 r. w sprawie Barkoci i Malik, C-257/99, ECLI:EU:C:2001:491).

[12] Generalny Inspektor Ochrony Danych Osobowych, opiniując projekty krajowych aktów prawnych, przygotowujących system prawny do wdrożenia reformy danych osobowych, stanowczo zwrócił uwagę, że w przedstawionych projektach przepisów powinny znaleźć się „wyłącznie regulacje, które mają na celu przygotowanie krajowego porządku prawnego do stosowania rozporządzenia 2016/679 oraz nowej ustawy o ochronie danych osobowych", a w konsekwencji niedopuszczalne jest projektowanie takich rozwiązań, które odbiegają od zawartych w RODO (uwagi GIODO do projektu ustawy – Przepisy wprowadzające ustawę o ochronie danych osobowych stanowiące załącznik nr 1 oraz GIODO do projektu ustawy o ochronie danych osobowych stanowiące załącznik nr 2 do Pisma GIODO do Minister Cyfryzacji z 20 października 2017 r., http://giodo.gov.pl/pl/1520280/10202). Zarazem potrzeba uchylenia bądź zmiany przepisów krajowych dotyczących ochrony danych osobowych i związanej z tym konieczności dokonania kompleksowej rewizji aktów prawnych według Rządowego Centrum Legislacji analizy dotyczy ok. 800 aktów prawnych (E. Bielak-Jomaa, D. Lubasz, *Polska i europejska reforma ochrony danych osobowych,* red. E. Bielak-Jomaa, Warszawa 2016, Legalis).

[13] Wyrok TS UE z 31 stycznia 1978 r., C-94/77, *Fratelli Zerbone Snc* przeciwko *Administrazione delle finanze dello Stato,* ECLI:EU:C:1978:17, cyt.za: K. Morawska, *Rola oraz status*….

ochrony osobom fizycznym i swobodnego przepływu danych osobowych w całej Unii, co uprawnia organy UE do korzystania ze środków właściwych dla stosowania zasady pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej (TUE) (motyw 170). Ponadto Komisji Europejskiej powierzone zostały uprawnienia wykonawcze (motyw 167), organ ten został też wyposażony w kompetencje wynikające z art. 290 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE), tj. uprawnienia do przyjmowania aktów o zasięgu ogólnym, które uzupełniają lub zmieniają niektóre, inne niż istotne, elementy aktu ustawodawczego (motyw 166).

Okoliczność wskazująca, że unijny prawodawca nie ograniczył się do korekty istniejących rozwiązań w zakresie ochrony danych osobowych, które były zawarte w dyrektywie 95/46/WE[14], ale zdecydował się na jej uchylenie i zastąpienie rozporządzeniem (RODO), a także mając na uwadze poszerzenie zakresu uprawnień przyznanych w RODO Komisji Europejskiej w tym o charakterze wykonawczym, jak i stanowiącym, oznacza, że w sferze ochrony danych osobowych nastąpiła fundamentalna zmiana. Ujawnia się ona nie tylko poprzez zastosowane w RODO rozwiązania, instytucje i narzędzia, ale przede wszystkim ze względu na przyjętą nową filozofię ochrony danych osobowych oraz ustalenie na nowo jej celów. Zmiany te muszą zarazem oddziaływać na sposób definiowania takich pojęć, jak „ochrona danych", „prawo do ochrony danych osobowych". Pojęciem centralnym staje się bowiem nie tylko termin „dane osobowe", ale pojęcie „dane" obejmujące te dane, które zostały pozbawione cechy pozwalającej na dokonywanie identyfikacji osoby, której one dotyczą. Przetworzenie danych osobowych w taki sposób, by nie można ich było powiązać z konkretną osobą, której dane dotyczą, bez użycia dodatkowych informacji[15], został określony jako pseudonimizacja (art. 4 pkt 5 RODO).

Nie pozostaje bez znaczenia, że RODO jest jednym z kilku aktów prawnych należących do pakietu dokumentów reformujących zasady ochrony danych osobowych w ramach Jednolitego Rynku Cyfrowego w UE. Obok RODO do pakietu tego należy dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości,

[14] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 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, s. 31).

[15] Pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (art. 4 pkt 5 RODO).

prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych[16].Innym, znajdującym się na etapie konsultacji dokumentem jest rozporządzenie w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej[17] uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej)[18], a także – znajdujące się na etapie konsultacji – rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej[19].

Rozporządzenie o e-Prywatności, jak wskazano w jego treści, stanowi *lex specialis* względem RODO, uszczegóławia je i uzupełnia w kwestii danych pochodzących z łączności elektronicznej, które można zakwalifikować jako dane osobowe. Oznacza to w konsekwencji, że zakresem RODO objęte są tylko te sprawy dotyczące przetwarzania danych osobowych, do których nie odwołano się bezpośrednio w rozporządzeniu o e-Prywatności[20]. Decyzja o przyjęciu rozporządzenia w miejsce dyrektywy jest uzasadniona celem, jaki stanowi zapewnienie spójności z RODO, oraz potrzebą zagwarantowania pewności prawa dla użytkowników i przedsiębiorstw oraz uniknięcie rozbieżnych interpretacji w państwach członkowskich[21]. Jak zauważa X. Konarski, rozporządzenie o e-Prywatności stanowi wdrożenie do prawa wtórnego UE prawa podstawowego[22], przewidzianego

[16] Dyrektywa uchyla decyzję ramową Rady 2008/977/WSiSW. Rozporządzenie zastąpi obowiązującą obecnie Dyrektywę 95/46/WE.

[17] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylające dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final z 10 stycznia 2017r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52017PC0010 – dalej jako projekt rozporządzenia o e-Prywatności.

[18] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz. U.L 201 z 31.7.2002, s. 37).

[19] COM(2017) 495 final z 13 września 2017 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017PC0495 – dalej jako projekt rozporządzenia o danych nieosobowych.

[20] Pkt 1.2. projektu rozporządzenia o e-Prywatności.

[21] Ibidem, pkt 2.4.

[22] Za zmianę o największym zasięgu, jaką przynosi rozporządzenie o e-Prywatności, X. Konarski uznaje objęcie jego zakresem szerokiej gamy usług łączności interpersonalnej (korzystanie z urządzeń mobilnych), dotychczas nieregulowanej przepisami dyrektywy 2002/58, jak również komunikacji maszyna – maszyna (Internet Rzeczy), związanej z przetwarzaniem danych o użytkownikach różnego rodzaju inteligentnych urządzeń (zob. X. Konarski, *Rozporządzenie o e-Prywatności jako regulacja sektorowa względem ogólnego rozporządzenia o ochronie danych osobowych (RODO)* (dodatek MoP 2017, nr 20), MP 2017, nr 20, s. 6).

w art. 7 Karty praw podstawowych[23]. Swoim zakresem obejmuje ono zarówno dane pochodzące z łączności elektronicznej, tj. treść komunikatów przesyłanych przez użytkowników końcowych (*content dat*a)[24] oraz związane z nim metadane (*metadata*)[25], jak i informacje przechowywane i dotyczące urządzeń końcowych użytkowników (*data emitted by terminal equipement*)[26].

Do pakietu nowych rozwiązań należy także, pozostające obecnie, podobnie jak rozporządzenie o e-Prywatności na etapie projektu, rozporządzenie w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej[27]. Celem zawartych w tym dokumencie rozwiązań jest zapewnienie na terytorium Unii swobodnego przepływu danych[28] innych niż dane osobowe poprzez ustanowienie przepisów w zakresie wymogów dotyczących lokalizacji danych, dostępno-

[23] Zgodnie z treścią art. 7 KPP „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się" (Karta praw podstawowych Unii Europejskiej z 30 marca 2010 r., Dz. Urz.UE.C 2010 nr 83, s. 389).

[24] Zgodnie z definicją z art. 4 ust. 3b projektu rozporządzenia o e-Prywatności – „treść łączności elektronicznej – oznacza treści przekazywane z wykorzystaniem usług łączności elektronicznej, takie jak tekst, głos, wideo, obrazy i dźwięk".

[25] Zgodnie z definicją z art. 4 ust. 3c projektu rozporządzenia o e-Prywatności, „metadane pochodzące z łączności elektronicznej" oznaczają dane przetwarzane w sieci łączności elektronicznej do celów przesyłania, dystrybuowania lub wymiany treści łączności elektronicznej; w tym dane służące do śledzenia i zidentyfikowania źródła i miejsca docelowego przypadku łączności, dane dotyczące lokalizacji urządzenia wygenerowane w związku ze świadczeniem usług łączności elektronicznej oraz daty, godziny, czasu trwania oraz rodzaju łączności".

[26] Termin ten obejmuje informacje przechowywane w urządzeniu końcowym użytkownika końcowego i dotyczą urządzenia końcowego użytkownika końcowego (art. 8 projektu rozporządzenia o e-Prywatności).

[27] Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, COM(2017) 495 final z 13 września 2017 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017PC0495 – dalej jako projekt rozporządzenia o danych nieosobowych.

[28] W projekcie podkreślono, że jest on spójny z obowiązującymi instrumentami prawnymi, a w szczególności z dyrektywą o handlu elektronicznym (Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 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. U..L 178 z 17.7.2000, s. 1), której celem jest stworzenie kompleksowego i skutecznie funkcjonującego jednolitego rynku unijnego dla szerszej kategorii usług społeczeństwa informacyjnego, oraz z dyrektywą usługową (Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym (Dz. U.L 376 z 27.12.2006, s. 36), która przyczynia się do pogłębienia jednolitego rynku usług w UE w pewnych sektorach (Rozporządzenie Parlamentu Europejskiego i Rady w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, COM (2017) 495 final z 13 września 2017 r., http://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52017PC0495).

ści danych dla właściwych organów i przenoszenia danych przez użytkowników profesjonalnych (art. 1 projektu rozporządzenia o danych nieosobowych). Przez użytkowników profesjonalnych rozumie się osobę fizyczną lub prawną, w tym podmiot sektora publicznego, korzystającą lub pragnącą skorzystać z usługi przechowywania lub innego rodzaju przetwarzania danych do celów związanych z jej działalnością handlową, gospodarczą, rzemieślniczą, zawodową lub wykonywanym zadaniem (art. 3 ust. 8 projektu rozporządzenia o danych nieosobowych). O ile projektodawca zastrzega, że rozporządzenie o danych nieosobowych dotyczy elektronicznych danych innych niż dane osobowe – i wobec tego nie ma ono wpływu na unijne ramy prawne w zakresie ochrony danych osobowych zawarte w RODO – to jednak należy zwrócić uwagę, że zastrzeżenie to, w myśl art. 13 ust. 1 projektu, obejmuje wyłącznie dane osobowe w wąskim rozumieniu tego pojęcia zawartym w art. 4 pkt 1 RODO[29].

Jeśli bowiem przyjąć, że zawarte w projekcie rozporządzenia o danych nieosobowych rozwiązania nie będą znajdowały zastosowania do tych danych, które pozwalają na zidentyfikowanie osoby, której dane te dotyczą, to uwzględnione w nim regulacje obejmować będą w dalszym ciągu te dane, które powstały w wyniku procesu pseudonimizacji. W efekcie oznacza to, że wskazane w projekcie rozporządzenia o danych nieosobowych rozstrzygnięcie nie uchyla w całości stosowania zawartych w nim przepisów w odniesieniu do tych danych, które utraciły osobowy charakter i stały się przedmiotem obrotu prawnego. W literaturze zauważono, że „cechą informacji stanowiącej dane osobowe jest możliwość połączenia tej informacji (przypisania jej) do konkretnej osoby fizycznej, której te dane dotyczą. Jeżeli informacja pozbawiona zostaje cechy identyfikowalności, wówczas nie może zostać

[29] Pojęcie „danych osobowych" zostało zdefiniowane w art. 4 pkt 1 RODO jako „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". Zaproponowana definicja rozstrzyga istniejące na gruncie systemów prawnych państw członkowskich UE rozbieżności co do zakresu pojęcia „dane osobowe" oraz wątpliwości interpretacyjne dotyczące sposobu ustalania znaczenia wyrażenia „osoby możliwej do zidentyfikowania" a nadto ustalenia przesłanek wskazujących na „możliwość" identyfikacji osoby, której dane osobowe dotyczą. Unijny prawodawca pozostawił otwarty katalog przesłanek pozwalających na stwierdzenie, że identyfikacja danej osoby jest możliwa, co w konsekwencji oznacza, że zaproponowana definicja ma charakter otwarty i pozwala na szeroką wykładnię terminu „dane osobowe".

uznana za informację stanowiącą dane osobowe. W tym kontekście informacja spseudonimizowana stanowi swoiste stadium pośrednie pomiędzy informacjami anonimowymi a danymi osobowymi: informacja poddana pseudonimizacji nie może być bowiem przypisana konkretnej osobie fizycznej bez dodatkowych informacji, które jednakże są przechowywane oddzielnie"[30].

3. Charakter prawa do (ochrony) danych osobowych w nowych rozwiązaniach prawnych UE

Prawo do ochrony danych osobowych jest w doktrynie i orzecznictwie postrzegane jako prawo o charakterze osobistym, będące emanacją prawa do prywatności i służące ochronie dobra niematerialnego, które nie podlega zrzeczeniu się lub zbyciu[31]. Na tle postanowień zawartych w RODO, a także rozwiązań projektowanych w rozporządzeniu o e-Prywatności oraz rozporządzeniu o danych nieosobowych zauważalna staje się potrzeba zapewnienia danym osobowym jako dobru prawnemu o szczególnie istotnej dla jednostek wartości dwojakiego rodzaju ochrony, tj. takiej, która będzie uwzględniała zarówno majątkowy, jak i niemajątkowych charakter praw przysługujących podmiotom tych danych. W literaturze zwrócono uwagę, że podstawowe konstrukcje ustaw mających na celu wprowadzenie powszechnej, kompleksowej regulacji odnoszącej się do ochrony danych osobowych oscylują między dwoma modelami. Pierwszy z nich, określany mianem modelu licencyjnego, uzależnia korzystanie z danych osobowych od udzielenia zgody organu państwowego. Fundamentem drugiego modelu jest przyjęcie istnienia swego rodzaju podmiotowego prawa do dysponowania danymi o własnej osobie[32]. W systemie ochrony danych osobowych przyjętym w UE zastosowanie znajduje drugie ze wskazanych rozwiązań. Zważywszy, że dane osobowe, a w szczególności te z nich, które zostały poddane procesowi pseudonimizacji, uzyskały autonomiczny status dóbr, a zarazem mają sprawdzalną i poddającą się

[30] Komentarz do art. 4 RODO, [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018.

[31] W piśmiennictwie wskazuje się, ze ochrona danych osobowych stanowi jeden z podstawowych aspektów prawa do prywatności (zob. M. Krzysztofek, *Ochrona danych osobowych w Unii Europejskiej*, Warszawa 2014, s. 36 i n.) Na takie ujęcie ochrony danych osobowych w regulacjach krajowych i międzynarodowych zwracają także uwagę J. Barta i R. Markiewicz, ciż, *Ochrona danych osobowych. Komentarz*, Kraków 2007, s. 116.

[32] J. Barta, R. Markiewicz, *Ochrona danych osobowych*, s. 54.

weryfikacji wartość majątkową, konieczne stało się poszukiwanie odmiennych instrumentów ochrony od tych, jakie były dotychczas stosowane w odniesieniu do ochrony prywatności.

W obliczu kształtowania się Jednolitego Rynku Cyfrowego, którego warunkiem istnienia i rozwoju jest dostęp do danych osobowych i możliwość ich komercyjnego wykorzystania, za nieodpowiadające potrzebom zapewnienia równowagi praw uczestnikom obrotu gospodarczego uznać należy pominięcie majątkowego aspektu ochrony tego prawa w odniesieniu do osób, których dane te dotyczą. Jeśli bowiem dane osobowe oraz dane powstałe w wyniku procesu pseudonimizacji mają wartość majątkową, co z uwagi na priorytety polityki europejskiej obejmujące rozwój gospodarki opartej na danych wydaje się okolicznością bezsporną, to w konsekwencji uznać trzeba, że katalog środków ochrony przysługujących osobom, których dane te dotyczą, powinien być adekwatny do rodzaju i charakteru dobra prawnie chronionego.

Uprawnione wydaje się bowiem spostrzeżenie, że przedmiotem obrotu pomiędzy uczestnikami jednolitego rynku cyfrowego stały się zarówno „dane osobowe" oraz „zbiory danych osobowych", jak i same „dane"[33]. Zarazem jednak gros „danych" stanowią dane powstałe w wyniku procesu pseudonimizacji. Jeśli zatem zakres pojęcia „dane osobowe" zasadniczo nie ulega zmianie, o tyle modyfikacji podlega katalog uprawnień składających się na prawo podmiotowe do danych osobowych. Katalog ten powinien zarazem odpowiadać na potrzeby związane z realizacją praw i wolności człowieka gwarantowane w art. 7 i art. 8 KPP oraz w art. 16 TFUE.

Nie pozostaje bez znaczenia, że prawo do ochrony danych osobowych prawodawca kwalifikuje jako prawo człowieka i sytuuje je w tym samym tytule KPP, w którym przyznaje ochronę takim wartościom, jak życie prywatne (art. 7), wolność myśli, sumienia i religii (art. 9), wolność wypowiedzi i informacji (art. 11), wolność zgromadzania się (art. 12), wolność sztuki i nauki (art. 13),prawo własności (art. 17). Prawo do ochrony danych osobowych znajduje ochronę w art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej[34] oraz art. 16 ust. 1 Traktatu

[33] Pojęcie danych jest definiowane w sposób negatywny. Obejmuje ono bowiem „dane inne niż dane osobowe, o których mowa w art. 4 pkt 1 rozporządzenia (UE) 2016/679" (art. 3 ust. 1 projektu rozporządzenia o danych nieosobowych).

[34] Karta praw podstawowych Unii Europejskiej z 30 marca 2010 r. (Dz. Urz.UE.C 2010 nr 83, s. 389 – dalej jako KPP).

o funkcjonowaniu Unii Europejskiej[35]. Jeśli zarazem przyjąć, że zawarte w KPP oraz TFUE postanowienia mają charakter blankietowy, a konkretyzacja zasad ochrony danych osobowych następuje w szczególności w RODO, to stwierdzić należy, że unijny prawodawca całkowicie pominął majątkowy aspekt ochrony danych osobowych oraz zignorował charakter danych osobowych jako dóbr, które ze względu na swój niematerialny status oraz przynależność do praw osobistych nie tracą bynajmniej wartości majątkowej. Konieczne staje się więc spostrzeżenie, że udzielenie zgody przez osobę, której dane dotyczą, innemu podmiotowi, w tym w szczególności przedsiębiorcy na wykorzystanie jej danych osobowych wywołuje skutek porównywalny z czynnością przysporzenia (darowizny) udzielonego na rzecz osoby trzeciej. Udzielenie zgody na wykorzystanie danych osobowych w szczególności w celach marketingowych oznacza *de facto* zezwolenie na wprowadzenie danych do obrotu gospodarczego. Wtórny w stosunku do udzielenia zgody, która legalizuje obrót danymi osobowymi jednostki, jest proces pseudonimizacji danych oraz profilowania.

4. Majątkowe aspekty prawa do ochrony danych osobowych

Przyznaniu jednostce praw o charakterze negatywnych, a w szczególności prawa do zgłoszenia sprzeciwu wobec przetwarzania jej danych osobowych (art. 21 RODO), ich sprostowania (art. 16 RODO), prawa do usunięcia danych (prawo do bycia zapomnianym – art. 17 RODO), prawa do ograniczenia przetwarzania (art. 18 RODO) towarzyszyć powinno wyposażenie jednostki w uprawnienia o charakterze pozytywnym oraz powiązanie ich zakresu i sposobu realizacji z majątkowym charakterem dobra prawnie chronionego, jakim są dane osobowe. RODO, pomimo że przyznaje podmiotom danych osobowych uprawnienia o charakterze pozytywnym, jak w szczególności prawo do przenoszenia danych osobowych (art. 20 RODO), a także zaostrza wymogi dotyczące uzyskania przez administratorów danych zgody na ich przetwarzanie (art. 7 RODO), to jednak nie łączy jego wykonywania z uzyskiwaniem z tego tytułu wynagrodzenia przez osobę, której dane osobowe dotyczą. Z jednej strony zatem, co często podkreśla się w piśmiennictwie, prawodawca unijny, reformując zasady ochrony danych osobowych,

[35] Traktat o funkcjonowaniu Unii Europejskiej z 26 października 2012 r. (Dz. Urz.UE.C 2012 nr 326, s. 47 – dalej jako TFUE).

zamierzał przywrócić jednostce możliwość sprawowania faktycznej kontroli nad jej danymi[36], a z drugiej – prawodawca założył, że zasadniczym i jedynym motywem korzystania przez jednostkę z przyznanych jej w RODO uprawnień pozostanie potrzeba ochrony jej praw osobistych.

W myśl art. 20 ust. 1 RODO osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe. Administrator danych, do którego skierowano żądanie przeniesienia danych osobowych, powinien je spełnić bez zbędnej zwłoki, nie później jednak niż w terminie miesiąca od otrzymania żądania[37].

Administrator nie może sprzeciwić się podjętej przez jednostkę czynności zmierzającej do przeniesienia danych w szczególności wówczas, gdy uprzednio osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (art. 6 ust. 1 lit. a RODO), a także wówczas, gdy jej dane były wykorzystywane w związku z wykonania umowy, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. b RODO). Prawo do otrzymania, a następnie przeniesienia danych na rzecz innego administratora obejmuje nie tylko dane bezpośrednio oraz świadomie i celowo przekazane, ale i te, które powstały w wyniku automatycznego przetwarzania. Wskazówkę interpretacyjną zakresu uprawnienia wskazanego w art. 20 RODO przynosi treść motywu 68 preambuły. Prawodawca unijny wskazuje w nim, że aby zyskać większą kontrolę nad swoimi danymi w ramach zautomatyzowanego przetwarzania danych osobowych, osoba, której dane dotyczą, powinna mieć również możliwość otrzymywania dotyczących jej danych osobowych, które dostarczyła administratorowi, w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego i interpretacyjnym formacie oraz przesyłania ich innemu administratorowi. Administratorów danych należy zachęcać do opracowywania interoperacyjnych forma-

[36] K. Morawska, *Rola oraz status…*

[37] Miesięczny okres na przekazanie danych wnioskodawcy można przedłużyć do maksymalnie trzech miesięcy w przypadku skomplikowanych spraw, pod warunkiem, że poinformuje się osobę, której dane dotyczą, o przyczynach takiego opóźnienia w terminie miesiąca od otrzymania pierwotnego żądania. Zob. P. Litwiński, *Komentarz do art. 20 RPDO*, [w:] *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018.

tów umożliwiających przenoszenie danych. Prawo to powinno mieć zastosowanie w przypadkach, gdy osoba, której dane dotyczą, dostarczyła danych osobowych za własną zgodą lub gdy przetwarzanie jest niezbędne do wykonania umowy (motyw 68 RODO).

Wyłączenie stosowania uprawnień z art. 20 dotyczy przetwarzania, które opiera się na innej podstawie prawnej niż zgoda lub umowa. Prawa tego –z uwagi na jego charakter – nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych. Dlatego nie powinno ono mieć zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych technicznie systemów przetwarzania. Jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą, na podstawie niniejszego rozporządzenia. Prawo to powinno ponadto pozostawać bez uszczerbku dla prawa osoby, której dane dotyczą, do spowodowania, by dane osobowe zostały usunięte, oraz bez uszczerbku dla ograniczeń tego prawa określonych w niniejszym rozporządzeniu i nie powinno w szczególności skutkować usunięciem danych osobowych dotyczących osoby, której dane dotyczą, których osoba ta dostarczyła do wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy. O ile jest to technicznie możliwe, osoba, której dane dotyczą, powinna mieć prawo do spowodowania, by dane osobowe zostały przesłane przez jednego administratora bezpośrednio innemu administratorowi (motyw 68 RODO).

Zwraca uwagę, że ani treść przepisów normatywnych zawartych w RODO, w tym w szczególności, ani art. 20, ani odnoszący się do niego przepis interpretacyjny zawarty w motywie 68 preambuły nie wyłączają dopuszczalności zawarcia przez podmiot danych odrębnej umowy z administratorem na korzystanie z ustrukturyzowanych dotyczących jej danych osobowych, które może ona swobodnie przenosić między administratorami. Zawarciu takiej umowy nie sprzeciwiają się także przepisy warunkujące przetwarzanie danych od udzielenia zgody przez osobę, której dane osobowe dotyczą. O ile zatem w art. 6 RODO doprecyzowane zostały

warunki, jakim musi odpowiadać oświadczenie podmiotu danych udzielającego zezwolenia[38], to jednak prawodawca – jak się wydaje – dopuszcza, by podjęta przez jednostkę czynność udzielenie zezwolenia na przetwarzanie danych osobowych jej dotyczących miała charakter odpłatny i następowała na podstawie umowy wzajemnej, która łączy jednostkę z administratorem danych.

Odrębną kwestią jest ocena, czy realizacja powyżej wskazanego uprawnienia jednostki do przenoszenia danych osobowych w drodze zawarcia odpłatnej umowy na przeniesienie praw do danych osobowych, które jej dotyczą, choć od strony formalnej wydaje się dopuszczalna (brak zabronienia), jest do pogodzenia z celami RODO, a w szczególności wskazanym w preambule celem, jakim jest rozwój jednolitego rynku cyfrowego oraz gospodarki opartej na danych.

5. Majątkowy charakter prawa do ochrony danych osobowych a realizacja celów RODO

Cel RODO stanowi nie tylko wzmocnienie ochrony prywatności, na co zazwyczaj wskazuje się w literaturze[39], ale przede wszystkim utorowanie drogi tym przedsięwzięciom gospodarczym, których przedmiotem, a zarazem źródłem

[38] Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma np. formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy (motyw 32 RODO).

[39] W literaturze podkreśla się bowiem zazwyczaj, że RODO „ma jednak za zadanie wyeliminować wynikające z wdrażania dyrektywy i występujące w związku z tym różnice w stopniu ochrony praw oraz ma uniknąć fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w Internecie". Zob. K. Morawska, *Rola oraz status prawny motywów preambuły ogólnego rozporządzenia o ochronie danych – klucz do wykładni przepisów nowego prawa unijnego*, [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, Legalis.