INSTYTUT NAUK PRAWNYCH
POLSKA AKADEMIA NAUK

Dominik Sybilski

Wpływ ogólnego rozporządzenia o ochronie danych na realizację prawa do ponownego wykorzystywania informacji sektora publicznego

Rozprawa doktorska przygotowana pod opieką
dra hab. Grzegorza Sibigi, prof. INP PAN

Warszawa 2021

Spis treści

Wykaz skrótów

EKPC – Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 4 listopada 1950 r.

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. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.)

dyrektywa 2003/98/WE – dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003, str. 90)

dyrektywa 2013/37/UE – dyrektywa 2013/37/UE Parlamentu Europejskiego i Rady z dnia 26 czerwca 2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 175/1)

dyrektywa 2019/1024 – dyrektywa 2019/1024 Parlamentu Europejskiego i Rady z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 172/56)

Dz. U. – Dziennik Ustaw w rozumieniu ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461)

KC – ustawa z dnia 17 listopada 1964 r. – Kodeks postępowania cywilnego (t.j. Dz. U. z 2020 r. poz. 1575, 1578, 2320, z 2021 r. poz. 11)

KE/Komisja – Komisja Europejska

KK – ustawa z dnia 6 czerwca 1997 r. - Kodeks karny (t.j. Dz. U. z 2020 r. poz. 1444, 1517)

Konstytucja RP – Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz. U. z 1997 r. Nr 78, poz. 483, z 2001 r. Nr 28, poz. 319, z 2006 r. Nr 200, poz. 1471, z 2009 r., Nr 114, poz. 946)

KPA – ustawa z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695, 1298, 2320, z 2021 r. poz. 54, 187)

KPPUE – Karta praw podstawowych Unii Europejskiej (Dz. Urz. UE C 83 z 30.03.2010 s. 2)

M.P. – Dziennik Urzędowy Rzeczypospolitej Polskiej "Monitor Polski" w rozumieniu ustawy z dnia 20 lipca 2000 r. o ogłaszaniu aktów normatywnych i niektórych innych aktów prawnych (Dz. U. z 2019 r. poz. 1461).

NSA – Naczelny Sąd Administracyjny

RODO/ogólne rozporządzenie – 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 119 z 04.05.2016, str. 1)

rozporządzenie 1049/2001 - rozporządzeniu (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (Dz. Urz. UE L 145/43 z 31.05.2001)

TFUE – Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana) (Dz. Urz. UE C 83 z 30.03.2010 s. 1)

TK – Trybunał Konstytucyjny

TSUE – Trybunał Sprawiedliwości Unii Europejskiej

TUE – Traktat o Unii Europejskiej (wersja skonsolidowana) (Dz. Urz. UE C 83 z 30.03.2010 s. 1)

UE – Unia Europejska

UDIP – ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2020 r. poz. 2176.)

UPW – ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (t.j. Dz. U. z 2019 r. poz. 1446)

UODO1997 – ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922, z 2018 r. poz. 138, 723)

UODO2018 – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r. poz. 1781)

UWprowRODO - Ustawa z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679

z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. z 2019 r., poz. 730)

WSA – Wojewódzki Sąd Administracyjny

ZTP – Zasady techniki prawodawczej stanowiące załącznik do rozporządzenia Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (t.j. Dz. U. z 2016 r., poz. 283).

Wprowadzenie

Podmioty publiczne wytwarzają, gromadzą lub przetwarzają ogromne ilości informacji, od danych statystycznych, gospodarczych, medycznych, środowiskowych, poprzez materiały archiwalne, po zdigitalizowane zbiory dziedzictwa kulturowego. Na przestrzeni lat uległ zmianie paradygmat znaczenia informacji o charakterze publicznym, przestały być one postrzegane jedynie jako środek służący jawności i transparentności, umożliwiający kontrolę władzy publicznej przez obywateli. Wraz z rewolucją cyfrową informacje, czy szerzej dane są uznawane jako dobro wielokrotnego użytku, które stanowi cenny materiał wyjściowy dla tworzenia innowacyjnych produktów, usług czy aplikacji. Z tej perspektywy nie wystarcza sama dostępność informacji od lat gwarantowana w Polsce przepisami o dostępie do informacji publicznej[1] czy jak w ustawodawstwie innych państw dostępem do dokumentów urzędowych. Dla wykorzystania potencjału społecznego i gospodarczego danych konieczne było ustanowienie nowego uprawnienia informacyjnego umożliwiającego ponowne wykorzystywanie informacji sektora publicznego do dowolnych celów, tak gospodarczych jak i niekomercyjnych, przez każdego zainteresowanego użytkownika, np. obywatela, przedsiębiorcę czy organizację pozarządową.

Prawo do ponownego wykorzystywania informacji sektora publicznego jest prawem pochodnym Unii Europejskiej, którego podstawy i zakres wyznaczają od 2003 r. przepisy kolejnych dyrektyw o ponownym wykorzystywaniu informacji sektora publicznego. Na gruncie krajowym prawo to podlega samodzielnej regulacji przepisami ustawy z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego[2] wykonującej przepisy prawa UE.

Jednocześnie z powstaniem i rozwojem prawa do ponownego wykorzystywania szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno podmioty prywatne, jak i organy publiczne, mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności.

Dane osobowe mogą stanowić jednocześnie informację sektora publicznego, jak np. imię i nazwisko osoby pełniącej funkcję publiczną. Dane osobowe mogą być ujawnione w dokumentach urzędowych czy podlegać publikacji na stronach internetowych podmiotów

[1] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2020 r. poz. 2176), dalej: UDIP.
[2] Ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego (t.j. Dz. U. z 2019 r. poz. 1446); dalej: UPW.

publicznych, jak Biuletyn Informacji Publicznej czy portal dane.gov.pl. Mogą również być zawarte w publicznie dostępnych zbiorach czy rejestrach państwowych, takich np. jak Krajowy Rejestr Sądowy, Krajowy Rejestr Urzędowy Podmiotów Gospodarki Narodowej – REGON czy Centralna Ewidencja Pojazdów i Kierowców.

Ryzyko naruszenia ochrony danych osobowych podczas ponownego wykorzystywania potęguje dynamiczny wzrost gospodarki opartej o dane, który nie byłby możliwy bez przetwarzania dużych zbiorów danych (*big data*), przetwarzania danych w chmurze obliczeniowej (*cloud computing*) rozbudowy aplikacji na urządzenia mobilne czy rozwoju nowoczesnych zastosowań, jak sztuczna inteligencja (*artificial inteligence*) czy Internet rzeczy (*Internet of things*).

Ponowne wykorzystywanie informacji sektora publicznego może jednocześnie stanowić przetwarzanie danych osobowych w rozumieniu przepisów o ochronie danych osobowych, którego podstawowym źródłem prawa na terytorium Unii Europejskiej pozostaje obecnie ogólne rozporządzenie o ochronie danych[3].

Celem głównym rozprawy jest zbadanie wpływu, jakie wywiera prawo ochrony danych osobowych, opierające się na przepisach ogólnego rozporządzenia o ochronie danych, na realizację prawa do ponownego wykorzystywania informacji sektora publicznego. Podstawą prowadzonych rozważań jest teza, że prawo do ochrony danych osobowych stanowi istotną barierę dla ponownego wykorzystywania informacji sektora publicznego, zarazem jednak w sposób kategoryczny nie eliminuje możliwości dalszej eksploatacji informacji sektora publicznego zawierającej dane osobowe. Przeprowadzona analiza pozwoliła na zidentyfikowanie węzłowych zagadnień i jednocześnie kluczowych wyzwań dla stosujących przepisy będących konsekwencją wpływu ogólnego rozporządzenia na ponowne wykorzystywanie informacji sektora publicznego związanych z realizacją podstawowych zasad przetwarzania danych. Dla omawianej tematyki pierwszorzędne znaczenie ustalono dla zasady legalności, przejrzystości oraz celowości. W mojej opinii z wykonaniem tych zasad wiążą się najważniejsze wyzwania dla ponownego wykorzystywania danych osobowych, czyli wybór właściwej podstawy prawnej przetwarzania danych osobowych w ramach ponownego wykorzystywania, sposób realizacji zasady związania celem przetwarzania oraz wykonanie

[3] 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 119 z 04.05.2016, str. 1); dalej: RODO lub ogólne rozporządzenie.

obowiązków informacyjnych przez podmioty zobowiązane do ujawnienia danych w ramach informacji sektora publicznego, jak i użytkowników informacji.

Prawo do ponownego wykorzystywania informacji sektora publicznego oraz prawo do ochrony danych osobowych pozostają wobec siebie w określonej relacji. Pierwszoplanowym zagadnieniem badawczym była zatem konieczność ustalenia specyfiki tej relacji, zidentyfikowania wspólnych obszarów regulacji i konsekwencji krzyżowania się dwóch reżimów prawnych. Prawodawca europejski zawarł dyspozycję zaadresowaną do państw członkowskich pogodzenia prawa do ochrony danych osobowych z prawem do ponownego wykorzystywania informacji, nie dając jednocześnie żadnych wytycznych jak cel ten zrealizować. Jak zostanie wykazane w rozprawie, nie można mówić o pełnym wykonaniu tej dyspozycji w prawie krajowym. Kwestią fundamentalną dla stosujących przepisy UE i prawa krajowego pozostaje ustalenie, czy i w jakich okolicznościach może dojść do ujawnienia danych osobowych w ramach ponownego wykorzystywania informacji sektora publicznego oraz jakie wywoła to konsekwencje dla wszystkich zainteresowanych uprawnionych i zobowiązanych.

Zagadnieniem badawczym mającym kluczowe znaczenie dla przedmiotu rozprawy jest ustalenie właściwej podstawy prawnej przetwarzania danych osobowych w ramach ponownego wykorzystywania, gdy informacja sektora publicznego zawiera lub stanowi jednocześnie dane osobowe. Ponowne wykorzystywanie z definicji oznacza wykorzystywanie informacji do innych celów niż została ona pierwotnie wytworzona w ramach realizacji zadania publicznego. W tym aspekcie podstawowego znaczenia badawczego nabiera problematyka spełnienia zasady ograniczenia celu oraz kwestia zmiany celu przetwarzania związana z tą zasadą.

Kolejne zagadnienia badawcze obejmują konsekwencje ujawnienia danych osobowych w ramach informacji sektora publicznego zarówno z perspektywy osoby, której dane dotyczą, jak i podmiotu zobowiązanego i użytkownika informacji. Istotną kwestią prawną mającą jednocześnie doniosłe znaczenie dla praktyki pozostaje ustalenie warunków ponownego wykorzystywania informacji sektora publicznego zawierającej dane osobowe. Obok mechanizmu oceny skutków dla ochrony danych, warunki ponownego wykorzystywania danych osobowych, mogą odegrać kluczową rolę dla zapewnienia ochrony danych osobowych ujawnianych w ramach informacji sektora publicznego. Wreszcie – jak pokazuje praktyka stosowania przepisów RODO – wyzwaniem pozostaje skuteczna realizacja praw osób, których dane dotyczą w ramach ponownego wykorzystywania danych osobowych, w szczególności uprawnień informacyjnych podmiotu danych. Konieczne pozostaje rozstrzygnięcie sposobu spełnienia obowiązku informacyjnego przez administratora oraz odpowiedź na pytanie

dotyczące dopuszczalności zwolnienia ze spełnienia przedmiotowego obowiązku w ramach ponownego wykorzystywania.

Ponadto w pracy podjęto również kwestię realizacji innych praw i obowiązków wynikających z przepisów ogólnego rozporządzenia, które mogą mieć zastosowanie w ramach ponownego wykorzystywania informacji sektora publicznego. Swoje źródła mają w pozostałych podstawowych zasadach przetwarzania danych, takich jak ograniczenie przechowywania, minimalizacja danych, prawidłowość oraz integralność i poufność.

Problem wpływu ochrony danych osobowych na realizację prawa do ponownego wykorzystywania informacji sektora publicznego pozostaje niezwykle aktualny nie tylko ze względów społecznych, gospodarczych czy technologicznych, ale również prawno-legislacyjnych. W dniu 20 czerwca 2019 r. została przyjęta nowa dyrektywa 2019/1024[4], która powinna zostać transponowana do prawa krajowego do 17 lipca 2021 r. Obecnie trwają prace nad implementacją tego aktu, które zgodnie z zapowiedzią projektodawcy oznaczać będą uchwalenie nowej horyzontalnej ustawy zastępującej UPW w dotychczasowym brzmieniu. Nowa dyrektywa nie tylko poszerza zakres ponownego wykorzystywania o nowe podmioty i zasoby, ale uwzględnia kwestie ochrony danych osobowych. Znamiennym jest, że jest to pierwsza dyrektywa o ponownym wykorzystywaniu przyjęta po wejściu w życie przepisów ogólnego rozporządzenia. Nie bez znaczenia jest również rola dyrektywy na rynku wewnętrznym UE i zapowiedzianego jednolitego runku danych. Dyrektywa 2019/1024 i ogólne rozporządzenie o ochronie danych stanowią instrumenty prawa UE realizacji jednolitego rynku cyfrowego.

W ciągu ponad dwóch lata obowiązywania ogólnego rozporządzenia wydane zostały decyzje Prezesa Urzędu Ochrony Danych Osobowych, zapadły też rozstrzygnięcia sądów administracyjnych; nie mają one jednak pierwszoplanowego znaczenia dla podjętej w rozprawie głównej problematyki. Jednocześnie prawna ochrona danych osobowych, jak i ponowne wykorzystywanie informacji opierające się na przepisach dostępowych nie są zagadnieniem nowym, są przedmiotem ugruntowanego orzecznictwa i obszernej literatury wypracowanych na gruncie ustawy o ochronie danych osobowych z 1997 r.[5] i ustawy o dostępie do informacji publicznej. Dorobek ten został uwzględniony i umożliwił na wyprowadzenie wniosków w obowiązującym stanie prawnym.

[4] Dyrektywa 2019/1024 Parlamentu Europejskiego i Rady z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 172/56); dalej dyrektywa 2019/1024.

[5] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922, z 2018 r. poz. 138, 723); dalej: UODO1997.

Badania zostały przeprowadzone przy wykorzystaniu metody formalno-dogmatycznej. Dokonano analizy właściwych aktów normatywnych, którą uzupełniono o powołanie orzecznictwa oraz wypowiedzi przedstawicieli nauki prawa. Badanie przeprowadzono w oparciu o obowiązujący stan prawny wyznaczony przez ogólne rozporządzenie i przepisy o ponownym wykorzystywaniu informacji sektora publicznego. W tym drugim wypadku konieczne było oparcie rozważań nie tylko o przepisy krajowe, dla których podstawowym źródłem jest UPW, ale również przepisy wykonanej w UPW dyrektywy 2003/98/WE[6] w brzmieniu nadanym dyrektywą 2013/37/WE[7]. Prawo UE wymaga w tym obszarze regulacyjnym jedynie minimalnej harmonizacji przepisów i można zaobserwować różnice między aktem polskim a unijnym. Ponadto konieczne było również odwołanie się do postawień nowej dyrektywy 2019/1024 o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, która nie została jeszcze transponowana do krajowego porządku prawnego, ale zawiera nowe rozwiązania istotne dla podjętej w pracy tematyki.

Pomocniczo zastosowano również metodę prawnoporównawczą w zakresie porównania przyjętych w rozwiązań w ustawodawstwie wybranych państw UE oraz metodę historyczną w zakresie ewolucji instytucji i pojęć będących przedmiotem rozprawy.

Rozprawa doktorska składa się z wprowadzenia, dziesięciu rozdziałów wraz z podrozdziałami oraz wniosków końcowych. Ponadto zawiera wykaz skrótów oraz bibliografię.

Dla podjęcia zasadniczej problematyki konieczne było przedstawienie w pierwszych rozdziałach rozprawy zagadnień o charakterze ogólnym. W Rozdziale 1. została wyjaśniona istota ponownego wykorzystywania oraz jej znaczenie dla koncepcji otwartego rządu, polityki publicznej otwierania danych oraz miejsce tego prawa na jednolitym rynku cyfrowym UE. Zasadne również było rozróżnienie ponownego wykorzystywania informacji sektora publicznego od dostępu do informacji publicznej. Rozdział zamyka omówienie podstaw prawa UE i krajowego w obszarze ponownego wykorzystywania informacji sektora publicznego.

W Rozdziale 2. wyjaśniono genezę prawa ochrony danych osobowych oraz istotę i cele ogólnego rozporządzenia oraz wskazano podstawowe źródła prawa krajowego i europejskiego ochrony danych osobowych.

[6] Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 345 z 31.12.2003, str. 90); dalej: dyrektywa 2003/98/WE.

[7] Dyrektywa 2013/37/UE Parlamentu Europejskiego i Rady z dnia 26 czerwca 2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 175/1); dalej dyrektywa 2013/37/UE.

W Rozdziale 3. omówiono podmiotowy i przedmiotowy zakres prawa do ponownego wykorzystywania informacji sektora publicznego oraz ogólnego rozporządzenia, w tym wyjaśniono podstawowe pojęcia, wyznaczono również wspólny obszar obu regulacji.

Rozdział 4. i 5. poświęcony jest podstawowym zasadom i wynikającym z nich uprawnieniom odpowiednio ponownego wykorzystywania oraz przetwarzania danych osobowych. W pierwszym wypadku konieczne było również omówienie przepisów proceduralnych, które mają zastosowanie również dla udostępnienia lub przekazania danych osobowych do ponownego wykorzystywania.

Kolejne rozdziały poświęcone zostały kluczowym zagadnieniom dla zasadniczego przedmiotu rozprawy. W Rozdziale 6. przeprowadzono rekonstrukcję relacji pomiędzy prawem do ochrony danych osobowych oraz prawem do ponownego wykorzystywania informacji sektora publicznego w oparciu o art. 86 RODO i dopełniający go motyw 154 motyw preambuły, przepisy dyrektyw o ponownym wykorzystywaniu oraz przepisy krajowe. Kluczowe okazało się odwołanie do wypracowanej w doktrynie koncepcji współstosowania i komplementarności przepisów o ochronie danych osobowych oraz ponownego wykorzystywania informacji. Konieczna również była analiza prywatności jako przesłanki ograniczającej ponowne wykorzystywanie. W rozdziale tym podjęto również próbę oceny wykonania art. 86 RODO w prawie krajowym.

W Rozdziale 7. omówione zostały przesłanki legalizujące przetwarzanie danych osobowych, które mogą stanowić podstawę dla ponownego wykorzystywania danych. Pozostałe przesłanki wymienione w art. 6 RODO zostały omówione jedynie w niezbędnym zakresie dla zrozumienia ich istoty.

Rozdział 8. poświęcony jest zagadnieniu zmiany celu przetwarzania danych osobowych w związku z ich ponownym wykorzystywaniem. Zasadne było opisanie elementów składowych tzw. testu zgodności, ustalenie obowiązku jego przeprowadzania, wskazanie podmiotów obowiązanych oraz próba zidentyfikowania dopuszczalnych celów ponownego wykorzystywania.

W Rozdziale 9. połączono zagadnienia proceduralne związane z ujawnieniom danych osobowych w ramach informacji sektora publicznego. Ponadto omówiono kluczowe zagadnienia dla praktyki ochrony danych osobowych w związku z ich ponownym wykorzystywaniem, które w mojej opinii obejmują problem spełnienia wypełnienia obowiązku informacyjnego oraz ustalenie warunków ponownego wykorzystywania uwzględniających ochronę danych osobowych. Omówiono również znaczenie oceny skutków dla ochrony danych

w kontekście ponownego wykorzystywania. Rozdział zamyka omówienie zagadnienia anonimizacji.

W Rozdziale 10 omówiono wpływ innych uprawnień i obowiązków wynikających z ogólnego rozporządzenia na realizację prawa do ponownego wykorzystywania, które mają swoje źródła w zasadach ogólnych przetwarzania danych, takich jak ograniczenie przechowywania, minimalizacja danych, prawidłowość oraz integralność i poufność.

We wnioskach końcowych zawarto przegląd najważniejszych ustaleń, które zostały poczynione w wyniku prowadzonych badań związanych z wpływem ochrony danych osobowych na realizację prawa do ponownego wykorzystywania. Przedstawiono również uwagi *de lege lata* oraz *de lege ferenda*.

Rozprawa doktorska uwzględnia stan prawny na dzień 1 kwietnia 2021 r.

Rozdział 1. Istota, znaczenie i źródła prawa ponownego wykorzystywania informacji sektora publicznego

1.1. Od otwartego rządu do otwartych danych – koncepcje ponownego wykorzystywania informacji

Zapoczątkowana na przełomie XX i XXI wieku koncepcja tzw. otwartego rządu (*open government*) jest ściśle związana z postępującym rozwojem technologicznym, dostępnością cyfrowych narzędzi ułatwiających komunikację oraz usieciowieniem funkcjonowania jednostek i instytucji[8]. Model otwartego rządu opiera się na idei zwiększenia zaangażowania obywateli w procesy rządzenia poprzez zapewnienie im dostępu do informacji i zasobów publicznych, a także stworzenie procedur umożliwiających uczestnictwo w procesie podejmowania decyzji należących do sfery publiczno–prawnej. Partycypacja w procesie decyzyjnym obejmuje jawność działania władzy publicznej umożliwiająca poznanie przyczyn, motywacji lub materiałów wykorzystywanych w procesie stanowienia lub stosowania prawa, otwartość *sensu stricto* rozumiana jest z kolei w ten sposób, że rząd wysłuchuje obywateli i bierze ich stanowisko pod uwagę w trakcie projektowania polityk oraz odpowiedzialność władzy publicznej wobec suwerena za działania i zaniechania[9]. W literaturze przedmiotu zwraca się uwagę, że podstawowym elementem standardu otwartego rządu czy też otwartości organów władz publicznych i podlegających im struktur, pozostaje prawo dostępu do informacji publicznej. Podstawą otwartości jest jawność organizacji i działalności instytucji publicznych wobec wszystkich zainteresowanych członków społeczeństwa[10].

Obecnie przyjmuje się, że model otwartych rządów obejmuje obok „tradycyjnych" działań wzmacniających demokrację partycypacyjną (obok dostępu do informacji publicznej, można wskazać obywatelską inicjatywę ustawodawczą, referendum, konsultacje społeczne czy budżet partycypacyjny) nowe typy działań (takie jak dostęp do otwartych danych publicznych oraz ich ponowne wykorzystywanie przez obywateli)[11].

---

[8] Na temat otwartego rządu zob. m.in. *A. Piskorz-Ryń*, Jawność działania administracji publicznej z perspektywy „otwartego rządu" [w:] *I. Lipowicz (red.)*, Władza-Obywatele-Informacja. Ku nowemu porządki prawnemu. Księga pamiątkowa ku czci prof. T. Górzyńskiej, Warszawa 2014.

[9] *B. Banaszak, M. Bernaczyk*, Konsultacje społeczne i prawo do informacji w procesie prawotwórczym na tle Konstytucji RP oraz postulatu "otwartego rządu, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2012, nr 4, s. 19.

[10] *H. Izdebski, M. Kulesza*, Administracja publiczna – zagadnienia ogólne, Warszawa 2004, s.323.

[11] *G. Młynarski, A. Tarkowski, Ł. Jachowicz*, Otwarty rząd w Polsce. Kulisy programu Opengov, Fundacja Projekt: Polska, Wydanie internetowe – wersja 1.0, Warszawa 2013, s. 13. https://ngoteka.pl/bitstream/handle/item/169/Otwarty-rzad-w-Polsce-Publikacja-OPENGOV-v1-0%20%281%29.pdf?sequence=1 (dostęp: 10.08.2020).

Podmioty publiczne wytwarzają, gromadzą i przetwarzają ogromne ilości informacji, poczynając od danych statystycznych, gospodarczych lub środowiskowych, poprzez materiały archiwalne, po zdigitalizowane księgozbiory lub kolekcje dzieł sztuki. Dyskusja na temat potencjału informacyjnego danych przetwarzanych przez władze publiczne toczyła się w latach 70. i 80. XX wieku[12]. Wraz z pojawieniem się Internetu informacje zaczęto uznawać za aktywa o wartości gospodarczej. Rewolucja cyfrowa sprawiła, że wzrosła wartość tego źródła dla innowacyjnych produktów lub usług wykorzystujących takie zasoby. Wraz z rozwojem technologicznym umożliwiającym przetwarzanie danych na masową skalę pojawiła się potrzeba nowego prawa informacyjnego nowej generacji, czyli prawa do korzystania z danych publicznych[13] (*re-use of information*), dla którego pierwsze horyzontalne ramy regulacyjne wyznaczył prawodawca UE przyjmując w dnia 17 listopada 2003 r. dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego. Dyrektywa stanowiła zwieńczenie prac podjętych przez Komisję Europejską od lat '80 XX w.[14], formalnie zainicjowanych wydaniem w 1989 r. Wytycznych dla zwiększenia synergii pomiędzy sektorami publicznym i prywatnym na rynku informacyjnym[15], a następnie rozwiniętych w Zielonej Księdze z 1998 r.[16]

Z punktu widzenia ponownego wykorzystywania nie liczy się sama dostępność informacji, ale również ich jakość, forma utrwalenia oraz sposób dystrybucji umożliwiający maszynowe przetwarzanie. Dlatego też obecnie na szczeblu ponadnarodowym, tj. przede wszystkim Unii Europejskiej oraz OECD[17], jak też krajowym, regionalnym i lokalnym, administracje publiczne prowadzą politykę otwierania danych lub otwartych danych (*open data*), dla których ramy prawne dostępu do informacji (dokumentów) i ponownego jej wykorzystywania są jednym z niezbędnych środków dla „uwalniana" danych z zasobów publicznych.

---

[12] *J. Andraško, M. Mesarčík*, Quo Vadis Open Data?, "Masaryk University Journal of Law and Technology" 2018, vol. 12 (2), Brno, s. 184.

[13] W literaturze przedmiotu sformułowana została koncepcja prawa do danych publicznych, a prawo do ponownego wykorzystywania „jest prawną formą zabezpieczenia dostępu do danych" zob. szerzej *A. Piskorz-Ryń,* Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, Warszawa 2018, s. 65-79.

[14] Zob. szer. *K. Janssen, J. Dumortier*, Towards a European Framework for the Re-use of Public Sector Information: a Long and Winding Road, "International Journal of Law and Information Technology" 2003, vol. 11, Issue 2, s. 184.

[15] Guidelines for improving the synergy between the public and private sectors in the information market, 31.12.1989.

[16] Public sector information: a key resource for Europe - Green Paper on public sector information in the information society COM (1998) 585.

[17] Na szczeblu OECD używa się sformułowania *open government data.* Zob. https://www.oecd.org/gov/open-government/ (dostęp: 01.10.2020 r.).

Administracja publiczna wykonując swoje zadania określone przepisami prawa gromadzi niezliczoną ilość informacji, jednak nie wszystkie informacje pochodzące z szeroko pojętego sektora publicznego można jednak uznać za dane otwarte. O ile o kwalifikacji informacji jako informacji sektora publicznego decyduje kryterium pochodzenia, o tyle dla uznania informacji będącej w posiadaniu podmiotów publicznych za dane otwarte decydujące znaczenie ma kryterium jakościowe.

Można przyjąć za definicją sformułowaną przez Open Knowledge Foundation, że dane otwarte to dane, które mogą być swobodnie używane, ponownie wykorzystywane i redystrybuowane przez każdego – z zastrzeżeniem co najwyżej wymogu uznania autorstwa (źródła pochodzenia, *atrribution*) i dalszego rozpowszechniania na tych samych warunkach (na których pierwotnie pozyskano dane – *share alike*)[18]. W definicji tej można zatem zidentyfikować dwie konstytutywne cechy tzw. otwartych licencji, tj. licencji Creative Commons[19]. Konotacja z otwartymi licencjami nie jest przypadkowa, otwarte dane wpisują się bowiem – obok otwartego oprogramowania, tj. oprogramowania o otwartym kodzie źródłowym[20] (*open source*), otwartej nauki, czyli otwartego dostępu do treści naukowych i edukacyjnych[21] (*open access*) czy otwartej kultury (*open culture*) – w szerszą inicjatywę uwalniania zasobów i treści na cele ogólnospołeczne.

Aby dane mogły zostać uznane za otwarte muszą spełniać określone kryteria odwołujące się do aspektów prawnych i jakościowych. Wymagania te zawarte są w kilku dokumentach organizacji ponadnarodowych czy pozarządowych, m.in. w Karcie otwartych danych (Open data charter[22]) przyjętej przez państwa stowarzyszone w Partnerstwie na rzecz otwartych rządów (Open government partnership[23]) czy Podręczniku otwartych danych

[18] Zob. szerzej: Open data handbook http://opendatahandbook.org/guide/en/what-is-open-data/ (dostęp: 01.10.2020 r.).
[19] Licencji Uznanie autorstwa-Na tych samych warunkach (CC BY-SA) https://creativecommons.org/licenses/by-sa/3.0/deed.pl (dostęp: 01.10.2020 r.).
[20] Zob. m.in. Open Source Initiative https://opensource.org/ (dostęp: 01.10.2020 r.).
[21] Zob. m.in. Zalecenie Komisji (UE) 2018/790 z dnia 25 kwietnia 2018 r. w sprawie dostępu do informacji naukowej oraz jej ochrony (Dz. Urz. UE L 134/12), inicjatywy Koalicji Otwartej Edukacji https://koed.org.pl/?lang=pl oraz inicjatywy MNISW: https://www.gov.pl/web/nauka/otwarty-dostep-do-publikacji-naukowych (dostęp: 01.10.2020 r.).
[22] Międzynarodowa Karta Otwartych Danych to zbiór zasad i najlepszych praktyk w zakresie udostępniania rządowych otwartych danych. Karta została formalnie przyjęta przez siedemnaście rządów krajów, stanów i miast na światowym szczycie Open Government Partnership Global Summit w Meksyku w październiku 2015 r. https://opendatacharter.net/principles/
[23] Partnerstwo na rzecz otwartego rządu (OGP) to wielostronna międzynarodowa inicjatywa powołana 8 września 2011 r., której celem jest zabezpieczenie konkretnych zobowiązań ze strony rządów krajowych i samorządów terytorialnych w zakresie promowania otwartego rządu, wzmacniania pozycji obywateli, zwalczania korupcji i wykorzystywania nowych technologii do wzmocnienia zarządzania. W duchu wielostronnej współpracy, OGP jest nadzorowany przez komitet sterujący, w skład którego wchodzą przedstawiciele rządów i organizacji społeczeństwa obywatelskiego. Obecnie w skład OGP wchodzi 79 państw członkowskich. Polska nie jest członkiem OGP.

opracowanym przez Open Government Foundation. Na szczeblu krajowym implementacja kryteriów otwartości, zwanych również filarami otwartości została dokonana w Programie Otwierania Danych Publicznych[24], a następnie rozwinięta w przygotowanym przez Ministerstwo Cyfryzacji „Standardzie otwierania danych"[25]. W rozumieniu dwóch ostatnich dokumentów za dane otwarte uznaje się dane, które łącznie są:

1) dostępne – udostępnione bez żadnych ograniczeń szerokiemu gronu użytkowników do dowolnych celów;

2) upublicznione w wersji źródłowej – dane dostępne w oryginalnej i niezmienionej formie, a nie w postaci np. analiz, podsumowań, skrótów czy streszczeń, tak aby możliwe było m.in. łączenie danych z różnych źródeł (chodzi zatem o dostęp do danych w tzw. postaci surowej, a nie tylko zagregowanej lub zmodyfikowanej);

3) kompletne – udostępnione w całości, bez wyłączania poszczególnych części lub danych;

4) aktualne – udostępnione na tyle szybko, aby zachować wartość tych danych;

5) odczytywalne maszynowo – udostępnione w formatach umożliwiających automatyczne odczytywanie przez przeglądarkę lub system komputerowy (przykładami takich formatów są XML, JSON, RDF, CSV; formaty te ułatwiają dostęp i umożliwiają bardziej zaawansowane analizy dużej ilości informacji; korzystanie w sposób zautomatyzowany z danych udostępnionych w formacie PDF, HTML czy w formie pliku tekstowego, jest utrudnione, ponieważ wymaga przetworzenia do ustrukturyzowanego formatu otwartego);

6) udostępnione niedyskryminująco – dostępne dla każdego bez konieczności rejestracji, posiadania konta internetowego, weryfikacji tożsamości poprzez podawanie hasła, loginu czy podpisywania jakichkolwiek umów oraz równe traktowanie użytkowników pobierających dane udostępniane przez systemy teleinformatyczne z uwzględnieniem uprzywilejowania grupy podmiotów, którym dostęp do danych jest niezbędny do realizacji ich ustawowych zadań oraz przypadków umów na wyłączność;

---

[24] Program Otwierania Danych Publicznych stanowiący załącznik do Uchwały Nr 107/2016 Rady Ministrów z 20 września 2016 r. Program został przyjęty na lata 2016-2020.
Obecnie Program ten jest kontynuowany przez nowy Program Otwierania Danych na lata 2021-2027.
https://www.gov.pl/web/cyfryzacja/program-otwierania-danych-na-lata-2021-2027--ruszaja-prekonsultacje-spoleczne (dostęp: 20.03.2021 r.).

[25] Dokument zawiera zalecenia dotyczące ram prawnych, pozwalające na powszechny i swobodny dostęp do danych i ich ponowne wykorzystywanie. Prezentuje zagadnienia prawne istotne przy podejmowaniu decyzji o udostępnianiu danych w sposób otwarty, m.in. kwestie licencjonowania oraz ochrony praw autorskich. Standard porusza także kwestie barier w udostępnianiu danych publicznych w sposób otwarty, filarów otwartości danych oraz wzorca otwartości.
https://dane.gov.pl/pl/knowledgebase/useful-materials/standardy-otwartosci-danych (dostęp: 01.10.2020 r.).

7) dostępne bez ograniczeń licencyjnych – dane nie są przedmiotem praw autorskich, patentów, znaków towarowych lub tajemnicy handlowej i mogą być wykorzystywane w dowolnych celach bez konieczności ubiegania się o jakąkolwiek zgodę na ich używanie;
8) niezastrzeżone – dostępne w formacie powszechnie stosowanym, który nie jest kontrolowany przez żaden podmiot (np. dane zostaną udostępnione w formacie, którego obsługa wymaga specjalistycznego, niestandardowego oprogramowania)[26].

Dane otwarte to te informacje sektora publicznego, które spełniają jednocześnie wszystkie kryteria otwartości. Z punktu widzenia ponownego wykorzystywania dane otwarte mają fundamentalne znaczenie, ze względu na ich utrwalenie w otwartych formatach są to dane wielokrotnego użycia, które dostępne bez ograniczeń licencyjnych mogą być wykorzystywane przez każdego zainteresowanego użytkownika.

Łączne spełnienie kryteriów otwartości jest niezbędne dla zapewnienia interoperacyjności otwartych danych, rozumianej jako zdolność różnych systemów i organizacji do współpracy (współdziałania). Interoperacyjność jest kluczowa dla budowania dużych złożonych systemów, ponieważ umożliwia współpracę różnych komponentów, np. wymiany lub łączenia różnych zbiorów danych niezbędną do budowania dużych[27].

Co istotne, dotychczas pojęcie otwartych danych nie posiada definicji legalnej. Na szczeblu krajowym w odniesieniu do danych pochodzących z sektora publicznego używa się co do zasady terminów zdefiniowanych w dwóch ustawach informacyjnych, których zakres przedmiotowy wyznaczają pojęcia informacji publicznej oraz informacji sektora publicznego[28].

Pojęcie otwartych danych nie występowało w ogóle na gruncie dyrektyw 2003/98/WE. Z kolei dyrektywa 2013/37/UE[29] była jednym z trzech dokumentów opublikowanych przez Komisję Europejską w ramach pakietu *Open Data Package*, który zakładał lepsze wykorzystanie potencjału informacji sektora publicznego dla wzrostu konkurencyjności i innowacyjności gospodarki europejskiej. Dyrektywa nie wprowadzając jednak prawnego pojęcia otwartych danych, stanowiła jednocześnie o „polityce otwartego dostępu" (motyw 3 preambuły) oraz „otwartych formatach" (motywy 21 oraz 26 preambuły), co można interpretować jako zapowiedź zmiany tytułu i zakresu najnowszej dyrektywy 2019/1024, której nadano tytuł „o otwartych danych i ponownemu wykorzystywaniu informacji sektora publicznego".

[26] Standardy otwartości danych. Standard prawny, Ministerstwo Cyfryzacji 2020, s. 24-28.
[27] Open data handbook, http://opendatahandbook.org/guide/en/what-is-open-data/ (dostęp: 01.10.2020 r.).
[28] O problemach definicyjnych zob. Rozdział 3.2.1.
[29] Dyrektywa 2013/37/UE Parlamentu Europejskiego i Rady z dnia 26 czerwca 2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz. Urz. UE L 175/1); dalej: dyrektywa 2013/37/UE.

Natomiast, wbrew tytułowi z niewyjaśnionych w preambule przyczyn, również dyrektywa 2019/1024 nie wprowadziła w części normatywnej definicji legalnej otwartych danych, wciąż zakres przedmiotowy ponownego wykorzystywania opierając na pojęciu dokumentu (informacji sektora publicznego). Niemniej w motywie 16 prawodawca UE wskazał, że „pojęcie otwartych danych ogólnie odnosi się do danych w otwartym formacie, które mogą być swobodnie wykorzystywane, ponownie wykorzystywane i udostępniane przez wszystkich do dowolnego celu. Polityka otwartych danych propagująca szeroką dostępność i ponowne wykorzystywanie informacji sektora publicznego do celów prywatnych lub komercyjnych, przy minimalnych ograniczeniach prawnych, technicznych lub finansowych bądź bez takich ograniczeń, i wspierająca obieg informacji przeznaczonych nie tylko dla podmiotów gospodarczych, lecz przede wszystkim dla opinii publicznej, może odegrać ważną rolę we wspieraniu zaangażowania społecznego oraz w zapoczątkowaniu i stymulowaniu rozwoju nowych usług opartych na nowatorskich sposobach łączenia takich informacji i korzystania z nich. W związku z tym państwa członkowskie zachęca się do wspierania tworzenia danych w oparciu o zasadę <otwartości w fazie projektowania i otwartości domyślnej> w odniesieniu do wszystkich dokumentów objętych zakresem stosowania dyrektywy".

De lege lata nie można zatem mówić o prawnej regulacji otwartych danych *sensu stricto* ani o harmonizacji przepisów o otwartych danych. Należy raczej mówić o polityce (publicznej) otwartych danych (*open data policy*).

Przez politykę publiczną (*public policy*) należy rozumieć wszelkie świadome działania (i zaniechania) tych podmiotów czy aktorów, których obejmuje zakres pojęcia rządu[30], które są podejmowane w odpowiedzi na najważniejsze problemy danego społeczeństwa. Z zasady formułowanie działań ma być oparte na zobiektywizowanej i aktualnej w danym czasie wiedzy, a ich wykonywanie – w ramach usystematyzowanego procesu ich projektowania i wdrażania. Ich celem jest stworzenie warunków trwałego rozwoju społeczeństwa i jego członków[31]. Przyjmuje się, że przedmiotem polityki publicznej może każda aktywność państwa, nie sposób wyznaczyć zamkniętego katalogu zagadnień, które mogą być przedmiotem interwencji.

Polityka otwartych danych ma na celu stworzenie efektywnego otoczenia instytucjonalnego, regulacyjnego i technologicznego dla najpełniejszego wykorzystania potencjału społeczno-gospodarczego danych pochodzących z sektora publicznego, w tym

[30] *T. R. Dye*, Understanding public policy, Harlow 2014, s. 3. Zob. szerzej *R. Szarfenberg*, Polityka publiczna - zagadnienia i nurty teoretyczne, „Studia z polityki publicznej" 2016, nr 1, s. 45-75
[31] Zob. *A. Zybała*, Polityki publiczne, Warszawa 2012, s. 19-45.

przede wszystkim danych otwartych zgodnie z zasadą „tak otwarte jak to możliwe, zamknięte jak to tylko niezbędne" (*as open as possible and as closed as necessary*[32]).

Ponowne wykorzystywanie informacji sektora publicznego jest podstawowym instrumentem regulacyjnym polityki publicznej otwierania danych lub po prostu otwartych danych realizowanej w Unii Europejskiej. Innymi słowy przepisy te są środkiem prawnym służącym realizacji celów polityki otwartych danych.

Realizacja polityki publicznej otwartych danych na szczeblu UE opiera się na działaniach legislacyjnych, których głównym instrumentem pozostają kolejne dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego, ale również działania infrastrukturalne, polegające na stworzeniu warunków technologicznych służących dystrybucji danych do dalszej eksploatacji, w ramach których głównym działaniem pozostaje budowa europejskiego portalu otwartych danych[33] oraz finansowe polegające na wsparciu państw członkowskich w procesie cyfryzacji w ramach kolejnych perspektyw finansowych (np. Program UE „Cyfrowa Europa" na lata 2021 – 2027, *Digital Europe Programme*[34]).

Na szczeblu krajowym polityka publiczna otwierania danych poza kreowaniem otoczenia regulacyjnego, które co do zasady zdeterminowane jest przepisami dyrektyw o ponownym wykorzystywaniu informacji sektora publicznego, polega na tworzeniu przyjaznego otocznia instytucjonalno-organizacyjnego oraz podobnie jak na szczeblu UE, infrastrukturalnego. Głównym środkiem realizacji polityki w aspekcie technologicznym pozostaje portal otwartych danych (dane.gov.pl pełniący funkcję centralnego repozytorium informacji publicznej[35]), ale również inicjatywy ukierunkowane na dostosowaniu baz danych (rejestrów publicznych) do zautomatyzowanego udostępniania danych przez interfejsy programowania aplikacji (API)[36]. Dokumentem strategicznym wyznaczającym cele i środki realizacji polityki otwartych danych jest obecnie Program Otwierania Danych zaś narzędziem operacyjnym jest tzw. sieć pełnomocników do spraw otwartości danych (tzw. *open data officers*), powołanych na mocy Programu we wszystkich ministerstwach, Kancelarii Prezesa Rady Ministrów oraz Głównym Urzędzie Statystycznym. Rolę koordynatora polityki otwartych danych w Polsce pełni minister właściwy do spraw informatyzacji.

---

[32] Motyw 28 preambuły dyrektywy 2019/1024.

[33] Obecnie istnieją równolegle dwa portale otwartych danych na szczeblu UE, tj. EU Open data portal (https://data.europa.eu/euodp/en/home) oraz docelowy European data portal (https://www.europeandataportal.eu).

[34] https://ec.europa.eu/digital-single-market/en/europe-investing-digital-digital-europe-programme (dostęp: 20.11.2020)

[35] Dalej: centralne repozytorium lub CRIP.

[36] Zob. projekty realizowane na szczeblu rządowych Otwarte dane: dostęp, standard, edukacja oraz Otwarte dane plus. https://www.gov.pl/web/cyfryzacja/otwarte-dane-publiczne

Dobrym przykładem czym są dane otwarte i jaką rolę społeczno-gospodarczą mogą odegrać, są dane transportowe. Po tym jak „uwolniono" dane o transporcie publicznym w Londynie, powstało ponad 500 aplikacji na urządzenia mobilne oferujące usługi wyszukiwania najdogodniejszych i stale aktualizowanych połączeń różnymi środkami transportu miejskiego w aglomeracji stolicy Zjednoczonego Królestwa[37]. Z kolei krajowym przykładem wykorzystania otwartych danych, mogą być aplikacje wykorzystujące dane o jakości powietrza udostępnianie przez Inspekcję Ochrony Środowiska, aplikacja Polskie Zabytki czy portal „Na co idą moje pieniądze"[38].

Źródeł polityki otwierania danych należy upatrywać w idei otwartego rządu. Koncepcje otwartych danych i otwartego rządu osadzone są tym samym fundamencie aksjologicznym związanym z zasadą jawności i transparentności życia publicznego. Współcześnie inicjatywy te służą jednak realizacji zasadniczo odmiennych celów, które mogą się jednak krzyżować. Koncepcja otwartego rządu związana jest prawem dostępu do informacji publicznej, zatem uprawnieniem co do zasady politycznym. Z kolei otwarte dane są elementem prawa użytkowego służącego celom społecznym i gospodarczym. Dane otwarte mogą stanowić materiał wyjściowy dla budowania produktów i usług o różnorodnym zastosowaniu, jednocześnie wpisują się w idee otwartego rządu i transparentnej administracji.

1.2. Istota ponownego wykorzystywania informacji sektora publicznego

Sektor publiczny jest „nieprzebranym, nieograniczonym i nieuporządkowanym zbiorem (rezerwuarem) informacji"[39]. Jest jednak niedostatecznie eksploatowany, a jego niewykorzystywanie powoduje niewspółmierne straty[40]. Potrzeba wprowadzenia regulacji prawnej ponownego wykorzystywania wzięła się z przeświadczenia, że cele ekonomiczne i społeczne danych pochodzących z sektora publicznego nie mogą zostać zrealizowane przez uznane i ukształtowane przez lata prawo dostępu do informacji publicznej (dostępu do dokumentów urzędowych), nie gwarantuje ono bowiem samo przez się ich dalszego wykorzystywania. W tym należy upatrywać motywów ustanowienia „pokrewnego" prawa do wykorzystywania tych samych informacji, ale do innych celów, niż zostały wytworzone,

[37] Zob. https://data.london.gov.uk/
[38] http://powietrze.gios.gov.pl/pjp/current# (dostęp: 20.11.2020). Przykłady aplikacji wykorzystujących dane otwarte dostępne są na rządowym portalu otwartych danych https://dane.gov.pl/application
[39] *T. Górzyńska*, Prawna regulacja ponownego wykorzystywania [w:] *G. Sibiga (red.)*, Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej, Warszawa 2014, s. 241.
[40] *Ibidem*.

gromadzone, przetwarzane i rozpowszechniane[41]. Zamiar i konieczność uregulowania szczegółowych kwestii przypisanych prawu do ponownego wykorzystywania nie były traktowane jako uzupełnienie, wprowadzenie zmian udoskonalających prawo dostępu, ale uregulowanie nowego obszaru zagadnień, wynikających z potrzeby wykorzystywania tych informacji, do których zasady dostępu zostały już prawnie ustalone[42].

Po raz pierwszy do obiegu prawnego definicję legalną ponownego wykorzystywania informacji sektora publicznego wprowadził prawodawca unijny w dyrektywie 2003/98/WE. Z kolei jej treść w prawie krajowym wyznaczają obecnie przepisy UPW. Próba interpretacji znaczenia normatywnego tego pojęcia została podjęta w Rozdziale 3.

Co istotne, dyrektywa 2003/98/WE została przyjęta na podstawie art. 95 Traktatu ustanawiającego Wspólnotę Europejską (podobnie jak dyrektywa 2019/1024 w oparciu o art. 114 Traktatu o Funkcjonowaniu Unii Europejskiej, stanowiący odpowiednik art. 95 TWE). Celem dawnego art. 95 TWE, a obecnie art. 114 TFUE jest ustanowienie przepisów funkcjonowania rynku wewnętrznego. Celem zaś ustanowionych przez dyrektywy ram prawnych jest zapewnienie warunków, które maksymalnie zwiększą potencjalne korzyści z ponownego wykorzystywania zasobów danych publicznych w Europie. Zarówno podstawa prawna, jak i cele, o których mowa w preambule do dyrektywy, akcentują gospodarczy charakter regulacji.

Na płaszczyźnie ekonomicznej podkreśla się, że informacja sektora publicznego pozwoli na wykorzystanie potencjału przedsiębiorców w państwach Unii Europejskiej. W tym kontekście rozwój produktów i usług opartych na tej informacji przyczynia się do wzrostu gospodarczego i tworzenia miejsc pracy, w tym dzięki powstającym małym przedsiębiorcom typu *start-up*. Nie można jednak ignorować również aspektów pozaekonomicznych. Bezpośrednio z ponownego wykorzystywania informacji sektora publicznego będą korzystali, poza użytkownikami profesjonalnymi tworzącymi w oparciu o informację wartość dodaną, która nie musi zawsze mieć charakter zarobkowy (np. w działalności organizacji pozarządowych) również końcowi użytkownicy (czyli konsumenci produktów i usług opartych na informacji), zyska również ogół społeczeństwa, w którym rozwój technik informacyjno-telekomunikacyjnych i zwiększony dostęp do wiedzy, pozwala na dalszą ewolucję w kierunku społeczeństwa informacyjnego. Zwraca się także uwagę na korzyści dla samych podmiotów sektora publicznego, bowiem mechanizmy ponownego wykorzystywania wspierają ich przejrzystość i odpowiedzialność oraz zapewniają informację zwrotną od użytkowników

[41] *Ibidem*, s. 242.
[42] *Ibidem*.

i użytkowników końcowych, która pozwala zainteresowanemu podmiotowi na poprawę jakości gromadzonych informacji[43].

Istotę zagadnienia ponownego wykorzystywania dobrze wyjaśnił projektodawca dyrektywy 2013/37/UE. Komisja Europejska w ocenie skutków wniosku zmiany dyrektywy 2003/98/WE wskazuje, iż ponowne wykorzystywanie informacji sektora publicznego oznacza wszelkie twórcze wykorzystywanie danych, np. poprzez zwiększenie wartości danych, łączenie danych z różnych źródeł w celu wytworzenia pożądanego rezultatu i rozwijania aplikacji, zarówno w celach komercyjnych, jak i niekomercyjnych. Instytucja ponownego wykorzystywania koncentruje się na wykorzystywaniu gospodarczej wartości informacji sektora publicznego, gdzie służy ona jako materiał surowy dla rozwoju nowych produktów i usług. Podczas gdy podmioty publiczne są twórcami i dostawcami oryginalnego materiału, sektor prywatny odgrywa istotną rolę jako uczestnik i pośrednik procesu przetwarzania informacji pomiędzy źródłem informacji (podmiot publiczny) a końcowym użytkownikiem[44].

G. Vickery zaproponował następujący schemat schemat ponownego wykorzystywania w celach komercyjnych (*commercial re-use of public sector information*). Polega on na transferze „surowej" informacji sektora publicznego od podmiotu publicznego (*public body*), poprzez pośrednika, czyli podmiot prywatny będący użytkownikiem informacji do końcowego użytkownika informacji już przetworzonej (*end users*) w postaci produktu lub usługi. Transfer zwrotny pomiędzy użytkownikiem końcowym a podmiotem publicznym należy traktować jako wpływy do budżetu z tytułu podatków za zakupioną usługę lub produkt od podmiotu prywatnego (pośrednika). Komercyjne ponowne wykorzystywanie należy odróżnić od udostępniania treści publicznych (*making available public sector content*), np. informacji publicznej, gdzie następuje bezpośrednie przekazanie treści (informacji) między podmiotem publicznym a końcowym użytkownikiem (uprawnionym), co do zasady nieodpłatnie, bez pośrednictwa podmiotu prywatnego[45].

Przedsiębiorstwa mogą wykorzystywać informacje sektora publicznego na wiele sposobów: do własnych celów biznesowych (np. analiz, prognoz, raportów); do wytworzenia produktów i usług, (np. aplikacje na urządzenia mobilne) czy jako wkład do wytwarzania produktów dla przemysłu (np. dane zasilające sztuczną inteligencję).

---

[43] Zob. Motyw 4 preambuły dyrektywy 2013/37/UE.

[44] Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information COM(2018) 234 final, s. 6. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018SC0127

[45] *G. Vickery*, Review of recent studies on psi re-use and related market developments, Paryż 2011, s. 12. https://ec.europa.eu/digital-single-market/en/news/review-recent-studies-psi-reuse-and-related-market-developments (dostęp: 20.11.2020).

Co istotne, rolą regulacji ponownego wykorzystywania jest wprowadzenie gwarancji również dla końcowych użytkowników informacji (konsumentów produktów, usług, aplikacji, przetworzonych w inny sposób treści), choć nie są oni bezpośrednio związani relacją podmiot publiczny (dostawca informacji) – użytkownik wykorzystujący informację (odbiorca danych – pośrednik). O ile przepisy dostępowe regulują jedynie stosunek między pomiotem wykonującym zadania publiczne (podmiotem udostępniającym informację) oraz osobą wykonującą prawo do informacji, o tyle w ponownym wykorzystywaniu pozyskana przez użytkownika informacja będzie użyta w produktach i usługach skierowanych do ich konsumentów (końcowych użytkowników). Ponieważ informacja pochodzi ze sfery publicznej podmiot sektora publicznego (udostępniający informację) może wpływać na kolejny stosunek związany z ponownym wykorzystywaniem, tj. stosunek użytkownik (odbiorca danych) – końcowy użytkownik (konsument), w celu polepszenia sytuacji drugiej z tych stron[46]. Służą temu warunki ponownego wykorzystywania informacji sektora publicznego (licencje), które może określić podmiot publiczny polegające m.in. na zobowiązaniu użytkownika do poinformowania końcowych użytkowników o źródle, czasie wytworzenia i pozyskania informacji publicznej od podmiotu publicznego oraz o przetworzeniu informacji ponownie wykorzystywanej[47]. Użytkownik realizuje wspomniane warunki w ramach stosunku z końcowym użytkownikiem (nabywcą towarów lub usług użytkownika), przez co ten drugi staje się lepiej poinformowany w zakresie informacji wykorzystywanych w produkcie lub usłudze[48].

1.3. Znaczenie ponownego wykorzystywania informacji sektora publicznego na jednolitym rynku cyfrowym Unii Europejskiej

Od przyjęcia w 2003 r. pierwszej dyrektywy 2003/98/WE do ostatniego jej przekształcenia w postaci dyrektywy 2019/1024 ponowne wykorzystywanie informacji sektora publicznego przestało być wyłącznie utożsamiane z polityką otwartych danych. Wprawdzie od samego początku podkreślano gospodarczy charakter prawa, którego celem jest stymulowanie rozwoju nowych usług opartych na nowatorskich sposobach łączenia i korzystania z informacji,

[46] *G. Sibiga*, Ponowne wykorzystanie informacji sektora publicznego – stan obecny i perspektywy rozwoju. Wybrane zagadnienia [w:] *A. Mednis*, Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość, Warszawa 2016, s. 111 i nast.
[47] Zob. motyw 17 preambuły dyrektywy 2003/98/WE, motyw 26 dyrektywy 2013/37/UE, motyw 44 dyrektywy 2019/1024 oraz art. 14 UPW.
[48] *G. Sibiga*, op. cit.

pobudzanie wzrostu gospodarczego i budowania gospodarki opartej na wiedzy[49], to niewątpliwym przełomem dla roli ponownego wykorzystywania informacji sektora publicznego było ogłoszenie przez Komisję Europejską w dniu 6 maja 2015 r. Strategii jednolitego rynku cyfrowego dla Europy[50].

Ideą jednolitego rynku cyfrowego (*digital single market*) jest zasadniczo usunięcie krajowych ograniczeń dotyczących transakcji dokonywanych za pośrednictwem Internetu. Idea ta opiera się na koncepcji wspólnego rynku, której celem jest wyeliminowanie barier handlowych między państwami członkowskimi w celu zwiększenia dobrobytu gospodarczego i którą przekształcono następnie w koncepcję rynku wewnętrznego określanego jako obszar bez granic wewnętrznych, w obrębie którego zapewniony jest swobodny przepływ towarów, osób, usług i kapitału. Będąca kontynuacją strategii lizbońskiej strategia Europa 2020[51] wprowadziła europejską agendę cyfrową[52] stanowiącą jedną z siedmiu inicjatyw przewodnich, co podkreśliło kluczową rolę, jaką odegrają technologie informacyjno–komunikacyjne. Komisja w swojej Strategii jednolitego rynku cyfrowego uznała ten rynek za priorytet.

Strategia jednolitego rynku cyfrowego opiera się na trzech filarach: 1) zapewnienie konsumentom i przedsiębiorstwom łatwiejszego dostępu do towarów i usług cyfrowych w całej Europie; 2) tworzenie odpowiednich i równych warunków funkcjonowania umożliwiających rozkwit sieci cyfrowych i innowacyjnych usług; 3) maksymalizacja potencjału wzrostu gospodarki cyfrowej.

Komisja złożyła już szereg wniosków ustawodawczych zmierzających do realizacji jednolitego rynku cyfrowego[53]. Co istotne dla omawianego zagadnienia częścią pakietu legislacyjnego w ramach budowy jednolitego rynku cyfrowego była zarówno reforma ochrony

[49] Zob. motyw 3 i 5 preambuły dyrektywy 2003/98/WE

[50] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Strategia jednolitego rynku cyfrowego dla Europy COM(2015) 192 final

[51] Europa 2020 – strategia na rzecz inteligentnego i zrównoważonego rozwoju sprzyjającego włączeniu społecznemu to długookresowy programem rozwoju społeczno-gospodarczego Unii Europejskiej na lata 2010-2020.

[52] https://ec.europa.eu/digital-single-market/ (dostęp:20.10.2020).

[53] Przykładowo celem wniosków ustawodawczych było rozwiązanie takich kwestii jak nieuzasadnione blokowanie geograficzne, transgraniczne usługi doręczania paczek, możliwość transgranicznego przenoszenia na rynku wewnętrznym usług online w zakresie treści, przegląd rozporządzenia w sprawie współpracy w zakresie ochrony konsumenta, audiowizualne usługi medialne, umowy sprzedaży towarów zawieranych przez Internet lub w inny sposób na odległość oraz umowy o dostarczanie treści cyfrowych. Kalendarium inicjatyw można prześledzić na: https://www.consilium.europa.eu/pl/policies/digital-single-market/ (dostęp: 20.10/2020). Wśród już przyjętych regulacji dotyczących realizacji strategii budowania jednolitego rynku cyfrowego wymienić można m.in. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 248/2014 z dnia 26 lutego 2014 r. zmieniające rozporządzenie (UE) nr 260/2012 w odniesieniu do przejścia na ogólnounijne polecenia przelewu i polecenia zapłaty; Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę czy dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE.

danych osobowych polegająca na przyjęciu ogólnego rozporządzenia oraz tzw. dyrektywa policyjna, jak i nowa dyrektywa w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego. Tym samym jednocześnie prawo ochrony danych osobowych i prawo do ponownego wykorzystywania zostały uznane za kluczowe narzędzia służące budowie gospodarki cyfrowej na rynku wewnętrznym UE.

Strategia jednolitego rynku cyfrowego i służące jej realizacji instrumenty legislacyjne zmieniły paradygmat podejścia do otwartych danych i ponownego wykorzystywania informacji sektora publicznego. Było to wyrazem szerszego zjawiska związanego z koncepcją budowy gospodarki opartej o dane (*data driven economy*)[54].

W erze cyfrowej dane stają się środowiskiem niezbędnym do kreowania nowych wartości i do zaspokajania ludzkich potrzeb. Dane generowane są zarówno przez naturalną aktywność człowieka, obserwację środowiska naturalnego oraz aktywność maszyn. Dane można postrzegać jako czynnik produkcji obok kapitału i pracy, jako niezbędną infrastrukturę do działania i podejmowania przedsięwzięć o charakterze społecznym lub ekonomicznym[55]. Dane w dzisiejszej gospodarce często porównuje się do surowca naturalnego, który napędza funkcjonowanie największych przedsiębiorstw na świecie. Przyjmuje się, że obecnie światowym najbardziej wartościowych zasobem nie jest już ropa, a dane[56]. Dlatego nie należy postrzegać danych, jak czyniono to w przeszłości, jako surowca, bo ten ze swej istoty jest wyczerpywalny. Bardziej zasadnym będzie myślenie o danych jako zasobie wielokrotnego użytku o niekonkurencyjnym i praktycznie nieograniczonym charakterze. Dane mogą być też wykorzystywane jednocześnie, wielokrotnie i niezależnie przez różnych uczestników życia społecznogospodarczego[57]. Przydatniej jest myśleć o danych, mniej jako o towarze do kupna lub sprzedaży, a bardziej jako o współdzielonym zasobie lub o dobru wspólnym[58].

Dane można definiować i klasyfikować w oparciu o różne kryteria. Przykładowo EUROSTAT dzieli dane według źródeł pochodzenia: dane z sieci społecznościowych –

---

[54] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów - Ku gospodarce opartej na danych (COM(2014) 442 final z 2.7.2014 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Budowa europejskiej gospodarki opartej na danych" COM (2017) 9 final z 10.1.2017 r.

[55] PRZEMYSŁ +. Gospodarka oparta o dane, Ministerstwo Cyfryzacji 2018. https://www.gov.pl/web/cyfryzacja/gospodarka-oparta-o-dane-przemysl- (dostęp: 04.08.2020).

[56] *D. Parkins,* Regulating the internet giants - The world's most valuable resource is no longer oil, but data [w:] The Economist, 06.05.2017 https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data (dostęp: 04.08.2020).

[57] PRZEMYSŁ+, s. 10.

[58] *T. Bass,* It's time to think about our data as a common good, British Council https://www.britishcouncil.org/anyone-anywhere/explore/communities-connections/rethinking-data (dostęp: 04.08.2020).

pochodzące z ludzkiej aktywności (relacje między osobami, blogi, komentarze, dokumenty osobiste, obrazy, wideo, wyszukiwania internetowe, wiadomości, e-maile, wearables); dane z tradycyjnych systemów informatycznych – ustrukturyzowane i przechowywane w systemach baz danych, monitorujące i rejestrujące transakcje publiczne, prywatne lub publiczno-prywatne (dane instytucji publicznych, dane medyczne, dane przedsiębiorstw, w tym transakcje handlowe i bankowe); dane generowane przez maszyny i czujniki (w tym Internet rzeczy) – ustrukturyzowane dane pochodzące z czujników stałych i ruchomych oraz z systemów komputerowych (automatyka przemysłowa, automatyka domowa, czujniki pogodowe i środowiskowe, kamery, czujniki produkcyjne, lokalizacja, zdjęcia satelitarne oraz logi)[59].

Dane możemy również podzielić ze względu na poziom ich jawności lub poufności, w szczególności na osobowe i nieosobowe oraz zawierające tajemnice objęte prawnymi i ustawowymi ograniczeniami jawności. Danymi nieosobowymi są dane elektroniczne – inne niż dane osobowe zdefiniowane w przepisach ogólnego rozporządzenia[60]. Dane nieosobowe nie dopuszczają do ustalenia tożsamości osoby fizycznej. Do takich informacji zaliczają się na przykład informacje dotyczące przeglądanych stron internetowych, dane zawierające liczbę wizyt oraz czas spędzony na konkretnej stronie internetowej, analizy *big data*, algorytmy informatyczne, dane związane z konserwacją maszyn przemysłowych, dane wytwarzane przez maszyny, zanonimizowane zbiory danych lub dane wytwarzane przez maszyny – o ile informacje te nie dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

Na przykład dane generowane przez domowe czujniki temperatury mogą mieć charakter osobowy, jeśli można przyporządkować je do danej osoby, natomiast dane dotyczące wilgotności gleby nie mają charakteru osobowego. Dane osobowe można przekształcić w dane nieosobowe w procesie anonimizacji[61].

Innym kryterium jakie można przyjąć jest kryterium podmiotowe, wówczas możemy podzielić dane na dane prywatne oraz dane publiczne. Szczególną kategorię stanowią dane publiczne lub informacje sektora publicznego, które ze względu na sposób pozyskania stanowią własność społeczną (wspólną). Spośród nich szczególne znaczenie mają zaś dane otwarte, które mogą być swobodnie wykorzystywane co do zasady bez ograniczeń licencyjnych czy technologicznych.

[59] PRZEMYSŁ+, s. 11.
[60] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz. Urz. UE L 303/59).
[61] Komunikat COM(2017) 9, s. 10.

W obrębie danych posiadanych przez podmioty prywatne istnieją ogromne obszary danych nie zawierające tajemnic przedsiębiorstwa (w tym maszynowe oraz komercyjne, będące w sferze zainteresowania publicznego – *data of public interest*), które w ślad za danymi otwartymi winny być udostępnione do ponownego użytku gospodarczego[62].

Dane generowane maszynowo powstają bez bezpośredniego udziału człowieka poprzez procesy, aplikacje lub usługi komputerowe bądź czujniki przetwarzające informacje dostarczane przez wirtualne lub fizyczne urządzenia, oprogramowanie lub maszyny. Dane generowane maszynowo mogą mieć charakter osobowy lub nieosobowy. Jeśli dane generowane maszynowo umożliwiają ustalenie tożsamości osoby fizycznej, uznawane są za osobowe, dopóki dane nie zostaną całkowicie zanonimizowane (np. dane dotyczące lokalizacji z aplikacji mobilnych)[63].

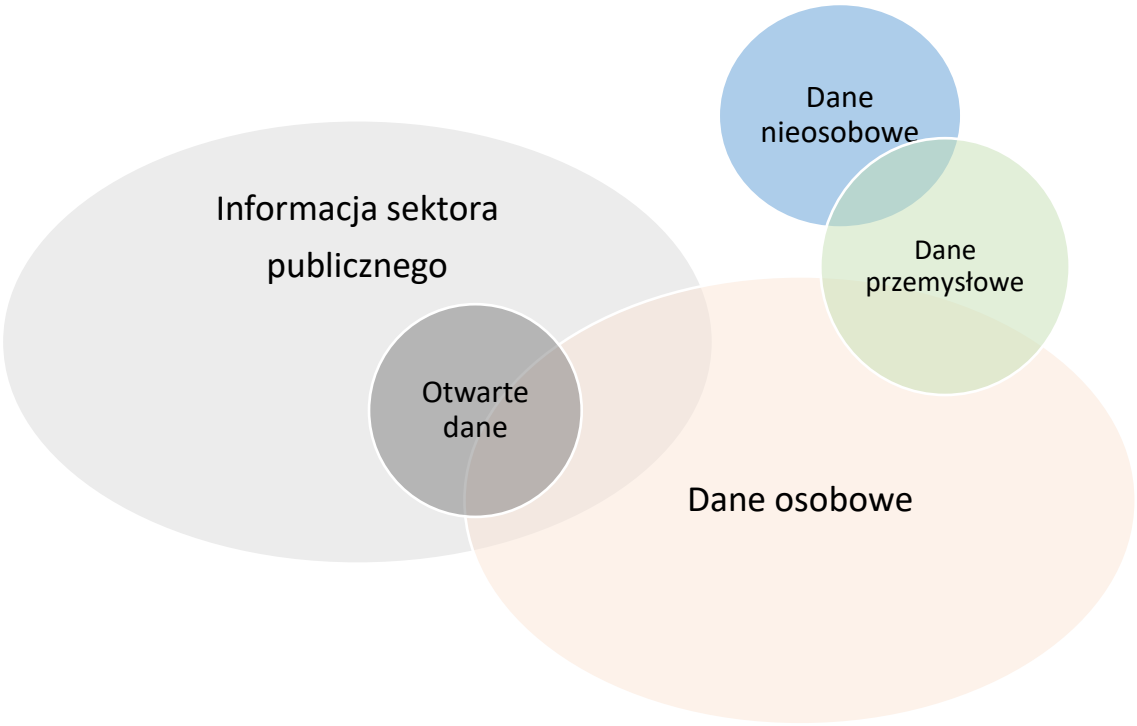
Kategorie danych przenikają się wzajemnie. Definicje legalne przyjęte w aktach prawnych na szczeblu UE i państw członkowskich dla różnych rodzajów danych są szerokie i nieostre, a w ślad za rozwojem gospodarczym i technologicznym ich interpretacja również oficjalna (autentyczna czy sądowa) bywa dynamiczna. Problem potęguję skomplikowany system regulacyjny w obszarze danych na terytorium UE, którego nie eliminują podejmowane od lat próby harmonizacji przepisów.

Wpływ danych przejawia się w pięciu kluczowych obszarach: technologicznej innowacji, nowatorskich modelach biznesowych, kreowaniu nowych rynków, innowacjach społecznych oraz politykach publicznych bazujących na danych. Są one szczególnie ważne dla podmiotów gospodarczych, które swoje modele biznesowe opierają na ich przetwarzaniu. Przykładem może być projektowanie technologii Internetu rzeczy (*Internet of Things – IoT*), analiza wielkich zbiorów danych (*big data*[64]), uczenie maszynowe (*machine learning*) czy rozwój sztucznej inteligencji (a*rtificial intelligence*). Istotnym z ekonomicznego punktu widzenia oraz biorąc pod uwagę wydajność całego sytemu pozostaje stworzenie tzw. łańcucha wartości danych, czyli nieskrępowanego przetwarzania danych przez różne podmioty na odmiennych etapach ich funkcjonowania. Na łańcuch wartości danych składają się m.in. ich

[62] PRZEMYSŁ+, s. 11.
[63] Komunikat COM(2017) 9, s. 10.
[64] Zdaniem *W.R. Wiewiórowskiego big data* to w istocie praktyka łączenia dużych zasobów informacyjnych, obejmujących zróżnicowane i pierwotnie rozproszone dane, oraz do analizowania tych zasobów przy pomocy rozbudowanych algorytmów, celem wydobycia informacji, która może być wykorzystana do celowego działania. Termin odnosi się nie tylko do rozwiązań technologicznych służących do zbierania i przechowywania dużych ilości danych, lecz również do analizy, rozumienia i skutecznego wykorzystania pełnej wartości niesionej przez dane. Szczególny nacisk kładziony jest w tych procesach na automatyczne przetwarzanie danych przy pomocy specjalnie stworzonych do tego aplikacji. Zob. szerzej: *W.R. Wiewiórowski*, Założenia wstępne dla zrównoważonego przetwarzania informacji, [w:] *T. Bąkowski (red.)*, Model regulacji [w:] *G. Szpor (red*.), Jawność i jej ograniczenia, Tom XII, Warszawa 2016, s. 2.

tworzenie, gromadzenie, agregacja, organizacja, wykorzystywanie, a następnie ponowne wykorzystanie[65]. Niewątpliwym wyzwaniem w tym procesie pozostaje zapewnienie ochrony danych osobowych.

Mozaikę kategorii danych i informacji na jednolitym rynku cyfrowych przedstawia następująca grafika.



Rysunek 1. *Jednolity rynek danych UE* (opracowanie własne)

Otwarte dane, czy szerzej informacje sektora publicznego stanowią jedynie jedną z kilku kategorii danych występujących w przestrzeni danych na jednolitym rynku cyfrowym, jednak ich wartość stale rośnie.

Obecnie szacuje się, że bezpośrednia wielkość rynku otwartych danych w UE wynosi 52 mld euro rocznie dla 28 Państw członkowskich łącznie[66]. Otwarte dane mogą również

[65] *A. Polanowski*, Przepływ danych nieosobowych. Ramy swobodnego przenoszenia informacji w prawie europejskim, Biuletyn Euro Info 2019, nr 1. https://en.parp.gov.pl/component/publications/publication/biuletyn-euro-info-1-2019 (dostęp: 04.08.2020).

[66] Impact Assessment Accompanying the document Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information COM(2018) 234 final, s. 6. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX:52018SC0127.

zwiększyć efektywność samej administracji, KE szacuje oszczędności generowane dzięki otwartym danym wysokości 1,7 mld euro rocznie dla administracji publicznej państw UE[67].

W wartości tego rynku oraz dynamice rozwoju nowych technologii należy upatrywać zmiany aksjologicznego i systemowego podejścia do instytucji ponownego wykorzystywania informacji sektora publicznego, którą postrzega się jako istotny instrument służący realizacji wyzwań gospodarczych na jednolitym rynku cyfrowym. W motywie 10 preambuły dyrektywy 2019/1024 potwierdził to prawodawca UE, stwierdzając że od czasu przyjęcia dyrektywy 2003/98/WE ilość danych na świecie, w tym danych publicznych, gwałtownie wzrosła oraz generowane i gromadzone są nowe rodzaje danych. Jednocześnie ma miejsce ciągła ewolucja technologii służących do analizy, wykorzystywania i przetwarzania danych. Ta szybko postępująca ewolucja technologiczna umożliwia tworzenie nowych usług i nowych zastosowań w oparciu o wykorzystywanie, agregację lub łączenie danych. Przepisy pierwotnie przyjęte w 2003 r. i zmienione w 2013 r. nie dotrzymują już kroku tym szybkim zmianom, co grozi utratą możliwości gospodarczych i społecznych, jakie oferuje ponowne wykorzystywanie danych publicznych. Informacje sektora publicznego lub informacje gromadzone, produkowane, reprodukowane i rozpowszechniane przy okazji wykonywania zadań publicznych lub świadczenia usług w interesie ogólnym są ważnym materiałem wyjściowym dla produktów i usług związanych z treściami cyfrowymi, a wraz z rozwojem zaawansowanych technologii cyfrowych, takich jak sztuczna inteligencja, technologie rozproszonego rejestru i Internet rzeczy, i staną się jeszcze ważniejszym ich zasobem. Zasadnicze znaczenie będzie mieć w tym kontekście także szeroki transgraniczny zasięg geograficzny (zob. motyw 13 dyrektywy 2019/1024).

Nie wyprzedzając dalszych rozważań wyrazem zmiany podejścia prawodawcy UE jest nie tylko poszerzanie zakresu ponownego wykorzystywania o nowe zasoby (dane badawcze) czy o nowe podmioty wykraczające poza krąg organów sektora publicznego (przedsiębiorstwa publiczne), ale wyeksponowanie znaczenia zautomatyzowanej dystrybucji danych do ponownego wykorzystywania za pomocą interfejsów programowania aplikacji (API), w tym nowych kategorii informacji sektora publicznego, tj. danych dynamicznych i danych o wysokiej wartości, w których w szczególności upatruje się najwyższego potencjału dla innowacyjnego dalszego użycia w produktach, usługach czy aplikacjach. Symbolem nowego podejścia jest

[67] Szerzej na temat gospodarczego oddziaływania otwartych danych zob. The Economic Impact of Open Data Opportunities for value creation in Europe, European Data Porta2020. https://www.europeandataportal.eu/sites/default/files/the-economic-impact-of-open-data.pdf (dostęp: 4.08.2020).

wreszcie wyodrębnienie spośród informacji sektora publicznego otwartych danych i wyeksponowanie pojęcia w zmienionym tytule dyrektywy.

Kolejny przełom dla znaczenia ponownego wykorzystywania informacji sektora publicznego na rynku wewnętrznym nastąpił w lutym 2019 r. wraz ogłoszeniem przez Komisję Europejską Europejskiej strategii w zakresie danych[68] oraz zapowiedzią utworzenia jednolitego rynku danych w UE. Zwiększenie dostępnego wolumenu danych jest postrzegane przez twórców Strategii jako szczególnie istotne z punktu widzenia nowych, opartych na danych technologiach jak sztuczna inteligencja czy Internet rzeczy. Stąd wynika też powiązanie Europejskiej strategii z Białą Księgą w sprawie sztucznej inteligencji (COM(2020)65). Oba komplementarne wobec siebie dokumenty tworzą pierwszy filar szerszej tworzonej przez obecną Komisję Europejską polityki cyfrowej UE. Podkreśla się, że sztuczna inteligencja to jedno z najważniejszych zastosowań gospodarki opartej na danych. Sztuczna inteligencja to zbiór technologii łączących dane, algorytmy i moc obliczeniową. Główną siłą napędową obecnego rozwoju sztucznej inteligencji są postępy w dziedzinie obliczeń i coraz większa dostępność danych[69]. Z kolei Internet rzeczy to sieć łącząca przewodowo lub bezprzewodowo urządzenia charakteryzujące się autonomicznym (niewymagającym zaangażowania człowieka) działaniem w zakresie pozyskiwania, udostępniania, przetwarzania danych lub wchodzenia w interakcje z otoczeniem pod wpływem tych danych. Jest to koncepcja budowy sieci telekomunikacyjnych i systemów informatycznych o wysokim stopniu rozproszenia, które służyć mogą między innymi tworzeniu inteligentnych systemów kontrolnopomiarowych, analitycznych, czy układów sterowania, praktycznie w każdej dziedzinie życia, gospodarki czy nauki[70]. Dostęp do danych nie stanowi istoty funkcjonowania tych systemów informacyjnych, ale warunek konieczny ich działania, który dla którego z kolei podstawą pozostaje działanie algorytmów nieznanych przeciętnemu użytkownikowi, które przekształcają informację wejściową zebraną przez czujniki w informację wyjściową[71].

Bez danych rozwój sztucznej inteligencji, Internetu rzeczy i innych zastosowań cyfrowych nie jest możliwy.

Stąd też poprawa dostępności do danych w celu dalszej ich eksploatacji i zarządzania nimi jest kwestią o zasadniczym znaczeniu. Wspólne europejskie zasady funkcjonowania

[68] Komunikat Komisji do Parlamentu Europejskiego i Rady Europejska strategia w zakresie danych COM(2020) 66 z 19.2.2020 r.
[69] Białą Księgą w sprawie sztucznej inteligencji, s. 2.
[70] IoT w polskiej gospodarce, Ministerstwo Cyfryzacji 2018, https://www.gov.pl/web/cyfryzacja/polska-przyszlosci-to-polska-z-internetem-rzeczy (dostęp: 04.08.2020).
[71] Zob. szerzej: *W.R. Wiewiórowski*, Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach *big data*, s. 15.

jednolitego rynku oraz skuteczne mechanizmy ich egzekucji zagwarantują swobodny przepływ danych w ramach EU oraz miedzy sektorami, przestrzeganie europejskich zasad i wartości dotyczących m.in. ochrony konsumentów, prywatności, prawa konkurencji, niedyskryminacyjny, równy dla wszystkich, oparty o jasne i funkcjonalne zasady dostępu do danych[72]. Aby to osiągnąć, Komisja w Strategii w zakresie danych potwierdziła, że zaproponuje, po pierwsze, ustanowienie właściwych ram regulacyjnych dotyczących zarządzania danymi, dostępu do nich i ich ponownego wykorzystania między przedsiębiorstwami (*business-to-business – B2B – data-sharing*), między przedsiębiorstwami a administracją publiczną (*business-to-government – B2G – data sharing*) oraz w ramach administracji (*sharing of data between public authorities*). Oznacza to również szersze udostępnienie danych sektora publicznego poprzez otwarcie zbiorów danych o wysokiej wartości w całej Unii Europejskiej i umożliwienie ich ponownego wykorzystania (*government-to-business – G2B – data sharing*). W ramach tej części Europejskiej strategii w zakresie danych Komisja zaproponuje ramy regulacyjne dla wspólnych europejskich przestrzeni danych[73], przyjmie akt wykonawczy dotyczący danych wysokiej jakości, o którym mowa w dyrektywie 2019/1024 oraz zaproponuje w 2021 r. horyzontalny akt o danych (*Data Act*).

Ponowne wykorzystywanie informacji sektora publicznego jest podstawowym instrumentem dla wymiany danych w relacji *G2B*. Niemniej mechanizm ten może być wykorzystany również dla wymiany danych zarówno w relacji pomiędzy przedsiębiorcami (podmiotami prywatnymi) *B2B*, jak przekazywaniu danych z sektora prywatnego do publicznego, tj. *B2G*[74]. Jako przykład szerszego udostępniania danych będących w posiadaniu podmiotów prywatnych podać można rozwiązania przyjęte we Francji. Francuski ustawodawca przyjął daleko idące rozwiązania legislacyjne, które zakładają szerokie dzielenie się danymi nie tylko przez podmioty publiczne ale i prywatne. Ustawa nr 2015-1779 z 2015 r.[75] oraz ustawa

[72] W tym ostatnim przypadku nie chodzi o dostęp rozumiany jako dostęp do informacji publicznej, który nie podlega harmonizacji jako kompetencją wyłączną państw członkowskich.
[73] 25 listopada 2020 r. Komisja opublikowała pierwszy z zapowiedzianych wniosków legislacyjnych, tj. Proposal for a Regulation Of The European Parliament And Of The Council on European data governance (Data Governance Act) COM(2020) 767 final.
[74] Zob. szerzej na temat wymiany danych *C. Arnaut, M. Pont, E. Scaria, A. Berghmans, S. Leconte*, Study on data sharing between companies in Europe. Final report, European Commission DG Communications Networks, Content & Technology, 2018.
https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en
[75] Loi relative à la gratuité et aux modalités de la réutilisation des information du secteur public https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000031701525/

nr 2016-1321 z 2016 r.[76] (dalej*: Loi numerique*) wprowadziły zasadę domyślnej bezpłatności oraz zasadę domyślnej otwartości. *Loi numerique* wprowadza pojęcie danych mających znaczenie dla interesu ogólnego (*données d'intérêt général*), które muszą być udostępniane zarówno przez podmioty publiczne jak i prywatne. Kategorie tych danych obejmują: dane dotyczące wykonywania usług publicznych (w transporcie, gospodarce wodnej, gospodarowaniu odpadami itp.), dane dot. produkcji i konsumpcji energii elektrycznej i gazu, a także takie rodzaje danych jak dane dotyczące zamówień publicznych i koncesji, dane powstałe podczas wykonywania umowy koncesji, dane dotyczące dotacji publicznych oraz dane niezbędne do oficjalnych statystyk. Wszystkie podmioty prywatne, które są w posiadaniu ww. kategorii i rodzajów danych, są zobowiązane, na równi z podmiotami publicznymi, do ich udostępniania do ponownego wykorzystywania, bezpłatnie i w otwartym formacie.

Konkludując, znaczenie instytucji ponownego wykorzystywania informacji sektora publicznego na przestrzeni 17 lat obowiązywania przepisów ewoluowało w kierunku nadawania jej coraz istotniejszej roli na rynku wewnętrznym Unii Europejskiej. Wraz z ustanowieniem jednolitego rynku cyfrowego ponowne wykorzystywanie informacji sektora publicznego obok przepisów ogólnego rozporządzenia o ochronie danych osobowych oraz rozporządzenia w sprawie swobodnego przepływu danych nieosobowych pozostaje jednym z głównych instrumentów prawnych służących budowie gospodarki cyfrowej UE. Razem z zapowiedzią utworzenia jednolitego rynku danych Unii Europejskiej rola ponownego wykorzystywania informacji sektora publicznego będzie nabierać na znaczeniu. Jest to związane z wzrostem wolumenu danych oraz wartością rynku danych, w tym danych otwartych. Ponowne wykorzystywanie informacji sektora publicznego odgrywać będzie ważną rolę w rozwoju nowych technologii wykorzystujących i przetwarzających dane, jak sztuczna inteligencja czy Internet rzeczy. Rozwiązania legislacyjne znane z prawa ponownego wykorzystywania informacji sektora publicznego mogą stanowić podstawę zapowiedzianych przez Komisję instrumentów legislacyjnych w obszarze europejskich przestrzeni danych, jak i wymiany danych pomiędzy podmiotami o różnym statusie.

[76] Loi pour une République numérique
https://www.legifrance.gouv.fr/dossierlegislatif/JORFDOLE000031589829/

1.4. Ponowne wykorzystywanie informacji sektora publicznego a dostęp do dokumentów urzędowych i informacji publicznej

W literaturze podkreśla się na konieczność rozdzielania bliskich sobie, lecz nie identycznych praw: dostępu, czyli możliwości żądania, zdobycia (otrzymania), rozpowszechniania informacji publicznych i ponownego – komercyjnego lub niekomercyjnego – wykorzystywania informacji[77]. Aby zrozumieć różnicę pomiędzy realizacją prawa dostępu do informacji sektora publicznego (*access to public sector information*), a dalszą eksploatacją informacji pozyskanych w ten sposób (*re-use of public sector information*), konieczne jest najpierw ustalenie znaczenia pierwotnego uprawnienia, tj. dostępu do informacji.

Prawo do informacji postrzegane jest jako jedno z podstawowych praw politycznych oraz prawo człowieka. Prawo to stanowi istotny składnik demokratycznego otwartego rządu oraz otwartości organów władz publicznych. Prawo do informacji obejmuje przede wszystkim dostęp do dokumentów publicznych. Podstawą otwartości jest jawność organizacji i działalności instytucji publicznych wobec wszystkich zainteresowanych.[78] Historycznie prawo do informacji po raz pierwszy zostało sformułowane w Szwecji w XVIII w. Ustawodawstwo w tym zakresie zaczęło się jednak rozwijać w II. poł. XX w., poczynając od amerykańskiej *Freedom od Information Act* z 1966 r. (po tzw. aferze Watergate), poprzez ustawy francuskie (1979), regulacje w Australii i Nowej Zelandii (1982), Kanady (1983)[79].

Trzeba jednak wspomnieć, że tradycyjnie – zwłaszcza na kontynencie europejskim – w przeszłości zasadą działania władz publicznych i administracji był brak jawności działania i w konsekwencji brak mechanizmów obywatelskiej kontroli działalności władzy i aparatu państwowego. To co robiła administracja poza jej „produktami zewnętrznymi" było niedostępną dla obywateli *res interna,* co odpowiadało podstawowemu celu administracji jakim był służenie wykonywania imperium państwowego.[80]

Współcześnie owej „zamkniętości" działań państwa i jego struktur przeciwstawia się postulat transparentności i otwartości, który jest możliwy do osiągnięcia dzięki gwarancji prawa do informacji. W doktrynie ponadto wskazuje się, iż celem wprowadzenia prawa do informacji jest realizacja idei jawności życia publicznego[81]. Z kolei cele, którym ma służyć

[77] *T. Górzyńska*, Prawna regulacja, s. 242.
[78] *H. Izdebski, M. Kulesza,* Administracja publiczna – zagadnienia ogólne, Warszawa 2004, s.323.
[79] *Ibidem*.
[80] *H. Izdebski H., M. Kulesza*, s. 327.
[81] Na temat zasady jawności zob. szerzej: *T. Górzyńska*, Prawo do informacji i zasada jawności administracyjnej, Warszawa 1999 r.

urzeczywistnianie w życiu społecznym wartości jaką jest jawność życia publicznego, można w sposób pogrupować je w cztery podstawowe kategorie: 1) demokratyzacja życia publicznego; 2) dążenie do wzrostu zaufania społecznego do władzy publicznej, 3) walka z korupcją; 4) sprawne funkcjonowanie administracji publicznej[82].

Prawo do informacji występuje w aktach organizacji międzynarodowych, jak Europejska Karta Praw Człowieka[83] (art. 10) czy w prawodawstwie Unii Europejskiej, zarówno w źródłach prawa pierwotnego, jak i pochodnego.

Regulacje dotyczące informacji publicznej zawarte w regulacjach Unii Europejskiej dotyczą przede wszystkim dokumentów wytworzonych i gromadzonych przez instytucje UE. Już na wstępie należy zaznaczyć, iż regulacje te nie operują pojęciem informacji publicznej, a pojęciem dokumentu.

Podstawowe znaczenie dla prawa dostępu do informacji miał Traktat z Amsterdamu z 1997 r.[84], który ustanowił prawo dostępu do dokumentów. Wejście w życie tej regulacji poprzedzone było długim okresem, w którym dostęp do informacji o działaniu struktur UE był znacznie ograniczony[85]. Szczegółowe postanowienia o publicznym dostępie do dokumentów instytucji znalazły się w art. 255 Traktatu WE. Artykuł ten – na mocy traktatu lizbońskiego – został artykułem 15 ust. 3 Traktatu o funkcjonowaniu Unii Europejskiej[86], zgodnie z którym każdy obywatel Unii i każda osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę statutową w Państwie Członkowskim ma prawo dostępu do dokumentów instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy.

Artykuł 15 TFUE dał podstawę prawną rozporządzeniu (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[87]. Przepisy te mają odpowiednio zastosowanie także do dokumentów Rady Europejskiej, co stwierdzono w art. 10 ust. 2 regulaminu wewnętrznego Rady Europejskiej[88].

---

[82] *A. Piskorz-Ryń*, Nadużywanie prawa do informacji publicznej, uwagi de lege lata i de lege ferenda, „Kontrola Państwowa" 2008, nr 6, s. 39. Zob. na temat m.in. *T. Górzyńska*, Prawo do informacji, *op. cit.*; *J. Stefanowicz*, Idee leżące u podstaw prawa dostępu do informacji publicznej [w:] *H. Izdebski* (red.) Dostęp do informacji publicznej. Wdrażanie ustawy, Warszawa 2001.

[83] Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 4 listopada 1950 r.; dalej: EKPC.

[84] Dz. Urz. UE C 340 z 10.11.1997, str. 1—144

[85] *G. Rydlewski, Szustakiewicz P., K. Golat*, Udzielanie informacji publicznej przez administracje publiczną. Teoria i praktyka, Warszawa 2012, s. 35.

[86] Dz. Urz. UE C 115/47 z 9.5.2008; dalej: TFUE.

[87] Dz. Urz. UE L 145/43 z 31.05.2001; dalej: rozporządzenie 1049/2001.

[88] Regulamin wewnętrzny Rady Unii Europejskiej przyjęty Decyzją Rady z dnia 1 grudnia 2009 r. (OJ L 325, 11.12.2009, s. 35–35).

Normatywną klamrą spinającą powyższe regulacje dotyczące prawa do informacji jest Karta Praw Podstawowych Unii Europejskiej[89]. Zgodnie z jej art. 42 każdy obywatel UE i każda osoba fizyczna lub prawna zamieszkała lub mająca siedzibę zarejestrowaną w państwie członkowskim ma prawo dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji.

Prawo do informacji jako prawo podmiotowe zostało wyrażone w art. 61 Konstytucji RP. Zgodnie z jego brzmieniem obywatel ma prawo do uzyskiwania informacji o działalności organów władzy publicznej oraz osób pełniących funkcje publiczne. Prawo to obejmuje również uzyskiwanie informacji o działalności organów samorządu gospodarczego i zawodowego a także innych osób oraz jednostek organizacyjnych w zakresie, w jakim wykonują one zadania władzy publicznej i gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa. Prawo do uzyskiwania informacji obejmuje dostęp do dokumentów oraz wstęp na posiedzenia kolegialnych organów władzy publicznej pochodzących z powszechnych wyborów, z możliwością rejestracji dźwięku lub obrazu.

Prawo to nie ma charakteru bezwzględnego, podlega ograniczeniom ze względu na ochronę wolności i praw innych osób, podmiotów gospodarczych oraz ochronę porządku publicznego, bezpieczeństwa lub ważnego interesu gospodarczego państwa. Ograniczenie to może wystąpić wyłącznie w formie ustawy (art. 61 ust. 3). Dla wprowadzenia regulacji ustawowej zmierzającej do ograniczenia prawa do informacji muszą być spełnione wymagania proporcjonalności, określone w art. 31 ust. 3 Konstytucji.

Ustawodawca, formułując w Konstytucji RP zasadę "prawa do informacji", wyznaczył tym samym podstawowe reguły wykładni tego uprawnienia. Jeżeli bowiem stanowi ono prawo konstytucyjne, to ustawy określające tryb dostępu do informacji powinny być interpretowane w taki sposób, aby gwarantować szerokie uprawnienia w tym zakresie, a wszelkie wyjątki od tej reguły powinny być rozumiane wąsko. Oznacza to stosowanie w odniesieniu do tych ustaw takich zasad wykładni, które sprzyjają poszerzaniu, a nie zawężaniu obowiązku informacyjnego[90].

Norma konstytucyjna wyznacza zatem zakres materialny oraz granice prawa do informacji, lecz nie został uregulowany tryb udzielania informacji (ust. 4). Ten uregulowany jest w ustawach szczegółowych, w tym ustawie fundamentalnej dla realizacji prawa do informacji, czyli ustawie z dnia 6 września 2001 r. o dostępie do informacji publicznej[91].

[89] Karta Praw Podstawowych Unii Europejskiej (2016/C 202/02) (Dz.Urz. UE C 326 z 26.10.2012, str. 391-407); dalej: KPPUE.
[90] Zob. wyrok NSA z 14.11.2003 r., II SAB 199/03.
[91] t.j. Dz. U. z 2020 r. poz. 2176.

Korelatem prawa do informacji jest spoczywający w pierwszym rzędzie na organach władzy publicznej obowiązek udzielania obywatelom określonych informacji o działalności instytucji. Obowiązek ten polega zatem nie tyle na dostępności określonych informacji dla odbiorcy, ale przynajmniej co do zasady oznacza konieczność aktywnego działania ze strony organu udzielającego informacji, które polega na dostarczeniu osobie zainteresowanej na jej żądanie pewnego zakresu informacji. Informacja powinna być związana z działalnością publiczną[92].

Wyrażone w art. 61 Konstytucji, prawo do informacji zawiera w swej treści uprawnienie do żądania informacji o funkcjonowaniu instytucji publicznych, przede wszystkim zaś instytucji władzy publicznej. Chodzi np. o informacje dotyczące istniejących w ramach danej instytucji procedur i wyznaczanych zadań, procesie ich realizacji oraz inwestycjach czy organizowanych przetargach[93]. Na gruncie tego przepisu – zdaniem TK - Konstytucji nie można przynajmniej *prima facie* wykluczyć, że realizacja prawa do informacji będzie dotykała pośrednio nie tylko działalności publicznej osób publicznych, co jest oczywiste wówczas, gdy jest to działalność wykonywana w ramach i w bezpośrednim związku z funkcjonowaniem określonej instytucji publicznej, ale również sfery z pogranicza ich życia publicznego i prywatnego. Wydaje się jednak, że nie można z góry wykluczyć objęcia tej sfery zakresem konstytucyjnego prawa do informacji, bez zbadania, czy i w jakim zakresie ingerencja taka nie jest usprawiedliwiona na gruncie innych norm konstytucyjnych.

Trybunał w wyroku w sprawie K 17/05 określił zakres prawa do informacji, który ma istotne znaczenie dla zdefiniowania pojęcia informacji publicznej. Zakres prawa do informacji o działalności organów władzy publicznej i osób pełniących funkcje publiczne obejmuje:
- informacje, których natura i charakter może naruszać interesy i prawa innych osób, nie mogą wykraczać poza niezbędność określoną potrzebą transparentności życia publicznego, ocenianą zgodnie ze standardami przyjętymi w demokratycznym państwie;
- muszą to być zawsze informacje mające znaczenie dla oceny funkcjonowania instytucji oraz osób pełniących funkcje publiczne;
- nie mogą to być informacje – co do swej natury i zakresu – przekreślające sens (istotę) ochrony prawa do życia prywatnego.

W wyroku z 31 maja 2004 r., OSK 205/04 NSA wskazał, że regulacja ta wynika z zasady udziału obywateli w życiu publicznym i sprawowania społecznej kontroli. W celu realizacji tej zasady obywatel ma prawo uzyskania wiedzy o sprawach publicznych. Prawo do

[92] Wyrok TK z 20.03.2006 r., K 17/05.
[93] *Ibidem*.

uzyskania takiej wiedzy w postaci prawa dostępu do informacji nie obejmuje nośników tej informacji, czyli form w jakich ta informacja występuje, np. dokumentów, które są zasadniczymi nośnikami informacji. Wobec tego prawo wglądu do dokumentu oznacza prawo do dysponowania czy zapoznania się z jego treścią a nie prawo do dysponowania samy dokumentem.

Z treści art. 61 Konstytucji wynika podmiotowo - przedmiotowy charakter informacji publicznej. Przedmiotem informacji publicznej w odniesieniu do organów władzy publicznej i osób pełniących funkcje publiczne jest ich działalność. Prawo pozyskiwania informacji od pozostałych podmiotów wymienionych w art. 61 ogranicza się wyłącznie do ich działalności w zakresie w jakim wykonują zadania publiczne lub gospodarują majątkiem komunalnym lub majątkiem Skarbu Państwa. Taka wykładnia prawa do informacji i definicji informacji publicznej na gruncie art. 61 Konstytucji determinuje definicję tego pojęcia na gruncie przepisów o dostępie do informacji publicznej. Ma to szczególnie istotne znaczenie w kontekście próby określenia zakresu znaczeniowego pojęcia informacji sektora publicznego, na gruncie przepisów prawa UE oraz krajowych. Wzajemne relacje pomiędzy pojęciem informacji publicznej oraz pojęcia informacji sektora publicznego zostały omówione w Rozdziale 2.

Podstawowe zasady realizacji prawa do informacji zostały określone w ustawie zasadniczej. Cztery lata po jej uchwaleniu przyjęta została ustawa z 6 września 2001 r. o dostępie do informacji publicznej[94], która weszła w życie 1 stycznia 2002 r. Stanowi ona konkretyzację obywatelskiego prawa, o którym mowa w art. 61. Ustawa określa w sposób szczegółowy procedurę i formę prawną udzielania informacji publicznej oraz odmowy jej udzielenia, wskazuje procedurę odwoławczą, a także wymieniania także organy na których ciąży obowiązek informacyjny.

Zwraca się uwagę, że ustawodawca wyszedł poza zakres podmiotowy i przedmiotowy art. 61 Konstytucji, ustawa wiąże bowiem nie tylko organy władzy publicznej, ale co może budzić wątpliwości konstytucyjne, ale także związki zawodowe i ich organizacje oraz partie polityczne. Z drugiej strony zagwarantował prawo o znacznie szerszym zakresie niż zostało to przyjęte w innych państwach, obejmuje ono dostęp nie tylko do dokumentów urzędowych i wymienionych w art. 61 Konstytucji wstępu na posiedzenia kolegialnych organów jednostek samorządu terytorialnego pochodzących z powszechnych wyborów, ale i innych kategorii informacji o sprawach publicznych[95].

[94] Dz.U. 2001 nr 112 poz. 1198 z późń. zm.; dalej: UDIP.
[95] *H. Izdebski, M. Kulesza,* op. cit., s. 326.

Ustawa od początku obowiązywania wzbudzała liczne kontrowersje. Dotyczyły one przede wszystkim dwóch kwestii fundamentalnych, tj. definicji informacji publicznej (o czym mowa będzie w kolejnym rozdziale) oraz normy kolizyjnej wymienionej w art. 1 ust. 2 UDIP. Zgodnie z tym przepisem przepisy UDIP nie naruszają przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi. Doktryna negatywne ocenia przyjęte założenie, którego konsekwencją jest to, że UDIP, nie jest ustawą tzw. „matką", czyli ustawą organiczną, która w wyczerpujący, horyzontalny sposób regulowałaby zasady i wyjątki od niej[96]. Wprost przeciwnie, wprowadzona została wymieniona norma kolizyjna, której konsekwencją jest to, iż dostęp do informacji publicznych regulowany jest w wielu różnych aktach normatywnych, przy czym tajemnice prawnie chronione, które ograniczają prawo dostępu do informacji uregulowane były w momencie jej uchwalenia w ponad 250 aktach[97]. Rozproszenie regulacji określających własne tryby dostępu do informacji niewątpliwie utrudnia realizację konstytucyjnego prawa do informacji. Należy zatem uznać UDIP za ustawę ustrojową, która nie realizuje w pełni uprzednio zakładanego celu jej uchwalenia, czyli systemowego określenia ram prawnych obowiązku informacyjnego oraz zasady dostępu do informacji publicznej.

Od zdefiniowanego pojęcia prawa do informacji należy odróżnić prawo do ponownego wykorzystywania informacji sektora publicznego. Rozróżnienia dwóch powiązanych ze sobą uprawnień można dokonać na kilka płaszczyznach.

Jak wskazano wcześniej, prawo do ponownego wykorzystywania informacji sektora publicznego jest prawem „pokrewnym" dostępowi do informacji publicznej, realizuje jednak odmienne cele[98]. Podczas gdy celem prawa dostępu do informacji jest, uogólniając, demokratyzacja życia publicznego, to w ponownym wykorzystywaniu akcentuje się użytkowy charakter informacji realizujący cele ekonomiczne i pozaekonomiczne, decydującą rolę

[96] *I. Kamińska, M. Rozbicka-Ostrowska*, Ustawa o dostępie do informacji publicznej. Komentarz, Warszawa 2012, s. 9.
[97] *Ibidem.*
[98] W doktrynie wyrażony był również pogląd, że przepisy UDIP pozostawały skuteczne dla realizacji ponownego wykorzystywania przez co nie było konieczności implementacji dyrektywy 2003/98/WE do krajowego porządku prawnego (zob. *D. Adamski, M. Bernaczyk,* Znaczenie dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego, „Elektroniczna Administracja", marzec-kwiecień 2006, s. 3 i nast.). Argumentacja nie została podzielona przez Komisję Europejską, która złożyła skargę do TSUE przeciwko Rzeczpospolitej Polskiej w sprawie uchybienia zobowiązaniom państwa członkowskiego polegającą na braku transpozycji dyrektywy 2003/98/WE. Wyrokiem TSUE Polska została zobowiązana do transpozycji przepisów dyrektywy (zob. wyrok TSUE z dnia 27 października 2011 r. w sprawie C-362/10).

odgrywają pierwsze z nich[99], choć nie można również bagatelizować skutków pozaekonomicznych.

Źródeł prawa dostępu do informacji, o czym pisałem wyżej, należy poszukiwać w aktach prawa podstawowego. Prawo to zakotwiczone jest źródłach prawa pierwotnego Unii Europejskiej, wreszcie znajduje swoje podstawy w Konstytucji. Z kolei prawo do ponownego wykorzystywania informacji sektora publicznego zostało sformułowane w prawie pochodnych UE. Obowiązek jego harmonizacji oparto na odrębnych od reżimu dostępowego regulacjach (materialnych i proceduralnych) ponownego wykorzystywania, chociaż te dwa rodzaje przepisów pozostają ze sobą powiązane. Natomiast harmonizacji nie podlegają przepisy dotyczące dostępu do informacji (dostępu do dokumentów publicznych), które (jako stanowiące realizację prawa do informacji) pozostawiono w kompetencji wyłącznej prawodawcy krajowego.

Prawodawca UE dokonał wyraźnego rozróżnienia pomiędzy oba prawami. Reguły określone w dyrektywie 2003/98/WE podkreślają specyfikę i odrębność instytucji ponownego wykorzystywania od procedury dostępu. O ile ponowne wykorzystywanie dokumentów wymaga uprzedniego dostępu do nich, o tyle procesy te pozostają odmienne[100].

W obecnym stanie prawnym dostęp do informacji i ponowne wykorzystywanie są wyodrębnione względem siebie (przedmiotowo i podmiotowo), ale równocześnie pozostają w określonej relacji. Ustalenia tej relacji dokonał sam prawodawca unijny tworząc *quasi* kolizyjną normę w art. 1 ust. 3 dyrektywy 2003/98/WE (powtórzonej w dyrektywie 2019/1024), który stanowi, iż „niniejsza dyrektywa opiera się na i jest bez uszczerbku dla istniejących w Państwach Członkowskich systemów dostępu". Zwrot „opiera się" można w tym przypadku tłumaczyć w ten sposób, iż wykorzystywana może być jedynie taka informacja, która na podstawie przepisów o dostępie do informacji publicznej jest jawna (nie każda informacja publiczna jest jawna, ponieważ zachodzą ustawowe przesłanki ograniczające jawność)[101].

Inaczej ujmując, pierwotną regulacją prawną jest „system dostępu". Natomiast przedmiotem ponownego wykorzystania jest wtórna eksploatacja informacji (jawnej i dostępnej), w szczególności w celach komercyjnych, co ma szczególne znaczenie, gdy

[99] Zob. *A. Piskorz-Ryń*, Prawo dostępu do informacji a ponowne wykorzystywanie informacji sektora publicznego – glosa do wyroku TS z 27.10.2011 r., C-362/10, Komisja Europejska przeciwko Polsce, „Europejski Przegląd Sądowy" 2015, nr 5.
[100] Zob. wyrok TSUE z 27.10.2011 r., C-362/10.
[101] *G. Sibiga*, Ponowne wykorzystanie informacji sektora publicznego – stan obecny i perspektywy rozwoju. Wybrane zagadnienia, s. 117.

informacje funkcjonują jako utwór lub baza danych, chronione prawami własności intelektualnej.

Jednak podstawowym mankamentem konstrukcji „oparcia" jednego uprawnienia o drugie pozostaje odmienny zakres znaczeniowy pojęć „dokument" i „informacja sektora publicznego" oraz „informacja publiczna". Ostatnie z tych pojęć nie odnosi się do całości informacji znajdujących się w posiadaniu podmiotu zobowiązanego, pomimo że to reżim dostępowy ma być pierwotnym wobec ponownego wykorzystywania, na nim opiera się bowiem wykorzystywanie[102] (o różnicach między tymi pojęciami zob. Rozdział 3).

Przepisy dotyczące ponownego wykorzystania nie mogą naruszać samego prawa dostępu, co znajduje potwierdzenie w przepisach UPW. Po pierwsze, zgodnie z art. 7 ust. 1 UPW przepisy ustawy nie naruszają prawa dostępu do informacji publicznej ani wolności jej rozpowszechniania, ani przepisów innych ustaw określających zasady, warunki i tryb dostępu lub ponownego wykorzystywania informacji będących informacjami sektora publicznego. Po drugie, art. 6 ust. 3 UPW stanowi, że prawo do ponownego wykorzystywania podlega ograniczeniu w zakresie informacji będących informacjami sektora publicznego, do których dostęp jest ograniczony na podstawie innych ustaw. Przepisy o ponownym wykorzystywaniu informacji sektora publicznego przyznają więc pierwszeństwo przepisom „dostępowym" w tym UDIP w sytuacji, w której przewidują one ograniczenia w dostępności informacji i inne odstępstwa od ogólnych reguł wyznaczonych przepisami UPW.

1.5. Źródła ponownego wykorzystywania informacji sektora publicznego

Źródeł prawa do ponownego wykorzystywania informacji sektora publicznego należy poszukiwać w aktach prawa UE oraz stanowiących ich implementację przepisach krajowych rangi ustawowej. Jest to bowiem prawo silnie zdeterminowane przez unijne prawo pochodne w postaci dyrektyw oraz przepisów prawa miękkiego w formie Wytycznych Komisji Europejskiej[103].

Ponowne wykorzystywanie informacji sektora publicznego, jak zostało wcześniej wyjaśnione, można uznać za pokrewne do prawa dostępu do informacji publicznej, którego standard wyznacza art. 61 Konstytucji. W doktrynie prezentowany jest pogląd, że podstaw

[102] *Ibidem*, s. 118.
[103] Zob. Obwieszczenie Komisji z 24.7.2014 r. Wytyczne w sprawie zalecanych licencji standardowych, zbiorów danych i opłat za ponowne wykorzystanie dokumentów (2014/C 240/01) (Dz. Urz. UE C 240/1). Wytyczne te w odniesieniu do zalecanych licencji omówione zostaną dalej.

konstytucyjnych ponownego wykorzystywania należy upatrywać w wolności rozpowszechniania informacji na podstawie art. 54 ustawy zasadniczej[104]. W rozprawie przyjęto pogląd o odrębności prawa do ponownego wykorzystywania od prawa dostępu do informacji czy wolności rozpowszechniania.

1.5.1. Dyrektywa 2003/98/WE

Dyrektywa 2003/98/WE zakładała minimalną harmonizację reguł i praktyk krajowych dotyczących ponownego wykorzystywania dokumentów sektora publicznego. Prawodawca UE dostrzegł potrzebę wyznaczenia ogólnych ram dla warunków regulujących ponowne wykorzystywanie dokumentów sektora publicznego w celu zapewnienia uczciwych, proporcjonalnych i niedyskryminacyjnych warunków wykorzystywania tych informacji. Z perspektywy 13 lat od uchwalenia dyrektywy można uznać ją za rozwiązanie dość zachowawcze. Akt ten nie zawierał żadnego zobowiązania, aby zezwalać na ponowne wykorzystywanie dokumentów. Organy sektora publicznego mogły podejmować dyskrecjonalną decyzję o wydaniu lub niewydaniu zgody na ich ponowne wykorzystywanie. Nie zostało zatem sformułowane prawo do ponownego wykorzystywania, którego korelatem po stronie organów sektora publicznego byłby obowiązek udostępniania do ponownego wykorzystywania dokumentów. Organy sektora publicznego zgodnie z treścią dyrektywy powinny udostępniać dokumenty w ich istniejącym formacie lub języku, przy wykorzystaniu środków elektronicznych tylko tam gdzie jest to możliwe i właściwe. Również możliwość pobierania opłat przez organy sektora publicznego była dość szeroka. Całkowity dochód mógł obejmować koszty zbierania, produkowania, reprodukowania i rozpowszechniania dokumentów, wraz z rozsądnym zyskiem z inwestycji, ze względu na wymagania samofinansowania zainteresowanego organu sektora publicznego, tam gdzie to jest stosowne.

Z drugiej zaś strony dyrektywa wprowadziła po raz pierwszy do obrotu prawnego definicję ponownego wykorzystywania, które oznacza wykorzystywanie przez osoby fizyczne lub prawne dokumentów będących w posiadaniu organów sektora publicznego, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla których te dokumenty zostały wyprodukowane. Ponownym wykorzystywaniem nie jest wymiana dokumentów między organami sektora publicznego

[104] Zob. *A. Syryt*, Konstytucyjne uwarunkowania ponownego wykorzystywania informacji sektora publicznego [w:] *A. Piskorz-Ryń (red.),* Dostęp i wykorzystywanie, *G. Szpor (red.),* Jawność i jej ograniczenia. Tom V, Warszawa 2015, s. 185-199 i przywołana tam literatura.

wyłącznie w wykonaniu ich zadań publicznych. Definicja ta do dziś budzi wiele wątpliwości interpretacyjnych, w szczególności w praktyce trudno jest wyznaczyć jednoznaczne rozróżnienie pomiędzy ponowny wykorzystywaniem a dostępem do informacji. Zakres przedmiotowy dyrektywy wyznaczało z kolei pojęcie informacji sektora publicznego. Posłużono się tutaj występującą już chociażby w rozporządzeniu (WE) NR 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji definicją dokumentu, którym jest jakakolwiek treść niezależnie od zastosowanego nośnika (zapisaną na papierze lub zapisaną w formie elektronicznej lub zarejestrowaną w formie dźwiękowej, wizualnej albo audiowizualnej).

Dyrektywa powinna była zostać wdrożona do krajowego porządku prawnego do dnia 1 lipca 2005 r., ale Polska była ostatnim państwem UE, który wykonał tą dyrektywę, a stało się to dopiero w drugiej połowie 2011 r.

1.5.2. Dyrektywa 2013/37/UE

Kolejnym krokiem zmierzającym do pogłębienia harmonizacji krajowych przepisów o ponownym wykorzystywaniu był opublikowany przez Komisję Europejską Komunikat Otwarte dane – siła napędowa innowacji, wzrostu gospodarczego oraz przejrzystego zarządzania. Komunikat ten to jeden z trzech dokumentów opublikowanych przez Komisję Europejską w dn. 12 grudnia 2011r. w ramach pakietu *Open Data Package*, który zakłada lepsze wykorzystanie potencjału zasobów publicznych dla wzrostu konkurencyjności i innowacyjności gospodarki europejskiej[105].

W Komunikacie podkreślono, iż działania te koncentrują się na obszarach, w których funkcjonowanie rynku wewnętrznego ma duże znaczenie oraz w przypadku których wspólne standardy i rozwiązania przyczynią się do powstania nowych, lepszych usług i produktów informacyjnych dla europejskich konsumentów.

Wraz z Komunikatem opublikowany został projekt tzw. drugiej dyrektywy *re-use*, czyli projekt zmieniający dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania

[105] Komunikat z 12.12.2011 Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów Otwarte dane – siła napędowa innowacji, wzrostu gospodarczego oraz przejrzystego zarządzania, KOM(2011) 882.
https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:52011DC0882&from=EN

informacji sektora publicznego. Projekt ostatecznie został w dniu 26 czerwca 2013 r. przyjęty przez Parlament Europejski i Radę.

Dyrektywa 2013/37/UE stanowi wykonie celów, o których mowa w Komunikacie (2011) 882. Podstawową zmianą jest znaczne rozszerzenie zakresu dyrektywy również na biblioteki, muzea i archiwa. Treści będące w posiadaniu tych podmiotów na gruncie dyrektywy 2003/98/WE podlegały wyłączeniu z ponownego wykorzystywania. W dokumencie „The Cultural Institutions in the Commission proposal to amend Directive 2003/98/EC on re-use of public sector information" przedstawiono opinię, iż rozszerzenie zakresu dyrektywy odzwierciedla jedynie stan rzeczywisty, gdyż wiele instytucji już obecnie udostępnia treści do ponownego wykorzystywania do celów komercyjnych i niekomercyjnych.

Zdaniem unijnego prawodawcy biblioteki, muzea i archiwa posiadają bogaty zbiór cennych zasobów informacji sektora publicznego, w szczególności od kiedy przedsięwzięcia w dziedzinie digitalizacji zwielokrotniły ilość dorobku cyfrowego wchodzącego w zakres domeny publicznej. Te zbiory dziedzictwa kulturowego wraz z powiązanymi z nimi metadanymi stanowią potencjalną podstawę treści cyfrowych w zakresie produktów i usług oraz mają ogromny potencjał w dziedzinie innowacyjnego ponownego wykorzystywania w takich sektorach jak edukacja i turystyka.

Co istotne, dyrektywa ta nałożyła na państwa członkowskie zapewnienie możliwości ponownego wykorzystywania dokumentów, do których dyrektywa ma zastosowanie do celów komercyjnych lub niekomercyjnych zgodnie z warunkami określonymi w jej przepisach.

1.5.3. Dyrektywa 2019/1024/UE

W wyniku przeglądu stosowania dyrektywy 2003/98/WE Komisja Europejska 25 kwietnia 2018 r. przedstawiła wniosek legislacyjny zawierający projekt dyrektywy w sprawie ponownego wykorzystywania informacji sektora publicznego COM (2018) 234[106]. Tym razem, w związku z licznymi zmianami, projektodawca unijny zaproponował formę prawną przekształcenia dyrektywy (*recast*), co oznacza utratę mocy dyrektywy 2003/98/WE. Przegląd ten stanowił jednocześnie ważny element inicjatywy w sprawie dostępności i ponownego wykorzystania publicznych oraz publicznie finansowanych danych, zapowiedzianej przez Komisję w komunikacie w sprawie przeglądu śródokresowego realizacji strategii jednolitego

[106] Zob. https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A52018PC0234 (25.6.2018 r.).

rynku cyfrowego[107]. W wyniku przeglądu Komisja uznała, że nowa dyrektywa powinna podejmować takie kwestie jak:

1. zapewnienie dostępu w czasie rzeczywistym do danych dynamicznych za pośrednictwem API;
2. zwiększenie podaży danych publicznych o wysokiej wartości z myślą o ich ponownym wykorzystaniu, w tym danych pochodzących z sektora przedsiębiorstw publicznych, organizacji prowadzących badania naukowe oraz instytucji finansujących badania;
3. zapobieganie pojawianiu się nowych form umów o wyłączność;
4. ograniczenie stosowania wyjątków od zasady pobierania opłat odpowiadających kosztowi krańcowemu, oraz
5. wyjaśnienie relacji między dyrektywą re-use a niektórymi powiązanymi instrumentami prawnymi (jak np. system informacji przestrzennej).

Po ponad roku prac legislacyjnych Parlament Europejski i Rada 20 czerwca 2019 r. przyjęła dyrektywę 2019/1024 nadając ostatecznie tytuł *w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego*. W związku z licznymi nowymi rozwiązaniami, dyrektywa 2019/1024 zasługuje na szerszy komentarz tym bardziej, że jej przepisy nie zostały jeszcze implementowane do polskiego porządku prawnego. Polski ustawodawca ma czas do 17 lipca 2021 r. na przyjęcie przepisów niezbędnych do wykonania niniejszej dyrektywy.

Uwzględnienie w tytule dyrektywy 2019/1024 otwartych danych ma przede wszystkim wymiar aksjologiczny. Oznacza uznanie instytucji ponownego wykorzystywania jako instrumentu służącemu realizacji działań na rzecz otwierania danych publicznych przez państwa członkowskie. Po raz pierwszy pojęcie otwartych danych zostało uwzględnione przez prawodawcę unijnego w dokumencie legislacyjnym będącym źródłem prawa UE. Wbrew nowemu tytułowi, zasadnicze elementy konstrukcyjne nowej dyrektywy pozostały bez zmian, tj. definicje podstawowych pojęć (w tym definicje informacji sektora publicznego i ponownego wykorzystywania), zasady ponownego wykorzystywania czy postępowania z wnioskami o ponowne wykorzystywanie[108].

Przede wszystkim niezmieniona została podstawowa zasada, zgodnie z którą państwa członkowskie mają obowiązek zapewnienia możliwości ponownego wykorzystywania wszystkich dokumentów, z wyjątkiem dokumentów, do których dostęp jest ograniczony lub

[107] COM (2017) 228.
[108] Zob. *D. Sybilski, Projekt nowej dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego*, „Informacja w Administracji Publicznej" 2018, nr 3, s. 3.

wyłączony na mocy przepisów prawa krajowego oraz z zastrzeżeniem pozostałych wyjątków określonych w dyrektywie (m.in. ze względu na poufność informacji, ochronę danych osobowych czy prawa własności intelektualnej). Zasadnicza zmiana dotychczasowych przepisów dyrektywy 2003/98/WE, podobnie jak i jej ostatnia zmiana wprowadzona dyrektywą 2013/37/UE, dotyczy rozszerzenia zakresu ponownego wykorzystywania o nowe podmioty (instytucje naukowe, przedsiębiorstwa publiczne) i nowe kategorie zasobów (dane badawcze, dane dynamiczne, dane o wysokiej wartości)[109].

Państwa członkowskie zostały również zobowiązane do opracowania polityki dotyczącej otwartego dostępu do danych badawczych pochodzących z badań naukowych finansowanych ze środków publicznych, przy zachowaniu elastyczności we wdrażaniu tego obowiązku (art. 10 ust. 1 projektu dyrektywy). W praktyce oznaczać to będzie konieczność opracowania przez rząd dokumentu typu strategicznego w obszarze tzw. otwartej nauki, czy też otwartego dostępu (*open access*). Polityka otwartego dostępu ma w szczególności na celu zapewnienie naukowcom i ogółowi społeczeństwa dostępu do danych badawczych na jak najwcześniejszym etapie procesu rozpowszechniania oraz umożliwienie korzystania z nich i ponownego wykorzystywania. Otwarty dostęp przyczynia się do podniesienia jakości, ograniczenia konieczności zbędnego powielania badań, przyspieszenia postępu naukowego, zwalczania oszustw w dziedzinie nauki, a także ogólnie sprzyja wzrostowi gospodarczemu i innowacyjności.[110] W tym kontekście należy przypomnieć, że 17.7.2012 r. Komisja przyjęła zalecenie w sprawie dostępu do informacji naukowej oraz jej ochrony, zaktualizowane 25.4.2018 r.[111]

Co do zasady przepisy ograniczające ponowne wykorzystywanie nie uległy zmianom. Dyrektywa 2019/1024 została przyjęta już po wejściu w życie RODO, dlatego też konieczność zapewnienia ochrony danych osobowych, została przez prawodawcę UE mocniej zaakcentowana niż w poprzednich dyrektywach. Nie tylko bowiem zaktualizowano przesłankę ograniczającą ponowne wykorzystywanie ze względu na przepisy RODO („Dyrektywa nie wpływa na ochronę osób fizycznych w odniesieniu do przetwarzania danych osobowych na podstawie prawa unijnego i krajowego, w szczególności na podstawie rozporządzenia (UE) 2016/679 i dyrektywy Parlamentu Europejskiego i Rady 2002/58/WE w tym także uzupełniających przepisów prawa krajowego" – art. 1 ust. 4), ale w motywie 52 doprecyzowano, że ponowne wykorzystywanie danych osobowych jest dopuszczalne jedynie,

[109] Zagadnienia te zostaną omówione w Rozdziale 3.
[110] Motyw 23 preambuły projektu dyrektywy.
[111] C(2018) 2375.

gdy jest ono zgodne z zasadą celowości, o której mowa w art. 5 ust. 1 lit. b) i art. 6 RODO. Ponadto zgodnie z motywem 53 preambuły dyrektywy przy podejmowaniu decyzji w sprawie zakresu i warunków ponownego wykorzystywania dokumentów sektora publicznego zawierających danych osobowe, wymagane może być przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 RODO. Zagadnienia te zostaną szerzej omówione w dalszych rozdziałach niniejszej rozprawy.

1.5.4. Ewolucja regulacji krajowej

W Polsce długo negowano potrzebę odrębnego, poza dostępem do informacji publicznej, unormowania ponownego wykorzystywania na zasadach określonych w dyrektywie 2003/98/WE, co w konsekwencji doprowadziło do niekorzystnego dla Polski wyroku TSUE, w którym potwierdzono uchybienie transpozycji przepisów przedmiotowej dyrektywy[112]. W wyroku z 27.10.2011 r. TSUE stwierdził, że krajowe przepisy dotyczące dostępu do informacji publicznych same w sobie nie są w stanie zapewnić wdrożenia przepisów dyrektywy.

Pełna implementacji dyrektywy 2003/98/WE została przez Polskę dokonana dopiero ustawą z 16 września 2011 r. o zmianie ustawy o dostępie do informacji publicznej i niektórych innych ustaw[113]. Nowelizacja ta wprowadziła do ustawy z 6 września 2001 r. rozdział 2a Ponowne wykorzystywanie informacji publicznej. Oznacza to, iż pomimo pierwotnych zamierzeń zakres przedmiotowy ponownego wykorzystywania wyznaczało pojęcie informacji publicznej. Wprowadzono ramy prawne dla ponownego wykorzystywania informacji, w tym udostępniania informacji na wniosek (wzór formularza wniosku został określony rozporządzaniem ministra administracji i cyfryzacji), zasady niewyłączności, niedyskryminacji i przejrzystości, ograniczenia i warunki ponownego wykorzystywania oraz przepisy o ofercie.

Przede wszystkim zaproponowano rozwiązanie wykraczające poza minimum określone dyrektywą, tj. sformułowano uprawnienie, iż każdemu przysługuje prawo do ponownego wykorzystywania informacji publicznej. Takie rozwiązanie wprowadziło konsekwencję nałożenia obowiązku na podmioty zobowiązane do przekazywania informacji publicznych do ponownego wykorzystywania. W tym zakresie ustawa była bardziej korzystna dla

[112] Zob. *D. Adamski, M. Bernaczyk*, Znaczenie dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego dla ustawy o dostępie do informacji publicznej, „Elektroniczna Administracja" marzec–kwiecień 2006, s. 3 i n.
[113] Dz.U. Nr 204, poz. 1195.

korzystających z informacji sektora publicznego w porównaniu do postanowień dyrektywy 2003/98/WE.

Ponadto zaproponowano korzystniejsze niż w dyrektywie 2003/98/WE zasady nakładania opłat za ponowne wykorzystywanie. Ograniczono możliwość pobierania opłat jedynie do tzw. kosztów bezpośrednich związanych z przekazaniem informacji do ponownego wykorzystywania.

Warto również odnotować, iż implementując dyrektywę 2003/98/WE wprowadzono jednocześnie w ustawie o dostępie do informacji publicznej ramy prawne dla uruchomienia centralnego repozytorium informacji publicznej, czyli obecnego portalu otwartych danych. Jest ono z jednej strony technicznym rozwiązaniem ułatwiającym pozyskiwanie zasobów informacyjnych do wykorzystywania, ale stanowi ono również kolejny tryb (obok Biuletynu Informacji Publicznej) bez wnioskowego dostępu do informacji publicznej i ponownego wykorzystywania.

W dniu 16 czerwca 2016 r. weszła w życie ustawa z dnia 25 lutego 2016 r. o ponownym wykorzystywaniu informacji sektora publicznego. Ustawa implementowała dyrektywę 2013/37/UE zmieniającą dyrektywę 2003/98/WE (tzw. druga dyrektywa *re-use*). Ustawa uwzględniała podstawową zmianę dyrektywy 2003/98/WE, którą było rozszerzenie jej zakresu podmiotowego o biblioteki, muzea i archiwa. Treści będące w posiadaniu tych podmiotów do tej pory, na gruncie poprzedniej dyrektywy, podlegały wyłączeniu z ponownego wykorzystywania. Po wejściu w życie ustawy cyfrowe zasoby bibliotek, archiwów i muzeów, które nie korzystają z ochrony praw autorskich, jak np. zdigitalzowane dzieła sztuki, reprodukcje materiałów archiwalnych czy publikacje elektroniczne, mogły być już ponownie wykorzystywane na zasadach określonych w ustawie.

Przygotowując ustawę projektodawca zaproponował nowy sposób wdrożenia zmienianej dyrektywy w polskim porządku prawnym, który miał zapewnić, że rozwiązania dotyczące ponownego wykorzystywania będą bardziej przejrzyste i łatwiejsze w stosowaniu. Uregulowanie zasad ponownego wykorzystywania w UDIP po ponad 4 lat obowiązywania przepisów spotkało się z krytyką[114]. W praktyce pojawiały się trudności z rozróżnieniem zwykłego dostępu do informacji a ponownym wykorzystywaniem. Ponadto wdrażając dyrektywę w 2011 r. „zbyt optymistycznie przyjęto, odnosząc się do orzecznictwa sądów administracyjnych, że odpowiednik pojęcia „dokument" stanowi informacja publiczna, o której

[114] W literaturze od samego początku poddano rozwiązanie krytyce, zob. *M. Jaśkowska*, Jakość i spójność rozwiązań prawnych w świetle nowelizacji ustawy o dostępie do informacji publicznej, s. 362 i nast.

mowa w art. 1 ust. 1 UDIP”[115]. Dlatego też, zaproponowano wyodrębnienie przepisów o ponownym wykorzystywaniu z ustawy o dostępie do informacji publicznej i uregulowanie tej materii w ustawie o ponownym wykorzystywaniu informacji sektora publicznego. Fundamentalną zmianą było oparcie zakresu przedmiotowego – zgodnie z treścią dyrektywy 2003/98/WE w jej pierwotnym, jak i zmienionym brzemieniu dyrektywą 2013/37/UE – o pojęcie informacji sektora publicznego („dokumentu urzędowego”).

Niemniej elementy konstrukcyjne nowej ustawy, takie jak zasady, warunki i dwa tryby udzielenia informacji do ponownego wykorzystywania, w tym postępowanie ofertowe, co do zasady zachowane te określone w poprzedniej ustawie. Niewątpliwym pozytywem – wykraczającym poza minimum dyrektywy 2013/98/UE – było umożliwienie stałego dostępu do informacji sektora publicznego dystrybuowanej elektronicznie na podstawie jednokrotnie złożonego wniosku w okresie 12 miesięcy.

Konsekwencją poszerzenia zakresu regulacji o zasoby bibliotek, archiwów i muzeów spowodowało konieczność zmiany przepisów o opłatach i warunkach w odniesieniu do tylko tych podmiotów, co z perspektywy czasu należy ocenić jako rozwiązanie zbyt kazuistyczne i w efekcie dysfunkcjonalne.

Niestety wbrew zamierzeniom – podobnie jak UDIP – regulacja ta nie stała się ustawą organiczną, która w sposób wyczerpujący regulowałaby zagadnienie ponownego wykorzystywania w całym systemie prawnym. Zgodnie z art. 7 ust. 1 przepisy UPW ani przepisów innych ustaw określających zasady, warunki i tryb dostępu lub ponownego wykorzystywania informacji będących informacjami sektora publicznego. Ponadto przepisy UPW nie naruszają prawa dostępu do informacji publicznej ani wolności jej rozpowszechniania. Oparcie przepisów UPW – wzorem dyrektywy 2003/98/WE - o przepisy dostępowe bez zmiany definicji samej informacji publicznej powoduje trudności interpretacyjne dla wyznaczenia *de lege lata* zakresu przedmiotowego ponownego wykorzystywania[116].

Ostatnie dwie nowelizacje przepisów UPW miały związek z zapewnieniem stosowania przepisów ogólnego rozporządzenia. Dostosowanie przepisów UPW do wymagań ogólnego rozporządzenia o ochronie danych osobowych odbyło się w dwóch etapach[117].

---

[115] Zob. szerzej: *G. Sibiga,* Ponowne wykorzystanie informacji sektora publicznego – stan obecny i perspektywy rozwoju. Wybrane zagadnienia, s. 111-126.

[116] O czym będę jeszcze pisał w Rozdziale 3.

[117] Zob. *D. Sybilski*, Nowelizacja ustawy o ponownym wykorzystywaniu informacji sektora publicznego dostosowująca do przepisów ogólnego rozporządzenia o ochronie danych osobowych, „Prawo Mediów Elektronicznych” 2019 nr 4, s. 74–79.

W pierwszej kolejności przepisami ustawy z 10.5.2018 r. o ochronie danych osobowych[118] nadano nowe brzmienie art. 7 ust. 2 UPW zgodnie z którym „przepisy ustawy nie naruszają przepisów o ochronie danych osobowych". Była to w istocie jedynie zmiana porządkująca, bowiem w poprzednim brzmieniu art. 7 ust. 2 stanowił o tym, że przepisy niniejszej ustawy nie naruszają przepisów ustawy z 29.8.1997 r. o ochronie danych osobowych, która została uchylona nową ustawą o ochronie danych osobowych służącej stosowaniu RODO.

Projektodawca uznał, że konieczne jest jednak szersze uwzględnienie przepisów RODO w UPW, dlatego też w ramach ustawy z 21.2.2019 r. zmieniającej sto sześćdziesiąt dwie ustawy w związku z zapewnieniem stosowania ogólnego rozporządzenia o ochronie danych[119] zmieniono również przepisy o ponownym wykorzystywaniu informacji sektora publicznego. Nowelizacja objęła zmianę art. 7 ustawy polegającą na ograniczeniu wykonania obowiązków informacyjnych, o których mowa w art. 13, 14 i 19 RODO w związku z realizacją prawa do ponownego wykorzystywania informacji stanowiących lub zawierających dane osobowe. Ponadto dodano w – wymienionym w art. 14 ust. 4 UPW – katalogu warunków ponownego wykorzystywania pkt 4 dotyczący „informacji sektora publicznego zawierającej dane osobowe". Tym samym przesądzono w sposób nie budzący wątpliwości, że możliwe jest ponowne wykorzystywanie danych osobowych w ramach informacji sektora publicznego.

W bliskiej perspektywie czasu niewątpliwie dojdzie do kolejnej zmiany przepisów o ponownym wykorzystywaniu informacji sektora publicznego w związku z koniecznością wdrożenia do krajowego porządku nowej dyrektywy z 2019 r.

Rozdział 2. Geneza i źródła prawa ochrony danych osobowych oraz istota i cele ogólnego rozporządzenia

2.1. Geneza prawnej ochrony danych osobowych

W literaturze przedmiotu przyjmuje się, że prawo do ochrony danych osobowych stanowi refleks ogólnej zasady autonomii informacyjnej człowieka i swego rodzaju emanację ogólnego prawa do prywatności ze względu na to, że dane osobowe są częścią życia prywatnego bądź posługiwanie się danymi dotyczącymi innej osoby wkracza w przyznaną jej

[118] Dz.U. z 2018 r. poz. 1000.
[119] Ustawa z 21.2.2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.4.2016 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. z 2019 r. poz. 730); dalej jako: WprowRODOU.

kompetencję decydowania o swoim życiu osobistym[120]. Ochrona danych osobowych stanowi zatem wyspecjalizowaną postać prawa do prywatności i stąd też w tym obszarze należy poszukiwać genezy prawnej ochrony danych osobowych[121].

Prawo do prywatności jest znacznie starsze od prawa ochrony danych osobowych. Pierwszą próbę zdefiniowana tego pojęcia podjęli pod koniec XIX w. *S.D. Warren* i *L.D. Brandeis* utożsamiając „prywatność" z „prawem do bycia pozostawionym w spokoju" (*right to be let alone*)[122]. Pojęcie prywatności wymyka się precyzyjnej i jednoznacznej definicji. Dookreślając zakres pojęcia autorzy odwołują się do takich wartości jak samotność, odosobnienie, tajemnica czy autonomia[123]. Można przyjąć w ogólności, że prywatność szeroko rozumiana to stan, w którym jednostka podejmuje decyzje bez ingerencji ze strony osób trzecich[124]. W węższym rozumieniu prywatność jest ujmowana jako prawo jednostki do wyłącznego dysponowania informacjami o swoim życiu osobistym[125]. Wąskie rozumienie prawa do prywatności pozwala na wyodrębnienie tzw. prywatności informacyjnej – prawa jednostki umożliwiającego kontrolowanie treści i obiegu dotyczących jej informacji[126]. Stąd też bywa określane jako prawo do informacyjnego samookreślenia się jednostki, które jest podstawowym warunkiem funkcjonowania wolnej społeczności demokratycznej, opartej na zdolności działania i współdziałania obywateli[127].

A. Kopff, który jako pierwszy w polskiej doktrynie zaproponował kompleksowe ujęcie prawa do prywatności, zdefiniował ją jako „prawo jednostki do życia własnym życiem układanym według własnej woli z ograniczeniem do niezbędnego minimum wszelkiej ingerencji zewnętrznej"[128]. Autor ten zaproponował podział sfer życia prywatnego na trzy stopnie, w jakich jednostka ma możliwość odosobnienia tj. sfery intymności, prywatności oraz powszechnej dostępności. Nawet w przypadku tej ostatniej nie można mówić o pełnej

---

[120] *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych osobowych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018, s. 82-83. Por. *J. Barta, R. Markiewicz, P. Fajgielski*, Ochrona danych osobowych. Komentarz, Warszawa 2015, s. 26-261.

[121] Zob. *A. Mednis*, Prawna ochrona danych osobowych, Warszawa 1995, s. 5; *G Sibiga*, Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003, s. 11.

[122] *S.D. Warren, L.D. Brandeis*, The right to privacy, „Harvard Law Review", vol. IV, 1890, s. 193–220, artykuł został wydrukowany w: *R. Wacks*: Privacy, vol. II, Dartmouth 1993. Zob. *Z. Mielnik*, Prawo do prywatności (wybrane zagadnienia), „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 2.

[123] *G. Sibiga*, Postępowanie w sprawach ochrony danych, s. 12.

[124] Z. *Mielnik*, Prawo do prywatności, s. 29.

[125] *A. Mednis*, op.cit., s. 8.

[126] *A. Mednis*, Ochrona prawna danych osobowych a zagrożenia prywatności – rozwiązania polskie [w:] *M. Wyrzykowski (red.)*, Ochrona danych osobowych, , Warszawa 1999, s. 167; *G. Sibiga*, Postępowanie w sprawach ochrony danych osobowych, s. 13.

[127] Wyrok Sądu Konstytucyjnego RFN z 1983 r., FTK (BrerGE) 65, za: *G. Sibiga*, Postępowanie w sprawach ochrony danych osobowych, s. 13.

[128] *A. Kopff*, Koncepcja praw do intymności i do prywatności życia osobistego (Zagadnienia konstrukcyjne), „Studia Cywilistyczne" 1972, nr 20, s. 6 i n.

dostępności informacji na swój temat, jest ona uzależniona od „usprawiedliwionego zainteresowania”[129].

Prywatność powinna podlegać ochronie ze względu na przyznanie jednostce prawa do wyłącznej kontroli tych aspektów jej życia, które nie dotyczą innych, a wolność od ciekawości z zewnątrz jest warunkiem koniecznym jej rozwoju i zachowania indywidualizmu[130]. Za dobro osobiste w postaci życia prywatnego można bowiem uznać wszystko to, co ze względu na uzasadnione odizolowanie się jednostki od ogółu służy jej do rozwoju fizycznej i psychicznej osobowości oraz zachowania osiągniętej pozycji społecznej[131]. Prawo do prywatności stało się jednym z najważniejszych dóbr osobistych człowieka, a z punktu widzenia prawa cywilnego w szeroko ujętym prawie do prywatności mieści się m.in. tajemnica korespondencji, dane osobowe, nietykalność mieszkania czy wizerunek[132]. Konieczność ochrony prywatności ukształtowało uprawnienie, na podstawie którego jednostka „może domagać się, aby nieuprawnione osoby nie mieszały się do jego życia prywatnego, zwłaszcza przez rozpowszechnianie wiadomości (chociażby nieprawdziwych)”[133].

Prawo do prywatności podlega ciągłej ewolucji, determinowane jest postępującym rozwojem technologicznym. Jednym z czynników wpływających na ewolucję poglądów jest niewątpliwie rozwój techniki, w tym środków umożliwiających ingerencję w życie prywatne jednostek wbrew ich woli i bez ich wiedzy[134].

Prawo do prywatności zostało zagwarantowane w najważniejszych konwencjach dotyczących praw człowieka[135]. Wśród praw uwzględnionych w EKPC znajduje się także – wyrażone w art. 8 – prawo do poszanowania życia prywatnego i rodzinnego, mieszkania i 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 innych osób. W orzecznictwie Europejskiego Trybunału Praw Człowieka, prawo do życia prywatnego, jest interpretowane

[129] *Ibidem,* s. 35.
[130] *M. Safjan*, Prawo do ochrony życia prywatnego [w:] *L. Wiśniewski (red.)*, Podstawowe prawa jednostki i ich sądowa ochrona, Warszawa 1997, s. 127–128.
[131] *A. Kopff*, op. cit., s. 3.
[132] *M. Sakowska-Baryła*, Dostęp do informacji publicznej a ochrona danych osobowych, Wrocław 2014, s. 227.
[133] *A. Szpunar*, O ochronie sfery życia prywatnego [w:] *L. Wiśniewski (red.)*, op. cit., s. 128.
[134] *A. Mednis*, Prawna ochrona danych osobowych, s. 5.
[135] Zob. art. 12 Powszechnej Deklaracji Praw Człowieka (przyjęta i proklamowana rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) w dniu 10 grudnia 1948 r.) i art. 17 Międzynarodowego Paktu Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 16 grudnia 1966 r. (Dz. U. z 1977 r. nr 38, poz. 167).

szeroko i może obejmować swoim zakresem różne aspekty przetwarzania danych osobowych. ETPC, oceniając ingerencję w prawo do życia prywatnego, bada, czy jest ona przewidziana przez prawo i czy to prawo jest odpowiedniej jakości, jak również czy taka ingerencja jest uzasadniona jednym z celów określonych w EKPC, a także czy jest konieczna w demokratycznym społeczeństwie [136].

Początkowo traktowano zatem ochronę danych wyłącznie z punktu widzenia poufności, jednak szybki rozwój technik informacyjno-komunikacyjnych doprowadził do postrzegania zagadnienia danych osobowych w szerszej perspektywie uwzględniającej nowe zagrożenia dla prywatności[137]. Pojawienie się przepisów prawa regulujących kwestie przetwarzania danych osobowych było odpowiedzią na zagrożenia, jakie niósł ze sobą rozwój techniki i automatyzacja procesów przetwarzania danych, w drodze których starano się stworzyć niezbędne gwarancje ochrony prywatności zapewniające bezpieczeństwo informacji o obywatelach[138]. Ochrona danych osobowych jako elementu prawa do prywatności – chronionej w drodze cywilnoprawnej – stała się niewystarczająca. Nie zapewniała bowiem ochrony „prewencyjnej". Odpowiedzialność za ochronę przejęło zatem państwo i działające w jego imieniu organy[139]. Tworzenie prawa ochrony danych stanowiło przejaw jurydyzacji obszarów wcześniej wolnych od publicznoprawnej ingerencji[140]. Pojawiło się prawodawstwo krajowe dotyczące ochrony danych osobowych. Najpierw w Niemczech (pierwsza ustawa o ochronie danych osobowych została uchwalona przez kraj związkowy Hesja w 1970 r.), a później w kolejnych państwach kolejno uchwalano akty prawne, których celem jest zapobieganie naruszeniom ochrony danych osobowych (pierwszą ustawą na szczeblu państwowym była regulacja szwedzka z 1973 r.)[141]. Regulacje te były odpowiedzią na zagrożenia, jakie niósł ze sobą rozwój techniki. W drodze przepisów starano się stworzyć

[136] *P. Drobek*, Ryzyka dla ochrony danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego [w:] *A. Piskorz-Ryń (red.)*, Dostęp i wykorzystywanie. Tom V, G. Szpor (red.), Jawność i jej ograniczenia, Warszawa 2015 r., s. 237.
[137] *E. Milczarek*, Prywatność wirtualna. Unijne standardy ochrony prawa do prywatności w Internecie, Warszawa 2020, s. 38.
[138] *A. Mednis*, Prawna ochrona danych osobowych, s. 5.
[139] *G. Sibiga*, Postępowanie w sprawach ochrony danych osobowych, s. 15.
[140] *G. Szpor*, Publicznoprawna ochrona danych osobowych, „Przegląd Ustawodawstwa Gospodarczego" 1999, nr 12, s. 10.
[141] W roku 1971 opracowany został projekt niemieckiej ustawy federalnej (weszła1.01.1979 r.). W latach siedemdziesiątych XX w. uchwalone zostały ustawy o ochronie danych osobowych we Francji, Luksemburgu, Austrii, Danii, Norwegii. W kolejnych dekadach regulacje uchwaliły m.in.: Islandia (1981 r.), Wielka Brytania (1984 r.), Finlandia (1987 r.), Holandia (1988 r.), Irlandia (1988 r.), Portugalia (1991 r.), Hiszpania (1992 r.), Szwajcaria (1992 r.) i Belgia (1992 r.). Ochrona danych osobowych wywarła też wpływ na prawo konstytucyjne i same ustawy zasadnicze. Odniesienia do ochrony danych pojawiły się w szeregu konstytucji państw europejskich – m.in. Portugalii w 1976 r. (art. 35) i Hiszpanii w 1978 r. (art. 18). Zob. *M. Czerniawski*, Prawo do ochrony danych osobowych jako prawo podstawowe (Karta Praw Podstawowych Unii Europejskiej, europejskie prawo pierwotne i wtórne, Konstytucja RP) [w:] *D. Lubasz (red.)*, Meritum, Warszawa 2020, s. 39.

niezbędne gwarancje ochrony prywatności zapewniające bezpieczeństwo informacji o obywatelach[142]. W ustawodawstwie tym starano się pogodzić prawo do ochrony informacji o jednostce z koniecznością wszechstronnego wykorzystania danych, przy zastosowaniu coraz bardziej złożonych narzędzi[143].

W latach 70. XX w. próby uregulowania kwestii przetwarzania danych rozpoczęła Rada Europy, zwieńczeniem wieloletnich prac była przyjęta w 1981 r. Konwencja Nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[144]. Konwencja weszła w życie dnia 1 października 1985 r.[145]. Określa minimalne dla państw-stron wymogi w zakresie ochrony danych osobowych. Do dziś pozostaje ona jednym z najważniejszych aktów prawnych w tej dziedzinie w prawie międzynarodowym. Dokument stworzył siatkę pojęciową definicji związanych z przetwarzaniem danych. Konwencja nr 108 oddziałuje jedynie w sferze publicznoprawnej, tzn. jest adresowana do państw, które ją ratyfikowały i nie wywołuje skutków prawnych po stronie ich obywateli[146]. Niemniej stanowiła ona pierwszy krok w stronę harmonizacji przepisów o ochronie danych osobowych na poziomie międzynarodowym. Akt ten w swojej istocie przyjęty przez Radę Europy nie stanowi *acquis communautaire.*

2.2. Unijne standardy ochrony danych osobowych

Unia Europejska od początku swojego funkcjonowania skupiała się na tworzeniu wspólnego dziedzictwa w zakresie ochrony godności człowieka, jego podstawowych praw i wolności. Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych znajduje swe źródła w prawie pierwotnym Unii Europejskiej. W porządku prawnym Unii Europejskiej prawo do ochrony danych osobowych ma charakter prawa podstawowego zagwarantowanego przepisami KPPUE oraz TFUE.

Po pierwsze, zgodnie z art. 7 KPPUE każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się. Z kolei w myśl art. 8 każdy ma prawo do ochrony danych osobowych, które go dotyczą, a dane te muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie

[142] *A. Mednis*, Prawna ochrona danych osobowych, s. 5.
[143] *G. Sibiga*, op. cit., s. 16.
[144] Sporządzona w Strasburgu 28.1.1981 r. (Dz.U. z 2003 r. Nr 3, poz. 25).
[145] Po jej ratyfikacji przez Francję, Republikę Federalną Niemiec, Norwegię, Hiszpanię i Szwecję. Polska ratyfikowała Konwencję 108 dopiero dnia 24 kwietnia 2002 r.
[146] *P. Barta, P. Fajgielski, R. Markiewicz*, Ochrona danych osobowych. Komentarz, Kraków 2004, s. 71.

przewidzianej ustawą. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania. Przepis wskazuje zatem warunki, których spełnienie legalizujące przetwarzanie danych osobowych, konstytuując zasadę zgodności z prawem (legalności) takiego przetwarzania. Natomiast ograniczenia tego prawa, tak jak ograniczenia pozostałych praw i wolności uznanych w KPPUE, muszą być przewidziane ustawą i szanować istotę tych praw i wolności. Z zastrzeżeniem zasady proporcjonalności, ograniczenia mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób (art. 52 ust 1 KPPUE).

Po drugie, należy wskazać, że ochrona danych osobowych jest dziedziną wchodzącą w zakres unijnej przestrzeni wolności, bezpieczeństwa i sprawiedliwości, która zgodnie z art. 4 ust. 2 lit. j) TFUE zalicza się do tzw. kompetencji dzielonych (Unia dzieli kompetencje z Państwami Członkowskimi, jeżeli Traktaty przyznają jej kompetencje, które nie dotyczą dziedzin określonych w artykułach 3 i 6). Państwa członkowskie zaś wykonują swoje kompetencje w zakresie w jakim UE nie skorzysta ze swej prerogatywy. Z kolei w myśl art. 16 TFUE każda osoba ma prawo do ochrony danych osobowych jej dotyczących, a Parlament Europejski i Rada, stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określają zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez Państwa Członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. Przestrzeganie tych zasad podlega kontroli niezależnych organów. Przepis ten, którego źródłem jest art. 286 TWE, znajduje zastosowanie do przetwarzania danych osobowych zarówno przez państwa członkowskie, jak i organy i instytucje unijne[147]. Zamieszczenie art. 16 TFUE w tytule II TFUE pt. "Postanowienia ogólne" nie pozostawia wątpliwości, że ma on stanowić samodzielną podstawę prawną dla ochrony danych osobowych jako jednego z fundamentalnych praw w UE, wywierającą horyzontalny skutek w tym zakresie[148].

Pierwszym aktem prawa pochodnego UE a zarazem fundamentalnym źródłem prawa wspólnotowego była dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych

[147] *J. Sobczak*, Komentarz do art. 16 [w:] *D. Miąsik, N. Półtorak, A. Wróbel (red.)*, Traktat o funkcjonowaniu Unii Europejskiej. Komentarz, t. 1, Warszawa 2012, s. 329.
[148] *P. Litwiński (red.)*, Wprowadzenie, akapit 6 [w:] *P. Barta, P. Litwiński (red.), M. Kawecki*, Rozporządzenie UE, Legalis/Wyd. 2018.

osobowych i swobodnego przepływu tych danych[149]. Dyrektywa 95/46/WE była pierwszą kompleksową próbą harmonizacji zasad przetwarzania danych osobowych w Unii Europejskiej wieńczącą prace rozpoczęte jeszcze w 1990 r. Dyrektywa jako akt pochodny prawa UE wymagający implementacji zakładała transpozycję jej przepisów przez państwa członkowskie UE odpowiednich rozwiązań legislacyjnych do końca 1998 r.

Dyrektywa 95/46/WE zawierała wyjaśnienia podstawowych pojęć odnoszących się do dziedziny danych osobowych oraz wyznaczała zasady zbierania, gromadzenia, przechowywania i udostępniania danych osobowych. Ustanawiała także zasady i warunki zgodności przetwarzania danych osobowych z prawem oraz prawa osób, których dane dotyczą. Zasadniczym celem jej uchwalenia było pogodzenie interesów podmiotów informacji oraz interesów administratorów wykorzystujących dane osobowe w swojej działalności[150]. Dyrektywa dotyczyła danych przetwarzanych automatycznie oraz będących częścią lub mających być częścią nieautomatycznych zbiorów danych, w których informacje dostępne są na podstawie określonych kryteriów. Pomimo jednak rozbudowanych postanowień dotyczących zasad przetwarzania danych osobowych, dyrektywa nie wyeliminowała rozdrobnienia ustawodawstw państw członkowskich w tym zakresie[151]. Główną przyczyna takiego stanu był wybór instrumentu legislacyjnego przez prawodawcę unijnego zakładającego minimalna harmonizację, wiążącym państwa członkowskie wyłącznie co do wskazanego w niej celu, pozostawiając im swobodę w wyborze środków realizujących takie cele. Przez co z uwagi na dużą swobodę w jej implementacji dyrektywa nie wyznaczała nawet minimalnego standardu ochrony[152]. W efekcie państwa członkowskie w swoich ustawodawstwach bardzo różnie zdefiniowały nawet podstawowe instytucje ochrony danych osobowych. Po drugie, przyczyny braku ujednolicenia ustawodawstw państw członkowskich UE należy poszukiwać w charakterze norm samej dyrektywy 95/46/WE. Dopuszczała ona bowiem, aby to przepisy krajowe w niektórych przypadkach przewidywały wyjątki od postanowień dyrektywy. Mogły one dotyczyć m.in. przesłanek legalizujących przetwarzanie szczególnych kategorii danych osobowych (art. 8 ust. 4), prawa dostępu do danych (art. 12) czy obowiązku notyfikowania faktu przetwarzania danych właściwemu organowi państwowemu (art. 18 ust. 3). Ustawodawca UE zatem w zbyt wielu przepisach dyrektywy wskazał wprost na swobodę państw

[149] Dz. Urz. WE L 281 z 23.11.1995, str. 31, z późn. zm.; Dz. Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, str. 355, z późn. zm.; dalej: dyrektywa 95/46/WE.
[150] *P. Fajgielski*, Ochrona danych osobowych w telekomunikacji – aspekty prawne, Lublin 2003, s. 34.
[151] *P. Litwiński*, op. cit., akapit 11.
[152] *P. Barta, P. Litwiński*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2013, s. 5–6.

członkowskich w jej implementacji, czego wyrazem są znaczne odrębności pomiędzy normami prawa krajowego państw członkowskich w tym zakresie[153].

Co istotne, dyrektywa 95/46/WE nie objęła swoim zakresem przetwarzania danych osobowych przez instytucje unijne. Przetwarzanie danych osobowych przez te podmioty uregulowane zostało rozporządzeniem 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych[154], które następnie zostało zastąpione przez rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE[155].

Dyrektywa 95/46/WE to nie jedyny akt prawa UE, który regulował ówcześnie ochronę danych osobowych. Do odnoszących się do tego zagadnienia regulacji należy wymienić w szczególności dyrektywę 2002/58/WE o prywatności i łączności elektronicznej, która nadal obowiązuje[156].

2.3. Reforma prawa ochrony danych osobowych w Unii Europejskiej

Reforma prawa ochrony danych osobowych przeprowadzona między 2012 a 2018 r. stanowiła kolejny etap rozwoju europejskiego podejścia do ochrony danych osobowych, mającego swe korzenie w latach 70 i 80 XX wieku[157]. Bazuje ona na wszystkich doświadczeniach zebranych przez państwa członkowskie UE w trakcie prawie 40 lat obowiązywania Konwencji 108 Rady Europy oraz kilkunastu lat praktycznego wykorzystywania rozwiązań dyrektywy 95/46 oraz rozporządzenia 45/2001.

Niemniej obowiązujące rozwiązania, stosunkowo restrykcyjne w związku z szybkim postępem technologicznym okazały się przestarzałe. W szczególności, tak Konwencja nr 108, jak i dyrektywa 95/46/WE, stanowiące przez długi czas podstawę systemu ochrony danych osobowych na terytorium Unii Europejskiej, były projektowane jeszcze za nim nastąpił

[153] *P. Litwiński (red.)*, op. cit., akapit 11.
[154] Dz. Urz. UE L 008 z 12.01.2001 r., str. 1 – 22.
[155] Dz. Urz. UE L 295 z 21.11.2018 r., str. 39—98.
[156] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) Dz. Urz. UE L 201 z 31.7.2002, str. 37—47.
[157] *W.R. Wiewiórowski, H. Wolska*, Wstęp, Rok RODO, Warszawa 2019, s. VIII. Pierwsza ustawa o ochronie danych osobowych została uchwalona w Hesji w roku 1970.

gwałtowny rozwój sieci Internet i technik komputerowych. Chociaż uwzględniały one automatyzację procesów przetwarzania danych osobowych (która była bezpośrednią przyczyną ich powstania), to nie mogły brać pod uwagę łatwości przekazywania informacji związanej z upowszechnieniem się Internetu, łatwości, z jaką można obecnie uzyskać dostęp do narzędzi umożliwiających masowe przetwarzanie danych osobowych, a także skali danych, które każdy użytkownik obecnie pozostawia po sobie w cyberprzestrzeni[158].

Dynamiczny rozwój nowych technologii podważył dotychczasowe znaczenie fundamentalnych pojęć w dziedzinie ochrony danych osobowych, lecz także wymusił konieczność stworzenia podstawowych ram prawnych ich funkcjonowania. Doszło bowiem do „rozwarstwienia między zakresem regulacji ochrony danych osobowych a możliwym do osiągnięcia na ich podstawie stopniem ich ochrony"[159]. Po 20 latach zasadniczo zmieniły się warunki przetwarzania informacji od momentu rozpoczęcia obowiązywania dyrektywy 95/46/WE. Wyzwania te zaadresowała Komisja Europejska przedstawiając pakiet prawodawczy z 25.1.2012 r., zawierający dwa wnioski legislacyjne, których zasadniczym celem była aktualizacja i modernizacja zasad ochrony danych wynikających z dotychczasowych przepisów. Pakiet obejmował projekt rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych), COM(2012)11 oraz projekt dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych, COM(2011)10.

Pakiet nowych unijnych zasad ochrony danych osobowych przewidzianych ogólnym rozporządzeniem oraz dyrektywą 2016/680 miał stanowić istotny krok na drodze umacniania praw podstawowych obywateli UE w erze cyfrowej i ułatwiania działalności gospodarczej poprzez uproszczenie zasad dla administratorów rynku wspólnotowego[160].

Funkcjonowanie w społeczeństwie cyfrowym wiąże się dla podmiotów danych nieodzownie z ryzykiem łatwej utraty kontroli nad własnymi danymi. Celem projektowanego rozporządzenia było przede wszystkim wzmocnienie ochrony danych osobowych obywateli,

[158] *M. Czerniawski*, Prawo do ochrony danych osobowych jako prawo podstawowe [w:] *D. Lubasz (red.)*, Meritum, s. 39.
[159] *P. Litwiński (red.)*, op. cit., akapit 12.
[160] Zob. *E. Bielak-Jomma*, Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?, „Monitor Prawniczy" 2017, nr 20 (dodatek), s. 3 i nast.

w tym zapewnienie im jak najpełniejszej kontroli nad ich danymi, przy jednoczesnym zachowaniu szans na rozwój nowatorskich rozwiązań oraz poprawę jakości już istniejących wiążących się z przetwarzaniem m.in. dużych zbiorów zawierających różne kategorie danych (*big data*) czy łatwiejsze transfery danych osobowych do państw trzecich, przy jednoczesnym zachowaniu odpowiedniego poziomu ich ochrony. Innymi słowy zamierzeniem projektodawcy unijnego było pogodzenie wysokiego poziomu praw podmiotów danych, które przekłada się wzrost zaufania społeczeństwa do usług *online* i do gospodarki cyfrowej, co przekłada się na większy popyt na tego usługi społeczeństwa informacyjnego, a w efekcie doprowadza do wzrostu gospodarczego, wymianę informacji i rozwój innowacyjności[161].

Jednocześnie Komisja uznała, że obszar współpracy w sprawach karnych jest na tyle szczególny, że ochrona danych osobowych przetwarzanych do celów związanych ze zwalczaniem przestępczości również musi być uregulowana w sposób szczególny. W tym wypadku wydaje się, że wybór dyrektywy jako instrumentu harmonizacji miał uwzględniać większy margines swobody (suwerenności) państw członkowskich UE i potrzebę samodzielnego kształtowania przepisów regulujących funkcjonowanie organów w państwowych w obszarze zwalczania przestępczości[162].

Po czterech latach prac legislacyjnych w dniu 27 kwietnia 2016 r. Parlament Europejski uchwalił ostateczną wersję ogólnego rozporządzenia. W tym samym dniu nastąpiło przyjęcie ostatecznej wersji dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW[163]. Rozporządzenie weszło w życie w ciągu 20 dni od daty promulgacji w Dzienniku Urzędowym Unii Europejskiej, tj. 24 maja 2016 r., a jego stosowanie nastąpiło 2 lata od tej daty, czyli od dnia 25 maja 2018 r. Z kolei termin implementacji dyrektywy 2016/680 wyznaczono dla państw członkowskich na dzień 6 maja 2018 r. W drodze wyjątku dopuszczono pewne odstępstwa od tego terminu, związane z koniecznością dostosowania już istniejących

[161] Zob. *M. Boni*, Nowe ramy ochrony danych osobowych w Unii Europejskiej – ważne wyzwanie dla Polski, „Monitor Prawniczy" 2013, nr 8 (dodatek), s. 3-4.
[162] *A. Grzelak, M. Wróblewski,* Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości z uwzględnieniem dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 [w:] *D. Lubasz (red.)*, Meritum, s. 556.
[163] Dz. Urz. L Nr 119 z 4.5.2016 r., s. 89.

w tym momencie zautomatyzowanych systemów przetwarzania danych do wymogów dyrektywy (art. 63)[164].

2.4. Cele ogólnego rozporządzenia

Podstawowy cel ogólnego rozporządzenia został sformułowany w jego art. 1. Zgodnie z tym przepisem z jednej strony celem rozporządzenia jest ochrona praw i wolności osób fizycznych w związku z przetwarzaniem ich danych (a nie ochrona danych osobowych *per se*[165]), z drugiej zaś równorzędnym celem jest nieograniczanie ani niezakazywanie swobodnego przepływu danych osobowych w ramach Unii. Oba cele normatywne RODO należy rozpatrywać, jako elementy istotne z punktu widzenia urzeczywistnienia rynku wewnętrznego Unii Europejskiej, w tym kontekście RODO – podobnie jak dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego – stanowią kluczowy instrument realizujący cele jednolitego rynku cyfrowego UE. Cele te są równoważne i współzależne[166]. W tym znaczeniu wpływają na interpretację przepisów całego rozporządzenia. Choć można zaobserwować pewne napięcie pomiędzy celem ekonomicznym a gwarancjami praw człowieka w odniesieniu do regulacji kwestii ochrony danych osobowych w UE[167].

Celem przyjęcia RODO było również usunięcie niespójności w systemie prawa ochrony danych osobowych, jakie istniały w związku z implementacją – nierzadko w sposób różniący się od siebie – dyrektywy 95/46/WE w poszczególnych państwach UE[168].

Cele aksjologiczne ogólnego rozporządzenia sformułował prawodawca UE w motywie 4 preambuły RODO. Przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Akt ten stanowi zatem próbę odpowiedzi na aktualne wyzwanie cywilizacyjne wyważenia i pogodzenia dwóch wartości, jakimi pozostaje prawo do ochrony

---

[164] Zakres stosowania RODO i dyrektywy 2016/680 w swoim założeniu jest rozłączny (zob. szerzej:. *A. Grzelak, M. Wróblewski,* op. cit., s. 1209). W art. 2 ust. 2 lit. c RODO wskazano wyraźnie, że nie ma ono zastosowania do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. To jest właśnie zakres dyrektywy 2016/680.Problematyka ochrony danych osobowych w obszarze zapobiegania i zwalczania przestępczości wykracza poza główny obszar badawczy, w związku z tym treść dyrektywy 2016/680 została w dalszej części pracy pominięta.

[165] *D. Lubasz*, Wprowadzenie [w:] *D. Lubasz (red.)*, Meritum s. 69.

[166] *D. Lubasz*, Komentarz do art. 1 [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, Warszawa 2018 s. 108.

[167] *M. Sakowska-Baryła*, Komentarz do art. 1, pkt 6 [w:] *M. Sakowska – Baryła (red.)*, Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Legalis/Wyd. 2018.

[168] *P. Litwiński (red.)*, op. cit., Komentarz do art. 1, pkt 4.

danych osobowych i autonomia informacyjna jednostki oraz swobodny przepływ danych osobowych w UE. Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. RODO nie narusza bowiem praw podstawowych, wolności i zasad uznanych w KPPUE – zapisanych w Traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej.

Rozporządzenie ma wprowadzać wysoki stopień ochrony adekwatny do szybkiego postępu technicznego i globalizacji, które przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych (motyw 6 preambuły RODO).

Należy również wymienić cel integracyjny ogólnego rozporządzenia. Celem RODO jest bowiem również zapobieżenie sytuacji, w której ochrona danych osobowych uniemożliwi ich przepływ między państwami członkowskimi UE. RODO ma więc na celu wzmocnienie wynikających z prawa pierwotnego Unii Europejskiej swobód, gwarantując jej stały rozwój gospodarczy[169].

2.5. Ogólne rozporządzenie jako źródło prawa ochrony danych osobowych

Zgodnie z art. 288 TFUE rozporządzenie ma zasięg ogólny, wiąże w całości, co do wszystkich zawartych w nim postanowień, i jest bezpośrednio stosowane we wszystkich państwach członkowskich. Ze swej natury staje się ono częścią krajowych systemów prawnych bez potrzeby dokonywania jakichkolwiek czynności transpozycyjnych i wywiera skutki

[169] *P. Litwiński (red.)*, op. cit., pkt 4.

bezpośrednie w stosunku do jednostek (*direct effect*). Rozporządzenia obejmują wertykalny i horyzontalny skutek bez wyjątku.

Ogólne rozporządzenie uchyliło dyrektywę 95/46/WE, przejmując jej rolę aktu harmonizującego prawo ochrony danych osobowych w państwach członkowskich. Określa to wyraźnie treść art. 94 RODO, który wskazuje nie tylko na utratę mocy obowiązującej dyrektywy, ale również na to, że wszelkie odesłania do uchylonej dyrektywy zawarte w innych aktach należy odczytywać jako odesłania do RODO. Konsekwencją utraty mocy dyrektywy 95/46/WE jest naturalnie uchylenie obowiązującej przed rozpoczęciem stosowania ogólnego rozporządzenia ustawy z 29.8.1997 r. o ochronie danych osobowych[170], która wraz z kolejnymi ustawami ją zmieniającymi służyła implementacji dyrektywy 95/46/WE (zob. Rozdział 2.7.2).

Konsekwencją uchylenia UODO1997 było również usunięcie z porządku prawnego jej art. 5. Powołany przepis wskazywał, że jeżeli normy odrębnych ustaw, które odnoszą się do przetwarzania danych, przewidują dalej idącą ich ochronę, niż wynika to z UODO1997, stosuje się przepisy tych ustaw. Treść powołanego artykułu opera się na zasadzie *lex specialis derogat legi generali*, jednakże z tą różnicą, że *legis specialis* znajdują zastosowanie w sytuacjach, gdy przewidują one dalej idącą ochronę. W RODO brak jest analogicznej normy, co wskazuje na pierwszeństwo norm w nim zawartych nie tylko przed normami prawa krajowego, ale również przed regulacjami dotyczącymi ochrony danych osobowych przewidzianymi w aktach prawa UE[171].

RODO nie wprowadziło jednak pełnej harmonizacji, rozumianej jako zupełne ukształtowanie regulacji danego obszaru przedmiotowego, bez dopuszczalności stosowania regulacji krajowych[172]. Przeciwieństwem harmonizacji pełnej jest harmonizacja częściowa, w której pozostawia się państwom członkowskim większą lub mniejszą aktywność w danej dziedzinie po wejściu w życie aktu harmonizującego[173]. W ramach takiej harmonizacji częściowej, której przykładem jest właśnie ogólne rozporządzenie, w enumeratywnie określonych sytuacjach pozostawia się państwu możliwość wyboru kierowania się w ustalonych kwestiach przedmiotowych regulacjami unijnymi lub regulacjami krajowymi (harmonizacja fakultatywna). Nawet w sytuacji wyboru przez państwo opcji wprowadzenia przepisów krajowych akt harmonizujący może ingerować w kształt tych przepisów. Akt

[170] Dz.U. 1997 nr 133 poz. 883; dalej: UODO1997.
[171] *P. Litwiński (red.)*, op. cit., Wprowadzenie, akapit 27.
[172] *G. Sibiga*, Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych – wybrane zagadnienia, „Monitor Prawniczy" 2016, Nr 20 (dodatek), s. 17.
[173] *J. Osiejewicz*, Harmonizacja prawa państw członkowskich Unii Europejskiej, Warszawa 2016, s. 59–60.

harmonizujący może bowiem ustanawiać wymogi wobec regulacji prawnej państwa członkowskiego. Co ważne, w przypadku ogólnego rozporządzenia – w myśl motywu 8 – przewidziano również możliwość włączenia elementów rozporządzenia do przepisów krajowych, jeżeli będzie to niezbędne dla zachowania spójności i zrozumiałości przepisów dla osób, do których mają zastosowanie[174], co potencjalnie należy uznać za niezgodne z podstawowymi zasadami techniki prawodawczej, w tym wyrażonego w § 4 ust. 1 ZTP ogólnego zakazu powtarzania w ustawie postanowień umów międzynarodowych ratyfikowanych przez Rzeczpospolitą Polską oraz dających się bezpośrednio stosować postanowień aktów normatywnych ustanowionych przez organizacje międzynarodowe lub organy międzynarodowe[175]. Nawet w kwestii podlegającej harmonizacji w drodze rozporządzenia może dojść do nałożenia obowiązku na państwo członkowskie określenia w prawie krajowym sposobu i formy realizacji wymogów z rozporządzenia.

W celu zapewnienia stosowania rozporządzenia w krajowych porządkach prawnych, mimo bezpośredniego stosowania, konieczna była ingerencja ustawodawcza na poziomie prawa krajowego państw członkowskich. Wynika to przede wszystkim z przyjętej w prawie europejskim zasady autonomii proceduralnej państw członkowskich. Konieczne było zatem stworzenie na szczeblu krajowym odpowiednich przepisów obejmujących zagadnienia instytucjonalne i proceduralne[176].

Ponadto państwa członkowskie zostały upoważnione do interwencji legislacyjnej w prawie krajowym w zakresie wprost wskazanym w RODO, tj. w przypadkach w których rozporządzenia w ogóle nie znajduje zastosowania (art. 2 ust. 2) oraz w przypadkach określonych w klauzulach kompetencyjnych[177] (poprzez odesłania do prawa krajowego).

Zawarte w ogólnym rozporządzeniu odesłania mają na celu doprecyzowanie lub zawężenie w prawie krajowym przepisów ogólnego rozporządzenia, o ile jest to niezbędne, a przepisy krajowe mają być spójne i zrozumiałe (motyw 8 RODO). Charakter odesłań jest jednak niejednolity[178]. Pod względem konsekwencji jakie wywołują dla krajowego ustawodawcy można je podzielić na odesłania określające obligatoryjny zakres regulacji prawnej niezbędny do dostosowania prawa krajowego do RODO[179] oraz odesłania określające

[174] G. *Sibiga*, Dopuszczalny zakres, s. 17
[175] Zob. rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej" (Dz. U. Nr 100, poz. 908 z późń. zm.).
[176] *D. Lubasz*, Wprowadzenie, s. 66.
[177] *Ibidem*.
[178] G. *Sibiga*, Dopuszczalny zakres, s. 18.
[179] Dotyczą one organów nadzorczych (art. 54 RODO) oraz środków ochrony prawnej, odpowiedzialności i sankcji, a w szczególności zagadnień proceduralnych (art. 77 i art. 83 ust. 8 RODO).

fakultatywny zakres krajowej regulacji dopuszczony w ogólnym rozporządzeniu[180]. W powyższym zakresie przepisy rozporządzenia tworzą swoiste upoważnienie dla prawodawcy krajowego do wydania aktów normatywnych służących stosowaniu RODO. Inny charakter mają szczególne odesłania określające wymagania wobec regulacji krajowej co do podstaw prawnych przetwarzania danych osobowych znajdujących się w prawie krajowym (art. 6 ust. 1 lit. c i e oraz ust 2 i 3 RODO[181].

Ze względu na obowiązki notyfikacyjne wobec Komisji Europejskiej przepisy krajowe wykonujące upoważnienia wynikającego z odesłań zawartych w rozporządzeniu można również podzielić na wymagające (np. art. 51 ust. 4, art. 85 ust. 2, art. 88 ust. 3, art. 90 ust. 2 RODO) i niewymagające notyfikacji (art. 86 i art. 89 ust. 3 RODO), a w przypadku wymagających notyfikacji można wyróżnić szczególną kategorię przepisów wymagających notyfikacji do dnia rozpoczęcia stosowania ogólnego rozporządzenia (art. 51 ust. 4, art. 84 ust. 2, art. 88 ust. 3, art. 90 ust. 2)[182].

Szczególną kategorię tworzą odesłania do przepisów krajowych zawarte w Rozdziale IX (*Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem*). W tym rozdziale określono kilka przypadków, w których szczegółowo wskazano dopuszczalny zakres ingerencji prawodawcy krajowego: przetwarzanie danych do celów dziennikarskich oraz wypowiedzi akademickiej, artystycznej i literackiej (art. 85), przetwarzanie danych w ramach publicznego dostępu do dokumentów urzędowych (art. 86), funkcjonowanie krajowego numeru identyfikacyjnego (art. 87), przetwarzanie w kontekście zatrudnienia (art. 88), przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (art. 89), prawne obowiązki tajemnic względem organu nadzorczego (organu w sprawach ochrony danych) (art. 90).

Większość przepisów rozdziału IX RODO opartych została na dopuszczalności przyjmowania przepisów krajowych pod określonymi warunkami. Według ogólnego rozporządzenia rolą przepisów krajowych jest pogodzenie i zapewnienie równowagi między prawem do ochrony danych osobowych oraz wchodzącymi w kolizję z nim dwóch rodzajów konkurencyjnych uprawnień, tj. wolnością wypowiedzi i informacji, w tym wypowiedzi

[180] Chodzi o upoważnienia przewidujące możliwość wydania szczególnych przepisów krajowych (np. 8 ust. 1 RODO), o odesłania, w których od regulacji prawa krajowego RODO uzależnia obowiązywanie przepisu ogólnego rozporządzenia lub zawężenie stosowania przepisu tego rozporządzenia (np. art. 23 RODO) oraz odesłania określające dopuszczalny zakres regulacji krajowej co do podstaw przetwarzania danych osobowych, które doprecyzowują ogólne rozporządzenie (np. art. 6 ust. 1 lit. c) i e) i ust. 2–3, art. 9 ust. 4 RODO) Zob. szerz. *G. Sibiga.*, Dopuszczalny zakres, s. 18 – 21.
[181] Zob. Rozdział 7.
[182] G. *Sibiga*, Dopuszczalny zakres, s. 18.

dziennikarskiej, akademickiej, artystycznej lub literackiej (art. 85 RODO) oraz prawa publicznego dostępu do dokumentów urzędowych (art. 86 RODO). Konieczność owego pogodzenia jest szczególnego rodzaju przypadkiem przepisów, które również powinny zostać obligatoryjnie przyjęte w prawie krajowym[183].

W zakresie przetwarzania danych osobowych dla celów dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej rolą przepisów krajowych jest w niezbędnych sytuacjach potrzebnych do pogodzenia ochrony danych osobowych z wolnością wypowiedzi (informacji) określenie odstępstw lub wyjątków od wymienionych w art. 85 ust. 2 RODO praw podmiotów danych oraz obowiązków administratorów danych (przetwarzających)[184].

Z kolei zgodnie z art. 86 przewiduje, że dane osobowe zawarte w dokumentach urzędowych mogą zostać w celu wykonania zadania realizowanego w interesie publicznym, ujawnione zgodnie z prawem Unii lub prawem państwa członkowskiego. Przepisy te powinny pogodzić publiczny dostęp do dokumentów urzędowych z prawem do ochrony danych osobowych. W opinii autora przepis ten ma fundamentalne znaczenie dla niniejszej pracy, ponieważ będzie miał również zastosowanie do ponownego wykorzystywania informacji sektora publicznego. Zagadnieniu temu poświęcono Rozdział 6.

2.6. Podstawowe zmiany w prawie ochrony danych osobowych wprowadzone ogólnym rozporządzeniem

Podstawowe rozwiązania ogólnego rozporządzenia trudno uznać za rewolucyjne, można jednak mówić o nowym podejściu, który istotnie wpływa na praktykę stosowania przepisów o ochronie danych osobowych. Zamiast o rewolucji, trafniej jest pakiet reform określić ewolucją dobrze znanego standardu[185] czy też ewolucyjnym podejściem zmierzającym do zapewnienia spójności regulacji w całej UE, w celu poprawy skuteczności ochrony danych osobowych oraz uwzględnienia postępu technicznego[186].

[183] *G. Sibiga*, Dopuszczalny zakres, s. 19. Zobacz: Rozdział X.
[184] Chodzi o odstępstwa lub wyjątki od rozdziału II (Zasady), rozdziału III (Prawa osoby, której dane dotyczą), rozdziału IV (Administrator i podmiot przetwarzający), rozdziału V (Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych), rozdziału VI (Niezależne organy nadzorcze), rozdziału VII (Współpraca i spójność) oraz rozdziału IX (Szczególne sytuacje związane z przetwarzaniem danych).
[185] *K. Szymielewicz*, Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony?, „Monitor Prawniczy" 2016, nr 20 (dodatek), s. 10 i nast.
[186] *P. Fajgielski*, Komentarz, 2018, s. 82.

Jednak za pewną rewolucją należy uznać z perspektywy obywateli, jak i podmiotów przetwarzających dane osobowe, poszerzenie zakresu stosowania europejskich standardów i ich ujednolicenie w ramach samej UE (art. 3 RODO). Od 2018 r. we wszystkich państwach UE obowiązują jednakowe przepisy dotyczące ochrony danych osobowych, te same reguły będą musiały przestrzegać zagraniczne przedsiębiorstwa (bez względu na lokalizację swojej siedziby czy serwerów), jeśli tylko oferują usługi obywatelom UE lub monitorują ich zachowanie w Internecie[187]. Sam więc wybór rozporządzenia jako instrumentu regulacji dziedziny ochrony danych osobowych na terytorium Unii Europejskiej, które zastąpiło z natury samej dyrektywy rozwiązania bardzie elastyczne, można uznać za rewolucyjny, jak i ze względu na przebudowę narzędzi, które pozostawać będą w rękach Komisji Europejskiej, europejskich organów ochrony danych oraz organów krajowych[188].

Uwzględniając postęp technologiczny, RODO ma realizować równocześnie postulat technologicznej neutralności regulacji. Ochrona danych osób fizycznych nie powinna zależeć od stosowanych technik, ponieważ w przeciwnym razie wystąpiłoby poważne ryzyko obchodzenia prawa. Założenie to w istotny sposób wpływa na zakres obowiązków podmiotów zobowiązanych do odpowiedniego zabezpieczenia danych osobowych, także już na etapie projektowania rozwiązań służących do ich przetwarzania[189].

Z perspektywy osób, których dane dotyczą niewątpliwe najistotniejsze rozwiązania obejmują nowe uprawnienia, takie jak prawo do ograniczenia przetwarzania (art. 18 RODO), prawo do przenoszenia danych (art. 20) czy tzw. prawo do bycia zapomnianym (art. 17)[190].

Zasadniczo nowe podejście przejawia się w przeniesieniu znacznie większego ciężaru odpowiedzialności za przestrzeganie zasad i obowiązków wynikających w nowych przepisów na administratorów danych osobowych[191].

Rozporządzenie wprowadza odmienny, proaktywny model ochrony, oparty na podejściu bazującym na ryzyku (*risk-based approach*). Odchodzi tym samym od sztywnych ram regulacyjnych i wyabstrahowanych od kategorii administratora, zakresu jego działania, zwłaszcza jego związku z przetwarzaniem danych osobowych i skali tego przetwarzania, które były charakterystyczne dla UODO1997 i rozporządzeń wykonawczych do niej, a zwłaszcza rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.

[187] *Ibidem*.
[188] *W.R., Wiewiórowski*, Nowe ramy ochrony danych osobowych w Unii Europejskiej, „Monitor Prawniczy" 2012, nr 7 (dodatek), s. 2 i nast.
[189] *D. Lubasz*, Wprowadzenie [w:] *D. Lubasz (red.)*, Meritum, s. 67.
[190] Zob. Rozdział 5.2.
[191] *E. Bielak-Jomma*, Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?, „Monitor Prawniczy" 2017, nr 20 (dodatek), s. 4.

w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[192]. Według RODO administratorzy danych mają obowiązek przyjęcia środków, które zapewnią poziom bezpieczeństwa odpowiedni do kategorii danych i zagrożeń. Wyrażone w RODO podejście oparte na ryzyku określa sposób, w jaki należy podchodzić do przetwarzania danych, tj. zawsze analizować ryzyko, jakie może spowodować dla prywatności osób, których te dane dotyczą. Przejawia się to m.in. w konieczności przestrzegania zasady zabezpieczenia danych (wdrażania środków zabezpieczenia technicznego i organizacyjnego) odpowiedniego do ryzyka (art. 32 RODO).

Nową zasadą w systemie ochrony danych wprowadzoną przez ogólne rozporządzenie jest zasada rozliczalności[193] (*accountability)*. Zgodnie z nią, na każdym administratorze danych spoczywa obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych zapewniających zgodność z wymogami RODO (np. wprowadzenie rozwiązań umożliwiających realizację praw osób, których dane dotyczą) i przede wszystkim wykazania ich zgodności z jego wymogami. Ważnym aspektem realizacji tej zasady będzie wykazanie przez administratora przestrzegania prawa, np. poprzez udokumentowane wdrożenie instrumentów prawnych określonych w ogólnym rozporządzeniu, takich jak przeprowadzona ocena skutków dla ochrony danych (art. 35 RODO) [194] oraz uprzednie konsultacje (art. 36 RODO), rejestracja czynności przetwarzania danych (art. 30 RODO) i obowiązki związane z naruszeniami ochrony danych (art. 33-34 RODO), wdrożenie zasady ochrony danych w fazie projektowania oraz domyślnej ochrony danych (art. 25 RODO; *privacy by design* i *privacy by default*) [195] lub też stosowanie nowych mechanizmów zgodności z przepisami o ochronie danych osobowych, czyli zatwierdzonych kodeksów postępowania i certyfikacje (art. 40-43 RODO).

Wdrożenie właściwych środków organizacyjnych i technicznych oraz wykazanie ich zgodności z ogólnym rozporządzeniem należy do administratora (lub podmiotu przetwarzającego). Natomiast inspektor ochrony danych wspiera administratora (lub podmiot przetwarzający) w wykonywaniu zadań związanych z przetwarzaniem danych. Jest on zarówno punktem kontaktowym dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych, jak i dla osób, których dane dotyczą, we wszystkich sprawach

[192] *D. Lubasz,* Wprowadzenie [w:] *D. Lubasz (red.),* Meritum, s. 65.
[193] Art. 5 ust. 2 RODO.
[194] Zob. m.in. *A. Mednis,* Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych, „Monitor Prawniczy" 2016, nr, 20 (dodatek), s. 29-33.
[195] Zob. m.in. *M. Bienias,* Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych, „Monitor Prawniczy" 2016, nr 20 (dodatek), s. 53-57.

związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw[196]. Inspektor ochrony danych ma kluczowe znaczenie w procesie administrowania danymi, w związku z czym w ogólnym rozporządzeniu dokładnie określono warunki jego wyznaczania, status oraz katalog zadań[197] (w poprzednim stanie prawnym podobne funkcje pełnił na gruncie art. art. 18 ust. 2 oraz art. 20 ust. 2 dyrektywy 95/47/WE urzędnik ds. ochrony danych osobowych - *data protection official,* a w prawie krajowym administrator bezpieczeństwa informacji[198]).

2.7. Krajowe źródła prawa ochrony danych osobowych

2.7.1. Konstytucja RP

W polskim systemie prawnym ochrona danych osobowych wywodzi się z przepisów Konstytucji RP[199].

Po pierwsze w art. 47 Konstytucja RP gwarantuje każdemu prawo do ochrony życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym. Po drugie zaś w art. 51 Konstytucji RP zawarte zostały bezpośrednie gwarancje ochrony danych osobowych[200], a unormowania w nim zawarte mają charakter kompleksowy i gwarantują należytą ochronę danych osobowym w sferze prywatnej i publicznej[201]. Należy wśród nich wymienić

1) prawo do samodzielnego decydowania każdej osoby o ujawnianiu dotyczących jej informacji;

---

[196] Zob. m.in. *K. Syska*, Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań, „Monitor Prawniczy" 2016, nr 20 (dodatek), s. 75-81. *G. Sibiga, K. Syska,* Działania organizacyjne i informacyjne związane z wyznaczeniem i wykonywaniem funkcji inspektora ochrony danych, „Monitor Prawniczy" 2017, nr 20 (dodatek), s. 23-27.

[197] Zob. art. 37-39 RODO

[198] Przed nowelizacją UODO1997 z 1.1.2015 r. szczątkowa regulacja dotycząca administratora bezpieczeństwa informacji przewidziana była w art. 36 ust. 3. Po nowelizacji instytucja administratora bezpieczeństwa informacji zyskała po raz pierwszy ustawowo określone prawa i obowiązki, a także pozycję prawną w organizacji zgodnie z art. 36a–36c UODO1997 w brzmieniu po 1.1.2015 r.

[199] Szerzej na temat zob. m.in. *M. Wyrzykowski,* Ochrona danych – zagadnienia konstytucyjne [w:] *M. Wyrzykowski (red.),* Ochrona danych osobowych, red., Warszawa 1999; *M. Wyrzykowski*, Status informacyjnych obywatela, [w:] Prawo i ład społeczny. Księga jubileuszowa dedykowana Profesor Annie Turskiej, Warszawa 2000; *M. Safjan*, Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych, „Kwartalnik Prawa Prywatnego" 2002, z. 1; *M. Sakowska-Baryła*, Konstytucjonalizacja prawa do ochrony danych osobowych w Polsce, „Przegląd Prawa Konstytucyjnego" 2016, nr 4 (32), s. 125-144.

[200] *G. Sibiga*, Postępowanie w sprawach ochrony danych, s. 22.

[201] *M. Sakowska-Baryła*, Konstytucjonlizacja, s. 125.

2) prawo każdej osoby do sprawowania kontroli nad informacjami na swój temat, gwarantowane prawem dostępu do dotyczących jej urzędowych dokumentów i zbiorów danych;
3) prawo do weryfikowania lub żądania usunięcia danych osobowych[202].

W literaturze przyjmuje się, że art. 47 Konstytucji RP ustanawiając normę ogólną, sprawia, że w zakresie, w jakim ochrona prywatności nie jest realizowana przez regulacje szczególne, możliwe jest odwołanie się do regulacji ogólnych, np. prywatność odnosi się m.in. do ochrony informacji dotyczących danej osoby oraz możliwości decydowania o zakresie i zasięgu udostępniania i komunikowania innym osobom informacji o swoim życiu[203]. Gwarancje proklamowane w tym przepisie przyznają jednostkom ochronę w zakresie nieobjętym innymi przepisami, a odnoszącym się bądź do samej autonomii (możliwości decydowania o życiu osobistym), bądź też do koniecznych jej warunków (pozwalających się przyporządkować do kategorii życia prywatnego, rodzinnego, czci lub dobrego imienia), które stanowią warunek konieczny dla decydowania o swoim życiu osobistym[204]. Tak jak pozostałe wolności i prawa, również prawo do prywatności podlegać może ograniczeniom wynikającym z reguły ogólnej ich wprowadzania ustanowionej w art. 31 ust. 3 Konstytucji RP.

Prawo do prywatności, o którym mowa w art. 47, zagwarantowane jest m.in. w aspekcie ochrony danych osobowych, przewidzianej w art. 51 Konstytucji RP[205]. Artykuł 51 konstytuuje zasadę autonomii informacyjnej[206]. Można przyjąć, że prawo do ochrony danych osobowych jest „wyspecjalizowaną konstrukcją", służącą ochronie tych samych wartości, które chroni art. 47 Konstytucji[207]. *I. Lipowicz* wskazuje również na rolę prawa ochrony danych osobowych jako instrumentu ochrony przed dyskryminacją[208]. Artykuł 51 Konstytucji RP pełni zatem funkcję gwarancyjną wobec wartości chronionych dyspozycją art. 47, jego celem jest bowiem „konkretyzacja prawa do prywatności w aspektach proceduralnych"[209].

Na ogół przyjmuje się, że prywatność odnosi się m.in. do ochrony informacji dotyczących danej osoby i gwarancji pewnego stanu niezależności, w ramach której człowiek może decydować o zakresie i zasięgu udostępniania i komunikowania innym osobom

[202] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 120–122.
[203] *M. Wild*, Komentarz do art. 47, akapit 47 [w:] *M. Safjan, L. Bosek (red.),* Konstytucja RP. Tom I. Komentarz do art. 1–86, Legalis/Wyd. 2016.
[204] Zob. wyr. TK z 19.5.1998 r., U 5/97.
[205] *Ibidem*.
[206] Wyrok TK z 12.11.2002, SK 40/01.
[207] *I. Lipowicz*, Konstytucyjne podstawy ochrony danych osobowych [w:] *P. Fajgielski (red.),* Ochrona danych osobowych w Polsce, s. 47.
[208] *Ibidem*, s. 49.
[209] Wyrok TK z dnia 19.05.1998 r., U 5/97.

informacji o swoim życiu, jest więc pojęciem szerszym niż sama ochrona danych osobowych[210]. W orzecznictwie Trybunału Konstytucyjnego akcentuje się wspólny „korzeń aksjologiczny" prawa do prywatności i prawa do ochrony danych osobowych, który decyduje w dużym stopniu o potrzebie poszukiwania wspólnego uzasadnienia dla uznania za dopuszczalną ingerencji zewnętrznej w świat „odosobnienia jednostki". Przedmiotem ochrony są na tle prywatności wartości akcentujące możliwość prowadzenia swych spraw, decydowania o swym życiu i o rodzajach więzi personalnych z innymi z maksymalną swobodą, a zarazem z najmniejszym stopniem ingerencji świata zewnętrznego w tę sferę, która jest domeną własnej aktywności jednostki[211].

Zakres wzorca konstytucyjnego wynikającego z art. 51 można zrekonstruować w oparciu o orzecznictwo Trybunału. Najbardziej zasadnicze elementy składające się na treść prawa do ochrony życia prywatnego to: „respekt dla autonomii informacyjnej jednostki, a więc sam obowiązek udostępnienia danych ograniczony do ściśle określonych ustawowo sytuacji; ograniczenie arbitralności ustawodawcy – ustawa nie może zakresu obowiązku kształtować dowolnie, przy czym Konstytucja operuje w tym wypadku ograniczeniami dwojakiego rodzaju (co do formy – obowiązek udostępnienia danych musi być wprowadzony przez ustawę oraz co do materii – obowiązek jest uzasadniony jedynie w takim zakresie, w jakim jest to niezbędne w demokratycznym państwie prawnym); prawo do dostępu do informacji gromadzonych przez władzę publiczną; wreszcie prawo sprostowania informacji nieprawdziwej, niepełnej lub zebranej niezgodnie z ustawą"[212].

2.7.2. Ustawa o ochronie danych osobowych z 1997 r.

W art. 51 ust. 5 Konstytucji RP zawarto zapowiedź uchwalenia ustawy regulującej "zasady i tryb gromadzenia oraz udostępniania informacji". Jak powszechnie przyjmuje się w literaturze[213] wykonaniem tej zapowiedzi stało się uchwalenie ustawy z 29.8.1997 r. o ochronie danych osobowych. UODO1997 przyjęta została również w wykonaniu

[210] *Ibidem.*
[211] Wyrok TK z dnia 12 listopada 2002 r., SK 40/41.
[212] *Ibidem.*
[213] Zob. m.in. *A. Mednis*, Ochrona prawna danych osobowych a zagrożenia prywatności – rozwiązania polskie, [w] *M. Wyrzykowski (red.),* Ochrona danych osobowych, Warszawa 1999, s. 168.

zobowiązania zapewnienia przez Rzeczpospolitą Polską zgodności jej przyszłego ustawodawstwa z unijnym porządkiem prawnym, przede wszystkim z dyrektywą 95/46/WE[214].

Ustawa w swoich założeniu miała w sposób całościowy uregulować zagadnienia przetwarzania danych osobowych, bez względu na formę ich zapisu (informatyczną lub papierową) i z szerokim określeniem zakresu podmiotów podlegających jej przepisom. UODO1997 wraz z aktami wykonawczymi[215] normowała trzy rodzaje spraw: zasady i tryb postępowania przy przetwarzaniu danych osobowych; prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane w zbiorach danych oraz sposób wykonywania tych uprawnień; zakres działania oraz zasady organizacji i funkcjonowania organu do spraw ochrony danych osobowych (ustawa ustanowiła nowy ówcześnie organ państwowy – Generalnego Inspektora Ochrony Danych Osobowych)[216]. Można zatem uznać, że prawodawca starał się nadać UODO1997 kompleksowy charakter i to na kilku płaszczyznach. Obok głównego przedmiotu regulacji, jakim była ochrona interesów tych, których dotyczą przetwarzane dane, ustawa adresowała – choć fragmentarycznie i na dalszym planie – również kwestie wolności informacji, udostępniania danych osobowych, interes osób trzecich (instytucji, obywateli) związany z dostępem i wykorzystywaniem informacji[217]. Poszukiwała w tym zakresie sposobu pogodzenia do pewnego stopnia sprzecznych interesów, przy czym nie wprowadziła wyraźnych przepisów o obrocie zbiorami (bazami) danych osobowych[218].

W chwili uchwalenia UODO1997 nie można było jednak mówić o jej pełnej zgodności z dyrektywą 95/46/WE, a co za tym idzie, ustawa w pierwotnym brzmieniu nie mogła zostać uznana za implementację dyrektywy[219]. Przykładowo dyrektywa 95/46/WE przewidziała kilka instrumentów prawnych umożliwiających przekazywanie danych poza UE, to jednak polski ustawodawca pierwotnie nie uwzględnił ich w przepisach UODO1997. Z tego powodu

---

[214] Zgodnie z art. 68 Układu Europejskiego ustanawiającego stowarzyszenie między Rzecząpospolitą Polską, a Wspólnotami Europejskimi i ich Państwami Członkowskimi sporządzonego w Brukseli 16.12.1991 r. (Dz.U. z 1994 r. Nr 11, poz. 38 ze zm.).

[215] Rozporządzenie Prezydenta Rzeczypospolitej Polskiej w sprawie nadania statutu Biuru Generalnego Inspektora Ochrony Danych Osobowych (Dz. U. Nr 73, poz. 464); rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie określenia wzorów wniosku o udostępnienie danych osobowych, zgłoszenia zbioru danych do rejestracji oraz imiennego upoważnienia i legitymacji służbowej inspektora Biura Generalnego Inspektora Ochrony Danych Osobowych (Dz.U. 1998 Nr 80, poz. 522); Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. 1998 Nr 80, poz. 521).

[216] *G. Sibiga*, Postępowanie w sprawach ochrony danych osobowych, s. 26-27.

[217] *J. Barta, P. Fajgielski, M. Markiewicz*, Ochrona danych osobowych. Komentarz, Warszawa 2011, s. 100.

[218] *Ibidem*.

[219] *P. Barta*, Rozdział 1. Przepisy ogólne. Wprowadzenie, pkt 10 [w:] *P. Barta, P. Litwiński*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2016, Wyd. 4/Legalis.

konieczne stały się jej dwie istotne nowelizacje, dokonane w 2001 i 2004 r.[220] oraz kolejne zmiany, które weszły w życie 1.1.2015 r.[221] Warto podkreślić, że UODO1997 była zgodna z wymogami Konwencji nr 108, co znalazło swoje odzwierciedlenie w ratyfikacji aktu przez Polskę dnia 24 kwietnia 2002 r.

2.7.3. Wykonanie przepisów ogólnego rozporządzenia w prawie krajowym

Zastosowanie rozporządzenia jako formy harmonizacji sprawiło, że ustała podstawa prawna dalszego obowiązywania UODO1997 (jako ustawy wykonującej dyrektywę 95/46/WE), która w sposób całościowy reguluje zasady postępowania przy przetwarzaniu danych osobowych oraz prawa osób, których dane są przetwarzane. Z punktu widzenia RODO w ogóle zakazane stanie się stosowanie rozwiązań nieprzewidzianych w rozporządzeniu i nie pozostawionych w nim wyraźnie do uregulowania w prawie krajowym[222].

Podstawowe znaczenie dla zakresu prawa krajowego mają przepisy samego ogólnego rozporządzenia. Z perspektywy RODO jedynie w zakresie w nim dozwolonym przepisy krajowe mogą regulować materię objętą rozporządzeniem. Należy również pamiętać, że przepisy państwa członkowskiego stanowią wyjątek od zasady jednolitej regulacji ochrony danych w ogólnym rozporządzeniu i nie powinny prowadzić do fragmentaryzacji prawa ochrony danych osobowych, czemu przecież przeciwdziałać miał wybór rozporządzenia jako aktu harmonizującego[223].

W związku z upoważnieniem państw członkowskich do przyjmowania środków prawa krajowego w zakresie wprost wskazanym w RODO, polski ustawodawca korzystając z przedmiotowego uprawnienia, dla prawidłowego stosowania ogólnego rozporządzenia przeprowadził istotne zmiany legislacyjne. Krajowa reforma przepisów o ochronie danych osobowych odbyła się w dwóch etapach.

Po pierwsze uchwalono ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych[224]. Wejście w życie ustawy skorelowano z rozpoczęciem stosowania rozporządzenia, tj. od dnia 25 maja 2018 r. , co wynikało wprost z art. 99 ust. 2 RODO.

---

[220] Ustawa z dnia 25 sierpnia 2001 r. o zmianie ustawy o ochronie danych osobowych (Dz.U. Nr 100, poz. 1087) oraz ustawa z dnia 22 stycznia 2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz.U. Nr 33, poz. 285).
[221] Wprowadzone ustawą z 7.11.2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz.U. z 2014 r. poz. 1662 ze zm.).
[222] *W.R. Wiewiórowski*, Nowe ramy ochrony danych osobowych w Unii Europejskiej, s. 3.
[223] *G. Sibiga*, Dopuszczalny zakres, s. 17.
[224] Dz.U. 2018 poz. 1000; dalej: UODO2018.

UODO2018 stosuje się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 RODO. Zatem jej materialny zakres stosowania wyznacza zakres stosowania samego ogólnego rozporządzenia. W art. 1 ust 2 ustawodawca wyznaczył zakres przedmiotowy ustawy, która określa: podmioty publiczne obowiązane do wyznaczenia inspektora ochrony danych oraz tryb zawiadamiania o jego wyznaczeniu; warunki i tryb akredytacji podmiotu uprawnionego do certyfikacji w zakresie ochrony danych osobowych, akredytowanego przez Polskie Centrum Akredytacji; podmiotu monitorującego kodeks postępowania oraz certyfikacji; tryb zatwierdzenia kodeksu postępowania; organ właściwy w sprawie ochrony danych osobowych; postępowanie w sprawie naruszenia przepisów o ochronie danych osobowych; tryb europejskiej współpracy administracyjnej; kontrolę przestrzegania przepisów o ochronie danych osobowych; odpowiedzialność cywilną za naruszenie przepisów o ochronie danych osobowych i postępowanie przed sądem; odpowiedzialność karną i administracyjne kary pieniężne za naruszenie przepisów o ochronie danych osobowych[225]. Ponadto UODO2018 reguluje również, choć w katalogu w art. 1 nie wymienia, zagadnienia proceduralne, dotyczące ogólnych zasad postępowania toczącego się przed Prezesem Urzędu Ochrony Danych Osobowych, wskazując na jednoinstancyjność postępowania prowadzonego w zakresie nieuregulowanym ustawą w rozdziałach 4–7 i 11 w oparciu o przepisy KPA i przewidując skargę na decyzję Prezesa do sądu administracyjnego (art. 7 UODO2018). Ponadto ustawa określa zagadnienia związane z wyłączeniem stosowania niektórych przepisów RODO (np. redagowania, przygotowywaniu, tworzeniu lub publikowaniu materiałów prasowych[226], a także innych spraw wymienionych w art. 2-5 UODO2018).

Związek między zakresem zastosowania UODO2018 a ogólnym rozporządzeniem ma charakter przedmiotowy i podmiotowy. Ustawa obejmuje zarówno podmioty prywatne, jak publiczne, to tylko w zakresie ich aktywności podlegającej RODO. Tym samym będą występowały takie przypadki, w których podmioty, zwłaszcza publiczne zobowiązane będą do stosowania, zależnie od aktywności, przepisów RODO, a w konsekwencji również podlegać

[225] Na temat UODO2018 zob. m.in. w: *P. Litwiński, P. Barta, D. Dörre-Kolasa*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018; Ustawa o ochronie danych osobowych. Komentarz, pod red. *B. Marcinkowskiego*, Warszawa 2018; *P. Fajgielski*, Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2018.
[226] W rozumieniu ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe.

będą regulacji ustawy o ochronie danych, jak i ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości[227].

Ponadto ustawa wprowadziła zmiany przepisów szczególnych, które stanowiły w większości konsekwencję przyjęcia nowej regulacji (m.in. zmiany odesłań do UODO1997 czy też zmiany przepisów zawierających poprzednią nazwę organu nadzorczego, tj. z Generalnego Inspektora Ochrony Danych Osobowych na Prezesa Urzędu Ochrony Danych Osobowych). Jednak wśród 57 zmienionych ustaw znalazły się również zmiany wykraczające poza wskazany powyżej zakres, a odnoszące się do zagadnień szczególnych – do kilku ustaw dodano przepisy odnoszące się do monitoringu[228]. UODO2018 pozostaje podstawową regulacją prawną, stanowiącą uzupełnienie RODO.

Jednak dla zapewnienia zgodności przepisów krajowych z przepisami ogólnego rozporządzenia konieczne było również dokonanie zmian w wielu regulacjach szczególnych. Prawodawca dokonał tego uchwalając ustawę z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[229]. Ustawa weszła w życie w dniu 4 maja 2019 r.

Konieczność uchwalenia UWprowRODO wynikała z potrzeby zapewnienia skutecznego stosowania przepisów RODO. Ze względu na liczbę i charakter zmian koniecznych do wprowadzenia, a także w trosce o zapewnienie spójnego podejścia, zdecydowano się dokonać ich w jednym akcie normatywnym[230]. Konieczne okazało się usunięcie przepisów, które są sprzeczne z RODO lub które powielają rozwiązania RODO, a także dostosowanie RODO do specyfiki polskiego porządku prawnego. Osiągnąć te cele miała zmiana 162 ustaw szczególnych w zakresie przepisów dotyczących przetwarzania i ochrony danych (która objęła również przepisy UPW, o czym piszę w następnych Rozdziałach). Zmiany te mają charakter zróżnicowany, niekiedy są ograniczone do uchylenia bądź modyfikacji istniejących przepisów, w większości jednak polegają na dodaniu nowych

[227] Zob. *D. Lubasz,* Zakres zastosowania ustawy o ochronie danych osobowych [w:] *D. Lubasz (red.)*, Meritum, s. 423.
[228] Zob. m.in. art. 111 (w ustawie z dnia 26 czerwca 1974 r. – Kodeks pracy), art. 114 (w ustawie z dnia 8 marca 1990 r. o samorządzie gminnym) czy art. 154 (w ustawie z dnia 14 grudnia 2016 r. – Prawo oświatowe)
[229] Dz.U. z 2019 r. poz. 730; dalej: UWprowRODO.
[230] Zob. Uzasadnienie do projektu ustawy o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679, druk Sejmu VIII kadencji nr 3050 z 23.11.2018 r., s. 9.

przepisów i odmiennym ukształtowaniu zagadnień związanych z przetwarzaniem i ochroną danych osobowych[231].

Odrębnym przedmiotem regulacji stała się ochrona danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. W dniu 14 grudnia 2018 r. nastąpiło uchwalenie ustawy wdrażającej dyrektywę 2016/680[232]. Przedmiotową ustawą w przepisach zmieniających dokonano dalszej nowelizacji 42 ustaw. Zgodnie z art. 1 ustawa z 14 grudnia 2018 r. określa m.in. zasady i warunki ochrony danych osobowych przetwarzanych przez właściwe organy w celu rozpoznawania, zapobiegania, wykrywania i zwalczania czynów zabronionych, w tym zagrożeń dla bezpieczeństwa i porządku publicznego, a także wykonywania tymczasowego aresztowania, kar, kar porządkowych i środków przymusu skutkujących pozbawieniem wolności. Ustawa ma zastosowanie do wszystkich „właściwych organów", które przetwarzają dane osobowe w celach wynikających z jej art. 1. Pojęcie to jest kluczowe dla określenia podmiotowego zakresu stosowania ustawy. Ustawodawca wskazuje, że należy je rozumieć jako organ władzy publicznej, jednostkę organizacyjną lub inny podmiot uprawniony na podstawie odrębnych przepisów do przetwarzania danych osobowych (art. 4 pkt 16 ustawy). Chodzi zatem o organ władzy publicznej właściwy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom i w związku z tym uprawniony do przetwarzania danych osobowych[233].

Rozdział 3. Zakres ponownego wykorzystywania informacji sektora publicznego i ogólnego rozporządzenia o ochronie danych osobowych. Wspólny obszar regulacji

3.1. Zakres przedmiotowy i podmiotowy przepisów o ponownym wykorzystywaniu informacji sektora publicznego

Prawo do ponownego wykorzystywania na gruncie prawa polskiego regulowane jest przepisami UPW. Zakres stosowania przepisów wyznaczają podstawowe pojęcia informacji

[231] Zob. szerzej: *P. Fajgielski*, Dostosowanie krajowych przepisów do wymogów ogólnego rozporządzenia o ochronie danych, „Monitor Prawniczy" 2019, nr 22 (dodatek), s. 4-8.
[232] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz. U. z 2019 poz. 125).
[233] Zob. *A. Grzelak, M. Wróblewski*, Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, s. 566.

sektora publicznego, ponownego wykorzystywania, podmiotu zobowiązanego oraz użytkownika, które zostaną omówione poniżej. Uwzględnione zostaną odrębności wynikające z dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE. Przepisy polskiej ustawy nie dokonują bowiem w tym zakresie wprost transpozycji przepisów prawa UE, w wielu miejscach dookreślając normy dyrektyw ze względu na specyfikę krajowego ustawodawstwa. Konieczne wreszcie będzie uwzględnienie zmian, jakie wprowadza dyrektywa 2019/1024, które w mojej opinii mają kluczowe znaczenie dla wyznaczenia zakresu ponownego wykorzystywania informacji sektora publicznego.

UPW określa zasady i tryb udostępniania i przekazywania informacji sektora publicznego w celu ponownego wykorzystywania; podmioty, które udostępniają lub przekazują informacje sektora publicznego; warunki ponownego wykorzystywania oraz zasady ustalania opłat za ponowne wykorzystywanie (art. 1 UPW). Ustawa konstytuuje przysługujące każdemu prawo do ponownego wykorzystywania informacji sektora publicznego udostępnionych w systemie teleinformatycznym, a w szczególności na stronie podmiotowej Biuletynu Informacji Publicznej podmiotu zobowiązanego lub w centralnym repozytorium informacji publicznej lub w inny sposób oraz przekazanych na wniosek o ponowne wykorzystywanie (art. 5 UPW).

Dla ustalenia zakresu przedmiotowego UPW konieczne będzie zatem zdefiniowanie pojęć informacji sektora publicznego oraz ponownego wykorzystywania. W celu zaś wyznaczenia zakresu podmiotowego zdefiniować należy pojęcie podmiotu zobowiązanego (podmiotu który udostępnia lub przekazuje informacje sektora publicznego) oraz podmiotu uprawnionego (użytkownika). Pojęcie przekazania lub udostępnienia związane jest ze źródłem pozyskania informacji sektora publicznego, które wyznacza jedocześnie tryb ponownego wykorzystywania. Zagadnienie to, podobnie jak zasady i warunki, zostały omówione w Rozdziale 4.

3.1.1. Informacja sektora publicznego

Przepisy UPW wprowadziły do polskiego porządku prawnego nowe pojęcie informacji sektora publicznego. Przed wejściem w życie tej ustawy zakres przedmiotowy ponownego wykorzystywania wyznaczało pojęcie informacji publicznej. Obecnie zakres ten wyznacza informacja sektora publicznego. Zakres pojęcia informacji sektora publicznego jest szerszy od pojęcia informacji publicznej i odpowiada wprost definicji dokumentu, o którym mowa w art. 2 pkt 3 dyrektywy 2003/98/WE. Przepisy dyrektywy 2019/1024 rozszerzając zakres

ponownego wykorzystywania lub wyodrębniając szczególne kategorie informacji sektora publicznego wciąż opierają się na pojęciu dokumentu, którego definicja została co do zasady niezmieniona. Zgodnie z art. 2 pkt 6 dyrektywy 2019/1024 „dokument" oznacza: a) dowolną treść niezależnie od jej nośnika (papier lub forma elektroniczna lub zapis dźwiękowy, wizualny bądź audiowizualny); lub b) dowolną część tej treści. Dodatkowo można wskazać motywie 11 preambuły dyrektywy 2003/98/WE, który dookreśla, że pojęcie dokumentu obejmuje wszelkie posiadane przez organy sektora publicznego przejawy działań, faktów lub informacji – oraz wszelkie kompilacje takich działań, faktów lub informacji – niezależnie od zastosowanego w tym celu środka (zapisane na papierze, zapisane w formie elektronicznej lub zarejestrowane w formie dźwiękowej, wizualnej lub audiowizualnej).

Należy odnotować, że prawodawca UE posłużył się znaną z rozporządzenia 1049/2001 definicją, w myśl której „dokument" oznacza wszelkie treści bez względu na nośnik (zapisane na papierze, przechowywane w formie elektronicznej czy jako dźwięk, nagranie wizualne czy audiowizualne) dotyczące kwestii związanych z polityką, działalnością i decyzjami mieszczącymi się w sferze odpowiedzialności tych instytucji (art. 3).

Tak szeroko ujęte pojęcie dokumentu powoduje, że podmioty objęte mocą dyrektywy będą podlegały zasadom ponownego wykorzystywania w zakresie wszelkich posiadanych i utrwalonych informacji. Nie oznacza to jednak, że te wszystkie dokumenty będą przez te podmioty udostępniane do ponownego wykorzystywania, decydujące znaczenie będą miały przepisy dotyczące wyłączeń i ograniczeń stosowania przepisów ze względu na dobra chronione, np. związane z poufnością informacji, prawami własności intelektualnej czy szczegółowymi kategoriami podmiotów. Główną normą kolizyjną, jak już wspominano, pozostaje art. 1 ust. 3 dyrektywy 2019/1024, zgodnie z którym dyrektywa opiera się na unijnych i krajowych systemach dostępu i pozostaje bez uszczerbku dla nich. Istotne dla zakresu pojęcia dokumentu ma również art. 1 ust. 2 lit. d, na mocy którego dyrektywa 2019/1024 nie ma zastosowania do dokumentów wyłączonych z dostępu na podstawie systemów dostępu państw członkowskich (poprzednio art. 1 ust. 2 lit. c dyrektywy 2003/98/WE).

Przede wszystkim zaś dla rekonstrukcji zakresu przedmiotowego dokumentu będzie miał znaczenie art. 1 ust. 2 lit. a dyrektywy 2019/1024[234] zgodnie z którym ponownym wykorzystywaniem nie będę objęte dokumenty, których wydawanie jest działalnością

[234] Brzmienie art. 1 ust. 2 lit. a dyrektywy 2003/98/WE było nieznacznie odmienne, ale sens pozostaje ten sam, tj. dyrektywa nie ma zastosowania dokumentów, których dostarczanie jest działalnością leżącą poza zakresem zadań publicznych zainteresowanych organów sektora publicznego określonych prawem lub innymi wiążącymi regułami w Państwie Członkowskim lub – w braku takich reguł – określonych zgodnie z powszechną praktyką administracyjną w danym Państwie Członkowskim.

wykraczającą poza zakres zadań publicznych zainteresowanych organów sektora publicznego określonych przepisami ustawowymi lub innymi wiążącymi przepisami w państwie członkowskim lub, w przypadku braku takich przepisów, określonych zgodnie z powszechną praktyką administracyjną w zainteresowanym państwie członkowskim, o ile zakres zadań publicznych jest przejrzysty i podlega przeglądowi.

Co ciekawe, choć w tytule dyrektyw zakres przedmiotowy ponownego wykorzystywania wyznacza informacja sektora publicznego, pozostaje ona na gruncie przepisów prawa UE niezdefiniowana, a w tekście dyrektyw prawodawca europejski posługuje się wyłącznie pojęciem dokumentu.

3.1.1.1. Definicja normatywna

Zgodnie z art. 2 ust. 1 UPW informacją sektora publicznego jest każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotów zobowiązanych. Definicja legalna opiera się zatem na trzech elementach konstrukcyjnych, tj. zakresie przedmiotowym (treść) oraz wymogów jej utrwalenia i posiadania przez podmiot zobowiązany.

Ustawodawca – wzorem z definicji dokumentu - nie wprowadził żadnego ograniczenia o charakterze przedmiotowym. Informacją sektora publicznego jest każda informacja (cały zasób informacyjny podmiotu zobowiązanego) pod warunkiem spełnienia innych warunków wskazanych w definicji. Dla uznania danej treści jako informacji sektora publicznego bez znaczenia pozostaje, czego ona dotyczy. Przy kwalifikowaniu więc danej informacji do kategorii informacji sektora publicznego nie podlega ocenie jej treść, ale jedynie fakt utrwalenia i posiadania przez podmioty zobowiązane[235].

Przez utrwalenie informacji należy rozumieć jako zapisanie określonej treści lub jej części na jakimkolwiek nośniku[236], przy czym wymienione przez ustawodawcę sposoby utrwalenia mają jedynie charakter przykładowy. Informacja sektora publicznego musi zatem

[235] *A. Piskorz-Ryń*, Zakres przedmiotowy stosowania przepisów o ponownym wykorzystywaniu [w:] *E. Badura., M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń., M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, Ponowne wykorzystywanie informacji sektora publicznego, Warszawa 2016, s. 36.

[236] *A. Piskorz-Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 170-171.

być obligatoryjnie utrwalona, może być wyrażona w dowolnej formie i zapisana w dowolnej postaci[237].

Ostatnim elementem konstrukcyjnym definicji stanowi kryterium posiadania. Treść musi być faktycznie w posiadaniu podmiotu zobowiązanego, przy czym dla jej zakwalifikowania jako informacji sektora publicznego bez znaczenia jest to, kto daną treść wytworzył i czy w ogóle pochodzi ona od podmiotu publicznego. „Posiadaczem" informacji sektora publicznego będą podmioty zobowiązane, które wytworzyły daną treść w związku z realizacją zadań publicznych, jak i te które otrzymały daną treść w związku z wykonywaniem tych zadań[238]. O powstaniu obowiązku udostępnia lub przekazania informacji sektora publicznego decyduje rzeczywisty i obiektywny fakt posiadania, a nie właściwość administracyjna[239]. Zobowiązanym jest każdy podmiot, który posiada informację niezależnie od tego, czy wiąże się ona z jego zakresem kompetencji lub powinien ją posiadać, z uwagi na zakres kompetencji[240].

Tak szeroko ujęta definicja informacji sektora publicznego powoduje, że obejmuje swoim zakresem informacje publiczne oraz wszelkie inne treści niemieszczące się w granicach pojęcia informacji publicznej, które pozostały utrwalone i są w posiadaniu podmiotów wymienionych w art. 3 UPW. W praktyce rekonstrukcja zakresu przedmiotowego UPW następować będzie na podstawie przepisów wyłączających stosowanie ustawy (tj. wyłączeń podmiotowych zgodnie z art. 4 ust 1 oraz przedmiotowych zgodnie z art. 4 ust. 2UPW) oraz przesłanek ograniczających ponowne wykorzystywanie (art. 6 UPW), nie oznacza to z kolei eliminacji danych treści z zakresu pojęcia informacji sektora publicznego. Treści te wciąż mieścić się będą w zakresie pojęcia informacji sektora publicznego, lecz ze względu na wystąpienie okoliczności wyłączającej lub ograniczającej nie będzie możliwe ich ponowne wykorzystywanie.

3.1.1.2. Szczególne rodzaje informacji sektora publicznego

Przepisy UPW nie rozróżniają szczególnych rodzajów czy typów informacji sektora publicznego. W dyrektywie 2019/1024 prawodawca europejski po raz pierwszy wyodrębnił w ramach ogólnego pojęcia dokumentu (informacji sektora publicznego) szczególne jego

[237] *A. Piskorz-Ryń*, Zakres przedmiotowy, s. 36.
[238] *A. Piskorz-Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 171.
[239] *A. Piskorz-Ryń*, Zakres przedmiotowy, s. 37.
[240] Wyrok NSA z 31.01.2013 r., I OSK 2571/12.

rodzaje. Pojęcia te wciąż mieścić się będą w zakresie definicji dokumentu, ze względu na odrębności w odniesieniu do zakresów podmiotowych czy szczególnych różnić w zakresie zasad i sposobu dystrybucji do ponownego wykorzystywania, zasadne było wyszczególnienie danych dynamicznych, danych badawczych czy danych o wysokiej wartości. Dyrektywa 2013/37/UE poszerzająca zakres podmiotowy o zasoby bibliotek, archiwów i muzeów przewidywała wprawdzie szczególne rozwiązania dla dokumentów będących w posiadaniu tych instytucji (np. ograniczenia ze względu na prawa własności intelektualnej czy umów na wyłączność), nie wprowadzono jednak definicji dla tych zasobów, tym samym przedmiotowo nie były wyodrębnione z pojęcia dokumentu.

Zagadnienie to zasługuje na omówienie, ponieważ determinować będzie przyszłe przepisy krajowe implementujące nową dyrektywę.

Niewątpliwie przełomową zmianą wprowadzoną przepisami dyrektywy 2019/1024 jest wprowadzenie nowej kategorii informacji sektora publicznego, czyli danych dynamicznych, które mają być udostępniane do ponownego wykorzystywania poprzez interfejs programowania aplikacji (API). Dane dynamiczne oznaczają dokumenty w formie elektronicznej podlegające częstym aktualizacjom lub aktualizacjom w czasie rzeczywistym (art. 2 pkt 8 dyrektywy 2019/1024). Za dane dynamiczne mogą być uznane rozkłady jazdy czy dane z czujników, jak np. dane meteorologiczne.

Jest to rozwiązanie, które jednocześnie może stanowić znaczące wyzwanie techniczne, jak i przede wszystkim finansowe dla podmiotów zobowiązanych[241]. Dlatego dyrektywa 2019/1024 przewiduje nałożenie na państwa członkowskie jedynie „miękkiego" obowiązku udostępniania danych dynamicznych dostępnych w czasie rzeczywistym oraz wprowadzenie wymogu, zgodnie z którym organy sektora publicznego są zobowiązane do nieodpłatnego udostępnienia tych danych za pomocą API. W tym zakresie istotny jest art. 5 ust. 6 dyrektywy, zgodnie z którym, jeżeli udostępnienie dokumentów (tj. danych dynamicznych) natychmiast po ich zgromadzeniu przekroczyłoby możliwości finansowe i techniczne organu sektora publicznego lub przedsiębiorstwa publicznego, udostępnia się je w terminie, który nie powoduje nadmiernego ograniczenia możliwości wykorzystania ich potencjału gospodarczego.

Co do zasady, dane dynamiczne należy udostępniać natychmiast po ich zgromadzeniu, za pośrednictwem API tak, aby ułatwić rozwój bazujących na tych danych aplikacji internetowych i mobilnych oraz aplikacji korzystających z chmury obliczeniowej. Ponowne wykorzystywanie i wymiana danych poprzez odpowiednie wykorzystanie API przynosi

[241] *D. Sybilski,* Projekt nowej dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego, „Informacja w Administracji Publicznej" 2018, nr 3, s. 4.

powszechne korzyści, gdyż umożliwia twórcom oprogramowania i przedsiębiorstwom typu *start-up* tworzenie nowych usług i produktów. Odgrywa również ważną rolę w tworzeniu cennych ekosystemów wokół danych, które często pozostają niewykorzystane. Podstawę konfiguracji i stosowania API musi stanowić kilka zasad: stabilność, utrzymanie przez cały cykl użytkowania, jednolitość sposobu korzystania i standardów, łatwość użytkowania oraz bezpieczeństwo[242].

Oprócz danych dynamicznych poprzez API będą również udostępniane zbiory danych o wysokiej wartości. Podstawowa różnica w dystrybucji obu kategorii danych polega na tym, że w przypadku tzw. danych o wysokiej wartości obowiązek udostępniania poprzez API jest bezwzględny i dane będą udostępniane nieodpłatnie (opłaty będą mogły pobierać przedsiębiorstwa publiczne oraz biblioteki, muzea i archiwa).

Nowym rozwiązaniem nieznanym poprzednim dyrektywom w sprawie ponownego wykorzystywania jest upoważnienie Komisji Europejskiej do określenia w drodze aktu wykonawczego szczególnych zbiorów danych o wysokiej wartości spośród 6 kategorii tematycznych wymienionych w Załączniku 1 do dyrektywy 2019/1024. Są to następującego rodzaju dane: geoprzestrzenne; dotyczące obserwacji Ziemi i środowiska; meteorologiczne; statystyczne; dotyczące przedsiębiorstw i ich własności oraz dotyczące mobilności.

Danymi o wysokiej wartości są te informacje sektora publicznego, których ponowne wykorzystywanie wiąże się z istotnymi korzyściami społeczno-ekonomicznymi, w szczególności ze względu na ich przydatność do tworzenia usług i zastosowań o wartości dodanej, a także znaczny krąg potencjalnych beneficjentów usług i zastosowań o wartości dodanej, opartych na tych zbiorach danych (art. 2 pkt 10 dyrektywy 2019/1024).

Zbiory danych o wysokiej wartości podmioty zobowiązane będą udostępniały nieodpłatnie, w formacie nadającym się do odczytu maszynowego i za pośrednictwem API. Warunki ponownego wykorzystywania tego rodzaju zbiorów danych muszą być zgodne z postanowieniami licencji na zasadzie otwartych standardów.

Jedną z ważniejszych projektowanych zmian jest włączenie w zakres ponownego wykorzystywania nowej kategorii informacji sektora publicznego, tj. danych badawczych. Z zakresu stosowania dyrektywy w dalszym ciągu wyłączone będą publikacje w czasopismach naukowych, gdyż wiążą się z nimi dodatkowe wyzwania związane z prawami własności intelektualnej (art. 2 pkt 7 dyrektywy 2019/1024). Należy podkreślić, że w zakres dyrektywy zostaną włączone jedynie te dane badawcze, które są finansowane ze środków publicznych oraz

[242] Motyw 28 preambuły dyrektywy 2019/1024.

są już dostępne w wersji cyfrowej, a dostęp do nich zapewniono za pośrednictwem repozytorium instytucjonalnego lub tematycznego (art. 10 ust. 2 dyrektywy 2019/1024). W praktyce dane badawcze obejmą dane statystyczne, wyniki eksperymentów, pomiarów, obserwacji prowadzonych w terenie, wyniki ankiet, nagrania wywiadów i zdjęcia. Obejmą one także metadane, specyfikacje i inne obiekty cyfrowe (motyw 23 preambuły dyrektywy). Dane badawcze nie będą udostępnianie na wniosek zainteresowanego użytkownika, oznacza to, że ponownym wykorzystywaniem będą objęte jedynie te dane badawcze, które już są publicznie dostępne.

3.1.2. Informacja sektora publicznego a informacja publiczna

Zgodnie z podstawową normą kolizyjną dyrektywa 2003/98/WE oraz dyrektywa 2019/1024 opiera się na unijnych i krajowych systemach dostępu i pozostaje bez uszczerbku dla nich. Oznacza to, że przepisy istniejących w państwach członkowskich systemów dostępu i to przepisy tych systemów powinny decydować o dostępności lub niedostępności informacji. W Polsce głównym aktem „systemu dostępu" pozostaje oczywiście UDIP, którego zakres przedmiotowy wyznacza pojęcie informacji publicznej. Aby wyznaczyć relację pomiędzy informacją sektora publicznego a informacją publiczną konieczne jest zdefiniowanie tej ostatniej.

Interpretacja pojęcia informacji publicznej ma również znaczenie dla głównego zagadnienia niniejszej pracy, ponieważ wyznaczenie zakresu pojęcia informacji publicznej bywa instrumentem używanym przez podmioty zobowiązane do ochrony poufności informacji, w tym prywatności i danych osobowych.

Artykuł 1 ust. 1 UDIP stanowi, iż „każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy." Przepis określając zakres przedmiotowy ustawy pozornie definiuje pojęcie informacji publicznej[243]. Definicja ta jest krytykowana przez wielu praktyków dostępu do informacji publicznej, jej ogólnikowość wywołuje trudności interpretacyjne oraz przede wszystkim obarczona jest błędem logicznym *ignotum per ignotum* (definiuje nieznane przez nieznane)[244].

Ponadto pomiędzy regulacją ustawową a konstytucją zachodzą rozbieżności. Konstytucja co prawda nie wprowadziła definicji informacji publicznej, ale odniosła ją do

[243] *Ibidem*, s. 12.
[244] *M. Jaśkowska*, Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego, Toruń 2002, s. 26.

kryterium podmiotowego (wykonywania lub przechowywania przez władze publiczne) i przedmiotowego (działalność władzy publicznej lub innych podmiotów wykonujących zadania publiczne)[245]. Natomiast ustawa posługuje się przedmiotową definicją „sprawy publicznej", co może prowadzić do interpretacji, iż istnieją inne sprawy niż publiczne, które nie podlegają udostępnieniu przez podmioty zobowiązane[246]. Taką interpretację należałoby jednak uznać za zawężającą konstytucyjne prawo do informacji i z tego powodu niedopuszczalną. Każda zatem działalność organów administracji publicznej dotyczy spraw publicznych. Problem zaś pojawi się w przypadku udostępniania informacji przez podmioty zobowiązane wymienione w art. 4, które realizują także inne niż publiczne zadania, np. osoby prawne, w których Skarb Państwa ma pozycję dominującą w rozumieniu przepisów o ochronie konkurencji i konsumentów (art. 4 ust. 1 pkt 5 UDIP).

Rekonstruując pojęcie informacji publicznej, trzeba posłużyć się łącznie kryterium podmiotowym oraz przedmiotowym[247]. Kryterium podmiotowe wskazuje, że informacja taka odnosi się "do działalności organów władzy publicznej oraz osób pełniących funkcje publiczne", a także innych podmiotów wykonujących zadania publiczne. Kryterium przedmiotowe nie zostało określone wprost, ale można uznać, że taka informacja powinna być wykonana lub przechowywana przez władze publiczne[248].

Z kolei *G. Szpor* opierając się na interdyscyplinarnej definicji pojęcia informacji (zob. Rozdział 3.3.1.) proponuje za informację publiczną uznać dobro (niematerialne) zmniejszające niepewność w sprawach polityki wewnętrznej i zagranicznej oraz innych, której obejmuje katalog wymieniony w art. 6 UDIP[249].

Orzecznictwo sądów administracyjnych przyjmuje szerokie pojęcie „informacji publicznej", odnoszące się zarówno do jej treści, jak i formy. NSA w swoim orzecznictwie wprost opowiada się za szerokim rozumieniem informacji publicznej, nawiązującym do art. 61 Konstytucji RP[250]. Zdaniem NSA informacją publiczną jest każda informacja wytworzona i posiadana przez szeroko rozumiane władze publiczne.

W ostatnich latach można wręcz zaobserwować linię orzeczniczą sądów administracyjnych przyjmujących szeroki zakres informacji podlegających udostępnieniu tak

[245] *W. Sokolewicz* [w:] *L. Garlicki (red.),* Komentarz do Konstytucji RP Warszawa 2005, cz. II, s. 20.
[246] *A. Sarota*, Granice dostępności informacji publicznej, „Kontrola państwowa" 2012, nr 6, s. 58.
[247] Zob. *M. Bidziński, M. Chmaj, P. Szustakiewicz*, Ustawa o dostępie do informacji publicznej. Komentarz, komentarz do art. 1 pkt 3, Legalis/Wyd. 2018.
[248] Zob. *M. Jaśkowska*, Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego, s. 28–29.
[249] *G. Szpor*, Pojęcie informacji a zakres ochrony danych osobowych [w:] *P. Fajgielski (red.)*, Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia, Lublin 2008, s. 8.
[250] Zob. np. wyrok NSA z 05.04.2013 r., I OSK 175/13.

w trybie UDIP, jak i innych ustaw szczególnych określających inne niż UDIP tryby dostępu[251]. Linia orzecznicza została wyznaczona wyrokami w 2002 r., zgodnie z którymi informacją publiczną jest każda wiadomość wytworzona lub odnoszona do szeroko rozumianych władz publicznych oraz wytworzona lub odnoszona do innych podmiotów wykonujących funkcje publiczne w zakresie wykonywania przez nie zadań władzy publicznej i gospodarowania mieniem komunalnym lub majątkiem Skarbu Państwa[252]. Informacją publiczną będzie zatem treść wszelkiego rodzaju dokumentów odnoszących się do organu władzy publicznej lub podmiotu niebędącego organem administracji publicznej, lecz wykonującego zadania publiczne (np. fundacja). Są informacją publiczną dokumenty bezpośrednio przez te podmioty wytworzone, ale i te, których używają one przy realizacji przewidzianych prawem zadań, nawet gdy wprost od nich nie pochodzą[253]. Szerokie rozumienie pojęcia informacji publicznej jest kontynuowane w orzecznictwie sądowoadministracyjnym[254].

Informacją publiczną w rozumieniu UDIP jest każda informacja o sprawach publicznych. Kluczowe zatem dla definicji informacji publicznej są dwa elementy *definiens*, czyli wyrażenia informacja oraz sprawa publiczna.

Według Słownika PWN w języku polskim słowo informacja oznacza „powiadomienie o czymś, zakomunikowanie czegoś, wiadomość wskazówka, pouczenie"[255]. Informacją jest każdy opis rzeczywistości niezależnie od tego czy zgodny z prawdą. Przekazując informację przekazuje się opis jakiegoś stanu rzeczywistości lub procesu[256]. Za informację należy uznać utrwalony w jakikolwiek sposób (także w pamięci człowieka) komunikat, wiedza, świadomość o jakimś fakcie[257].

Z kolei pod pojęciem "sprawy publicznej", zdaniem *H. Izdebskiego,* należy rozumieć każdy "przejaw aktywności władzy publicznej (jej organów), osób pełniących funkcje publiczne i samorządów oraz już tylko niektóre działania innych osób, jednostek organizacyjnych, a to tylko takie, które wiążą się z wykonywaniem zadań publicznych, przy jednoczesnym dysponowaniu majątkiem publicznym, przez które należy rozumieć również

[251] Mowa tu na przykład o ustawie z dnia 17 maja 1989 r. - Prawo geodezyjne i kartograficzne (Dz. U. z 2020 r. poz. 276, 284, 782, 1086).
[252] Zob. *M. Jaśkowska*, op. cit.
[253] Zob. m.in. wyroki NSA z dnia: 30.10.2002 r., II SA 1956/02; 25.03.2002 r., II SA 4059/02; 12.12.2006 r., I OSK 123/06; 20.01.2012 r., I OSK 2118/11; 29.02.2012 r., I OSK 2215/11; 01.12.2011 r., I OSK 1516/11; 01.12.2011r., I OSK 1150/11.
[254] Zob. np. wyrok NSA z 03.01.2012 r., I OSK 2157/11 oraz wyrok NSA z 20.01.2012 r., I OSK 2118/11.
[255] *S. Dubisz* (red.), Uniwersalny słownik języka polskiego PWN, Warszawa 2003.
[256] *T. R. Aleksandrowicz*, Komentarz do ustawy o dostępie do informacji publicznej, Warszawa 2006 r., s. 95.
[257] *M. Maciejewski*, Prawo informacji – zagadnienia podstawowe [w:] *W. Góralczyk*, Prawo informacji. Prawo do informacji, Warszawa 2006, s. 29.

środki publiczne w rozumieniu przepisów o finansach publicznych[258]" . Z kolei *M. Jabłoński* i *K. Wygoda* uznali, że w zakres pojęcia "sprawa publiczna" wchodzą wszystkie działania lub zaniechania osób (piastunów) tworzących skład osobowy organów władzy publicznej, jak i tych osób, które w zakresie wynikającym z powierzenia lub porozumienia uczestniczą w procesie realizacji powierzonych im zadań i kompetencji publicznoprawnych, w znaczeniu organizacyjnym (odnoszącym się do struktury podmiotów, organów, jak i pozostałych instytucji), materialnym oraz formalnym[259].

Nie stanowią informacji publicznej z kolei polemiki z dokonanymi ustaleniami[260] czy też interpretacja przepisów prawa czy konkretnego dokumentu. Informacja publiczna musi dotyczyć sfery istniejących już faktów, a nie niezmaterializowanych w jakiejkolwiek postaci zamierzeń podejmowania określonych działań, i może pochodzić od dowolnych podmiotów, jeżeli tylko dotyczy „sprawy publicznej"[261].

Wnioskiem o dostęp do informacji może być dotyczyć informacji o dany stan istniejący na dzień udzielania odpowiedzi. Realizacja wniosku nie może zmierzać do inicjowania działań ani dotyczyć przyszłych niesprecyzowanych zamierzeń[262]. W wyroku z 14.09.2012 r. (I OSK 1177/12) NSA stwierdził, że realizacja wniosku nie może prowadzić do preparowania informacji nowej, "pod wniosek " w oparciu o interpretację określonych gestów czy zachowań. Dopóki określona informacja istnieje tylko w pamięci przedstawiciela władzy publicznej i nie została utrwalona w jakiejkolwiek formie tak, aby można było w sposób nie budzący wątpliwości odczytać jej treść, dopóty informacja taka nie ma waloru informacji publicznej.

NSA uznał w wyroku z 27 stycznia 2012 r.(I OSK 2130/11) za informację publiczną opinie ekspertów wykonane na zlecenie Kancelarii Prezydenta RP, dotyczące konkretnego projektu ustawy przesłanego Marszałkowi Sejmu celem wszczęcia postępowania legislacyjnego. Nie są jednak informacjami publicznymi – zdaniem sądu w wyroku z 16 czerwca 2009 r., I OSK 89/09 – opinie zlecone przez organ administracji publicznej, jeżeli dotyczą nie faktów, lecz ewentualnych zamierzeń tego organu.

W innej sprawie NSA uznał, iż notatki ze spotkań służbowych urzędników stanowią informację publiczną[263]. Nieuprawniony byłby wniosek, iż warunkiem uznania danych

[258] *H. Izdebski*, Samorząd terytorialny: podstawy ustroju i działalności, Warszawa 2001, s. 209–210.
[259] *M. Jabłoński, K. Wygoda*, Dostęp do informacji i jego granice: wolność informacji, prawo dostępu do informacji publicznej, ochrona danych osobowych, Wrocław 2002, s. 177–178.
[260] Zob. wyrok NSA z 12.07.2011 r., I OSK 610/11.
[261] *I. Kamińska, M. Rozbicka-Ostrowska*, op. cit., s. 18.
[262] *Ibidem*.
[263] Por. wyrok WSA w Kielcach z 26.06.2008 r., II SAB/Ke 7/08, wyrok WSA w Warszawie z 29.10.2007 r., II SAB/Wa 85/07, wyrok WSA w Krakowie z 30.01.2009 r., II SAB/Kr 109/08, wyrok NSA z 30.10.2002 r., II SA 181/02.

publicznych za informację publiczną jest jedynie zmaterializowanie tej informacji w formie dokumentów urzędowych, o jakich mowa w art. 6 ust. 1 pkt 4 lit. a UDIP. Wyraz "informacja" obejmuje swoim znaczeniem znacznie szerszy zakres pojęciowy niż wyraz "dokumenty" i nie można zawężać i utożsamiać dostępu do informacji publicznej z dostępem do dokumentów. Należy jednak podnieść, że to dokument – w szerokim tego słowa rozumieniu – będzie podstawowym nośnikiem informacji publicznej.

Informacją publiczną jest nie tylko dokument urzędowy, tym niemniej informacja tego rodzaju winna być w jakiejś formie uprzednio uzewnętrzniona, utrwalona, a poprzez to możliwa do udostępnienia, czy w formie informacji prostej (nieprzetworzonej), czy to przetworzonej (np. wytworzonej w oparciu o istniejące zestawienia, rejestry).

Podsumowując definicję sprawy publicznej, należy uznać, iż jest nią działalność zarówno organów władzy publicznej, jak i samorządów oraz osób i jednostek organizacyjnych w zakresie wykonywania zadań władzy publicznej oraz gospodarowaniem mieniem publicznym (komunalnym lub Skarbu Państwa).[264] Informacja może dotyczyć sprawy publicznej nie tylko wtedy, gdy została wytworzona przez te podmioty, ale jest nią także informacja, która się do nich odnosi w zakresie w jakim podmioty te wykonują zadania publiczne lub gospodarują mieniem publicznym[265].

Natomiast sprawą publiczną nie jest konkretna indywidualna sprawa danej osoby lub podmiotu wykonujących wyżej wymienione funkcje publiczne, zwłaszcza o charakterze prywatnym. Nie może zostać uznana za sprawę publiczną, ta informacja, która dotyczy tego, tego co „prywatne, niepubliczne, osobiste, intymne"[266].

Niejednokrotnie jednak NSA odwołuje się do kryterium przedmiotowego, czyli realizacji zadania publicznego. W wyroku z dnia 9 lutego 2007 r. (I OSK 517/06) sąd uznał, że informacją publiczną są nie tylko dokumenty bezpośrednio zredagowane i technicznie wytworzone przez organ administracji publicznej, ale przymiot taki będą posiadać także te, których organ używa do zrealizowania powierzonych mu prawem zadań nawet, gdy prawa autorskie należą do innego podmiotu. Zatem informacją publiczną stanowią wszystkie materiały, które organ wykorzystuje do zrealizowania powierzonych prawem zadań, nawet wtedy, gdy nie posiada do nich praw autorskich. Podstawowe znaczenie ma w tym wypadku fakt, że dokumenty te służą realizacji zadań publicznych przez określone organy i zostały

[264] *I. Kamińska I.,M. Rozbicka-Ostrowska,* op. cit., s. 17.
[265] Zob. wyrok NSA z 25.03.2003 r., II SA 4059/02.
[266] *G. Sibiga*, Dostęp do informacji publicznej a prawa do prywatności jednostki i ochrony jej danych osobowych, „Samorząd Terytorialny" 2003, nr 11, s. 5-6.

wytworzone na zlecenie tych organów. Nie chodzi bowiem o rozporządzenie prawami autorskimi, lecz o dostęp do treści dokumentu stworzonego na zlecenie organu administracji publicznej w celu realizacji zadań publicznych[267].

Jak zostało wykazane powyżej definicja informacji publicznej zawarta w art. 1 UDIP jest bardzo ogólna i niedookreślona. Ustawodawca w art. 6 podjął próbę konkretyzacji przedmiotu informacji publicznej tworząc otwarty, przykładowy katalog źródeł i rodzajów informacji podlegających udostępnieniu.

Przedmiotowy katalog – jak powiedziano – poprzez użycie sformułowania „w szczególności" jest otwarty. Konsekwencją tego będzie przyjęcie, iż informacją publiczną mogą być inne informacje, niż te wymienione w art. 6. W przypadku wątpliwości, czy żądana informacja jest informacją publiczną, należy – zdaniem NSA – respektując zasadę powszechnego dostępu, interpretować przepisy na korzyść wykonującego prawo do takiej informacji[268].

Katalog ten ma przede wszystkim znaczenie dla obowiązku publikowania informacji w BIP. Wynika to wprost z art. 8 ust. 3 UDIP, informacje te, winny być obligatoryjnie udostępniane przez podmioty zobowiązane na prowadzonych przez nie stronach podmiotowych BIP.

Na tle problematyki dokumentu podlegającemu udostępnieniu w trybie UDIP nakłada się zasygnalizowane powyżej zagadnienie tzw. dokumentu wewnętrznego. „Dokument wewnętrzny" nie ma charakteru prawnego, nie jest on zdefiniowany na gruncie UDIP. Pojawił się on w obiegu w wyniku stosowania prawa, występuje w orzecznictwie sądów administracyjnych. W orzecznictwie wyrażany jest pogląd, iż organom władzy publicznej niezbędna jest możliwość podejmowania decyzji dopiero po zebraniu zasobu niezbędnych informacji, uzgodnieniu stanowisk i przeanalizowaniu kilku możliwych wariantów danego rozstrzygnięcia.

W orzecznictwie NSA można w tym zakresie zaobserwować pewną niekonsekwencję. Jak udowodniono powyżej dla udostępnienia dokumentu nie ma znaczenia jego wewnętrzny, roboczy czy też „prywatny" charakter. Istotna jest zaś zawartość dokumentu, do czego treść dokumentu się odnosi, czyli realizacji zadania publicznego. W wyroku w sprawie udostępnienia ekspertyz przez Kancelarię Prezydenta dotyczących OFE sąd dokonał dyskusyjnego podziału

[267] Por. wyroki NSA z: 15.7.2011 r., I OSK 667/11; 9.2.2007 r., I OSK 517/06; 7.12.2010 r., I OSK 1774/10; 18.9.2008 r., I OSK 315/08.
[268] Zob. wyrok NSA z 02.07. 2003 r., II SA 837/03.

na dwie kategorie dokumentów tj. podlegających i niepodlegających udostępnieniu[269]. Zdaniem NSA „wszystkie dokumenty i informacje znajdujące się w posiadaniu Kancelarii Prezydenta RP, w tym również wszystkie opinie prawne i ekspertyzy, stanowią informację publiczną (…) Opinie te nie są jednak informacją publiczną jeżeli nie dotyczą konkretnego aktu będącego już przedmiotem toczącego się procesu legislacyjnego. Są natomiast dokumentem wewnętrznym, służącym gromadzeniu informacji, które w przyszłości mogą zostać wykorzystane w procesie decyzyjnym. Trzeba przy tym dodać, że opinie i ekspertyzy mające jedynie charakter poznawczy nie odnoszą się wprost do przyszłych działań i zamierzeń podmiotu zobowiązanego mają jedynie poszerzyć zakres wiedzy i informacji posiadanych przez ten podmiot. Dlatego poddanie tego procesu ścisłej kontroli społecznej byłoby niecelowe i utrudniłoby wewnętrzny proces kształtowania się stanowisk uzgadniania i ścierania się opinii dotyczących istniejącego stanu rzeczy, jego oceny oraz ewentualnej potrzeby zmian. Odmiennie ocenić należy ekspertyzy i opinie dotyczące konkretnego projektu aktu prawnego, co do którego trwa proces legislacyjny. Akty te dotyczą faktów, bo do takich należy projekt aktu prawnego przedłożony Sejmowi".

Za dokumenty wewnętrzne zostały przez NSA także uznana korespondencja podmiotów zobowiązanych (np. urzędników), która ma charakter roboczy i odnosi się do spraw organizacyjnych i porządkowych[270].

Podsumowując linię orzeczniczą NSA w tym zakresie, dokumenty wewnętrzne służą realizacji zadania publicznego, ale nie przesądzają o kierunkach działania organu. Mają głownie charakter pomocniczy, ich celem jest bowiem wymiana informacji, zgromadzenie materiałów czy uzgodnienie stanowisk. Mogą mieć dowolną formę i być zapisane na dowolnym nośniku. Przede wszystkim zaś odróżnia je od dokumentów urzędowych to, iż nie prezentują one stanowiska organu, nie są wiążące co do sposobu załatwienia sprawy[271].

Trzeba zaznaczyć, iż koncepcja dokumentu wewnętrznego budzi kontrowersje, w literaturze przedmiotu podnosi się brak konstytucyjnego umocowania dokumentu wewnętrznego, wskazując że jest „przejawem prawa sędziowskiego"[272]. W orzecznictwie sądów administracyjnych po etapie szerokiego ujmowania pojęcia informacji publicznej wypracowanego na tle art. 1 ust. 1 UDIP zaczęły pojawiać się wyraźne tendencje do jej zawężania. „Są one wynikiem pewnych okoliczności obiektywnych, jak i przyczyn

[269] Wyrok NSA z 27.01.2012 r., I OSK 2130/11.
[270] Zob. wyrok NSA z 15.07.2010 r., I OSK 707/10.
[271] *I. Kamińska, M. Rozbicka-Ostrowska*, op. cit., s. 20-21.
[272] *M. Bernaczyk*, Dokument wewnętrzny jako ograniczenie konstytucyjnego prawa do informacji. Rozstrzyganie kolizji w teorii i praktyce prawa, Warszawa 2017.

subiektywnych. Znajdują wyraz m. in. w coraz częstszym odwoływaniu się do wąskiego przedmiotowego ujęcia informacji publicznej, bazującego na pojęciu sprawy publicznej (...) wykładanego w oderwaniu do treści art. 61 Konstytucji RP ”[273].

Od dokumentów urzędowych i wewnętrznych należy jeszcze odróżnić trzecią kategorię dokumentów, czyli tzw. dokument prywatny. Jest nim zgodnie z art. 245 KPC dowód tego, że osoba która go podpisała, złożyła oświadczenie zawarte w dokumencie. Dokument ten różni się od urzędowego, że nie pochodzi od organu państwowego i niczego w sposób urzędowy nie zaświadcza. Problem interpretacyjny polega na tym, że dokument prywatny jest w posiadaniu podmiotu zobowiązanego, nie został przez niego wytworzony, ale dotyczy sprawy publicznej i jest związany z realizowanym przez podmiot zadaniem publiczny[274]. W orzecznictwie sądów administracyjnych utrwalił się pogląd, że źródłem informacji publicznej są nie tylko dokumenty urzędowe, ale również dokumenty prywatne, o ile tylko dotyczą sprawy publicznej.

Przyjęcie nawet szerokiego rozumienia pojęcia informacji publicznej nie eliminuje jednak problemów interpretacyjnych, które wystąpią na gruncie art. 7 ust. 1 UPW (art. 1 ust. 3 dyrektywy 2019/1024) biorąc jako punkt wyjścia zasadę pierwszeństwa przepisów dostępowych (w tym przede wszystkim UDIP) przed przepisami UPW. Nie wszystkie bowiem informacje sektora publicznego, które z mocy UPW podlegają udostępnieniu lub przekazaniu spełniają przesłanki informacji publicznej. W mojej opinii problem ten będzie dotyczył przede wszystkim materiałów bibliotecznych czy muzealiów, a w mniejszym zaś stopniu materiałów archiwalnych. Zasoby bibliotek, archiwów i muzeów, jak pamiętamy zostały włączone wprost w zakres ponownego wykorzystywania dyrektywą 2013/37/UE. W zdaniem nie sposób uznać ustawy z dnia 21 listopada 1996 r. o muzeach czy ustawy z dnia 27 czerwca 1997 r. o bibliotekach, jako regulacje „dostępowe” (za taką z kolei można względnie uznać ustawę z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach). Przedmiotowe ustawy nie stanowią również „przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi”, w myśl art. 1 ust. 2 UDIP. Ponadto nie sposób jednoznacznie przesądzić, że przykładowo odzwierciedlenie cyfrowe (digitalizat) obiektu muzealnego wraz z powiązanymi z nim metadanymi czy elektroniczny katalog biblioteczny, stanowią informację publiczną. Gdyby ocena kwalifikacji danej treści jako informacji sektora publicznego była dokonywana w oparciu „test informacji publicznej”, powodowałoby to ryzyko, że część treści, które spełniają kryteria informacji sektora publicznego i nie podlegają wyłączeniu lub ograniczeniu w rozumieniu przepisów UPW, nie

[273] *M. Jaśkowska*, O pojęciu informacji publicznej raz jeszcze, „Zeszyty Prawnicze” 2020, nr 3, s. 231.
[274] *I. Kamińska, M. Rozbicka-Ostrowska*, op. cit., s. 21

będzie mogła być ponowne wykorzystywana. Sytuacja taka objęłaby chociażby wspominane materiały biblioteczne czy muzealia.

Problem ten ponadto potęguje niejednolite orzecznictwo sądowe. W części orzeczeń sądów administracyjnych nastąpiło odejście od podmiotowego rozumienia informacji publicznej na rzecz przedmiotowego. Definicja przedmiotowa odwołuje się do kryterium „sprawy publicznej”[275]. Zgodnie z tym stanowiskiem nie każda informacja posiadana przez władze publiczne spełnia kryteria informacji publicznej. Konsekwencją przyjęcia definicji przedmiotowej będzie opisane wyżej wyłączenie z zakresu pojęcia informacja publicznej m.in. dokumentów wewnętrznych[276]. Kwalifikacja pewnych informacji jako dokumentu wewnętrznego z perspektywy definicji informacji sektora publicznego jest irrelewantna. Należy zgodzić się z *G. Sibigą*, że takie przedmiotowe rozumienie pojęcia „informacja publiczna” pozostaje sprzeczne z definicją dokumentu zawartą w dyrektywie 2003/98/WE[277].

Dominująca linia orzecznicza dokonująca wykładni zakresu stosowania przepisów o ponownym wykorzystywaniu odwołuje się do przepisów dostępowych, których granice zastosowania wyznacza pojęcie informacji publicznej. Dotychczas sądy w sposób jednolity podkreślały, że pojęcie informacji sektora publicznego musi się mieścić w informacji publicznej. Wynika to z tego, że „nie może podlegać ponownemu wykorzystaniu informacja, która pierwotnie nie występowała w przestrzeni publicznej. Odmienna interpretacja powołanych przepisów prowadziłaby do wniosku, iż skoro podlega ponownemu wykorzystaniu każda treść lub jej część będąca w posiadaniu podmiotu zobowiązanego, bez względu na to, czy dotyczy spraw publicznych, czy też nie, to przepisy UDIP straciłyby rację bytu. Wnioskodawca na gruncie UPW uzyskałby dostęp do informacji, której nie otrzymałby w oparciu o przepisy ustawy o dostępie do informacji publicznej, np. dokumentu prywatnego”[278].

Co więcej, w orzecznictwie prezentowany jest pogląd, że nie może podlegać ponownemu wykorzystaniu informacja, która nie jest informacją publiczną[279]. Choć dostrzec można sprzeczność w argumentacji sądów. Skoro bowiem zdaniem WSA w Warszawie „ponowne wykorzystanie informacji przez użytkownika, obejmuje również informację

[275] Zob. NSA z 30.09.2015 r., I OSK 2093/14.
[276] Wyr. NSA z 08.06.2016 r., I OSK 3110/14.
[277] *G. Sibiga*, „Informacja publiczna” oraz „informacja sektora publicznego” – różnice między pojęciami wyznaczającymi zakres stosowania ustaw informacyjnych, „Informacja w Administracji Publicznej” 2016, nr 4, s. 41.
[278] Wyrok WSA w Warszawie z dnia 30.03.2017 r., II SA/Wa 1819/16.
[279] Zob. *P. Szustakiewicz,* Wzajemny stosunek dwóch ustaw tworzących polski system dostępu do informacji publicznej, „Informacja w Administracji Publicznej” 2017, nr 3, s. 62.

publiczną, która została już udostępniona lub podlega udostępnieniu", dopuszcza jednocześnie inne informacje niż publiczne, które mogą być ponowne wykorzystywane[280]. W tym samym orzeczeniu sąd stwierdził, że „informacja będąca w posiadaniu podmiotu zobowiązanego, aby mogła być ponownie wykorzystana, musi pierwotnie służyć celowi publicznemu, czyli powinna posiadać walor informacji publicznej, z wyjątkiem informacji stanowiącej zasób bibliotek, archiwów i muzeów, gdyż te, służąc celowi informacji publicznej, niejednokrotnie nie mogą zostać zakwalifikowane jako informacja publiczna na gruncie przepisów ustawy o dostępie do informacji publicznej".

Z kolei w wyroku z NSA z 1 sierpnia 2019 r. I OSK 2270/17 stwierdził, że „jeżeli określona informacja nie ma charakteru informacji publicznej z tego względu, że ma charakter ściśle techniczny lub związana jest ze sferą wewnętrzną podmiotów zobowiązanych do jej udostępnienia, nie może być również kwalifikowana jako informacja sektora publicznego. Nie jest bowiem informacją o takiej aktywności tych podmiotów, która ukierunkowana jest na bezpośrednie wypełnianie określonych zadań publicznych i realizowanie określonych interesów i celów publicznych. Nie może być w związku z tym traktowana jako informacja wytworzona w ramach działania zdeterminowanego prawnie i bezpośrednio ukierunkowanego na realizację interesu publicznego, tj. jako informacja wytworzona "dla celu publicznego".

W istocie, ze względu na różnice między omawianymi pojęciami informacji publicznej i informacji sektora publicznego dochodzi w prawie polskim do sytuacji, że system dostępu, mający mieć pierwotne znaczenie dla uprawień informacyjnych obywateli, ma węższy zakres stosowania niż wtórne wobec niego przepisy o ponownym wykorzystywaniu[281]. Zgodnie z motywem 9 preambuły dyrektywy 2003/98/WE oraz motywem 8 preambuły dyrektywy 2013/37/UE przepisy unijnej dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego nie mogą powodować zmian w systemach dostępu (do informacji) w państwach członkowskich. Dostęp do informacji w celu jej ponownego wykorzystania nie może naruszać przepisów UDIP, a co za tym idzie nie może być podstawą do udostępnienia informacji, które nie podlegają ujawnieniu. W ten sposób bowiem powstałby swoisty dualizm prawny, w którym dostęp do informacji publicznej, będący w założeniem narzędziem kontroli społeczeństwa nad organami władzy, byłby węższy niż dostęp do informacji w celu jej ponownego wykorzystania, który służy przede wszystkim umożliwieniu gospodarczego wykorzystania danych będących w posiadaniu podmiotów publicznych[282].

[280] Wyrok WSA w Warszawie z 16.3.2017 r., II SA/Wa 1890/16.
[281] *G. Sibiga*, „Informacja publiczna" oraz „informacja sektora publicznego", s. 41.
[282] *P. Szustakiewicz,* Wzajemny stosunek dwóch ustaw, s. 64.

W mojej opinii przyjęta przez krajowe sądy interpretacja jest niedopuszczalna. Stwarza realne ryzyko zawężania przez podmioty stosujące przepisy UPW pojęcia informacji sektora publicznego do informacji publicznej i wyłączania poza zakres stosowania przepisów UPW treści, które arbitralnie kwalifikowane być mogą jako dokumenty prywatne czy dokumenty wewnętrzne, które jako niepodlegające udostępnieniu, w konsekwencji nie będą mogły być ponownie wykorzystywane. Instrumentem służącym ochronie poufności informacji pozostawać powinny przepisy ograniczające odpowiednio dostęp do informacji publicznej i ponowne wykorzystywanie informacji sektora publicznego. Przyjęcie odmiennej interpretacji spowodować może, że cel regulacji ponownego wykorzystywania nie zostanie w pełni zrealizowany.

Pierwotnym źródłem opisanych problemów pozostają nie wtórne chronologicznie i celowościowo przepisy o ponownym wykorzystywaniu, a podstawowe dla realizacji uprawnień informacyjnych przepisy o dostępie do informacji publicznej, w szczególności zaś wadliwa definicja informacji publicznej. Skonstruowanie definicji informacji publicznej w oparciu o kryterium sprawy publicznej, spowodowało różnice w ustalaniu zakresu znaczeniowego tego pojęcia. Obecnie dominującym modelem przyjętym w ustawodawstwie państw europejskich, jest objęcie systemem dostępu wszelkich posiadanych informacji (dokumentów) przez podmioty publiczne, a wszelkie ograniczenia są wprost ustanawiane w akcie prawnym. Pojęcie „dokument" z dyrektyw 2003/98/WE i 2019/1024 jest potwierdzeniem tej praktyki zapoczątkowanej na poziomie UE rozporządzeniem 1049/2001. Definicja informacji publicznej doprowadziła do niespójności w prawie krajowym w zakresie dwóch uprawnień informacyjnych: prawa dostępu do informacji publicznej oraz prawa ponownego wykorzystywania informacji sektora publicznego[283].

Podsumowując, informacja sektora publicznego jest pojęciem szerszym znaczeniowo od pojęcia informacji publicznej. Na gruncie przepisów UPW można stwierdzić, że informacja publiczna zawiera się w szerszym zbiorze jakim jest informacja sektora publiczna. Innymi słowy, każda informacja publiczna stanowi jednocześnie informację sektora publicznego, lecz nie każda informacja sektora publiczna stanowić będzie informację publiczną.

[283] *G. Sibiga*, „Informacja publiczna" oraz „informacja sektora publicznego", s. 42.

3.1.3. Ponowne wykorzystywanie – definicja normatywna

Definicję normatywną ponownego wykorzystywania wprowadził prawodawca UE po raz pierwszy w dyrektywie 2003/09/WE, której treść co do zasady nie uległa zmianie (co prawda w dyrektywie 2019/1024 w definicji uwzględniono poszerzenie zakresu ponownego wykorzystywania o dokumenty będące w posiadaniu przedsiębiorstw publicznych, ale nie wpłynęło to na znaczenie samego pojęcia[284]). Ponownym wykorzystywaniem w myśl dyrektywy jest „wykorzystywanie przez osoby fizyczne lub prawne dokumentów będących w posiadaniu organów sektora publicznego, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla których te dokumenty zostały wyprodukowane. Ponownym wykorzystywaniem nie jest wymiana dokumentów między organami sektora publicznego wyłącznie w wykonaniu ich zadań publicznych".

Pojęcie ponownego wykorzystywania ma charakter zasadniczy dla tego aktu prawnego, a jego zdefiniowanie wpływa na kształt regulacji ustawowych w państwach członkowskich wyraźnie je determinując[285].

Zawarta w art. 1 ust. 3 UPW definicja ponownego wykorzystywania odpowiada art. 2 pkt 4 dyrektywy 2003/98/WE. Przez ponowne wykorzystywanie należy rozumieć wykorzystywanie przez osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej informacji sektora publicznego w celach komercyjnych lub niekomercyjnych innych niż pierwotny publiczny cel, dla którego informacja została wytworzona. Przy czym ponownym wykorzystywaniem nie jest udostępnianie lub przekazanie informacji sektora publicznego przez podmiot wykonujący zadania publiczne innemu podmiotowi wykonującemu zadania publiczne wyłącznie w celu realizacji takich zadań.

Definicja legalna ponownego wykorzystywania ma charakter projektujący (regulacyjny), bowiem ustawodawca odniósł się do zwrotu, który funkcjonuje w języku

[284] Art. 2 pkt 11 „ponowne wykorzystywanie" oznacza wykorzystywanie przez osoby fizyczne lub podmioty prawne dokumentów będących w posiadaniu: a) organów sektora publicznego, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla którego to celu dokumenty te zostały wyprodukowane, z wyjątkiem wymiany dokumentów między organami sektora publicznego służącej wyłącznie wykonywaniu ich zadań publicznych; lub b) przedsiębiorstw publicznych, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w zakresie świadczenia usług w interesie ogólnym, dla którego to celu dokumenty te zostały wyprodukowane, z wyjątkiem wymiany dokumentów między przedsiębiorstwami publicznymi a organami sektora publicznego służącej wyłącznie wykonywaniu zadań publicznych organów sektora publicznego.

[285] Zob. szerzej: *A. Piskorz-Ryń*, Pojęcie ponownego wykorzystywania informacji sektora publicznego w świetle dyrektywy 2003/98/WE, „Samorząd Terytorialny" 2015, nr 4.

naturalnym i pierwotne nieostre znaczenie użytych w nim słów przyjął jako podstawę do wprowadzenia nowego pojęcia[286].

Definiens pojęcia ponownego wykorzystywania składa się z następujących elementów: użytkowego (wykorzystywanie), teleologicznego (cel komercyjny i niekomercyjny inny niż pierwotny publiczny cel wytworzenia informacji), przedmiotowy (informacja sektora publicznego) oraz podmiotowy (użytkownik). Ostatnie dwa elementy definicji nie budzą wątpliwości interpretacyjnych, chodzi o ponowne wykorzystywanie informacji sektora publicznego, która została zdefiniowana w art. 2 ust. 1 UPW. Z kolei pojęcie użytkownik zostało wyjaśnione w samej definicji ponownego wykorzystywania, czyli osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej.

Pierwszy element definicji wskazuje na użytkowy charakter pojęcia ponownego wykorzystywania. Ustawodawca krajowy w ślad za europejskim poprzez posłużenie się w *definiens* zwrotem występującym w *definiendum*, popełnił klasyczny błąd logiczny *idem per idem* (ponownym wykorzystywaniem jest wykorzystywanie), dlatego też definicja zawarta w art. 2 ust. 2 UPW jest wyraźnie tautologiczna. Wyraz wykorzystywanie to forma rzeczownikowa czasownika wykorzystywać, który zgodnie ze Słownikiem Języka Polskiego oznacza „użycie czegoś dla osiągnięcia jakiegoś celu, zysku"[287]. Dla interpretacji pojęcia wykorzystywania nie wystarczy wykładnia językowa, należy posłużyć się wykładnią funkcjonalną i celowościową[288]. Ze względu na istotę i cel instytucji ponownego wykorzystywania należy mówić o wtórnej eksploatacji informacji[289]. Wykorzystywaniem nie będzie zatem samo zapoznanie się z treścią, konieczne jest użycie informacji sektora publicznego w określonym celu[290]. O sposobie wykorzystywania decyduje użytkownik. Użytkowy charakter prawa, co było wielokrotnie wskazywane, podkreśla prawodawca UE, jak

[286] Zob. *M. Omyła*, Terminy, pojęcia, definicje jako kategorie podstawowe dla budowy słownika odnoszącego się do jawności i jej ograniczeń [w:] *A. Gryszczyńska (red.),* Struktura tajemnic, *G. Szpor* (*red.),* Jawność i jej ograniczenia, t. VI , Warszawa 2014, s. 73 oraz *A. Piskorz – Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 125-126.

[287] Słownik Języka Polskiego PWN https://sjp.pwn.pl/so/wykorzystywac;4534291.html

[288] Zdaniem *M. Jaśkowskiej*, aby rozróżnić dostęp do informacji publicznej od ponownego jej wykorzystywania należy odwołać się do wykładni systemowej i celowościowej. Zob. *M. Jaśkowska*, Ponowne wykorzystywanie informacji sektora publicznego w świetle orzecznictwa sądów administracyjnych a zasada transparentności władz publicznych [w:] J. *Jagielski., M. Wierzbowski*, Prawo administracyjne dziś i jutro, Warszawa 2018, s. 144.

[289] *G. Sibiga*, Opinia prawna o projekcie ustawy o zmianie ustawy o dostępie do informacji publicznej, s. 3. Podobnie: *T. Górzyńska* za: *M. Maciejewski*, Prawna regulacja prawa ponownego wykorzystywania, s. 283.

[290] Podobnie *A. Piskorz – Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 129.

również ustawodawca krajowy[291]. Pod pojęciem ponownego wykorzystywania należy zatem rozumieć powtórne użycie informacji.

Kolejnym składnikiem definicji jest element teleologiczny, czyli cel. Ustawodawca krajowy w ślad za prawodawcą europejskim przyjął szeroką regulację celów ponownego wykorzystywania. W definicji wskazano cel komercyjny lub niekomercyjny, przy czym rozróżnienie to nie ma żadnego praktycznego znaczenia z punktu widzenia samej definicji, ma jednak istotne znaczenie ze względu na zakres informacji wskazywanych we wniosku o ponowne wykorzystywanie (zgodnie z art. 21 ust. 3 pkt 4 UPW konieczne jest wskazanie celu ponownego wykorzystywania - komercyjny albo niekomercyjny - w tym określenie rodzaju działalności, w której informacje sektora publicznego będą ponownie wykorzystywane, w szczególności wskazanie dóbr, produktów lub usług) oraz ze względu na odrębności dotyczące określenia warunków ponownego wykorzystywania przez muzea, archiwa i biblioteki w działalności komercyjnej w zakresie zbiorów o charakterze martyrologicznym (art. 14 ust 2 UPW). Można przyjąć, iż cele ponownego wykorzystywania obejmują wszystkie istniejące cele (inne niż pierwotny publiczny cel wytworzenia informacji), o ile inne przepisy prawa nie zabraniają ich osiągania[292]. Uprawniona będzie zatem konstatacja, że chodzi o jakikolwiek cel zgodny z prawem.

Kolejnym elementem teleologicznym, który trzeba rozstrzygnąć jest cel ponownego wykorzystywania inny niż „pierwotny publiczny cel, dla którego informacja została wytworzona". Pierwotny publiczny cel należy wiązać z wykonywaniem zadań określonych przepisami prawa przez podmiot zobowiązany. Należy podzielić pogląd *A. Piskorz-Ryń,* opowiadający się za szerokim rozumieniem pierwotnego celu publicznego. Zgodnie z wykładnią proeuropejską za pierwotny cel publiczny należy uznać zarówno cel wytworzenia, jak i inny cel w ramach zadań publicznych, dla których informacje zostały wyprodukowane (wytworzone)[293].

Z kolei „wytworzenie" informacji wydaje się terminem zbyt wąskim, podmioty zobowiązane realizując zadania publiczne nie tylko wytwarzają informacje, ale również je pozyskują, gromadzą i przetwarzają nie będąc jednocześnie pierwotnym twórcą („wytwórcą")

[291] Zob. Uzasadnienie rządowego projektu ustawy o ponownym wykorzystywaniu informacji sektora publicznego, Sejm VIII kadencja (druk 141).
[292] Zob. *M. Maciejewski,* Prawna regulacja ponownego wykorzystywania informacji publicznej [w:] *G. Sibiga (red.)*, Główne problemy, s. 281.
[293] *A. Piskorz-Ryń*, Zakres przedmiotowy stosowania przepisów stosowania przepisów o ponownym wykorzystywaniu [w:] *E. Badura., M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń., M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 34.

informacji. Należy zatem zgodzić się z *M. Maciejewskim*, że termin wytworzenie w tym kontekście obejmuje również pozyskiwanie i przechowywanie[294].

Jak wskazano ponownym wykorzystywaniem nie jest udostępnianie lub przekazanie informacji sektora publicznego przez podmiot wykonujący zadania publiczne innemu podmiotowi wykonującemu zadania publiczne wyłącznie w celu realizacji takich zadań. Ustawodawca krajowy, podobnie zresztą jak prawodawca UE (zob. motyw 8 preambuły 2003/98/WE), podkreślił, że poza zakresem ponownego wykorzystywania pozostaje przetwarzanie informacji, które następuje dla realizacji zadań publicznych[295].

Wykorzystywanie informacji należy zatem interpretować jako działanie na informacji po jej uzyskania. Wykorzystywaniem informacji nie będzie samo powzięcie jej do wiadomości, a więc skorzystanie z niej w celu wyłącznie poznawczym, nie jest bowiem ponownym wykorzystywaniem informacji (publicznej) sam fakt otrzymania do niej dostępu[296]. Choć w literaturze prezentowany jest również pogląd, że każdy dostęp do jakiekolwiek dokumentu urzędowego czy udzielnie informacji na wniosek jest wykorzystywaniem w innym celu, niż ten do którego dokument czy informacja zostały pierwotnie przeznaczone[297].

Definicja ustawowa ponownego wykorzystywania – pomimo prawie dziesięciu lat funkcjonowania w prawie polskim - wciąż budzi wątpliwości w doktrynie, stwarza również trudności interpretacyjne stosującym przepisy[298].

W niniejszej pracy przyjęto następujące funkcjonalne rozumienie ponownego wykorzystywania, jest nim użycie (eksploatacja) informacji sektora publicznego przez użytkownika w jakimkolwiek celu innym niż pierwotne przeznaczenie w ramach realizacji zadania publicznego dla której informacja ta została wytworzona, pozyskana lub przechowywana przez podmiot zobowiązany[299].

---

[294] *M. Maciejewski*, Prawna regulacja ponownego wykorzystywania informacji publicznej [w:] *G. Sibiga (red.)*, Główne problemy, s. 282.

[295] *A. Piskorz – Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 138.

[296] Zob. wyrok WSA w Krakowie z 16.10.2012 r., II SAB/Kr 138/12 (niepul.)

[297] Zob. *M. Jaśkowska*, Jakość i spójność rozwiązań prawnych w świetle nowelizacji ustawy o dostępie do informacji publicznej, s. 367 oraz *B. Banaszak, M. Bernaczyk*, Konsultacje, s. 29. Zob. również wyrok NSA z 05.04.2013, I OSK 196/13.

[298] Zob. m.in. *B. Dziliński*, Prawo do ponownego wykorzystywania informacji publicznej. Uwagi na tle transpozycji dyrektywy 2003/98/WE z 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2012, nr. 4, s. 37 i *M. Jaśkowska*, Ponowne wykorzystywanie informacji publicznej [w:] *J. Sługocki (red.)*, Dziesięć lat w Unii Europejskiej. Problemy prawnoadministracyjne, t. 2., Wrocław 2014, 280.

[299] *A. Piskorz-Ryń* zaproponowała następującą definicję funkcjonalną: „Ponowne wykorzystywanie informacji sektora publicznego to używanie przez każdego informacji sektora publicznego będącej w posiadaniu podmiotów zobowiązanych dla wytworzenia produktów, dóbr lub usług o wartości dodanej w innym celu niż wykonywanie zadań publicznych. Cel ponownego wykorzystywania może być komercyjny lub komercyjny". Zob. *A. Piskorz-Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 149.

3.1.4. Podmiot zobowiązany

UPW wyznacza katalog podmiotów, które udostępniają lub przekazują informacje sektora publicznego w celu jej ponownego wykorzystywania, które nazwano „podmiotami zobowiązanymi". Ustawodawca tworząc zamknięty katalog podmiotów zobowiązanych wzorował się na katalogu podmiotów, do których zastosowanie mają przepisy ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (zgodnie jej art. 3 ust. 1)[300].

Oparcie katalogu podmiotów obowiązanych do stosowania przepisów o ponownym wykorzystywaniu znajduje uzasadnienie w dyrektywie 2003/98/WE. Wprawdzie dla wyznaczenia zakresu podmiotowego posługuje się ona wyrażeniem „organ sektora publicznego" i „podmiot prawa publicznego", pojęcia te zostały jednak zapożyczone z dyrektyw w sprawie zamówień publicznych[301].

Podmiotami zobowiązanymi do udostępniania lub przekazywania informacji sektora publicznego w celu ponownego wykorzystywania – zgodnie z art. 3 UPW - są:

1) jednostki sektora finansów publicznych w rozumieniu przepisów ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;

2) inne niż określone w pkt 1 państwowe jednostki organizacyjne nieposiadające osobowości prawnej;

3) inne niż określone w pkt 1 osoby prawne, utworzone w szczególnym celu zaspokajania potrzeb o charakterze powszechnym, niemających charakteru przemysłowego ani handlowego, jeżeli podmioty, o których mowa w tym przepisie oraz w pkt 1 i 2, pojedynczo lub wspólnie, bezpośrednio albo pośrednio przez inny podmiot finansują je w ponad 50% lub posiadają ponad połowę udziałów albo akcji, lub sprawują nadzór nad organem zarządzającym, lub mają prawo do powoływania ponad połowy składu organu nadzorczego lub zarządzającego;

4) związki wyżej wymienionych podmiotów.

Na podkreślenie zasługuje, że zgodnie z poszerzeniem zakresu podmiotowego przez dyrektywę 2013/37/WE – do grona podmiotów zobowiązanych trzeba zaliczyć:

1) muzea państwowe i muzea samorządowe w rozumieniu przepisów ustawy z dnia 21 listopada 1996 r. o muzeach,

---

W mojej opinii element wartości dodanej, pozostaje niezdefiniowany i co do zasady podlega subiektywnej ocenie. Używanie informacji nie zawsze może doprowadzić do powstania produktu, dobra i usługi, choć jest zasadniczym celem tej instytucji. Inną definicję sformowali *B. Banaszak* i *M. Bernaczyk,* której kluczowym elementem jest osiągnięcie przez wnioskodawcę „szeroko pojętej korzyści". Zob. *B. Banaszak, M. Bernaczyk,* Konsultacje s. 29.

[300] Dz. U. z 2019 r. poz. 1843 oraz z 2020 r. poz. 288, 1086.

[301] Obecnie jest to dyrektywa Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylająca dyrektywę 2004/18/WE (Dz.U. L 94 z 28.3.2014, s. 65).

2) biblioteki publiczne oraz biblioteki naukowe w rozumieniu przepisów ustawy z dnia 27 czerwca 1997 r. o bibliotekach,
3) archiwa tworzące państwową sieć archiwalną oraz innych jednostek organizacyjnych prowadzących działalność archiwalną w zakresie państwowego zasobu archiwalnego w rozumieniu art. 22 ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach).

Ponadto krajowy ustawodawca z własnej inicjatywy poszerzył zakres podmiotowy o Instytut Meteorologii i Gospodarki Wodnej oraz Państwowego Instytutu Geologicznego, co było podyktowane nowelizacją przepisów ustawy z dnia 18 lipca 2001 r. – Prawo wodne mającej na celu umożliwienie ponownego wykorzystywania informacji sektora publicznego będących w posiadaniu tych instytucji (np. danych meteorologicznych).

Spośród podmiotów wymienionych w art. 3 przepisy UPW nie znajdą z kolei zastosowania do:
1) jednostek publicznej radiofonii i telewizji w rozumieniu przepisów ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji oraz Polskiej Agencji Prasowej S.A.,
2) państwowych instytucji kultury, samorządowych instytucji kultury oraz innych podmiotów prowadzących działalność kulturalną, o której mowa w art. 2 ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej,
3) podmiotów, o których mowa w art. 7 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce,
4) bibliotek naukowych, których organizatorami nie są jednostki sektora publicznego,
5) podmiotów, o których mowa w art. 2 ustawy z dnia 14 grudnia 2016 r. – Prawo oświatowe – chyba że informacje te stanowią informacje publiczne podlegające udostępnieniu w Biuletynie Informacji Publicznej.

Na komentarz zasługuje poszerzenie zakresu podmiotowego ponownego wykorzystywania wprowadzone dyrektywą 2019/1024 o tzw. przedsiębiorstwa publiczne[302]. Za przedsiębiorstwa publiczne prawodawca unijny uznał każde przedsiębiorstwo, na które organy sektora publicznego mogą wywierać, bezpośrednio lub pośrednio, dominujący wpływ z racji bycia jego właścicielem, posiadania w nim udziału finansowego lub na mocy przepisów, które regulują działalność tego przedsiębiorstwa (art. 2 pkt 3 dyrektywy). Przy czym chodzi tu

[302] Dyrektywa 2019/1024 w wersji angielskiej posługuje się sformułowaniem *public undertakings*, co może oznaczać, że pojęcie to należy rozumieć szerzej od pojęcia przedsiębiorstwa, czyli jako podmioty prawa publicznego.

wyłącznie o przedsiębiorstwa publiczne działające w sektorach gospodarki wodnej, energetyki, usług pocztowych i transportu publicznego.

Dane z wymienionych sektorów niewątpliwie mają wysoki potencjał dla ponownego wykorzystywania. Poza zakresem stosowania przepisów dyrektywy pozostaną zaś wszystkie te informacje, będące w posiadaniu przedsiębiorstw publicznych, opracowane poza zakresem świadczenia usług w interesie ogólnym (art. 1 ust. 2 lit. b). W odniesieniu do dokumentów przedsiębiorstw publicznych, które będą mogły być ponownie wykorzystywane zastosowanie będzie miał ograniczony zestaw obowiązków – za udostępnianie danych podmioty te będą mogły pobierać opłaty przekraczające koszty krańcowe i nie będą zobowiązane do udostępniania danych, co do których podejmą decyzję o nieudostępnieniu. Dopiero wówczas, gdy przedsiębiorstwo publiczne podejmie decyzję o udostępnieniu danego dokumentu do ponownego wykorzystania, powinno przestrzegać odpowiednich obowiązków określonych w Rozdziałach III i IV dyrektywy, w szczególności obowiązków dotyczących formatów, pobierania opłat, przejrzystości, licencji, niedyskryminacji i zakazu stosowania umów o wyłączności. Przedsiębiorstwo publiczne nie ma natomiast obowiązku przestrzegania wymogów określonych w Rozdziale II, takich jak przepisy regulujące rozpatrywanie wniosków (art. 4 ust. 6 dyrektywy 2019/1024). Oznacza to, że potencjalni wnioskodawcy pozbawieni zostaną jakichkolwiek instrumentów gwarantujących rozpatrzenie wniosku o ponowne wykorzystywanie takich danych w odpowiednim terminie, jak i możliwości odwołania w przypadku odmowy zgody na ponowne wykorzystywanie. Uzasadnione zatem będzie twierdzenie, że przedsiębiorstwa publiczne stanowić będą szczególną kategorię podmiotów zobowiązanych do udostępnienia informacji, do których nie będą miały zastosowanie wszystkie przepisy o ponownym wykorzystywaniu.

Drugą zmianą w zakresie podmiotowym przepisów jest włączenie – w zakresie danych badawczych - będących w posiadaniu organizacji prowadzących badania naukowe i organizacji finansujących badania naukowe, w tym organizacji utworzonych na potrzeby transferu wyników badań naukowych.

Poszerzenie zakresu podmiotowego w dyrektywie 2019/1024 skutkuje koniecznością korekty katalogu podmiotów zobowiązanych wymienionego w przepisach UPW przez krajowego ustawodawcę.

3.1.5. Podmiot uprawniony – użytkownik

Podmiotem uprawnionym do ponownego wykorzystywania informacji sektora publicznego jest użytkownik. Zgodnie z art. 2 ust. 2 przez użytkownika należy rozumieć osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej, które ponownie wykorzystują informację sektora publicznego. Jednocześnie stosownie do treści art. 5 UPW zd. pierwsze prawo do ponownego wykorzystywania przysługuje „każdemu".

Z kolei dyrektywy o ponownym wykorzystywaniu posługują się wymiennie wyrazem „wnioskodawca" (art. 4 dyrektywy 2019/1024), „wnioskujący" (art. 7) „użytkownik" (art. 11 ust. 2), a w części nienormatywnej sformułowaniem „użytkownik końcowy" (motyw 14), co istotne nie definiując żadnego tych pojęć. Z kolei w definicji ponownego wykorzystywania mowa jest o wykorzystywaniu przez „osoby fizyczne lub podmioty prawne" bez precyzowania, że chodzi o użytkowników.

Jeśli chodzi o podmiot uprawniony do ponownego wykorzystywania na gruncie polskich przepisów zaobserwować można pewną niekonsekwencję krajowego ustawodawcy. Z jednej strony art. 5 UPW stanowi o tym, że prawa do ponownego wykorzystywania przysługuje „każdemu", z drugiej zaś podmiotem uprawnionym zgodnie z definicją ponownego wykorzystywania jest użytkownik, którym z kolei może być osoba fizyczna, osoba prawna i jednostki organizacyjne nieposiadające osobowości prawnej. Podzielić należy pogląd *P. Sitniewskiego*, że treść pierwszego zdania art. 5 należy traktować jako normę generalną zakazującą jakichkolwiek działań o charakterze dyskryminującym, czy też wyłączającym określone grupy z poszczególnych kategorii w realizacji prawa do ponownego wykorzystywania. Norma ta stanowi o tym, że każda osoba fizyczna, każda osoba prawna właściwie reprezentowana stosownie do przepisów ustawowych oraz norm o charakterze statutowym, oraz każda jednostka organizacyjna niemająca osobowości prawnej, mają prawo ponownie wykorzystywać informację sektora publicznego w trybie zarówno bezwnioskowym, jak i wnioskowym. Odmienna interpretacja prowadziłaby do konkluzji, że w jednym akcie prawnym ustawy obowiązywałyby dwie regulacje wzajemnie się wykluczające (tj. art. 2 ust. 2 i art. 5)[303].

Na tle definicji użytkownika pojawia się dylemat, czy użytkownikiem może być również podmiot publiczny w zakresie działalności przekraczającej wykonywanie zadań publicznych. W Polsce będzie to rzadkością ze względu na ograniczenia prawne związane

[303] *P. Sitniewski*, Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, komentarz do art. 5 pkt 1, Legalis/Wyd. 2017.

z wykonywaniem przez podmioty administrujące zadań niebędących zadaniami publicznymi[304], przynajmniej teoretycznie sytuacji takiej nie można wykluczyć, w szczególności w zakresie podmiotów zobowiązanych nie będących typowymi organami władzy publicznej, np. spółka Skarbu Państwa. O takiej możliwości przesądził ustawodawca formułując zasadę równego traktowania. W myśl art. 8 ust. UPW w przypadku gdy ponowne wykorzystywanie jest dokonywane przez użytkowników będących podmiotami wykonującymi zadania publiczne w ramach działalności wykraczającej poza realizację takich zadań, warunki ponownego wykorzystywania lub opłaty za ponowne wykorzystywanie określa się na takich samych zasadach jak w przypadku innych użytkowników. Zatem na gruncie przepisów UPW dopuszczalna jest sytuacja, że ten sam podmiot występować może zarówno w roli użytkownika, jak i podmiotu zobowiązanego[305].

3.2. Zakres stosowania ogólnego rozporządzenia i podstawowe pojęcia ochrony danych osobowych

Zakres ogólny stosowania przepisów RODO wyznacza jego art. 1. Tym samym prawodawca unijny wyznaczył granice zastosowania przepisów wyłącznie do ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych oraz swobodnym przepływie danych osobowych, jednocześnie akcentując potrzebę zapewnienia swobody przepływu danych jako filaru gwarantującego swobodę przepływu towarów, usług i kapitału w UE.

Zakres stosowania ogólnego rozporządzenia wyznaczają również jego art. 2 i 3, odpowiednio dotycząc problematyki zakresu przedmiotowego, czyli wskazując rodzaj przetwarzania danych osobowych podlegających regulacji (przetwarzanie danych w zbiorach danych oraz automatycznego przetwarzania danych) oraz zakresu terytorialnego zastosowania, wyznaczając terytorium oraz podmioty, w stosunku do których przepisy rozporządzenia mają zastosowanie.

Opisane w dalszej części rozdziału kluczowe pojęcia dla wyznaczenia ram stosowania RODO oczywiście nie wyczerpują w pełni problematyki podstawowych pojęć występujących w rozporządzeniu, których „słowniczek" został wymieniony w art. 4. Inne pojęcia relewantne

[304] *A. Piskorz-Ryń*, Zakres przedmiotowy stosowania przepisów o ponownym wykorzystywaniu [w:] *E. Badura., M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń., M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 44.
[305] Zob. *B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz*, Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, Wrocław 2017, s. 40.

dla omawianego zagadnienia zostały wyjaśnione w dalszej części rozprawy w zakresie w jakim było to niezbędne dla głównej tematyki rozprawy.

W rozprawie zrezygnowano również z szerszego omawiania zakresu terytorialnego ogólnego rozporządzenia[306]. Na potrzeby przedmiotu rozprawy należy wskazać, że w myśl art. 3 RODO ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.

Po drugie, RODO ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:

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

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

Po trzecie, RODO ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Do tego, aby przepisy RODO znalazły zastosowanie, wystarczy, że istnieje związek między czynnością przetwarzania danych a działalnością danej jednostki organizacyjnej znajdującej się na terytorium Unii Europejskiej[307]. Pojęcie „jednostka organizacyjna" (*establishment*) zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury, niezależnie od tego, czy chodzi o oddział, czy spółkę zależną posiadającą osobowość prawną, a zatem podmiotowość prawna nie jest czynnikiem decydującym przy kwalifikowaniu danej struktury jako „jednostki organizacyjnej" (motyw 22 preambuły RODO)[308]. Dotyczy to zarówno podmiotów publicznych (m.in. administracji publicznej), jak też podmiotów prywatnych (np. spółek)[309].

Regulacja art. 3 ust. 2 RODO stanowi istotną nowość w stosunku do przepisów dyrektywy 95/46/WE. Jest ona kluczowa dla administratorów lub podmiotów

[306] Zob. m.in. *M. Czerniawski,* Zakres terytorialny stosowania polskich i unijnych przepisów o ochronie danych osobowych w kontekście najnowszego orzecznictwa Trybunału Sprawiedliwości Unii Europejskiej [w:] *E. Bielak-Jomaa, D. Lubasz (red.),* Polska i europejska reforma ochrony danych osobowych, Warszawa 2016.

[307] *D. Lubasz,* Zakres terytorialny [w:] *D. Lubasz (red.),* Meritum. Ochrona danych osobowych, Warszawa 2019, s. 84.

[308] Do wykładni pojęcia „jednostki organizacyjnej" zachowują aktualność rozstrzygnięcia Trybunału Sprawiedliwości w sprawach C-131/12 *Google Spain,* C-230/14 *Weltimmo* oraz C1-91/15 *Verein fur Konsumenteninformation*.

[309] *P. Fajgielski,* Komentarz, 2018, s. 97.

przetwarzających, prowadzących działalność i zlokalizowanych w państwach trzecich, tj. poza Europejskim Obszarem Gospodarczym. W stosunku do tych podmiotów rozporządzenie będzie miało zastosowanie nie wtedy, gdy usługi tych administratorów będą dostępne w Unii, lecz wyłącznie wówczas, gdy będą oni nakierowywali swoją działalność na odbiorców w UE.

W myśl motywu 23 preambuły RODO koncepcja nakierowania wymaga uwzględniania takich czynników jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii.

3.2.1. Zakres przedmiotowy ogólnego rozporządzenia

Dla wyznaczenia zakresu przedmiotowego ogólnego rozporządzenia kluczowe pozostają przede wszystkim pojęcia danych osobowych, przetwarzania oraz zbioru danych.

Przed wyjaśnieniem podstawowych pojęć dla wyznaczenia zakresu przedmiotowego RODO konieczne jest wyjaśnienie ram materialnego stosowania przepisów rozporządzenia. Zakresem przedmiotowym zastosowania RODO jest przetwarzanie danych osobowych. Niemniej na gruncie art. 2 RODO należy wyróżnić dwa przypadki przetwarzania danych osobowych kwalifikujących je do objęcia zakresem rozporządzenia, tj. przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz przetwarzanie w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych. Dla przetwarzania danych w sposób całkowicie lub częściowo zautomatyzowany bez znaczenia jest czy dane w ten sposób przetwarzane staną się lub (mają) mogą stać się zbiorem danych. Z kolei dla drugiego przypadku przetwarzania relewantnego dla przepisów RODO, tj. w sposób inny niż zautomatyzowany, konieczne jest, aby dane w ten sposób przetwarzane stanowiły lub miały (mogły) stanowić zbiór danych[310].

Pojęcia przetwarzanie danych osobowych w sposób całkowicie lub częściowo zautomatyzowany nie zostało definiowane w rozporządzeniu, co jest wyrazem woli zachowania neutralności technologicznej regulacji. Pojęcia te należy jednak wykładać szeroko, co powoduje, że zakresem RODO będzie objęte nie tylko przetwarzanie w systemach teleinformatycznych, ale także inne sposoby automatycznego przetwarzania na innych urządzeniach, np. wideo rejestratorach samochodowych, *bodycam* czy kamerach na dronach, utrwalających zapis, z zastrzeżeniem wyłączeń zawartych w art. 2 ust. 2 RODO[311].

[310] *D. Lubasz*, Komentarz do art. 2 [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 125.
[311] *D. Lubasz*, Zakres przedmiotowy [w:] *D. Lubasz*, Meritum, s. 70.

Częściowo zautomatyzowane przetwarzanie danych tym się rożni od całkowicie zautomatyzowanego przetwarzania, że niektóre z etapów przetwarzania mają innych niż zautomatyzowany charakter − np. samo zbieranie danych w sposób niezautomatyzowany, jednakże z przeznaczeniem do późniejszego automatycznego przetwarzania np. w systemie teleinformatycznym[312]. Za takie przetwarzanie można również przyjąć sytuację, w której w prawdzie zestaw danych prowadzony jest w całości analogowo, ale wyposażony zostaje w zautomatyzowany system indeksujący[313].

Z kolei na gruncie motywu 15 preambuły RODO należy pod pojęciem przetwarzania innego niż zautomatyzowane przyjąć przetwarzania ręczne. Typowym przykładem przetwarzania danych osobowych w sposób niezautomatyzowany jest manualne przetwarzanie dokonywane w papierowych ewidencjach, kartotekach, skorowidzach czy innego tego rodzaju tradycyjnych zbiorach danych[314]. W przeciwieństwie do przetwarzania częściowo zautomatyzowanego przy przetwarzaniu manualnym na żadnym jego etapie i przy żadnej operacji przetwarzania nie dochodzi w ogóle do jakiejkolwiek formy przetwarzania automatycznego[315]. Prawnie relewantne jest, aby dane przetwarzane w ten sposób stanowiły lub miały stanowić część zbioru danych osobowych. Powstaje wątpliwość, jak należy rozumieć zwrot "mają stanowić część zbioru danych". W każdej sytuacji ocenę należy relatywizować i uwzględniać indywidualne okoliczności konkretnego przypadku – w przeciwnym bowiem razie każdy przypadek przetwarzania danych osobowych można by uznać za objęty zakresem zastosowania RODO, jako że – potencjalnie – każda informacja może podlegać przetwarzaniu w ramach istniejącego bądź tworzonego zbioru danych[316]. Należy podzielić poglądy doktryny wyrażone na gruncie UODO1997, zgodnie z którym dane osobowe podlegają ochronie bez względu na to, czy ostateczne znajdą się w zbiorze danych osobowych[317]. Ochrona danych osobowych, wynikająca z przepisów RODO, obejmuje więc informacje już na etapie ich gromadzenia, a zatem wówczas, gdy zbiór danych jeszcze nie istnieje, ale ma zostać utworzony na podstawie zbieranych danych[318].

Poza zakresem stosowania ogólnego rozporządzanie, zgodnie z art. 2 ust 2, znajdzie się:

[312] *Ibidem*, s. 71.
[313] *D. Lubasz*, Komentarz do art. 2 [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 127.
[314] *P. Fajgielski*, op.cit., s. 89.
[315] *D. Lubasz*, op. cit., s. 127.
[316] *P. Litwiński (red.)*, op. cit., Komentarz do art. 2, pkt 7.
[317] *J. Barta, P. Fajgielski, R. Markiewicz*, Ochrona danych osobowych. Komentarz, Kraków 2004, s. 335.
[318] *A. Mednis*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 1999 r., s. 15.

a) przetwarzanie w ramach działalności nieobjętej zakresem prawa Unii (chodzi o te działalności, które nie mają łącznika z prawem Unii, nie służą realizacji praw wywodzonych z prawa Unii, co do pojęcia dziedzin objętych prawem Unii i jego rozszerzającej wykładni w orzecznictwie TSUE[319]; w motywie 16 preambuły RODO jako przykład tego rodzaju sytuacji wskazuje się kwestie ochrony podstawowych praw i wolności oraz swobodnego przepływu danych osobowych w związku z działalnością dotyczącą bezpieczeństwa narodowego);
b) przetwarzanie przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE (tj. do kwestii związanych ze wspólną polityką zagraniczną i bezpieczeństwa);
c) przetwarzanie przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze (w motywie 18 wyjaśniono, że chodzi o działalność, która pozostaje bez związku z działalnością zawodową lub handlową; polegać ona może na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności; RODO znajdzie jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej, np. sieci społecznościowych);
d) przetwarzanie przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom (jeżeli dane osobowe przetwarzane są przez podmioty publiczne dla tych właśnie celów, takie przetwarzanie podlega dyrektywie 2016/680).

3.2.1.1. Pojęcie danych osobowych oraz ich podział na kategorie i rodzaje

Dane osobowe są dobrem chronionym przepisami ogólnego rozporządzenia. Definicję danych osobowych wprowadzono w „słowniczku" w art. 1 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

[319] *D. Lubasz,* Zakres przedmiotowy [w:] *D. Lubasz,* Meritum, s. 72 i przywołane tam orzecznictwo.

fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

Należy przypomnieć, że pierwszą definicją danych osobowych – choć pojęcie to oczywiście występowało w obrocie prawnym - o charakterze definicji legalnej była definicja sformułowana w art. 6 UODO1997, zgodnie z którą za dane osobowe uznawało 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. Rozumienie tego pojęcia nawiązywało do definicji zawartej w art. 2 lit. a dyrektywy 95/46/WE, zgodnie z którą za dane osobowe należy uznać wszelkie informacje odnoszące się do oznaczonej lub możliwej do oznaczenia osoby fizycznej.

Podstawowe elementy konstrukcyjne definicji pozostają więc niezmienne, są to: „informacje" (przedmiot), „o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej" (relacja), osoba fizyczna (podmiot). Powyższe trzy elementy muszą w konkretnej sytuacji występować łącznie, aby informacje można zakwalifikować do pojęcia dane osobowe[320].

Na gruncie RODO zachowuje aktualność założenie, zgodnie z którym charakter osobowy nie może zostać z góry przypisany żadnej kategorii danych. Przesądza o tym zwrot "informacje", użyty w definicji danych osobowych[321]. Zakres znaczeniowy pojęcia "informacja" powinien obejmować nie tylko znaki językowe, lecz także inne okoliczności towarzyszące znakom językowym lub tylko informacje pozajęzykowe, jak np. obraz, dźwięk czy informacje o właściwościach biologicznych (dane biometryczne). Nie ma znaczenia również postać utrwalenia, informacje mogą być zapisane na papierze, w pamięci systemu teleinformatycznego czy innym nośniku danych[322].

Każda informacja, niezależnie od sposobu i formy jej wyrażenia, podlegać może ocenie z punktu widzenia pojęcia danych osobowych i każda informacja może zostać uznana za informację o charakterze osobowym[323]. Konkretna informacja nie musi być powszechnie zrozumiała[324], charakter prawny tej informacji będzie bowiem oceniany indywidualnie dla

[320] Zob. na gruncie UODO1997 *A. Drozd*, Pojęcie danych osobowych [w:] *P. Fajgileski*, Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia, s. 23.
[321] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 1, pkt 2.
[322] *A. Drozd*, op. cit., s. 23.
[323] *P. Litwiński (red.)*, op. cit., pkt 4.
[324] *G. Sibiga*, Postępowanie w sprawach ochrony danych osobowych, Warszawa 2003, s. 33.

każdego jej dysponenta; nie musi być również prawdziwa[325], co należy rozumieć w ten sposób, że może dotyczyć okoliczności w sposób obiektywny nieistniejących, pod warunkiem jednak, iż może być przypisana do konkretnej, identyfikowalnej osoby fizycznej[326]. Status danych osobowych może zostać potencjalnie przyznany wszelkim informacjom odnoszącym się do osoby fizycznej.

Wykazanie relacji zachodzącej między informacją a osobą fizyczną stanowi kwalifikację z uwagi na określony stan faktyczny, w którym występują czynniki identyfikujące. Uwzględnia się przede wszystkim kontekst w jakim dochodzi do przetwarzania[327].

Związek między informacją a osobą fizyczną musi mieć charakter merytoryczny[328]. Informacja dotyczy osoby, jeżeli jest ona ta temat tej osoby[329]. Istniejący związek nie musi mieć charakteru osobowego, może dotyczyć m.in. majątku (czyli mieć charakter rzeczowy), jednak przynajmniej pośrednio musi odnosić się do konkretnej osoby fizycznej. Taka relacja nie zachodzi w przypadku danych zagregowanych o charakterze statystycznym[330].

Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny (motyw 26 preambuły RODO). Takie podejście do identyfikacji można uznać za subiektywne rozumienie przesłanki identyfikowalności, ponieważ odwołuje się nie tylko do sposobów identyfikacji, które są "rozsądnie prawdopodobne", ale i do takich, co do których istnieje "uzasadnione prawdopodobieństwo", że zostaną wykorzystane[331]. Prezentowany jest również pogląd odmienny, że uwzględnianie czynniki mają mieć charakter obiektywny, a nie relatywizowany

[325] *J. Barta, P. Fajgielski, R. Markiewicz,* Komentarz, 2004, s. 371.
[326] *P. Litwiński (red.)*, op. cit.
[327] *A. Drozd,* Pojęcie, s. 25.
[328] *D. Lubasz,* Komentarz do art. 4 pkt 1 [w:] *E. Bielak-Jomaa, D. Lubasz,* RODO, s. 173.
[329] *Grupa Robocza art. 29*, Opinia 4/2007 w sprawie pojęcia danych osobowych, 20.06.2007 r., WP 136.
[330] *D. Lubasz,* op. cit.
[331] Szerzej na temat koncepcji subiektywnej i obiektywnej przesłanki identyfikowalności zob. *P. Litwiński*, Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrik Breyer, „Europejski Przegląd Sądowy" 2017, nr 5, s. 5 i nast.

do perspektywy ocennej administratora czy innego podmiotu. Zobiektywizowane kryteria (np. koszt, czas, dostępna technologia) dają podstawę do dokonywania oceny ryzyka uznania danej informacji za osobową[332].

Informacja może zostać uznana za mającą charakter danych osobowych tylko wtedy, gdy dotyczy "osoby fizycznej". Pojęcie osoby fizycznej należy odnieść do nauki prawa cywilnego i wyrażonego w art. 8 par. 1 KC pojęcia zdolności prawnej, którą ma każdy człowiek od chwili urodzenia. Zdolność prawna to właściwość polegająca na zdolności do tego, aby być podmiotem praw i obowiązków[333]. Z uprawnień przewidzianych w przepisach o ochronie danych osobowych może korzystać człowiek od chwili swojego urodzenia[334]. Stąd do chwili urodzenia się dziecka informacje dotyczące *nasciturusa* powinny być traktowane jako mogące mieć charakter danych osobowych jego matki, ojca lub innych osób[335].

O ile nie budzi więc wątpliwości, że pojęcie osoby fizycznej odnosi się do człowieka, o tyle w pewnych szczególnych przypadkach wymaga rozstrzygnięcia, czy informacje o osobie będą mogły mieć potencjalnie charakter danych osobowych[336]. Na gruncie RODO nie budzi wątpliwości, że przepisy ogólnego rozporządzenia nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą jednak przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych (moty 27 preambuły RODO).

Danymi osobowymi nie są jedynie wymienione w RODO w otwartym katalogu przykładowe identyfikatory, które z założenia stanowią informacje dotyczące konkretnej osoby fizycznej, które pozwalają na jej zidentyfikowanie, ale są nimi również informacje, które przypisać można do konkretnej osobowy, jedynie zestawiając je z innymi informacjami.

Poufność nie jest elementem definiującym dane osobowe, co ma istotne znaczenie dla zasadniczego tematu rozprawy. Informacje publicznie dostępne, jeżeli dotyczą osoby fizycznej, nie tracą statusu danych osobowych[337].

Podstawowym podziałem danych osobowych na kategorie, jakiego można dokonać w oparciu o przepisy ogólnego rozporządzania, jest rozróżnienie danych na szczególne

[332] Za takim stanowiskiem opowiada się *D. Lubasz*, op. cit., s. 181 powołując się na stanowisko Trybunału Sprawiedliwości w sprawie C-582/14 wyrażone w pkt 46 wyroku, zgodnie z którym możliwą do zidentyfikowania nie będzie osoba, której dane dotyczą, jeżeli wykorzystanie określonego sposobu identyfikacji będzie niewykonalne w praktyce, przykładowo z powodu okoliczności, że wiąże się z nadmiernym nakładem czasu, kosztów i pracy ludzkiej.
[333] *A. Wolter, J. Ignatowicz, K. Stefaniuk*, Prawo cywilne. Zarys części ogólnej, Warszawa 2001, 158.
[334] *P. Litwiński (red.)*, op. cit., pkt 6.
[335] *A. Drozd*, Pojęcie, s. 29.
[336] *P. Litwiński (red.)*, op. cit..
[337] *M. Gumularz*, Ochrona danych osobowych w sektorze publicznym, Warszawa 2018, s. 30.

kategorie danych osobowych; dane osobowe dotyczące wyroków skazujących i naruszeń prawa oraz inne kategorie danych osobowych (dane osobowe zwykłe).

Zamknięty katalog szczególnych kategorii danych osobowych (zwanych danymi wrażliwymi[338]) wymienia art. 9 ust. 1 RODO, wprowadzający ogólną zasadę (chyba że zachodzi przesłanka legalizująca wymieniona w ust. 2) zakazu ich przetwarzania. Są to dane, 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[339]. Szczególnym kategoriami są dane osobowe:

- ujawniające pochodzenie rasowe lub etniczne,
- ujawniające poglądy polityczne, przekonania religijne lub światopoglądowe,
- ujawniające przynależność do związków zawodowych,
- genetyczne (oznaczające 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[340]),
- biometryczne (oznaczające 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[341]),
- dotyczące zdrowia (oznaczające dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia[342],
- dotyczące seksualności lub orientacji seksualnej tej osoby.

Kolejną odrębną kategorię w rozumieniu RODO stanowią dane osobowe dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa, które w myśl art. 10 RODO, przetwarzanie na postawie art. 6 ust. 1 RODO wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw

[338] Zob. motyw 10 preambuły RODO.
[339] Zob. motyw 51 preambuły RODO.
[340] Art. 4 pkt 13 RODO.
[341] Art. 4 pkt 14 RODO.
[342] Art. 4 pkt 15 RODO.

i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

W istocie należy tutaj odróżnić następujące elementy. Chodzi o informacje o "wyrokach skazujących", o których mowa w art. 413 § 2 KPK (lub art. 82 KPW; do tej kategorii nie będą więc należały wyroki umarzające lub warunkowo umarzające postępowanie albo też uniewinniające (art. 414 KPK); informacje o "naruszeniach prawa" to informacje o przypadkach popełnienia przestępstwa (naruszenia obowiązującego prawa) przez daną osobę fizyczną, ale niestwierdzonych wyrokami sądowymi (np. informacja o nałożeniu mandatu karnego, który ukarany przyjął) zaś "powiązane środki bezpieczeństwa" to środki zabezpieczające, które zostały wskazane w art. 93a § 1 KK[343].

Kategorii danych wrażliwych tradycyjnie przeciwstawiana jest kategoria tzw. danych zwykłych[344]. Za tzw. zwykłe dane osobowe należy uznać wszystkie pozostałe dane osobowe, które nie mieszczą się w dyspozycji art. 9 i 10 RODO. W ten sposób podział ten obejmuje wszystkie kategorie danych osobowych, a więc nosi cechy podziału zupełnego[345]. Należy podkreślić, że podział na dane zwykłe i wrażliwe jest podziałem sztucznym, nie jest podziałem doskonałym i jak każde uogólnienie nie jest zawsze prawdziwy. Bardzo prawdopodobne jest bowiem, że w konkretnych sytuacjach przetwarzanie niektórych z tzw. danych zwykłych (np. dane o sytuacji ekonomicznej, socjalnej) będzie niosło ze sobą znacznie większe zagrożenie dla prywatności niż przetwarzanie niektórych z tzw. danych wrażliwych (np. pochodzenia etnicznego czy rasowego)[346].

Rozwój technologii, takich jak Internet rzeczy oraz narzędzi służących do analizy dużych zbiorów danych (*big data*) sprawia, że tradycyjny scenariusz, w którym to podmioty danych świadomie podają swoje dane osobowe nie jest już jedynym lub dominującym sposobem, w jaki dane osobowe są zbierane. W wielu przypadkach dane wykorzystywane do celów analitycznych zostały wygenerowane automatycznie (maszynowo), na przykład przez obserwację działalności osób *on line*[347]. Dane wykorzystywane w analizie dużych zbiorów danych mogą być gromadzone za pośrednictwem tych nowych kanałów (np. poprzez czujniki urządzeń gospodarstwa domowego), ale alternatywnie mogą to być nowe dane generowane

[343] *P. Litwiński (red.)*, op. cit., Komentarz do art. 10, pkt 2-4.
[344] Zob. *G. Sibiga*, Postępowanie, s. 40.
[345] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 1, pkt 27.
[346] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 570.
[347] Information Commissioner, *Big data, artificial intelligence, machine learning and data protection*, 2017.09.04, Version: 2.2., s. 13.
https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf (dostęp:31.11.2020).

przez same narzędzia analityki danych, a nie świadomie dostarczane przez osoby. W tym kontekście można dokonać podziału danych osobowych ze względu na sposób pozyskania na następujące rodzaje[348].

Dane osobowe podane (*provided data*), są to dane świadomie podane przez osobę, której dane dotyczą, np. podczas wypełniania formularza dostępnego *on line*. Dane podane można z kolei podzielić na trzy podkategorie: dane zainicjowane (*initiated*), czyli dane podane przez osobę rozpoczynającą daną aktywność, np. rejestracją w systemie teleinformatycznym dane transakcyjne (*transactional*), podane w trakcie dokonywania transakcji w Internecie, np. za pośrednictwem karty kredytowej i dane opublikowane (*posted*), np. serwisach społecznościowych.

Dane osobowe zaobserwowane (*observed*), są to dane zapisywane jest rejestrowane automatycznie, np. za pomocą tzw. plików *cookies*, czujników *on line* lub monitoringu przemysłowego (*closed circuit television* – CCTV) połączone z rozpoznawaniem twarzy.

Dane osobowe pochodne (*derived*), są to dane wygenerowane z innych danych w relatywnie prosty i bezpośredni sposób, np. podczas obliczania zdolności kredytowej przez bank.

Dane osobowe wnioskowane (*inferred*) są to dane tworzone przy użyciu bardziej złożonych metod analityki danych w celu znalezienia odpowiedniej korelacji między zbiorami danych i ich kategoryzowania lub profilowania, np. przewidywania przyszłego stanu zdrowia. Są to dane wywnioskowane na podstawie prawdopodobieństwa i dlatego są mniej precyzyjne niż dane pochodne.

Dane można ze względu na sposób ich depersonalizacji w celu zachowania poufności można umownie podzielić na dane zanonimizowane oraz dane spseudonimizowane. Te pierwsze na gruncie RODO pozostają niezdefiniowane. Co ciekawe, definicję legalną anonimizacji na gruncie przepisów UE wprowadził prawodawca unijny w dyrektywie 2019/1024, uznając w art. 2 pkt 7 ją proces zmiany dokumentów w informacje anonimowe, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, lub dane osobowe zanonimizowane w taki sposób, że identyfikacja osoby, której dane dotyczą, nie jest lub już nie jest możliwa. Innymi słowy dane zanonimizowane to dane trwale

[348] Zob. szerzej *M. Abrams*, The origins of personal data and its implications for governance, The Information Accountability Foundation, 2014, s. 5 i nast.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2510927 (dostęp: 30.11.2020).
Zob. również *M. Gumularz*, op.cit., s. 36-38.

i nieodwracalnie zdepersonalizowane, które nie podlegają przepisom o ochronie danych osobowych, bowiem nie stanowią już danych osobowych.

Z kolei dane spseudonimizowane pozostają wciąż danymi osobowymi. Są to dane osobowe przetworzone w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, 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). Pseudonimizacja jest czynnością odwracalną, dlatego też takie dane należy traktować jak dane osobowe (por. motyw 26 preambuły RODO).

3.2.1.2. Zbiór danych

Pojęcie zbioru danych ma kluczowe znaczenie dla wyznaczenia materialnego zakresu stosowania przepisów ogólnego rozporządzenia[349]. Jak wskazano powyżej ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów nie powinny być objęte zakresem niniejszego rozporządzenia (zob. motyw 15 RODO).

Zgodnie z definicją zawartą w art. 4 pkt 6 zbiór danych oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Elementami konstytutywnymi pojęcia zbioru danych pozostają więc: zestaw danych osobowych, uporządkowanie (istnienie struktury) tego zestawu, dostępność danych osobowych zawartych w zestawie według określonych kryteriów.

Dane osobowe zawarte w zbiorze danych mogą być wyrażone w dowolny sposób, np. słowem, dźwiękiem, obrazem. Za zestaw należy uznać całość złożoną z odpowiednio dobranych elementów. Poprzez posłużenie się liczba mnogą „dane osobowe", przypadku występowania pojedynczej informacji o osobie nie można mówić o istnieniu zbioru danych osobowych tworzonego przez tę właśnie informację[350].

[349] Choć należy jednocześnie zauważyć, że jego znaczenie w RODO jest znacznie mniejsze niż w poprzednim porządku regulacyjnym. W przepisach UODO1997, gdzie stanowiło ono kluczowe pojęcie oraz zasadniczy punkt odniesienia przy realizacji wszelkich obowiązków wynikających z tej ustawy, przy regulacji których w sposób odnoszono się w niej do kategorii zbioru danych.
[350] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, s. 392.

Zestaw danych w zbiorze musi być uporządkowany, konieczne jest zatem, aby posiadał strukturę. Zbiór należy rozumieć jako całość złożoną z jednorodnych części, która jest czymś więcej niż sumą jej części, m.in. dzięki strukturze, tzn. ogółowi relacji między częściami (elementami), które są powiązaniami na tyle ścisłymi, że przestają być tylko układem, a stają się zestawem (systemem)[351]. Uporządkowanie powinno pozwolić na bezpośredni dostęp do poszukiwanej informacji, ponieważ główną cechą odróżniającą zbiór danych od innych zestawów jest istnienie cechy lub cech pozwalających na odnalezienie informacji bez potrzeby przeglądania całego zestawu[352]. Ta cecha zbioru danych osobowych odnosi się łącznie do dwóch pozostałych cech zbioru, tj. wymogu uporządkowania danych oraz zapewniania dostępu do danych osobowych według określonych kryteriów. To bowiem struktura zbioru danych osobowych powinna zapewnić dostęp do danych zawartych w zbiorze[353].

Dostęp do danych powinien być zatem realizowany za pomocą określonych kryteriów, decydujące jednak pozostaje to, czy konkretne dane osobowe konkretnej osoby w danym przypadku są dostępne, czyli czy można do danych w nim zawartych dotrzeć według jakichś kryteriów[354].

Dostęp do danych zwartych w zbiorze powinien być możliwy według określonych kryteriów. Istotą zbioru danych osobowych jest organizacja danych zawartych w zbiorze według co najmniej jednej cechy, która pozwala na szybkie odnalezienie danych konkretnej osoby[355]. Przy czym nie ma wymogu, aby kryteriów dostępności powinno w danej sytuacji być więcej niż jedno, mogą funkcjonować różne kryteria dostępu do danych zawartych w zbiorach danych[356]. Charakter kryterium porządkującego zbiór danych osobowych nie ma istocie znaczenia. Kryterium to może mieć charakter dowolny, także nieosobowy[357].

Należy podkreślić, że w RODO, w przeciwieństwie do koncepcji przyjętej w dyrektywie 95/46/WE i UODO1997, nie nakłada na administratorów i podmioty przetwarzające obowiązku prowadzenia jakichkolwiek rejestrów zbiorów danych, a zbiory takie nie stanowią kryterium nakładanych na administratorów oraz podmioty przetwarzające obowiązków. Zbiory takie nie muszą podlegać jednak żadnej systematyzacji, ewidencjonowaniu oraz rejestracji[358].

---

[351] *G. Szpor*, Publicznoprawna ochrona danych osobowych, Przegląd Ustawodawstwa Gospodarczego 1999, s. 6.
[352] *A. Mednis*, Ustawa, s. 27.
[353] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 6, pkt 3.
[354] *M. Sakowska – Baryła*, Komentarz do art. 4 pkt 6, pkt 8 [w:] *M. Sakowska – Baryła (red.)*, Ogólne rozporządzenie o ochronie danych osobowych. Komentarz, Legalis/Wyd. 2018.
[355] Zob. *G. Sibiga*, Postępowanie, s. 47.
[356] Zob. *M. Sakowska*, Pojęcie „zbiór danych" na gruncie ustawy o ochronie danych osobowych, „Radca Prawny" 2005, nr 2, s. 62.
[357] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 6, pkt 8.
[358] *Ibidem*, pkt 12.

Dał temu wyraz prawodawca UE w motywie 89 RODO, wskazując, że dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten, powodując jednak obciążenia administracyjne i finansowe, nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je skutecznymi procedurami i mechanizmami koncentrującymi się w zamian na tych rodzajach operacji przetwarzania.

3.2.1.3. Przetwarzanie danych osobowych

Przetwarzanie zgodnie z definicją sformułowaną w art. 4 pkt 2 RODO 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.

Istota pojęcia sprowadza się do działania podejmowanego na informacjach kwalifikowanych jako dane osobowe lub zestawach danych osobowych. Działanie takie musi być zależne od decyzji człowieka, czyli albo być bezpośrednio przez niego podejmowane, albo następować wprawdzie automatycznie, ale w sposób zależny od woli człowieka. W tym ostatnim przypadku Definicja przetwarzania zupełnie abstrahuje od woli i świadomości człowieka. Dla zaistnienia przetwarzania nie jest zatem istotne, czy dana osoba chce przetwarzać dane osobowe i czy zdaje sobie sprawę z tego, że informacje, na których dokonuje działań, są danymi osobowymi[359].

Przetwarzanie danych osobowych może być dokonywane w sposób zautomatyzowany albo niezautomatyzowany. W istocie ten element definicji wydaje się zbędny w świetle art. 2 ust. 1 RODO, w którym wyraźnie przeciwstawia się przetwarzanie całkowicie lub częściowo zautomatyzowane przetwarzaniu realizowanemu w sposób inny niż zautomatyzowany (zatem obejmującemu potencjalnie wszelkie pozostałe sposoby przetwarzania, czyli przetwarzanie niezautomatyzowane, np. ręcznego).

[359] *W. Chomiczewski*, Przetwarzanie [w:] *D. Lubasz (red.)*, Meritum, s. 84.

Definicja legalna przetwarzania opiera się na przykładowym i niewyczerpującym wyliczeniu czynności, które mogą składać się na przetwarzanie danych osobowych. Pogłębiona analiza każdego z wymienionych sposobów operowania na danych wykraczałoby poza główny temat rozprawy, niemniej w Rozdziale 3.3. zostaną omówione te operacje, które mogą mieć miejsce w ramach realizacji prawa do ponownego wykorzystywania i jednocześnie stanowić samo ponowne wykorzystywanie zgodnie z definicją zaprezentowaną wcześniej.

W tym miejscu w ramach pojęcia przetwarzania należy rozstrzygnąć kwestię czy samo zapoznanie się z danymi stanowić będzie ich zbieranie. Oceniając, czy konkretna czynność stanowi zbieranie danych osobowych, należy w pierwszej kolejności ustalić, w jakim celu osoba wchodzi w posiadanie danych osobowych. Jeżeli celem tym jest jedynie zapoznanie się z informacjami, bez ich dalszego przetwarzania, wówczas nie można mówić o zbieraniu danych osobowych a w konsekwencji ich przetwarzaniu. Celem wejścia w posiadanie informacji nie jest bowiem wyłącznie zapoznanie się z nimi, lecz poddanie ich dalszym operacjom przetwarzania[360]. Chociaż czynności zbierania danych i zapoznawania się z danymi osobowymi mogą stanowić czynności przetwarzania danych, należy je od siebie odróżnić z tego względu, że do przyjęcia, że mamy do czynienia ze zbieraniem danych osobowych, nie jest konieczne, żeby osoba, która dane zbiera, znała treść tych danych. Wystarczy bowiem wejście w posiadanie danych osobowych z zamiarem ich dalszego przetwarzania, żeby w konkretnej sytuacji można było mówić o zbieraniu danych osobowych[361]. Przykładowo sam wgląd w informacje o osobie zawarte w jej dokumencie tożsamości jest z pewnością operacją na danych osobowych, takie przetwarzanie danych nie podlega jednak przepisom ochronie danych osobowych, ponieważ nie istnieje nawet teoretyczna możliwość dalszego przetwarzania tych danych[362].

3.2.2. Zakres podmiotowy stosowania ogólnego rozporządzenia

Artykuł 3 RODO odnosi się do zakresu podmiotowego regulacji. Prawodawca UE nakazuje stosowanie rozporządzenia zarówno administratorom, jak i podmiotom przetwarzającym w przypadku, gdy przetwarzanie przez nich danych osobowych następuje w związku z działalnością ich jednostek organizacyjnych prowadzoną w UE. Ogólnie określić je można jako "podmioty zobowiązane do ochrony danych osobowych" w tym znaczeniu, że

[360] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 2, pkt 5.
[361] *Ibidem*, pkt 6.
[362] Zob. *G. Sibiga*, Postępowanie, s. 50.

mają one obowiązek przestrzegać procedur postępowania z danymi osobowymi wynikających z przepisów prawa, w tym przede wszystkim z RODO, a w pewnym zakresie także określonych w postanowieniach umownych[363].

Innym podmiotem, którego znaczenie należy wyjaśnić jest odbiorca danych osobowych. Pojęcie odbiorcy nie wpływa wprawdzie na wyznaczenie w art. 3 zakresu podmiotowego stosowania przepisów ogólnego rozporządzenia, niemniej pozostaje istotne zarówno z punktu widzenia wykonania niektórych praw i obowiązków RODO (obowiązki informacyjne, prawo dostępu do danych, obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, prowadzenie rejestrów czynności przetwarzania), jak i ma znaczenie z punktu widzenia ponownego wykorzystywania informacji sektora publicznego zawierającej danej osobowe (wyjaśniam to w dalszej części tego Rozdziału).

3.2.2.1. Administrator i podmiot przetwarzający dane

Administrator jest jednym z najważniejszych pojęciem dla określenia zakresu stosowania RODO. Kwalifikacja określonego podmiotu jako administratora, ma bowiem bardzo szerokie konsekwencje. Jest on adresatem zdecydowanej większości obowiązków wynikających z RODO. Administrator to kluczowy podmiot zobowiązany do ochrony danych osobowych, ponieważ zgodnie z przepisami RODO jego władztwo nad danymi osobowymi, obowiązki i odpowiedzialność mają najszerszy charakter[364]. To również na administratora mogą być nakładane kary pieniężne przewidziane w ogólnym rozporządzeniu.

Dla kwalifikacji określonej osoby fizycznej lub prawnej, organu publicznego, jednostki lub innego podmiotu jako administratora, konieczne jest – art. 4 pkt 7 RODO – by ustalał on, samodzielnie lub wspólnie z innymi podmiotami, 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.

Po pierwsze z definicji wyrażonej w art. 4 pkt 7 RODO wynika, że status administratora danych osobowych może przysługiwać osobie fizycznej lub prawnej, organowi publicznemu,

[363] *M. Sakowska – Baryła*, Komentarz do art. 4 pkt 7, pkt 2 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie, Legalis/Wyd. 2018.
[364] *M. Sakowska – Baryła*, op. cit.

jednostce lub innemu podmiotowi. Jest to więc katalog otwarty, który w szczególności nie wiąże przymiotu administratora danych z posiadaniem osobowości prawnej[365].

Organy publiczne, a więc organy państwowe i organy samorządu terytorialnego, mogą zostać uznane za administratorów danych osobowych. Co istotne RODO przewiduje możliwość ustalania we właściwych przepisach prawa, jaki podmiot z sektora publicznego pełni funkcję administratora danych osobowych w stosunku do konkretnych zbiorów. Administratorem danych osobowych jest zawsze sam organ administracji, nie zaś obsługujący go urząd[366]. Organy publicznej przetwarzają dane osobowe dla wykonywania określonych prawem zadań, co oznacza, że nie mogą samodzielnie decydować o wykorzystywaniu zbieranych danych. Wynika to z wyrażonej w art. art. 7 Konstytucji RP i art. 6 KPA zasady praworządności[367].

Po drugie, elementem przedmiotowym definicji administratora jest decydowanie o celach i sposobach przetwarzania danych osobowych, które łącznie składają się na sprawowanie władztwa nad przetwarzanymi danymi[368]. Podkreślić jednak należy, że posiadania przymiotu administratora danych osobowych nie można utożsamiać z faktycznym posiadaniem danych – podstawowym kryterium odróżniającym administratora danych osobowych od innych podmiotów przetwarzających dane jest sprawowanie faktycznej kontroli nad przetwarzaniem danych, a więc decydowanie o celach i sposobach przetwarzania, nie zaś faktyczne przetwarzanie, które może zostać powierzone innemu podmiotowi[369]. Status administratora ma głównie walor funkcjonalny – dostarcza kryteriów określenia, kto kontroluje procesy przetwarzania danych, niezależnie od tego, czy przetwarzanie to jest zgodne z prawem[370].

Za administratora danych osobowych nie można uznać każdego dysponenta danych, jest nim ten, kto decyduje o celach i środkach przetwarzania, przy czym zasadnicze znaczenie ma rodzaj i charakter nadanych przez prawo kompetencji z zakresu spraw publicznych[371].

Za cele przetwarzania należy uznać wartości, dla urzeczywistnienia których dochodzić będzie do przetwarzania danych osobowych. Natomiast pojęcie sposobów przetwarzania danych w aspekcie decydowania o tych sposobach oznacza dokonywanie wyboru technicznych sposobów przetwarzania danych[372].

---

[365] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 7, pkt 13.
[366] Por. *G. Sibiga*, Postępowanie, s. 55.
[367] *Ibidem.*
[368] *G. Sibiga*, Postępowanie, s. 53.
[369] *P. Litwiński (red.)*, op. cit., pkt 2.
[370] *M. Sakowska-Baryła*, op. cit., pkt 3.
[371] Zob. wyrok NSA z 30.1.2002 r., II SA 1098/01.
[372] *P. Litwiński (red.)*, op. cit., pkt 9.

Ocena, czy dany podmiot jest administratorem, następuje obiektywnie i niezależnie od jego woli. Nie ma też żadnego znaczenia świadomość pełnienia tej roli przez dany podmiot, ważne jest jedynie, czy spełnione są przesłanki określone w art. 4 pkt 7 RODO. Nie jest dopuszczalne zrzeczenie się statusu administratora lub jego przeniesienie na inną osobę w oparciu o umowę[373].

Na gruncie RODO możliwe jest ustalanie celów i sposobów przetwarzania samodzielnie przez danego administratora lub wspólnie z innymi administratorami. Wówczas współdziałanie między administratorami należy rozpatrywać w kontekście art. 26 RODO, regulującego przypadek ustalania celów i sposobów przetwarzania przez co najmniej dwóch administratorów działających jako współadministratorzy.

Od administratora należy odróżnić podmiot przetwarzający dane, czyli osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora (art. 4 pkt 8 RODO). Rozróżnienie pomiędzy administratorem danych a podmiotem przetwarzającym powinno opierać się na przesłankach natury czysto faktycznej, czyli na elemencie sprawowania faktycznego władztwa nad przetwarzanymi danymi[374]. Innymi słowy podmiot ten nie może – przetwarzając dane osobowe w imieniu administratora danych – realizować własnych celów przetwarzania danych.

W istocie chodzi o „podmiot przetwarzający na zlecenie"[375]. Określenie „podmiot przetwarzający" w powiązaniu z przetwarzaniem przez osobę fizyczną danych w imieniu administratora może prowadzić do błędnego uznawania, że w przypadku niektórych osób (np. pracownika) mamy do czynienia z „podmiotem przetwarzającym", podczas gdy istotą tego pojęcia jest nie tylko dokonywanie czynności w imieniu administratora, ale także na jego zlecenie, przez zewnętrzny podmiot, nieznajdujący się w strukturze organizacyjnej administratora[376].

3.2.2.2. Pojęcie odbiorcy

Zgodnie z art. 4 pkt 9 RODO odbiorcą jest osoba fizyczna, prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Przy czym, nie są odbiorcą organy publiczne, które mogą otrzymywać dane

[373] *W. Chomiczewski*, Administrator [w:] *D. Lubasz*, Meritum, s. 88.
[374] *L.A. Bygrave*, Data Protection Law: Approaching Its Rationale Logic and Limit, Kluwer Law International 2002, s. 21.
[375] Zob. *P. Fajgielski*, Komentarz, 2018, s. 124.
[376] *Ibidem*.

osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego.

Dla kwalifikacji danej osoby jako obiorcy musi być ona zatem kwalifikowana jako jeden z podmiotów wymienionych w definicji, np. musi być osobą prawną, oraz muszą zostać mu ujawnione dane osobowe.

Pojęcie odbiorcy ma znaczenie w szczególności przy realizacji obowiązków informacyjnych, ponieważ na podstawie art. 13 ust. 1 lit. e oraz art. 14 ust. 1 lit. e RODO administrator jest zobowiązany do przekazania podmiotowi danych informacji o odbiorcach danych osobowych lub kategoriach tych odbiorców. Następnie w art. 15 RODO informacja o odbiorcach lub kategoriach odbiorców jest elementem prawa dostępu do danych. Z kolei w art. 19 RODO ustanowiono obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcy, któremu ujawniono dane osobowe. Dlatego też właściwe określenie grona odbiorców, a więc prawidłowe zidentyfikowanie tych podmiotów ma decydujące znaczenie dla właściwej realizacji wskazanych obowiązków[377].

Typowymi przykładami odbiorcy będą: osoba, której dane dotyczą, inny administrator danych oraz podmiot przetwarzający[378]. Odbiorcą danych osobowych może być także strona trzecia, jeżeli ujawnia się jej dane osobowe.

Głównym powodem wyodrębnienia kategorii strony trzeciej jest konieczność jednoznacznego oddzielenia od siebie grupy osób i podmiotów mogących zapoznawać się z treścią danych (nie łamiąc przy tym tajemnicy danych osobowych) od tych, których dostęp (potencjalny lub faktyczny) do tych treści nie jest pewny. Dostęp do danych może mieć miejsce pod pewnymi warunkami, ale dopóki nie zostaną one sprawdzone lub zaistnieją, to co do zasady nie ma możliwości legalnego ujawnienia treści danych osobowych komukolwiek zakwalifikowanemu jako strona trzecia[379].

Stroną trzecią jest każdy podmiot inny niż – po pierwsze – osoba, której dane dotyczą, administrator oraz podmiot przetwarzający; po drugie - za stronę trzecią nie mogą zostać także uznane osoby, które mogą przetwarzać dane osobowe z upoważnienia administratora lub podmiotu przetwarzającego. Strona trzecia jest więc pewną zbiorczą kategorią podmiotów, które nie mogą wywodzić swojego uprawnienia do dostępu do danych osobowych z faktu, że dane osobowe dotyczą tej właśnie osoby (osoba, której dane dotyczą), z faktu decydowania

[377] *W. Chomiczewski*, Odbiorca [w:] *D. Lubasz*, Meritum, s. 92.
[378] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 9, pkt 4.
[379] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 4 pkt 10, pkt 1.

o celach i sposobach przetwarzania danych (administrator danych), z faktu działania w imieniu lub z upoważnienia administratora danych (podmiot przetwarzający i osoba upoważniona)[380].

Kłopotliwe może być jednoznaczne ustalenie statusu strony trzeciej po ujawnieniu jej danych osobowych. Jeśli zostanie ona włączona w proces przetwarzania, stanie się zazwyczaj samodzielnym administratorem danych osobowych (lub współadministratorem[381]). Jeżeli podejmie przetwarzanie w imieniu administratora, stanie się podmiotem przetwarzającym, a w sytuacji ujawnienia jej danych dotychczasowa strona trzecia może stać się odbiorcą[382]. Z uwagi na ograniczony zakres stosowania RODO może również dochodzić do ujawnienia danych stronie trzeciej niepodlegającej przepisom ogólnego rozporządzenia (np. osobie fizycznej wykorzystującej dane w celach osobistych). Trudno wówczas będzie przyjąć, że można stronę trzecią traktować jak nowego niezależnego administratora[383].

3.3. Wspólny obszar regulacji ogólnego rozporządzenia oraz przepisów o ponownym wykorzystywaniu informacji sektora publicznego

3.3.1. Pojęcie informacji i danych

Zwornikiem łączącym zakresy przedmiotowe dwóch porządków regulacyjnych jest pojęcie informacji. Na gruncie przepisów krajowych nie występuje definicja normatywna informacji, choć jest ona wykorzystywana jako element wyrażenia definiującego (*definiens*) innych pojęć definiowanych (*definiendum*), czego dobitnym przykładem jest właśnie definicja danych osobowych („dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej"). Innym - mniej trafnym z punktu widzenia poprawności budowy definicji – przykładem jest ustawowe wyjaśnienia pojęcia informacji publicznej („informacja publiczna to informacja o sprawach publicznych").

„Informacja" (łac. *informatio* – wyobrażenie, wyjaśnienie, zawiadomienie) według Słownika Języka Polskiego pozostaje „pojęciem w zasadzie niedefiniowalnym ze względu na jego pierwotny, elementarny charakter; rozpatrywana najczęściej w trzech aspektach: syntaktycznym (dotyczy ilości informacji, jaka może być potencjalnie zawarta

[380] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 10, pkt 1.
[381] Konsekwencją możliwości wspólnego podejmowania decyzji o celach i sposobach. Przetwarzania jest art. 26 RODO, który reguluje konstrukcję współadministrowania. Przepis ten wskazuje co współadministratorzy powinni między sobą określić w umowie o współadministrowaniu.
[382] *W. Chomiczewski*, Komentarz do art. 4 pkt 10 [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 237.
[383] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 4 pkt 10, pkt 1.

w danej wiadomości), semantycznym (znaczenia i zawartości treściowej wiadomości) i pragmatycznym (przydatności informacji, tj. wartości informacji zawartej w wiadomości ze względu na realizowany przez odbiorcę cel)". W języku potocznym wyraz informacja oznacza wiadomość czy konstatację stanu rzeczy[384].

Pojęcie to występuje w wielu obszarach nauk, m.in. naukach ścisłych, filozofii czy informatyce. Z tego powodu w literaturze prawniczej proponuje się próby wyjaśnienia pojęcia czerpiąc z dorobku różnych dziedzin. Interdyscyplinarne podejście zaproponowała *G. Szpor* definiując informację jako „przenaszalne dobro (niematerialne) zmniejszające niepewność"[385]. Bez znaczenia pozostaje zmaterializowanie informacji, a więc utrwalenie jej w jakiejkolwiek formie.

Odwołanie do ustaleń teorii prawa i teorii informacji, pozwala rozwinąć tezę, że informacja jako dobro zmniejszające niepewność (redukujące entropię) może być przekazywana przy użyciu określonych sygnałów (danych), a każdy przekaz sygnałów jest zjawiskiem fizycznym[386]. Informacja jest dobrem służącym do zaspokajania zróżnicowanych potrzeb ludzi, z których korzysta się indywidualnie i zbiorowo i które nadają się do rozdziału, tzn. do przemieszczania między ludźmi[387]. Z kolei przetwarzanie danych mających wartość informacyjną jest warunkiem korzystania z wielu dóbr i istotne znaczenie ma regulacja sposobów lokalizowania, filtrowania i kondensowania zasobów informacyjnych[388].

W literaturze przedmiotu przyjmuje się, że informacja ma pewne cechy, które determinują jej dalsze zastosowanie, tj. jest niezależna od obserwatora, przejawia cechę synergii, jest różnorodna, jest zasobem niewyczerpalnym, może być powielana i przenoszona w czasie i przestrzeni, można ją przetwarzać, nie powodując jej zniszczenia, ta sama informacja może mieć różne znaczenie dla różnych użytkowników, każda jednostkowa informacja opisuje obiekt tylko ze względu na jedną jego cechę[389].

Pojęcia informacji i danych nie można zatem traktować synonimicznie. Dane stanowią element pierwotny w strukturze poznania względem informacji, dlatego należy uznać, że nie wszystkie dane mają wartość informacyjną. Danymi będą wszystkie znaki w formie nadającej

---

[384] Słownik Języka Polskiego PWN https://encyklopedia.pwn.pl/haslo/informacja;3914686.html.
[385] *G. Szpor*, Pojęcie informacji a zakres ochrony danych osobowych [w:] *P. Fajgielski (red.)*, Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia, s. 8.
[386] Zob. szerzej: *G. Szpor*, Idee i pojęcia, t. 1 [w:] *G. Szpor (red.)*, Jawność i jej ograniczenia, Warszawa 2017, s. 103-106.
[387] *Ibidem*. Na temat podziałów dóbr publicznych zob. *S. Biernat*, Problemy prawne sprawiedliwego rozdziału dóbr przez państwo, Kraków 1985.
[388] *G. Szpor*, op. cit.
[389] Tak *B. Stefanowicz*, Informacyjne systemy zarządzania, Warszawa 1997 r., s. 25, za: *G. Wierczyński, W.R. Wiewiórowski*, Informatyka prawnicza, Gdańsk 2016, s. 40.

się do przetwarzania (litery, cyfry, impulsy), są mierzalne ilościowo i zapisywane na nośniku. Dane stanowią zatem źródło informacji. Innymi słowy informacja oznacza treść, jaką odczytać można z danych, znając konwencję znaczeniową zapisu danych, a więc „dane stanowią zakodowany zapis informacji”[390].

Niemniej analiza tekstów prawnych ukazuje niekonsekwentne posługiwanie się zarówno terminem dane jak i informacja oraz bezrefleksyjne kształtowanie ich wzajemnych relacji[391].

W ramach kryterium przedmiotowego (treściowego) rozróżnia się wiele różnych podkategorii danych, które mogą mieć wartość informacyjną, np. dane jednostkowe (osobowe i indywidualne) oraz statystyczne, dane publiczne i niepubliczne, dane przestrzenne i nieprzestrzenne[392].

Tak ujęte rozumienie informacji można odnieść zarówno do znaczenia pojęć informacji sektora publicznego, jak i danych osobowych. Oba pojęcia normatywnie zdefiniowane zawierać się będą w szerszej kategorii informacji wypracowanej w nauce prawa.

Odnosząc pojęcie informacji do danych osobowych można przyjąć, że informacja jest dobrem, ale nie dobrem osobistym, dzięki czemu możliwa jest jej przenaszalność. Ta cecha odróżnia ją od dóbr i wartości nieprzenaszalnych, jak prywatność, która jest dobrem osobistym. Dane dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, mogą nie stanowić informacji, tj. mieć zerową wartość informacyjną, przez co nie będą się mieścić z zakresie przedmiotowym regulacji ochrony danych osobowych[393]. Informacja o osobie składa się z kwantów (minijednostek), którymi są dane, a dane te uzyskują status danych osobowych w zależności od zasobu informacyjnego, który przetwarza dana osoba[394].

3.3.2. Informacja sektora publicznego a dane osobowe

Jak wykazano zakres pojęcia informacji sektora publicznego jest bardzo szeroki. O tym, że danej treści można przypisać status informacji sektora publicznego, decydujące znaczenie ma jedynie warunek jej utrwalenia oraz dysponowania („posiadania”) przez podmiot zobowiązany. Kryterium przedmiotowe jest prawnie irrelewantne dla takiej kwalifikacji.

[390] *P. Fajgielski*, Komentarz, 2018, s. 104. Zob. szerzej tego autora: Informacja w administracji publicznej. Prawne aspekty gromadzenia, udostępniania i ochrony, Wrocław 2007, s. 13 i nast.
[391] Zob. *G Szpor*, Idee i pojęcia, s. 106-111.
[392] *Ibidem, s. 113.*
[393] *G. Szpor*, Pojęcie informacji, s. 18.
[394] *W.R. Wiewiórowski*, Założenia wstępne dla zrównoważonego przetwarzania, s. 6.

Jedynie istotna może być z kolei przesłanka jakościowa dla kwalifikacji treści jako danych otwartych rozumianych jako podzbiór szerszego zbioru informacji sektora publicznego.

W konsekwencji relację między pojęciem informacji sektora publicznego i danych osobowych można rozpatrywać na kilku płaszczyznach.

Po pierwsze informacja sektora publicznego może stanowić dane osobowe. Przykładem jest imię i nazwisko funkcjonariusza publicznego, np. prezydenta Rzeczypospolitej Polskiej czy wójta gminy Prażmów.

Po drugie, dane osobowe mogą być zawarte w informacji sektora publicznego stanowiąc taką część ich treści, że eliminacja samych danych osobowych (np. poprzez anononimizację) nie spowoduję całkowitej utraty wartości poznawczej informacji sektora publicznego. Oczywiście sytuacja ta jest względna i jest uzależniona od perspektywy adresata informacji (np. depersonalizacja uzasadnienia orzeczenia sądowego nie eliminuje wartości informacyjnej takiej treści dla studenta prawa, może mieć jednak pejoratywne skutki poznawcze dla reportera; anonimizacja rejestru osób fizycznych prowadzących jednoosobową działalność gospodarczą nie usuwa wartości informacyjnej dla firmy badawczej analizującej rozwój samozatrudnienia w danym segmencie gospodarki, ale powoduje bezużyteczność takiego źródła informacji dla wywiadowni gospodarczej etc).

Po trzecie, dane osobowe mogą być zawarte w informacji sektora publicznego stanowiąc jednocześnie dominującą wartość informacyjną. Usunięcie danych osobowych powoduje utratę przez informację sektora publicznego przymiotu źródła informacji rozumianej jako dobro niematerialne eliminujące niepewność (np. imiona i nazwiska osób, którym udzielono zamówienie publiczne).

3.3.3. Ponowne wykorzystywanie informacji a przetwarzanie danych

Ponowne wykorzystywanie informacji sektora publicznego zawierających lub stanowiących dane osobowe w świetle przepisów ogólnego rozporządzenia będzie stanowiło przetwarzanie danych osobowych. Zarówno ponowne wykorzystywanie, jak i przetwarzanie, łączy się działaniem czy też operowaniem odpowiednio na informacji lub danych. W istocie z przetwarzaniem danych w ramach realizacji ponownego wykorzystywania może dochodzić na dwóch etapach, różne również będą podmioty przetwarzające dane.

Na pierwszym etapie do przetwarzania danych osobowych zawartych lub stanowiących dane osobowe będzie dochodzić w ramach ich przekazania lub udostępnienia przez podmiot zobowiązany do ponownego wykorzystywania (zob. Rozdział 4.3.). W pierwszym wypadku

dojdzie do ujawnienia danych osobowych oznaczonemu i konkretnemu wnioskodawcy, któremu informacja sektora publicznego zostanie przekazana w wyniku pozytywnie rozpatrzonego wniosku o ponowne wykorzystywanie. W drugim przypadku ujawnienie danych osobowych nastąpi w ramach udostępnienia informacji sektora publicznego w BIP, centralnym repozytorium lub w inny sposób, przy czym użytkownikiem informacji w rozumieniu UPW będzie nieoznaczony i nieznany podmiotowi zobowiązanemu ani podmiotowi danych krąg podmiotów, czyli osób fizycznych, osób prawnych lub jednostek organizacyjne nieposiadających osobowości prawnej.

Dla omawianej tematyki istotne jest, że w ramach przekazania lub udostępnienia informacji sektora publicznego (po spełnieniu określonych przesłanek opisanych w Rozdziale 7) dojdzie do ujawnienia danych osobowych, które na gruncie art. 4 pkt 2 RODO można uznać jako jedną z form wykonywania czynności na danych osobowych, a zatem stanowi ich przetwarzanie („ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie"). Oznacza to, że dane osobowe w konsekwencji tej operacji mogą być poznane przez inne osoby, które do tej pory ich nie znały. Istotne jest, że ujawnianie musi być skutkiem działania osoby przetwarzającej dane[395].

W przepisach ogólnego rozporządzenia brak jest legalnej definicji pojęcia ujawniania, rozpowszechniania i udostępniania danych osobowych. W doktrynie niemieckiej pod pojęciem ujawnienia rozumie się umożliwienie odbiorcy dostępu do danych, niezależnie od tego, w jaki sposób następuje. Nie jest wymagana żadna konkretna forma, by dane działanie kwalifikować jako ujawnienie danych. Ujawnieniem danych może być przeslanie informacji zawierających dane osobowe w dowolnej formie, przekazanie ich ustnie, umożliwienie dostępu do nich w formie tradycyjnej, papierowej czy elektronicznej[396].

Przesłanie danych osobowych wymaga aktywności ze strony osoby ujawniającej dane i może polegać na tradycyjnym wysłaniu danych osobowych pocztą lub kurierem, jak i transmisją danych poprzez sieć teleinformatyczną[397].

Rozpowszechnianie polega na publicznym udostępnieniu danych osobowych, którego skutkiem jest uzyskanie możliwości zapoznania się z informacjami przez nieograniczone grono osób.

W nauce prawa zwrócono natomiast uwagę, że z udostępnianiem danych osobowych będziemy mieli do czynienia wyłącznie wtedy, gdy odbiorcą danych jest inny administrator

[395] *W. Chomiczewski*, Komentarz do art. 4 pkt 2 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 196.
[396] *K. Witkowska-Nowakowska*, Komentarz d art. 4 pkt 9 [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 230.
[397] *Ibidem.*

danych, a więc podmiot decydujący o celach i środkach przetwarzania danych osobowych[398]. Należy podzielić pogląd, że z udostępnianiem danych osobowych mamy do czynienia wówczas, gdy następuje objęcie "danych w posiadanie" przez odbiorcę danych, który staje się wtedy administratorem danych osobowych[399]. Udostępnienie danych osobowych nastąpi zawsze wtedy, gdy administrator danych osobowych w sposób faktyczny przekaże bądź inaczej umożliwi zapoznanie się z takimi danymi innej osobie lub podmiotowi, który to podmiot pełnić będzie w stosunku do tych danych osobowych funkcję administratora danych. Samo "udostępnianie" danych ma przy tym charakter czynności faktycznej i może nastąpić w dowolny sposób – istotne jest tylko, żeby w wyniku tejże czynności odbiorca danych uzyskał faktyczny dostęp do danych i władztwo nad tymi danymi[400].

W drugim etapie może dojść do przetwarzania danych osobowych w ramach ponownego wykorzystywania informacji sektora publicznego przez użytkownika. Ponowne wykorzystywanie, jak zostało już udowodnione wcześniej, należy rozumieć jako każde użycie danych do dowolnego celu, które może między innymi polegać na przekształceniu informacji czy łączeniu informacji pochodzących z różnych źródeł w celu uzyskania pożądanego rezultatu, wzbogacaniu informacji o nowe treści. Każde zatem działanie na danych przez użytkownika może być uznane za jeden lub więcej sposobów przetwarzania wymieniony w art. 4 pkt 2 RODO. W ramach ponownego wykorzystywania może bowiem dojść do zbierania, utrwalania, organizowania, porządkowania, przechowywania, adaptowania lub modyfikowania, pobierania, przeglądania, wykorzystywania, ujawniania (poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie), dopasowywania lub łączenia, ograniczania, usuwania lub niszczenia. W mojej opinii jako przykład operowania na danych polegający na ich wykorzystywaniu, należy interpretować zgodnie z jego rozumieniem w języku naturalnym w oderwaniu od definicji legalnej ponownego wykorzystywania, choć niewątpliwie takie działanie w *per se* stanowić będzie zarówno jedną z form przetwarzania jak i ponownego wykorzystywania w rozumieniu przepisów UPW. W istocie, który z wymienionych sposobów przetwarzania będzie miał miejsce, nie ma znaczenia dla stosowania przepisów ogólnego rozporządzenia.

Przyjmując, że samo zapoznanie się z danymi osobowymi nie stanowi ich przetwarzania, jeżeli użytkownik po uzyskaniu danych osobowych w ramach informacji

[398] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 2, pkt.
[399] A. *Mednis*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 1999 r., s. 28.
[400] *P. Litwiński (red.)*, op. cit.

sektora publicznego, nie podejmie decyzji o ich ponownym wykorzystywaniu, pojawia się wątpliwość o skutek takiego biernego działania dla ochrony danych osobowych. Nabiera on praktycznego wymiaru w szczególności, gdy użytkownik w następstwie realizacji prawa do ponownego wykorzystywania jest posiadaniu danych osobowych (np. pobrał je z systemu teleinformatycznego podmiotu zobowiązanego albo otrzymał od podmiotu zobowiązanego zapisane na nośniku), z których nie czyni użytku. Racjonalnie rozumując, użytkownik podejmuje działania w celu otrzymania informacji sektora publicznego, aby uczynić z nich użytek. O ile w przypadku informacji sektora publicznego dostępnych w publiczne dostępnych źródłach (np. BIP czy centralne repozytorium) przed ich pobraniem użytkownik ma możliwość zapoznania się z treścią informacji, o tyle w przypadku uzyskania informacji na wniosek, dopiero po faktycznym otrzymaniu informacji może podjąć ostateczną decyzję o ich ponownym wykorzystywaniu lub zaniechaniu ponownego wykorzystywania (np. ze względu na zawartość merytoryczną, format danych). Sytuację tę – choć mamy do czynienia z intencją uzyskania danych - w organicznym zakresie można odnieść do tzw. biernego pozyskania danych. W przypadku biernych form zbierania danych podmiot pozyskujący informacje nie przejawia intencji pozyskania danych osobowych i prawdopodobnie nie będzie zainteresowany ich dalszym przetwarzaniem (np. pomimo braku prowadzenia naboru otrzyma z inicjatywy osoby ubiegającej się o zatrudnienie wiadomość e-mail zawierającą różne dane)[401]. W opinii *M. Sakowskiej-Baryły* samo uzyskiwanie takich informacji, pomimo braku woli podmiotu zbierającego dane, wymuszać jednak będzie odpowiednie stosowanie przynajmniej niektórych przepisów ogólnego rozporządzenia (np. dotyczących udokumentowania procesu przetwarzania, np. w zakresie usunięcia danych), nawet potencjalnie powodować odpowiedzialność za łamanie jego zasad po stronie zbierającego, zwłaszcza w sytuacji przetwarzania zautomatyzowanego[402].

W literaturze prezentowany jest również pogląd, że przy kwalifikowaniu danej czynności jako zbieranie danych, należy w pierwszej kolejności ustalić, w jakim celu osoba wchodzi w posiadanie danych osobowych. Zdaniem *P. Litwińskiego* „jeżeli celem tym jest wyłącznie zapoznanie się z informacjami, bez ich dalszego przetwarzania, wówczas nie można mówić o zbieraniu danych osobowych. Jeżeli natomiast odbywa się dalsze przetwarzanie zebranych informacji, wówczas przyjąć należy, że w istocie dochodzi do zbierania danych osobowych. Jeżeli natomiast dane nie zostały zebrane, nie można mówić o ich

[401] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 4 pkt 2, pkt 5.
[402] *Ibidem.*

przetwarzaniu”[403]. Z punktu widzenia pojęcia zbierania danych osobowych, a konsekwencji przetwarzania istotny jest więc także zamiar, z jakim osoba wchodzi w posiadanie danych osobowych. Celem wejścia w posiadanie informacji nie jest bowiem wyłącznie zapoznanie się z nimi, lecz poddanie ich dalszym operacjom przetwarzania[404].

W mojej opinii pobranie danych z systemu teleinformatycznego podmiotu zobowiązanego bez dokonywania dalszych operacji na danych należy co do skutku oceniać jak zapoznanie się z danymi osobowymi. O ile w potocznym rozumieniu tego słowa może dojść do „przeglądania”[405] danych osobowych, w istocie nie jest spełniona podstawowa przesłanka przetwarzania, czyli wykonania operacji lub zestawu operacji na danych, rozumianych jako czynności podjętej, aby wywołać określony efekt. Nie dochodzi do zautomatyzowanego przetwarzania danych, jak również do innego przetwarzania danych w zbiorze danych, a więc samo uzyskanie danych bez podejmowania przez użytkownika operacji na danych wykracza poza materialny zakres stosowania RODO. Z kolei w przypadku pozyskania danych osobowych na wniosek intencję ponownego użytkownika da się z góry odczytać. Cel i sposób ponownego wykorzystywania jest przez wnioskodawcę obligatoryjnie wskazany we wniosku, z tego powodu występuje przesłanka zamiaru dalszego przetwarzania danych osobowych.

3.3.4. Podmiot zobowiązany i użytkownik a administrator i odbiorca danych

Do krzyżowania się dwóch porządków regulacyjnych dochodzi również zakresie podmiotowym. Oczywistym jest, że krąg podmiotów zobowiązanych do udostępniania lub przekazywania informacji sektora publicznego w celu ponownego wykorzystywania jest węższy od zakresu podmiotowego pojęcia administratora na gruncie RODO. Przypomnijmy, że zgodnie z art. 4 pkt 7 RODO administratorem może być zarówno osoba fizyczna, osoba prawna lub inny podmiot zarówno z sektora prywatnego, jak i publicznego oraz organ publiczny. Podmiot zobowiązany, o którym mowa w art. 2 UPW, na gruncie przepisów RODO spełnia przesłanki podmiotowe administratora danych[406], o którym mowa w art. 4 pkt 7 RODO. Podmiot zobowiązany może być zarazem – co do zasady – organem publicznym albo względnie

[403] *P. Litwiński (red.)*, op. cit., pkt 5.
[404] *Ibidem.*
[405] W doktrynie stawia się zarzut nieścisłego tłumaczenia i postuluje się odejście od rozumienia operacji przeglądania jako zapoznawania się z treścią danych jedna po drugiej na rzecz przyjęcia, że przeglądanie to wyszukiwanie danych poprzez wpisanie odpowiednich haseł, które dzięki zastosowanemu mechanizmowi indeksującemu pozwalają na zapoznanie się z konkretnymi danymi (zob. szerzej *W. Chomiczewski*, w: E. *Bielak-Jooma, D. Lubasz*, Ogólne rozporządzenie o ochronie danych., 2018, s. 195.
[406] Podobne stanowisko na gruncie UDIP i UODO1997 prezentuje *M. Sakowska – Baryła*, Dostęp do informacji publicznej a ochrona danych osobowych, s. 109 i nast.

osobą prawną (np. państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych) albo „jednostką" (np. jednostka budżetowa). Dla nadania podmiotowi zobowiązanemu takiej roli obojętne będzie czy wskazano dany organ publiczny (podmiot lub jednostkę) jako administratora w przepisach prawa. Sytuacje wyraźnego wskazania we właściwych przepisach podmiotu pełniącego funkcję administratora danych osobowych należą jednak do rzadkości. Brak takich przepisów powoduje, że status administratora danych osobowych w sferze publicznej należy oceniać w świetle przedmiotowej dyspozycji art. 4 pkt 7 RODO[407]. Jednak w przypadku administratorów danych ze sfery prawa publicznego inaczej interpretuje się przesłankę decydowania o celach i sposobach przetwarzania danych osobowych. Swoboda przysługująca tym podmiotom w zakresie celów przetwarzania danych osobowych jest bowiem wyznaczana przez właściwe przepisy prawa określające realizowane przez nie zadania[408]. W przypadku podmiotów publicznych w praktyce może pojawić się wątpliwość polegająca na tym, czy cele i sposoby przetwarzania zostały ustalone przez prawodawcę. W literaturze prezentowany jest pogląd, zgodnie z którym w administracji publicznej cel przetwarzania danych będzie mniej lub bardziej ogólnie wyznaczony przepisami prawa, a określony ich administrator będzie, decydując o celu przetwarzania danych, będzie jedynie konkretyzował jego zakres, aby odpowiadał on bardziej szczegółowo określonym zadaniom publicznym[409]. W tym wypadku o kwalifikacji danego podmiotu jako administratora danych decyduje rodzaj i charakter nadanych mu przez prawo kompetencji z obszaru spraw publicznych oraz wyznaczone ustawowo zadania.

Przypisanie danemu podmiotowi zobowiązanemu roli administratora odbywa się w oderwaniu od przepisów o ponownym wykorzystywaniu, innymi słowy to przepisy o ochronie danych osobowych (potencjalnie w powiązaniu z innymi przepisami szczególnymi) mają decydujące znaczenie dla takiej kwalifikacji, a nie fakt, że podmiot zobowiązany przetwarza w ramach realizacji prawa do ponownego wykorzystywania dane osobowe.

Z kwalifikacji podmiotu zobowiązanego jako administratora wynikają określone na gruncie RODO konsekwencje. Spoczywają na nim obowiązki w zakresie odpowiedniego zabezpieczenia danych oraz przestrzegania tych przepisów RODO oraz innych przepisów z zakresu ochrony danych osobowych, które odnoszą się do organizacyjnej strony

[407] *P. Litwiński (red.)*, op cit., Komentarz do art. 4 pkt 7, pkt 16.
[408] *Ibidem.*
[409] *R. Hauser*, Przetwarzanie danych osobowych: cel i środki, „Rzeczpospolita", 6.04.1999 r. za: *P. Fajgielski*, Komentarz, 2018, s. 123.

przetwarzania danych[410]. W kontekście dystrybucji danych do ponownego wykorzystywania istotne jest wdrażanie odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać (art. 24 ust. 1 RODO), w tym wdraża następujące środki bezpieczeństwa odpowiednie do ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, tj. pseudonimizację i szyfrowanie danych osobowych; zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania; zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego; regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania (art. 32 RODO). Ponadto administrator musi uwzględnić ochronę danych w fazie projektowania oraz domyślna ochrona danych (art. 25 RODO). Wśród pozostałych istotnych obowiązków podmiotu zobowiązanego jako administratora danych trzeba wymienić realizację uprawnień osób, których dane dotyczą (zgodnie z rozdziałem III RODO); powołanie inspektora ochrony danych (art. 37 ust. 1 lit. a RODO) oraz szacowanie ryzyka naruszeń praw lub wolności osoby fizycznej lub ocena skutków dla ochrony danych osobowych (art. 24, art. 32, art. 35 RODO).

Problemy z jednoznacznym określeniem roli na gruncie przepisów RODO mogą pojawić się w odniesieniu do użytkownika w rozumieniu art. 2 UPW. W zależności od okoliczności użytkownik ponownie wykorzystujący (przetwarzający) dane osobowe stanowiące informacje sektora publicznego lub w nich zawarte może spełniać przesłanki zarówno administratora, jak i użytkownika. Określenie statusu użytkownika w reżimie przepisów o ochronie danych nie ma wymiaru teoretycznego, chodzi bowiem o to, żeby określić na kim ciążą obowiązki wynikające z faktu przetwarzania danych osobowych i kto odpowiada w związku z tym za to przetwarzanie.[411]

Upraszczając można przyjąć, że od strony podmiotowej pojęcie użytkownika (osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej) wchodzi w zakres pojęcia administratora (osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot), odbiorcy (osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot) oraz strony trzeciej (osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby,

[410] *B. Fischer, A. Piskorz-Ryń, M. Sakowska-Baryła, J. Wyporska-Frankiewicz*, Komentarz do art. 7, Pkt.2.4.5. [w:] Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, Lex/Wyd. 2019.
[411] Por. *M. Sakowska-Baryła*, Komentarz do art. 4 pkt 7, pkt 3 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie, Legalis/Wyd. 2018.

które z upoważnienia administratora lub podmiotu przetwarzającego mogą przetwarzać dane osobowe). Zatem za decydujące kryterium pozwalające na właściwą klasyfikację użytkownika na gruncie RODO stanowić będzie element przedmiotowy.

Niewątpliwie użytkownik posiadać będzie status odbiorcy, bowiem decydującym kryterium dla zakwalifikowania danego podmiotu jako odbiorcy jest to, by dane osobowe zostały mu ujawnione. Z kolei ujawnienie danych osobowych jest warunkiem koniecznym dla dalszego ich przetwarzania w ramach realizacji prawa do ponownego wykorzystywania przez użytkownika. Jeśli dane osobowe nie zostaną przekazane lub udostępnione w ramach informacji sektora publicznego lub zostanie przekazana informacja zanonimizowana nie można zatem mówić o ujawnieniu ich użytkownikowi w celu ponownego wykorzystywania, a zatem użytkownik informacji nie może zostać zakwalifikowany jako odbiorca danych.

Zakwalifikowanie użytkownika jako odbiorcę danych nie oznacza automatycznie, że będzie on objęty zakresem stosowania przepisów RODO. Podzielam pogląd *P. Litwińskiego*, zdaniem którego ujawnienie danych osobowych, o którym mowa w art. 4 pkt 9 RODO, ma szersze znaczenie niż zakres przedmiotowy zastosowania samego ogólnego rozporządzenia. W praktyce bowiem ujawnienie danych osobowych rozumiane jako umożliwienie zapoznania się z treścią danych osobowych może nie prowadzić do tego, że – zgodnie z art. 2 RODO – podmiot, któremu ujawniono dane, będzie w zakresie przetwarzania tych danych podlegał przepisom RODO. Nie można też wykluczyć sytuacji, w której jedyną operacją wykonywaną na danych osobowych będzie zapoznanie się z tymi danymi, a do dalszego przetwarzania danych w ogóle nie dojdzie. Nie zmienia to jednak kwalifikacji takiego podmiotu jako odbiorcy danych[412].

Jak wykazano administrator danych osobowych powinien samodzielnie decydować o tym, dla realizacji jakich celów dochodzić będzie do przetwarzania danych osobowych oraz w jaki sposób to przetwarzanie będzie następowało. Te cechy pozwalają na odróżnienie administratora danych osobowych od podmiotu przetwarzającego, który nie decyduje o celach przetwarzania danych osobowych, będąc uprawnionym do przetwarzania danych wyłącznie w celu ustalonym przez administratora danych[413]. Kwalifikacji danego podmiotu jako administratora dokonywać należy na podstawie ustaleń faktycznych, a więc całokształtu okoliczności przetwarzania danych osobowych w danym przypadku, stąd też należy brać pod

[412] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4 pkt 9, pkt 3. Do podobnych wniosków powołując się na błędy w tłumaczeniu polskiego tekstu RODO dochodzi *K. Witkowska-Nowakowska*, Komentarz do art. 4 pkt 9 [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 230 i nast.
[413] *P. Litwiński (red.)*, op. cit., pkt 9.

uwagę, kto faktycznie decyduje o tym, po co przetwarza się dane osobowe, do czego są one potrzebne, kto przesądza o sposobie wykorzystywania danych, ich treści i zakresie, o formie ich pozyskiwania, o ich przechowywaniu, ujawnianiu oraz o środkach technicznych i organizacyjnych, przy użyciu których odbywa się przetwarzanie. Pełnienie funkcji administratora można zatem uznać jako stan faktyczny, z którym związane są konsekwencje na gruncie prawa ochrony danych osobowych, do których w pierwszym rzędzie należy szereg obowiązków co do sposobu zorganizowania procesu przetwarzania danych i ich zabezpieczenia, realizacji praw osób, których dane dotyczą i odpowiedzialności za naruszenia w tym zakresie[414].

Za administratora należy uznać tego użytkownika, który przetwarza dane osobowe pozyskane w ramach realizacji ponownego wykorzystywania informacji sektora publicznego w celu osiągnięcia określonego rezultatu, np. produktu, usługi czy aplikacji, kiedy samodzielnie decyduje o celach i sposobach przetwarzania danych. O ile, faktycznie co do zasady użytkownik autonomicznie określa sposoby przetwarzania danych (ponownego wykorzystywania informacji), o tyle w przypadku celów sytuację tę należy niuansować. Co do zasady bowiem wnioskodawca (użytkownik) określa samodzielnie we wniosku cel ponownego wykorzystywania, o tyle podmiot zobowiązany może określić warunki ponownego wykorzystywania dla danych osobowych (zob. Rozdział 9). Dopuszczalna jest zatem okoliczność, że to podmiot zobowiązany determinował będzie możliwe cele przetwarzania danych osobowych przez użytkownika, np. z góry określając możliwe cele przetwarzania danych w warunkach ponownego wykorzystywania. Wówczas pojawia się pytanie czy zostanie spełniony warunek umożlwiający nadanie użytkownikowi statusu administratora (prawodawca unijny w definicji administratora poprzez spójnik „i" posłużył się koniunkcją, przez co zdanie nie będzie prawdziwe, ponieważ pierwszy czynnik – „samodzielnie ustala cele" nie jest prawdziwy, jedynie drugi czynnik zdania – „samodzielnie ustala sposób" pozostanie prawdziwy).

Decydowanie o celach i sposobach przetwarzania danych sprowadzić należy do faktycznego podejmowania decyzji w odniesieniu do przetwarzanych danych osobowych oraz samodzielności w podejmowaniu tych decyzji[415]. Administratorem będzie podmiot praw i obowiązków, który dokonując działań, rozporządzając prawami i zaciągając zobowiązania, rozstrzyga o procesach przetwarzania danych[416]. Kwalifikacji należy dokonywać w sposób

[414] *M. Sakowska-Baryła*, op. cit.
[415] *Ibidem*, pkt. 12.
[416] *G. Sibiga*, Postępowanie, s. 53

funkcjonalny tak, aby przypisywanie obowiązków i odpowiedzialności następowało tam, gdzie istnieje faktyczny, a nie jedynie formalny wpływ na ustalanie celów i sposobów przetwarzania[417]. Kluczowe jest, aby administrator podejmował decyzje o zasadniczym znaczeniu dla danego przetwarzania[418].

Ustalenie właściwego statusu danego podmiotu w reżimie ochrony danych osobowych w praktyce może okazać się trudne do wykonania. Jako przykład można podać przełomowy wyrok TS w tzw. sprawie *Google Spain*[419] w którym za administratora danych osobowych uznany został operator wyszukiwarki internetowej w stosunku do informacji zawierającej dane osobowe, przez niego przetwarzanych, lokalizowanych i indeksowanych w sposób automatyczny, czasowo przechowywyanych i udostępnianych użytkownikom Internetu w sposób uporządkowany, zgodnie z określonymi prewencjami. Trybunał uznał operatora wyszukiwarki za administratora, choć ten w istocie pośredniczy w udostępnianiu informacji pochodzących od podmiotów trzecich.

W mojej opinii nie można jednoznacznie przypisać roli administratora *in abstracto* każdemu użytkownikowi ponownie wykorzystującemu dane osobowe. Kwalifikację użytkownika należy dokonywać w konkretnych okolicznościach, a w szczególności w kontekście faktycznego podejmowania decyzji w sprawie określenia celów przetwarzania danych osobowych. W zależności od okoliczności użytkownikowi można przypisać atrybuty administratora, jak i innego obiorcy danych.

Rozdział 4. Zasady i tryby ponownego wykorzystywania informacji sektora publicznego

Dyrektywa 2003/98/WE w jej pierwotnym brzmieniu ustanawiała jedynie minimalny zestaw reguł określających ponowne wykorzystanie informacji sektora publicznego. Dyrektywa ta nie przewidywała obowiązku dotyczącego dostępu do dokumentów ani obowiązku zezwalania na ponowne ich wykorzystanie. Decyzję w sprawie zezwolenia na ponowne wykorzystywanie pozostawiono w gestii państw członkowskich lub organów sektora publicznego. Podkreślenia wymaga, że w ramach wdrożenia dyrektywy do krajowego porządku prawnego polski prawodawca ustanowił dodatkowe, nie przewidziane w instrumencie

[417] Zob. Grupa Robocza Art. 29, Opinia 1/2010 z 16.02.2010 r. w sprawie pojęć „administrator danych" i „przetwarzający" (WP 169), s. 10.
[418] *K. Witkowska – Nowakowska*, Komentarz do art. 4 pkt 7 [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 217.
[419] Wyrok z 13.05.2014 r., C-131/12, Google Spain SL i Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD) i Mariowi Costesze Gonzálezowi.

prawnym UE rozwiązanie dotyczące wprowadzenia obowiązku przekazywania przez podmioty zobowiązane informacji publicznych do ponownego wykorzystywania oraz związanego z tym powszechnego prawa jednostki do ponownego wykorzystywania. Ustawa o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw z dnia 16 września 2011 r.[420] implementująca dyrektywę 2003/98/WE, nadała art. 1 UDIP następujące brzmienie: „Każda informacja o sprawach publicznych stanowi informację publiczną w rozumieniu ustawy i podlega udostępnieniu i ponownemu wykorzystywaniu na zasadach i w trybie określonych w niniejszej ustawie." Dodano również art. 2a o treści: „Każdemu przysługuje, z zastrzeżeniem art. 5, prawo do ponownego wykorzystywania informacji publicznej."

Rozwiązanie to było wówczas unikalne wśród państw członkowskich UE. Ze względu na proponowany powszechny charakter prawa do ponownego wykorzystania informacji publicznej każdemu podmiotowi (zatem nie tylko z siedzibą w państwie Europejskiego Obszarze Gospodarczego) przyznano uprawnienie, co do zasady, bezpłatnego, komercyjnego wykorzystywania informacji posiadanych przez podmioty polskiego sektora publicznego (z zachowaniem ograniczeń wynikających z przepisów ustawy). Z kolei znacząca część państw unijnych przyjęła wówczas model opłat za ponowne wykorzystywanie informacji uwzględniający tzw. rozsądny zwrot z inwestycji (np. Litwa, Wielka Brytania, Niemcy, Grecja, Irlandia)[421].

Dzisiaj z perspektywy 10 lat obowiązywania krajowych przepisów o ponownym wykorzystywaniu należy uznać, że już od pierwszego wdrożenia polski ustawodawca przyjął ambitniejszy model transpozycji niż był wymagany przepisami prawa UE, który niejako antycypował przyszłe rozwiązania przyjęte przez unijnego prawodawcę w dyrektywie 2013/37/UE. Dopiero w 2013 r. prawodawca UE nałożył na państwa członkowskie wyraźny obowiązek zapewnienia możliwości ponownego wykorzystywania wszystkich dokumentów, z wyjątkiem dokumentów, do których dostęp jest ograniczony lub wyłączony na mocy prawa krajowego dotyczącego dostępu do dokumentów (art. 1 pkt 3 dyrektywy 2013/37/UE oraz motyw 8 preambuły). Zasada ta została następnie zachowana w dyrektywie 2019/1024.

Korelatem tego obowiązku jest prawo każdego zainteresowanego do ponownego wykorzystywania informacji sektora publicznego. Wszystkie pozostałe zasady ogólne ponownego wykorzystywania oraz szczegółowe obowiązki podmiotu zobowiązanego wynikają właśnie z tego podstawowego uprawnienia do ponownego wykorzystywania.

[420] Dz.U. Nr 204, poz. 1195.
[421] Zob. *G. Sibiga*, Opinia prawna o projekcie ustawy o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw, s.13.

4.1. Prawo do ponownego wykorzystywania jako publiczne prawo podmiotowe

Publiczne prawo podmiotowe do ponownego wykorzystywania zostało sformułowane wprost w art. 5 UPW stanowiącym o tym, że każdemu przysługuje prawo do ponownego wykorzystywania informacji sektora publicznego:

1) udostępnionych w systemie teleinformatycznym, a w szczególności na stronie podmiotowej Biuletynu Informacji Publicznej podmiotu zobowiązanego lub w centralnym repozytorium informacji publicznej lub w inny sposób;

2) przekazanych na wniosek o ponowne wykorzystywanie.

Konstrukcja przepisu wyraźnie wskazuje, że zostało w nim przyznane prawo podmiotowe (uprawnienie do ponownego wykorzystywania informacji sektora publicznego), a w konsekwencji na drugi podmiot został nałożony obowiązek prawny, o określonej treści (udostępnienie lub przekazanie informacji sektora publicznego do ponownego wykorzystywania). Konstrukcję prawa podmiotowego można ponadto wywieźć z art. 3 oraz art. 23 ust. 1 w zakresie w jakim zawiera dyspozycję zaadresowaną do podmiotu zobowiązanego polegającą na obowiązku przekazania (udostępnienia) informacji sektora publicznego. Skoro ustawa nakładana określony podmiot obowiązek, to drugiej zaś stronie *a contrario* będą przysługiwać prawa analogiczne do treści obowiązku[422].

Brzmienie przepisu przypomina sformułowane w art. 2 UDIP, na mocy którego każdemu przysługuje, z zastrzeżeniem art. 5, prawo dostępu do informacji publicznej, zwane dalej „prawem do informacji publicznej". Zasadnicza różnica polega oczywiście na innym zakresie przedmiotowym uprawnienia, które w pierwszym wypadku obejmuje uzyskanie informacji publicznej, w drugim zaś uzyskanie informacji sektora publicznego w celu ponownego jej wykorzystywania.

W mojej opinii obowiązującym stanie prawnym nie budzi wątpliwości, że jednostka dysponuje dwoma rozdzielnymi prawami podmiotowymi o informacyjnym charakterze, tj. prawem dostępu do informacji publicznej oraz prawem do ponownego wykorzystywania informacji sektora publicznego. Przedmiotem uprawnienia wyrażonego w art. 5 UPW pozostaje możliwość ponownego wykorzystywania informacji sektora publicznego, której realizacja, z natury rzeczy, uzależniona jest od dostępności informacji. Z dalszych przepisów UPW wynika wprost, że treścią uprawnienia może być samo umożliwienie użytkownikowi (poprzez np. poinformowanie o braku warunków) ponownego wykorzystywania posiadanych przez

[422] Zob. *M. Maciejewski*, Prawna regulacja ponownego wykorzystywania informacji publicznej [w:] *G. Sibiga (red.)*, Główne problemy, s. 269.

niego informacji sektora publicznego bez konieczności ich przekazywania lub udostępniania[423]. W mojej opinii *de lega lata* w odniesieniu do ponownego wykorzystywania można mówić o jednym uprawnieniu eksploatacyjnym przysługującym użytkownikowi, tj. prawie do ponownego wykorzystywania, którego korelatem po stronie podmiotu zobowiązanego jest umożliwienie realizacji tego prawa poprzez udostępnienie lub przekazanie informacji sektora publicznego w celu ponownego wykorzystywania lub poinformowanie użytkownika o możliwości ponownego wykorzystywania bez warunków lub zgodnie z warunkami przez podmiot określonymi. Konkludując, użytkownikowi przysługuje publiczne prawo podmiotowe do ponownego wykorzystywania, któremu odpowiada obowiązek podmiotu zobowiązanego do przekazania (udostępnienia) informacji sektora publicznego albo spełnienie obowiązku informacyjnego (powiadomienie w kwestii warunków ponownego wykorzystywania).

W art. 5 UPW określono jednocześnie sposób realizacji przedmiotowego uprawnienia, które wyznacza dychotomiczny podział na dwa tryby ponownego wykorzystywania, tj. tryb bezwnioskowy oznaczający prawo do ponownego wykorzystywania informacji sektora publicznego udostępnionych w systemie teleinformatycznym podmiotu zobowiązanego, a w szczególności jako system predefiniowany wskazano BIP oraz centralne repozytorium informacji publicznej, jak i w inny sposób oraz tryb wnioskowy. W pierwszym wypadku mamy zatem do czynienia z dostępnością informacji, która może być ponownie wykorzystywana przez każdego bez konieczności – co do zasady – wystąpienia z wnioskiem, przy czym dostępność informacji zapewniona jest przez podmiot zobowiązany wykonujący obowiązki publikacyjne z mocy przepisów prawa (w szczególności w BIP, centralnym repozytorium czy w innym systemie teleinformatycznym przez siebie prowadzonym, np. rejestrze państwowym) lub z własnej inicjatywy, ale zgodnie z zasadą legalizmu, tj. na podstawie prawa (np. publikacja tzw. rejestrów umów przez podmiot zobowiązany na stronie internetowej urzędu). W drugim wypadku, informacja nie jest dostępna, jej przekazanie zostaje zainicjowane przez zainteresowanego użytkownika poprzez złożenie wniosku, którego adresatem jest podmiot zobowiązany będący w posiadaniu żądanej informacji sektora publicznego.

[423] Zdaniem *M. Maciejewskiego* na gruncie Rozdziału 2a UDIP sprzed uchwalenia UPW można było mówić w tym wypadku o odrębnym „samoistnym prawie podmiotowym – prawie do ponownego wykorzystywania *sensu stricto"*, które należy odróżnić od użytkowego prawa dostępu. Zdaniem autora – bazując na koncepcji odrębności praw *M. Jaśkowskiej* (zob. *M. Jaśkowska*, Jakość i spójność rozwiązań prawnych w świetle nowelizacji ustawy o dostępie do informacji publicznej, s.387) – można zatem mówić o koncepcji potrójnej odrębności prawa dostępu do informacji publicznej, prawa dostępu do informacji publicznej w celu jej ponownego wykorzystywania i prawa do ponownego wykorzystywania (zob. *M. Maciejewski*, Prawna regulacja ponownego wykorzystywania informacji publicznej [w:] *G. Sibiga*, Główne problemy, s. 273).

4.2. Tryby ponownego wykorzystywania informacji sektora publicznego

Dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego zawierają jedynie szczątkowe regulacje dotyczące procedury przekazywana dokumentów do ponownego wykorzystywania. Przepisy te w dyrektywie 2019/1024 zostały ujęte w Rozdziale III „Wnioski o ponowne wykorzystywanie", które stanowią odzwierciedlenie przepisów dyrektywy 2003/98/WE ujętych w Rozdziale II o tym samym tytule, dlatego w dalszej części Rozdziału posłużono się numeracją jednostek redakcyjnych z dyrektywy 2019/1024.

Zgodnie z art. 4 dyrektywy 2019/1024 organy sektora publicznego przetwarzają, w miarę możliwości i stosownie do przypadku przy wykorzystaniu środków elektronicznych, wnioski o ponowne wykorzystywanie i udostępniają wnioskodawcy dokumenty do ponownego wykorzystywania lub, jeżeli potrzebna jest licencja, przedstawiają wnioskodawcy końcową ofertę licencji w rozsądnym terminie zgodnym z terminami określonymi dla przetwarzania wniosków o dostęp do dokumentów (ust. 1).

Jeżeli nie określono takich terminów ani nie ustanowiono innych przepisów regulujących terminowe udostępnianie dokumentów, organy sektora publicznego rozpatrują wnioski i dostarczają wnioskodawcy dokumenty do ponownego wykorzystywania lub, jeżeli potrzebna jest licencja, przedstawiają wnioskodawcy końcową ofertę licencji możliwie jak najszybciej, a w każdym przypadku w ciągu 20 dni roboczych od otrzymania wniosku. W przypadku obszernych lub złożonych wniosków termin ten może być przedłużony o kolejne 20 dni roboczych. W takich przypadkach możliwie jak najszybciej, a w każdym razie w ciągu trzech tygodni od daty pierwotnego wniosku zawiadamia się wnioskodawcę, że przetwarzanie jego wniosku wymaga więcej czasu, wskazując przyczyny (ust. 2).

W przypadku decyzji odmownej organy sektora publicznego informują wnioskodawcę o powodach odmowy opartych na odpowiednich przepisach systemu dostępu danego państwa członkowskiego lub przepisach transponujących niniejszą dyrektywę, w szczególności art. 1 ust. 2 lit. a)–h) lub art. 3. Jeżeli decyzja odmowna jest oparta na art. 1 ust. 2 lit. c), organ sektora publicznego zamieszcza odniesienie do osoby fizycznej lub prawnej, do której należą prawa własności intelektualnej (jeżeli jest znana), lub do licencjodawcy, od którego organ sektora publicznego uzyskał dany materiał. Do zamieszczenia takiego odniesienia nie są zobowiązane biblioteki, w tym biblioteki uniwersyteckie, muzea ani archiwa (ust. 3).

Decyzja dotycząca ponownego wykorzystywania zawiera informację o środkach odwoławczych przysługujących wnioskodawcy w odniesieniu do tej decyzji. Środki odwoławcze obejmują możliwość kontroli przez bezstronny organ odwoławczy posiadający

odpowiednią wiedzę specjalistyczną – taki jak krajowy organ ochrony konkurencji, odpowiedni organ regulujący dostęp do dokumentów, organ nadzorczy ustanowiony zgodnie z RODO lub krajowy organ sądowy – którego decyzje są wiążące dla danego organu sektora publicznego (ust. 4).

Podstawowa odrębność między przepisami obu dyrektyw polega na tym, że w dyrektywie 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE, zmodyfikowano przepis dotyczący organu rozpatrującego środek odwoławczy[424].

Należy również podkreślić, że o ile przepisy dyrektywy 2019/1024 akcentują konieczność proaktywnego podejścia mającego na celu zautomatyzowane upublicznianie danych, w tym danych dynamicznych czy danych o wysokiej wartości za pośrednictwem systemów teleinformatycznych poprzez interfejsy programowania aplikacji umożliwiające wzajemne komunikowanie się w relacji urządzenie-urządzenie (zob. motywy 31, 32, 60 preambuły dyrektywy), to proceduralnie *expressis verbis* nie rozróżniają trybów ponownego wykorzystywania na wnioskowy i bezwnioskowy. Dychotomiczny podział na dwa źródła dystrybucji informacji sektora publicznego do ponownego wykorzystywania wynika z krajowego modelu wdrożenia dyrektyw do polskiego porządku prawnego. Przeprowadzona w dalszej części analiza trybów ponownego wykorzystywania informacji sektora publicznego opierać się zatem będzie na przepisach UPW. Cechą wspólną obu trybów jest połączenie przez ustawodawcę elementów adminstracyjno- i cywilnoprawnych.

4.3.1. Bezwnioskowe tryby ponownego wykorzystywania

Istotnym elementem polityki otwierania danych publicznych są systemy teleinformatyczne służące do dystrybucji danych. Obecnie w Polsce funkcjonują dwa systemy elektronicznego bezwnioskowego udostępniania informacji, tj. BIP oraz centralne repozytorium informacji publicznej[425], realizujące funkcję krajowego portalu otwartych danych[426]. BIP i CRIP mają zbieżne cele, a więc zapewniają dystrybucję informacji wytwarzanych i gromadzonych przez administrację publiczną. Podczas gdy BIP pełnią funkcję

[424] Art. 3 ust. 4 dyrektywy stanowi, że każda decyzja dotycząca ponownego wykorzystywania zawiera odniesienie do środków odwoławczych na wypadek gdyby wnioskodawca chciał odwołać się od decyzji. Środki odwoławcze obejmują możliwość przeglądu przez bezstronny organ odwoławczy posiadający odpowiednią wiedzę specjalistyczną, taki jak krajowy organ ochrony konkurencji, krajowy organ regulujący dostęp do dokumentów lub krajowy organ sądowy, którego decyzje są wiążące dla danego organu sektora publicznego.

[425] Pojęcie centralnego repozytorium informacji publicznej ma charakter legalny, zaś jego zadania i funkcje realizuje rządowy portal otwartych danych prowadzony na stronie dane.gov.pl.

[426] Na temat portal zob. *A. Gos,* Serwis danepubliczne.gov.pl, „Informacja w Administracji Publicznej" 2017, nr 3, s. 44 i nast.

informacyjną, portal zapewnia dostęp do danych o dużym potencjale do dalszego ich innowacyjnego wykorzystywania. Z tego powodu sposób prezentacji treści, jak i funkcjonalności systemów znacząco się różnią[427].

Kluczowy dla ponownego wykorzystywania danych udostępnionych za pośrednictwem CRIP i BIP ma art. 21 ust. 1 pkt 1 UPW. Przepis ten wprowadza tzw. negatywną klauzulę wnioskowego trybu przekazywania informacji do ponownego wykorzystywania, oznaczającą, że z jednej strony adresat wniosku (podmiot zobowiązany) zwolniony jest z obowiązku przekazywania informacji, jeżeli została udostępniona w BIP lub CRIP, z drugiej zaś strony każdy zainteresowany może wykorzystywać tak udostępnione informacje do dowolnych celów komercyjnych lub niekomercyjnych, zgodnie z warunkami, o ile je określono. Złożenie wniosku będzie jedynie konieczne w sytuacji, w której użytkownik będzie chciał wykorzystywać informację w inny sposób niż to określono w warunkach ponownego wykorzystywania (art. 21 ust. 1 pkt 3 UPW).

Symetryczna negatywna klauzula wnioskowego trybu przekazywania informacji występuje również na gruncie UDIP. Zgodnie z art. 10 ust. 1 informacja publiczna, która nie została udostępniona w BIP lub centralnym repozytorium, jest udostępniana na wniosek o dostęp do informacji. Tym samym informacja, która została udostępniona w BIP lub CRIP przez organ administracji publicznej nie podlega udostępnieniu w trybie wnioskowym[428].

W przypadku informacji udostępnionej w BIP lub CRIP organ administracji nie ma obowiązku dokonywania wydruków z BIP lub CRIP i przesyłania ich żądającemu. Udostępnienie wnioskowanej informacji w CRIP zwalnia zatem od powtórnego jej wydania, jednak nie zwalnia również od udzielenia wnioskodawcy jakiejkolwiek odpowiedzi. Jeżeli podmiot będący adresatem wniosku uznał, że zakres żądania wyrażony we wniosku i zakres informacji znajdujący się w CRIP uprawnia do twierdzenia, iż są one identyczne, powinien powiadomić wnioskodawcę, że żądana informacja znajduje się w CRIP.

4.3.1.1. Biuletyn Informacji Publicznej

BIP to urzędowy publikator teleinformatyczny (art. 8 ustawy UDIP) będący systemem stron internetowych służący powszechnemu, ciągłemu i bezpłatnemu dostępowi do informacji publicznej. Dostęp do informacji zawartych w biuletynie jest możliwy poprzez: stronę główną

[427] Zob. *D. Sybilski*, Ewolucja realizacji prawa dostępu do informacji publicznej - od Biuletynów Informacji Publicznej po portale otwartych danych [w:] *W. Federczyk* (red), Stulecie polskiej administracji. Doświadczenia i perspektywy, Warszawa 2018, s. 202 i nast.
[428] *I. Kamińska, M. Rozbicka-Ostrowska*, Ustawa o dostępie, s. 231.

BIP[429], zawierającą podstawowe informacje o podmiotach (nazwa, dane teleadresowe, informacje o redaktorze strony) oraz strony podmiotowe, przygotowane przez podmioty ustawowo zobowiązane do ich prowadzenia. Podmiotami obowiązanymi do prowadzenia stron podmiotowych BIP są władze publiczne oraz inne podmioty wykonujące zadania publiczne, a w szczególności te wymienione w art. 8 ust. 2 w zw. z art. 4 ust. 1 i 2 UDIP.

Zakres informacji publikowanej w BIP określa otwarty katalog wymieniony w art. 8 ust. 1 UDIP. Szereg informacji publicznych podlegających obowiązkowej publikacji określają ponadto przepisy szczególne. Uogólniając można uznać, że w BIP podlegają przede wszystkim informacje podstawowe o podmiocie, wykonywanych przez niego zadaniach publicznych i gospodarowaniem mieniem publicznym. Podmioty zobowiązane z własnej inicjatywy mogą udostępniać na BIP również inne informacje spoza ustawowego katalogu (art. 8 ust. 3 zd. drugie UDIP). Można zatem powiedzieć, że BIP jest systemem otwartym[430].

Szczegółowe wymagania dotyczące układu ujednoliconego systemu stron BIP, jego struktury, zakresu i trybu przekazywania ministrowi właściwemu do spraw informatyzacji informacji do zamieszczenia na stronie głównej BIP oraz wymagania dotyczące zabezpieczania treści informacji udostępnianych w BIP określa rozporządzenie ministra spraw wewnętrznych i administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej[431].

Ustawodawca określił zatem minimalny standard merytoryczny BIP, a jego prowadzenie nie jest kwestią swobodnego uznania, lecz jest obowiązkiem prawnym. Wynika to wprost z art. 8 ust. 3 zd. pierwsze UDIP, ale przepis ten nie daje wskazówki co do stopnia szczegółowości lub sposobu zaszeregowania poszczególnych informacji publicznych[432].

Z punktu widzenia realizacji prawa do ponownego wykorzystywania informacji sektora publicznego istotne jest, że BIP jest uznawany za podstawowy, bezwnioskowy tryb ponownego wykorzystywania informacji publicznych, wyłączający konieczność udostępniania informacji w nim zawartych w trybie wnioskowym.

4.3.1.2. Centralne repozytorium informacji publicznej

Jak wskazano w Rozdziale 1 z punktu widzenia tworzenia dóbr i usług wykorzystujących dane, w tym informacje sektora publicznego kluczowe jest zapewnienie

[429] www.bip.gov.pl
[430] Zob. *M. Bernaczyk*, Obowiązek bezwnioskowego udostępniania informacji publicznej, Warszawa 2008, s. 133.
[431] Dz. U. 2007 r. poz. 68.
[432] *M. Bernaczyk, M. Jabłoński*, Praktyczne problemy wdrażania ustawy o dostępie do informacji publicznej, „Elektroniczna Administracja" 2006, nr 6 (7), s. 7.

stałego dostępu do danych przetwarzalnych maszynowo bez konieczności występowania z wnioskiem do podmiotu zobowiązanego. Cel ten jest realizowany przez portale otwartych danych, którego funkcje w Polsce spełnia centralne repozytorium informacji publicznej (czyli serwis dane.gov.pl). Zagadnienie to wymaga szerszego omówienia.

Ideą przyświecającą pomysłodawcom CRIP było stworzenie systemu teleinformatycznego będącego głównym punktem dostępu do jak największej ilości danych wytwarzanych i gromadzonych przez podmioty sektora publicznego, które mają potencjał dla ich dalszego wykorzystywania[433]. Dla rozwoju rynku ponownego wykorzystywania danych publicznych kluczowe jest, aby dostęp do danych był bezpłatny, bez konieczności składania wniosku i bez nadmiernych warunków ograniczających możliwość ich wykorzystywania.

Postulat uruchomienia CRIP był odpowiedzią na działania podejmowane w innych krajach czy to na szczeblu państwowym czy lokalnym polegających na tworzeniu portali otwartych danych. Wzorem był uruchomiony w maju 2009 r. portal brytyjski data.gov.uk czy pół roku później amerykański data.gov. Co istotne, poza aspektem gospodarczego wykorzystywania danych inicjatywy budowy publicznych portali otwartych danych wpisywały się w idee otwartego rządu.

Obecnie, przynajmniej na poziomie europejskim, prowadzenie rządy państw członkowskich UE portali otwartych danych stało się standardem. Obok portali krajowych prowadzone są serwisy otwartych danych również na szczeblu regionalnym czy lokalnym. Portal taki prowadzi również Komisja Europejska, tj. European Data Portal[434], który stanowi nie tylko punkt dostępu do danych pochodzących z instytucji i agend UE, ale również do danych pochodzących z portali państw członkowskich, w tym z CRIP .

Podstawy dla uruchomienia polskiego portalu otwartych danych zostały wprowadzone przy okazji implementacji w 2011 r. dyrektywy 2003/98/WE. Poza wdrożeniem dyrektywy wprowadzono również przepisy o nowym trybie udostępniania informacji publicznych oraz ich przekazywania do ponownego wykorzystywania w postaci CRIP.

Zgodnie z art. 9a ust. 1 UDIP w CRIP udostępnieniu podlegają zasoby informacyjne, będące szczególną kategorią informacji publicznych. Są to mianowicie informacje publiczne o szczególnym znaczeniu dla rozwoju innowacyjności w państwie i rozwoju społeczeństwa

[433] Zob. szerz. *D. Sybilski*, Centralne Repozytorium Informacji Publicznej jako tryb ponownego wykorzystywania informacji , Opolskie studia administracyjno-prawne 2018, nr XVI/2, s. 87-97.
[434] https://www.europeandataportal.eu

informacyjnego, które ze względu na sposób przechowywania i udostępniania pozwalają na ich ponowne wykorzystywanie, w sposób użyteczny i efektywny.

W związku z przeniesieniem regulacji ponownego wykorzystywania z UDIP do UPW można zaobserwować problem definicyjny zakresu przedmiotowego CRIP. Jak wskazano powyżej, zakres ponownego wykorzystywania obecnie wyznacza pojęcie informacji sektora publicznego. Mamy zatem do czynienia z różnym zakresem przedmiotowym. CRIP, który ma pełnić rolę głównego instrumentu dla bezwnioskowego ponownego wykorzystywania, odnosi się do zasobu informacyjnego, czyli podkategorii informacji publicznej, podczas gdy ponownemu wykorzystywaniu podlega – zgodnie z przepisami UPW – informacja sektora publicznego, w której zakresie mieści się pojęcie informacji publicznej.

Warto w tym miejscu przypomnieć, że potencjał dla ponownego wykorzystywania w praktyce mają dane otwarte. Z tego względu w CRIP jako krajowym portalu otwartych danych powinny być publikowane co do zasady informacje sektora publicznego spełniające kryteria otwartości opisane w Rozdziale 1, niemniej na portalu dostępne są również dane, które tych wymogów nie wypełniają.

Do przekazania w celu udostępnienia w CRIP posiadanych zasobów informacyjnych oraz metadanych opisujących ich strukturę nie są obowiązane wszystkie podmioty zobowiązane do udostępniania informacji publicznej a jedynie wymienione enumeratywnie w art. 9a ust. 2 UDIP, zwane dostawcami. Są to: organy administracji rządowej; fundusze celowe; Zakład Ubezpieczeń Społecznych; Kasa Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; państwowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyjątkiem uczelni, Polskiej Akademii Nauk oraz jednostek naukowych w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o zasadach finansowania nauki innych niż państwowe instytuty badawcze. Do katalogu podmiotów zobowiązanych – przepisami ustawy z dnia 16 kwietnia 2020 r. o szczególnych instrumentach wsparcia w związku z rozprzestrzenianiem się wirusa SARS-CoV-2[435] – dodano podmioty reprezentujące osoby prawne samorządu terytorialnego, jednostki organizacyjne samorządu terytorialnego, podmioty reprezentujące lub inne osoby prawne, w których jednostki samorządu terytorialnego mają pozycję dominującą w rozumieniu przepisów ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów. Co ciekawe, przedmiotowa nowelizacja UDIP skonkretyzowała dziedziny tematyczne z jakich jednostki samorządu terytorialnego mają udostępniać w CRIP zasoby informacyjne przy czym katalog ten ma charakter otwarty, tj.

[435] Dz.U. z 2020 r. poz. 695.

ochronę zdrowia; transport drogowy; pomoc społeczna; edukacja publiczna; kultura oraz ochrona zabytków; kultura fizyczna i turystyka; ochrona środowiska i przyroda; gospodarka komunalna. Zmianę tę należy ocenić pozytywnie, niewątpliwie jednostki samorządu terytorialnego posiadają wiele zasobów mających potencjał dla dalszego wykorzystywania, wiele z nich prowadzi portale otwartych danych, włączenie ich zatem w zakres podmiotowy CRIP jest w pełni uzasadnione. Określenie w ustawie obszarów tematycznych znajduje uzasadnienie w tym, że zasoby informacyjne samorządu terytorialnego nie są objęte tzw. rozporządzeniem zasobowym ministra właściwego do spraw informatyzacji, zatem ustawodawca pozostawił niejako swobodę jednostkom samorządu terytorialnego wyboru konkretnych informacji z wymienionych obszarów tematycznych do udostępnienia w CRIP, oczywiście spełniających przesłanki zasobu informacyjnego.

Do podstawowych zadań dostawców, które można zrekonstruować z przepisów UDIP dotyczących CRIP oraz rozporządzenia Rady Ministrów z dnia 12 marca 2014 r. w sprawie centralnego repozytorium informacji publicznej[436] należy dostosowanie danych do wymogów wskazanych w rozporządzeniu zasobowym (np. odpowiednie formaty danych), udostępnianie w portalu danych oraz metadanych i ich cyklicznie aktualizowanie, dbanie o jakość danych i reagowanie na zgłoszenia od użytkowników przesyłane za pośrednictwem portalu.

Spełnienie przez dostawcę obowiązku udostępnienia zasobu informacyjnego w CRIP może nastąpić bądź poprzez przekazanie zasobu i opisujących go metadanych (wówczas CRIP zgodnie ze swoją nazwą „przechowuje" dane, a więc pełni rolę typowego repozytorium) bądź też polega na przekazaniu samych metadanych opisujących dany zasób, który wciąż znajduje się dyspozycji dostawcy (w jego własnym systemie teleinformatycznym, np. dedykowanym portalu). Z tego też wzgląd nie można CRIP uznać za klasyczne repozytorium danych. CRIP jest systemem teleinformatycznym, który zapewnia stały dostęp do danych zarówno w nim zgromadzonych, jak i danych rozproszonych w innych systemach teleinformatycznych różnych podmiotów zobowiązanych, czyli dostawców.

Sposób weryfikacji zasobów informacyjnych oraz metadanych, jak i podstawowe funkcjonalności portalu i jego standardy techniczne zostały określone wspomnianym wyżej rozporządzeniem Rady Ministrów z dnia 12 marca 2014 r.

O tym, które informacje publiczne stanowią zasób informacyjny podlegający udostępnieniu w CRIP decyduje minister właściwy do spraw informatyzacji (za wyjątkiem zasobów będących w posiadaniu jednostek samorządu terytorialnego). Przepisy UDIP

[436] Dz. U. poz. 361.

upoważniły ministra do spraw informatyzacji do określenia w drodze rozporządzenia zasobów informacyjnych oraz metadanych przeznaczonych do udostępniania w CRIP. Minister rozporządzeniem ponadto określa harmonogram przekazania zasobów i metadanych, ich aktualizację oraz wymagania techniczne (format danych). Niemniej przepisy UDIP zapewniają pewną elastyczność. Po pierwsze, art. 9c UDIP daje podstawę do udostępnienia w CRIP także innych zasobów, niż te wskazane tzw. rozporządzeniem zasobowym, po drugie minister do spraw informatyzacji posiada kompetencje kontrolne, które pozwalają mu usunąć z centralnego repozytorium zasoby informacyjne, które nie mają szczególnego znaczenia dla rozwoju innowacyjności w państwie i rozwoju społeczeństwa informacyjnego. Dzięki takiemu rozwiązaniu możliwe jest udostępnianie zasobów informacyjnych mających potencjał dla ponownego wykorzystywania przez inne niż wymienione w art. 9a i 9aa UDIP podmioty zobowiązane. Podmioty też mogą z własnej inicjatywy udostępniać zasoby nieobjęte rozporządzeniem, a które w ich ocenie ze względu na treść i format mogą być atrakcyjne dla potencjalnych użytkowników. Ponadto administrator portalu, czyli minister właściwy do spraw informatyzacji ma możliwość sprawowania faktycznej kontroli nad jakością danych i usuwania danych o niskim potencjale.

4.3.1.3. Inne sposoby ponownego wykorzystywania

Zgodnie z art. 5 pkt 1 *in fine* UPW każdemu przysługuje prawo do ponownego wykorzystywania informacji sektora publicznego udostępnionych w inny sposób. Ustawodawca nie zdefiniował „innego sposobu", jak również nie wymienił przykładowego kanału dystrybucji informacji sektora publicznego, który uznaje za „inny sposób udostępnienia". W mojej opinii celowościowo należy „inny sposób" rozumieć, jako inny system teleinformatyczny – niż wymieniony na początku pkt 1, czyli BIP lub CRIP – prowadzony przez podmiot zobowiązany, na którym udostępnia się informacje sektora publicznego. Jako przykład takiego systemu teleinformatycznego można podać stronę informacyjną urzędu niebędącą BIP (w praktyce wiele urzędów prowadzi równolegle dwie „urzędowe strony", tj. BIP oraz stronę informacyjną, zazwyczaj bogatszą w treści i z bardziej atrakcyjną formą prezentacji zawartości informacyjnej[437]), jak również rejestry państwowe dostępne na stronach internetowych niebędących BIP (np. REGON, CEPIK, KRS i in.). Za taką

[437] Zob. np. Strony urzędu miasta stołecznego Warszawy https://www.um.warszawa.pl/ oraz https://bip.warszawa.pl/default.htm

interpretacją przemawia wymienienie „innego sposobu" w jednej jednostce redakcyjnej z BIP oraz CRIP, jak również posłużenie się sformułowaniem „udostępnione", które również w innych przepisach ustawy odnosi się do systemu teleinformatycznego.

Inne są również konsekwencje udostępnienia informacji „w inny sposób". W przeciwieństwie bowiem do BIP i CRIP zasada bezwnioskowego ponownego wykorzystywania będzie miała ograniczone zastosowanie, tj. jedynie do sytuacji, gdy podmiot zobowiązany publikując informację w innym systemie teleinformatycznym określi jednocześnie dla niej warunki ponownego wykorzystywania oraz opłaty lub wyraźnie poinformuje o ich braku. Zgodnie bowiem z art. 21 ust. 1 pkt 2 UPW wniosek o ponowne wykorzystywanie wnosi się, gdy informacja została udostępniona w sposób inny niż w BIP lub CRIP i nie zostały określone warunki ponownego wykorzystywania lub opłaty za ponowne wykorzystywanie albo nie poinformowano o braku takich warunków lub opłat. Informacja o warunkach i opłatach lub o możliwości ponownego wykorzystywania powinna być jednoznacznie powiązana z informacjami sektora publicznego, których dotyczy. Może mieć formę noty informacyjnej. W mojej opinii opatrzenie informacji sektora publicznego spełniających cechy praw własności intelektualnej notą licencyjną typu *Creative Commons* (lub innej tzw. wolnej licencji) spełnia warunek poinformowania o warunkach i opłatach w rozumieniu UPW.

4.3.2. Wnioskowe tryby ponownego wykorzystywania informacji sektora publicznego

Postępowanie w sprawie ponownego wykorzystywania na wniosek stanowi przykład szczególnej procedury, w której ustawodawca włączył konstrukcje cywilistyczne do procedury administracyjnej, dlatego można – zdaniem *M. Błachuckiego* i *G. Sibigi* o mówić o „przenikaniu się cywilnoprawnych i administracyjnoprawnych elementów" w tej procedurze administracyjnej[438]. Jest to świadomym wyborem ustawodawcy, który przyjął czynności prawa cywilnego jako podstawowe formy załatwienia sprawy, której przedmiotem nie jest samo przekazanie informacji wnioskodawcy, ponieważ nie każda dostępność określonej informacji przekłada się automatycznie na uprawnienia do korzystania z niej w celach komercyjnych lub niekomercyjnych[439]. Wybrany model administracyjno-prywatny jest uzasadniony

[438] Zob. *M. Błachucki, G. Sibiga*, Przenikanie się cywilnoprawnych i administracyjnoprawnych elementów w nowych procedurach administracyjnych na przykładzie postępowania w sprawie ponownego wykorzystywania informacji sektora publicznego przekazywanych na wniosek, „Opolskie Studia Administracyjno-prawne" 2018, nr XVI/1 (1), Opole, s. 21-31.
[439] *Ibidem*, s. 23.

w szczególności okolicznością, że informacje sektora publicznego mogą jednocześnie spełniać przesłanki przedmiotu praw własności intelektualnej (np. są utworem lub bazą danych). Ponadto szczególność postepowania w sprawie ponownego wykorzystywania przejawia się w znacznym ograniczeniu znaczenia przepisów KPA dla tego postępowania. Nie wyprzedzając dalszych rozważań można przyjąć, że UPW samodzielnie reguluje postępowanie wnioskowe, a podmiot zobowiązany będzie stosował KPA w bardzo ograniczonym zakresie[440].

Postępowanie indywidualne w sprawie ponownego wykorzystywania informacji sektora publicznego jest wszczynane wyłącznie na wniosek użytkownika. Zgodnie z art. 21 ust. 1 UPW wniosek o ponowne wykorzystywanie wnosi się w przypadkach, gdy informacja sektora publicznego:

1) nie została udostępniona w BIP lub w centralnym repozytorium;

2) została udostępniona w sposób inny niż określony w pkt 1 i nie zostały określone warunki ponownego wykorzystywania lub opłaty za ponowne wykorzystywanie albo nie poinformowano o braku takich warunków lub opłat;

3) będzie wykorzystywana na warunkach innych niż zostały dla tej informacji określone;

4) została udostępniona lub przekazana na podstawie innych ustaw określających zasady i tryb dostępu do informacji będących informacjami sektora publicznego.

Na gruncie tego przepisu można zatem wyodrębnić dwie okoliczności, w których użytkownik jest uprawniony do złożenia wniosku, i w związku z tym występują dwa cele postępowania. Kryterium rozróżniającym te dwie sytuacje jest fakt uprzedniego udostępnienia informacji sektora publicznego przed złożeniem wniosku.

Pierwsza okoliczność ma miejsc, kiedy informacja sektora publicznego nie jest w ogóle dostępna, czyli nie została udostępnienia w jakimkolwiek systemie teleinformatycznych, jak również nie została przekazana na podstawie innych ustaw określających zasady i tryb dostępu do informacji będących informacjami sektora publicznego. W tym wypadku przedmiotem wniosku będzie zarówno przekazanie wnioskodawcy informacji, jak i rozstrzygnięcie kwestii warunków ponownego wykorzystywania oraz opłat za ponowne wykorzystywanie. Złożenie wniosku będzie realizować równocześnie uprawnienie informacyjne (gwarantujące pozyskanie informacji) oraz prawo do ponownego wykorzystywania[441].

[440] *Ibidem, s. 24.*

[441] *M. Błachucki, G. Sibiga*, Postępowanie w sprawie ponownego wykorzystywania isp przekazywanych na wniosek [w:] *E. Badura., M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń., M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, Ponowne wykorzystywanie informacji sektora publicznego, s. 218.

Druga okoliczność ma miejsce, gdy wnioskodawca jest w posiadaniu informacji sektora publicznego, np. pobrał ją z systemu teleinformatycznego podmiotu zobowiązanego (innego niż BIP lub CRIP) lub uzyskał informację od podmiotu zobowiązanego na podstawie przepisów innych ustaw, np. w wyniku realizacji wniosku o dostęp do informacji publicznej. Przedmiotem wniosku nie będzie zatem przekazanie informacji sektora publicznego, celem postępowania będzie jedynie rozstrzygnięcie kwestii warunków ponownego wykorzystywania polegające albo na określeniu warunków ponownego wykorzystywania lub informacji o wysokości opłat za ponowne wykorzystywanie, jeśli nie zostały przez podmiot zobowiązany ustalone albo poinformowanie o ich braku. Będzie to konieczne, jeśli warunki ponownego wykorzystywania lub informacja o opłatach konkretnych informacji sektora publicznego nie zostały ustalone i zgodnie przez podmiot zobowiązany (za wyjątkiem udostępnienia informacji sektora publicznego w BIP lub CRIP) albo warunki lub wysokość opłat zostały ustalone, ale wnioskodawca zamierza wykorzystywać informacje na innych warunkach.

W przepisach UPW ustawodawca wyróżnił dwa rodzaje wniosków. Pierwszy rodzaj wniosku dotyczy żądania przekazania informacji sektora publicznego lub ustalenia warunków ponownego wykorzystywania dla informacji, która już jest dostępna. Stanowi on podstawowy rodzaj wniosku regulowanego przepisami rozdziału 5 UPW, można go zatem nazwać wnioskiem standardowym[442], zwykłym[443] lub podstawowym wnioskiem o ponowne wykorzystywanie[444]. Drugi szczególny rodzaj wniosku - określony w art. 21 ust. 2 – dotyczy stałego i bezpośredniego ponowne wykorzystywanie informacji sektora publicznego w czasie rzeczywistym w systemie teleinformatycznym podmiotu zobowiązanego, jednak w okresie nie dłuższym niż 12 miesięcy UPW. Celem wprowadzenie tego przepisu było umożliwienie użytkownikowi wykorzystywanie informacji bez konieczności wielokrotnego występowania z wnioskiem w odniesieniu do informacji sektora publicznego dystrybuowanych przez podmiot zobowiązany poprzez system teleinformatyczny, np. z wykorzystaniem API. Ma on znaczenie w szczególności dla informacji cechujących się zmiennością treści ze względu na ich częstą aktualizację (np. prognozy pogody, informacje o zanieczyszczeniu powietrza). Jego odmienność polega na tym, że ustawa określa nie tylko pewien szczegółowy sposób dostępu do wykorzystywanej informacji oraz czas tego dostępu, ale również przewiduje odmienności w rozpatrywaniu tego szczególnego wniosku.

[442] *Ibidem*, s. 223.
[443] *M. Błachucki, G. Sibiga*, Przenikanie się cywilnoprawnych i administracyjnoprawnych elementów, s. 22.
[444] *B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz*, Ustawa o ponownym, 2017, s. 303.

Wniosek standardowy o ponowne wykorzystywanie musi spełniać określone wymogi co do treści i w tym znaczeniu postępowanie w sprawie tego wniosku jest postępowaniem bardziej sformalizowanym niż udostępnianie informacji publicznej na wniosek, ponieważ w tamtym brak jest jakichkolwiek wymogów co do treści wniosku[445]. Podyktowane jest to przede wszystkim celem UPW oraz faktyczną możliwością realizacji innych wymogów regulacji, jak np. określenia adekwatnych warunków ponownego wykorzystywania, co nie byłoby możliwe bez posiadania wiedzy przez podmiot zobowiązany co do planowanego celu, rodzaju i zakresu ponownego wykorzystywania konkretnej informacji sektora publicznego.

Zgodnie z art. 21 ust 3 UPW wniosek standardowy zawiera w szczególności:

1) nazwę podmiotu zobowiązanego;

2) informacje o wnioskodawcy, w tym imię i nazwisko albo nazwę oraz adres umożliwiający dostarczenie odpowiedzi do wnioskodawcy albo pełnomocnika tego wnioskodawcy w sposób lub w formie wskazanych we wniosku;

3) wskazanie informacji sektora publicznego, która będzie ponownie wykorzystywana, a jeżeli jest już udostępniona lub przekazana, warunki, na jakich ma być ponownie wykorzystywana, oraz źródło udostępnienia lub przekazania;

4) wskazanie celu ponownego wykorzystywania (komercyjny albo niekomercyjny), w tym określenie rodzaju działalności, w której informacje sektora publicznego będą ponownie wykorzystywane, w szczególności wskazanie dóbr, produktów lub usług;

5) wskazanie formy przygotowania informacji sektora publicznego, a w przypadku postaci elektronicznej, także wskazanie formatu danych;

6) wskazanie sposobu przekazania informacji sektora publicznego, o ile nie została udostępniona lub przekazana w inny sposób.

Wniosek o stały dostęp musi zawierać wszystkie wymienione elementy oraz dodatkowo wskazywać sposób dostępu do informacji gromadzonych w systemie teleinformatycznym oraz wskazanie okresu, przez który podmiot zobowiązany będzie umożliwiał ponowne wykorzystywanie informacji sektora publicznego w sposób stały i bezpośredni w czasie rzeczywistym.

Wniosek wnosi się w postaci papierowej albo elektronicznej. Pojęcie postaci należy rozumieć w ten sposób, że postać jest materializacją formy i wiąże się z utrwaleniem treści na nośniku[446]. Co istotne, zarówno w odniesieniu do wniosku zwykłego, jak i wniosku o stały

[445] *M. Błachucki, G. Sibiga*, Postępowanie w sprawie ponownego wykorzystywania isp, s. 228.

[446] *K. Wojsyk* [w:] *M. Barczewski (red.), K. Grajewski, J. Warylewski,* Prawne problemy wykorzystywania nowych technologii w administracji publicznej i w wymiarze sprawiedliwości, Warszawa 2009, s. 148.

dostęp nie wprowadzono wymogu podpisania wniosku. Oznacza to, że w przypadku wykorzystania poczty elektronicznej do złożenia wniosku o ponowne wykorzystywanie brak jest obowiązku stosowania mechanizmów teleinformatycznego uwierzytelnienia wnoszącego żądanie[447]. Mamy tutaj do czynienia z paralelnym rozwiązaniem jak w przypadku dostępu do informacji publicznej. Zgodnie z orzecznictwem sądów administracyjnych ukształtowanym na gruncie UDIP za wniosek pisemny uznawać należy również przesłanie zapytania pocztą elektroniczną i to nawet, gdy do jego autoryzacji nie zostanie użyty podpis elektroniczny[448].

W przypadku niespełnienia warunków formalnych wniosku podmiot zobowiązany wzywa wnioskodawcę do usunięcia braków formalnych, wraz z pouczeniem, że ich nieusunięcie w terminie 7 dni od dnia otrzymania wezwania spowoduje pozostawienie wniosku bez rozpoznania. Terminu tego nie można wydłużyć. Pozostawienie wniosku bez rozpoznania oznacza stwierdzenie przez podmiot zobowiązany, że podanie zawiera kwalifikowaną wadę i że wskutek tego stało się bezskuteczne z mocy prawa[449]. W praktyce oznacza to opatrzenie wniosku stosowną adnotacją, jest on odkładany *ad acta,* a sprawa jest zamykana[450].

Zgodnie z art. 22 UPW rozpatrzenie wniosku następuje niezwłocznie, nie później jednak niż w terminie 14 dni od dnia otrzymania wniosku. Termin ten może zostać przez podmiot zobowiązany wydłużony do maksymalnie 2 miesięcy od dnia złożenia wniosku o ponowne wykorzystywanie, jeżeli wniosek ten nie może zostać rozpatrzony w terminie 14 dni. Podmiot zobowiązany zawiadamia w tym terminie wnioskodawcę o przyczynach opóźnienia oraz o terminie, w jakim rozpatrzy wniosek.

Szczególny charakter postępowania w sprawie ponownego wykorzystywania uwidacznia się w – wymienionych w zamkniętym katalogu w art. 23 UPW – sposobach merytorycznego załatwienia wniosku. Sposoby załatwienia sprawy można podzielić na pozytywne, polegające na przekazaniu żądanej informacji sektora publicznego lub zawiadomieniu o warunkach ponownego wykorzystywania albo też przedstawieniu oferty, oraz negatywne, w tym wypadku chodzi odmowę zgody na ponowne wykorzystywanie.

Zanim omówione zostaną wszystkie wymienione scenariusze rozpatrzenia wniosku, konieczne jest poczynienie uwagi dotyczącej istotnego zagadnienia proceduralnego – zasygnalizowanego na wstępie niniejszego podrozdziału – dotyczącego zakresu zastosowania w postępowaniu w sprawie ponownego wykorzystywania na wniosek przepisów KPA. Przepisy

[447] *M. Błachucki, G. Sibiga,* Postępowanie w sprawie ponownego wykorzystywania isp, s. 227.
[448] Wyrok NSA z dnia 30.11.2012 r., I OSK 1991/12.
[449] Wyrok NSA z 3.02.1992 r., IV SA 1377/91.
[450] *M. Błachucki, G. Sibiga,* op. cit., s. 234.

proceduralne UPW, jakkolwiek przewidują szczególne rozwiązania (np. o ofercie) to, co do zasady opierają się na znanym z przepisów UDIP postępowaniu w sprawie udostępnienia informacji publicznej na wniosek. Z tego powodu poglądy doktryny i wypracowane na kanwie UDIP orzecznictwo sądów administracyjnych dotyczące zastosowania KPA zachowują swoją aktualność również dla szczególnego postępowania w sprawie ponownego wykorzystywania.

Postępowania to charakteryzuje się znacznym ograniczeniem zastosowania przepisów KPA. Zgodnie z art. 25 ust. 1 UPW KPA ma zastosowanie jedynie do decyzji o odmowie wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego oraz do decyzji o warunkach ponownego wykorzystywania lub o wysokości opłat za ponowne wykorzystywanie na podstawie zgłoszonego przez wnioskodawcę sprzeciwu od oferty. UPW zasadniczo samodzielnie reguluje postępowanie wnioskowe, a podmiot zobowiązany będzie mógł stosować KPA jedynie w bardzo ograniczonym zakresie dopuszczonym przez UPW w sytuacji, gdy będzie wydawał decyzje administracyjne[451]. Z tego powodu należy uznać, że KPA będzie bezpośrednio stosowany dopiero na etapie wydawania przez podmiot zobowiązany decyzji w dwóch wspomnianych przypadkach[452]. Oznacza to, że podmiot zobowiązany nie będzie stosował KPA na etapie wszczęcia postępowania[453]. Podobnie jak to ma miejsce na gruncie UDIP, jedynym środkiem zwalczania bezczynności lub przewlekłego prowadzenia postępowania w sprawie rozpatrzenia wniosku o ponowne wykorzystywanie przez podmiot zobowiązany będzie skarga do sądu administracyjnego, a wyłączona jest możliwość składania zażalenia na bezczynność lub przewlekłość postępowania do organu odwoławczego[454].

Odmowa wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego oraz decyzja ustalająca warunki ponownego wykorzystywania lub wysokość opłaty za ponowne wykorzystywanie następują w drodze decyzji administracyjnej wydanej na podstawie KPA. Zatem decyzja ta musi spełniać wszystkie wymagania określone w art. 107 KPA**,** a także zawierać dodatkowe informacje (jeśli zachodzi sytuacja odmowy wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego ze względu na prawa własności intelektualnej na podstawie art. 23 ust. 6 UPW). Przyjęte w UPW rozwiązanie wpływa korzystnie na gwarancje procesowe wnioskodawców (użytkowników), bowiem jeżeli podmiot zobowiązany będzie zmierzał do wydania decyzji administracyjnej powinien zapewnić prawa procesowe wynikające z przepisów KPA (bezstronność rozpatrywania sprawy, składanie

[451] Zob. wyrok NSA z 06.09.2012 r., I OSK 1274/12.
[452] Zob. wyrok NSA z 01.09.2011 r., I OSK 1002/11.
[453] Zob. wyrok WSA w Szczecinie z 06.02.2014 r., II SAB/Sz 114/13.
[454] *M. Błachucki, G. Sibiga*, op. cit., s. 115.

wniosków dowodowych, dostęp do akt sprawy, wypowiedzenie się co do zebranego materiału dowodowego przed wydaniem decyzji, dwuinstancyjność postępowania)[455].

Swoboda wyboru przez podmiot zobowiązany sposobu załatwienia wniosku jest zdeterminowana kilkoma czynnikami.

Po pierwsze, podmiot zobowiązany musi stwierdzić, czy występują przesłanki ograniczające ponowne wykorzystywanie, wymienione w art. 6 UPW. Celem przepisu jest ochrona wartości i praw, które mają pierwszeństwo przed realizacją ponownego wykorzystywania informacji sektora publicznego w dowolnym celu. Chodzi to o ochronę informacji niejawnych oraz innych tajemnic ustawowo chronionych (ust.1), prywatność osoby fizycznej lub tajemnicę przedsiębiorcy (ust. 2), ograniczenie dostępu do informacji sektora publicznego podstawie ustaw szczególnych (ust. 3), informacje, których wytwarzanie przez podmioty zobowiązane nie należy do zakresu ich zadań publicznych określonych prawem (ust. 4 pkt 1), informacje powiązanych z depozytami znajdującymi się w posiadaniu podmiotu zobowiązanego, o ile ich właściciele umownie wyłączyli możliwość ich udostępniania lub przekazywania (ust. 4 pkt 2), informacje, do których prawa własności intelektualnej przysługują podmiotom innym niż podmioty zobowiązane (ust. 4 pkt 3), informacje będące w posiadaniu muzeów państwowych, muzeów samorządowych, bibliotek publicznych, bibliotek naukowych lub archiwów, w przypadku gdy pierwotnym właścicielem autorskich praw majątkowych lub praw pokrewnych były podmioty inne niż podmioty zobowiązane, a czas trwania tych praw nie wygasł (ust. 4 pkt 4). W przypadku wystąpienia którejkolwiek z przesłanek podmiot zobowiązany – zgodnie z art. 23 ust. 4 UPW – w drodze decyzji odmawia zgody na ponowne wykorzystywanie. Podkreślić trzeba, że decyzja ta ma charakter związany, podmiot zobowiązany nie ma w tym zakresie żadnego wyboru i ma obowiązek wydać decyzję odmowną, jeżeli stwierdzi istnienie przesłanek z art. 6 UPW[456].

Po drugie, podmiot zobowiązany w przypadku niestwierdzenia ograniczeń, może rozważyć, czy zachodzi okoliczność wymieniona w art. 10 UPW. Podmioty zobowiązane nie są obowiązane do tworzenia informacji sektora publicznego, ich przetwarzania w sposób lub w formie wskazanych we wniosku o ponowne wykorzystywanie oraz sporządzania z nich wyciągów, jeżeli spowoduje to konieczność podjęcia nieproporcjonalnych działań przekraczających proste czynności. Przepis ten ma na celu zwolnienie podmiotu zobowiązanego z obowiązku tworzenia lub opracowania informacji sektora publicznego, które co do formy lub sposobu przekazania żądanego przez wnioskodawcę powodowałoby

[455] *M. Błachucki, G. Sibiga*, Przenikanie się cywilnoprawnych i administracyjnoprawnych elementów, s. 25.
[456] *Ibidem,* s. 30.

konieczność podjęcia ponadstandardowych czynności wymagających nieproporcjonalnego wysiłku[457]. Podmiot zobowiązany – zgodnie z art. 23 ust. 5 ma możliwość odmówienia zgody na ponowne wykorzystywanie. Decyzja ta ma więc charakter uznaniowy, powinna zawsze zostać poprzedzona oceną, jakie nakłady sił i środków będą musiały być zaangażowane, aby zrealizować wniosek zgodnie z żądaniem[458].

Od przesłanki tej należy odróżnić niemożność przetworzenia wynikającą z braku technicznych możliwości, ze względu na niedysponowanie określonymi programami lub urządzeniami, które pozwoliłyby na przetworzenie w taki sposób lub w takiej formie, które zostały zawarte we wniosku. Należy podzielić pogląd, że takiej sytuacji nie powinno się wydawać decyzji, a jedynie informować o tym fakcie wnioskodawcę w drodze zwykłego pisma[459].

Podkreślenia wymaga, że odmowa przekazania informacji sektora publicznego jest wyjątkiem od ogólnej zasady dostępności informacji sektora publicznego w celu ponownego wykorzystywania[460]. Dyrektywą tą powinien zawsze kierować się podmiot zobowiązany i o ile jest to możliwe, wniosek powinien zostać rozpatrzony pozytywnie. Jest to szczególnie istotne gdy podmiot zobowiązany będzie oceniać proporcjonalność nakładów koniecznych do udostępnienia informacji sektora publicznego i czy będą przekraczały proste czynności[461].

Po trzecie, podmiot zobowiązany musi rozstrzygnąć kwestię określenia warunków ponownego wykorzystywania informacji, która warunkuje sposób pozytywnego załatwienia sprawy. Określenie warunków można podzielić na fakultatywne oraz obligatoryjne, z czego w pierwszym wypadku warunki mogą być zwykłe (standardowe) lub szczególne.

Podmiot zobowiązany fakultatywnie określa warunki ponownego wykorzystywania, które zgodnie z art. 14 UPW mogą dotyczyć:

1) obowiązku poinformowania o źródle, czasie wytworzenia i pozyskania informacji od podmiotu zobowiązanego;

2) obowiązku poinformowania o przetworzeniu informacji ponownie wykorzystywanej;

3) zakresu odpowiedzialności podmiotu zobowiązanego za udostępniane lub przekazywane informacje;

4) informacji sektora publicznego zawierającej dane osobowe.

---

[457] *B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz*., Komentarz, 2017, s. 229.
[458] *M. Błachucki, G. Sibiga*, Przenikanie się cywilnoprawnych i administracyjnoprawnych elementów, s. 30.
[459] *P. Sitniewski*, Komentarz do art. 10 pkt 4 , Legalis/Wyd. 2017.
[460] Na temat zasady dostępności zob. *A. Piskorz-Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 235-251.
[461] *M. Błachucki, G. Sibiga*, op. cit., s. 30

Warunki te mają standardowy charakter i mogą dotyczyć każdego rodzaju informacji sektora publicznego, choć oczywistym jest, że ostatni wymieniony warunek pozostaje relewantny wyłącznie w przypadku, gdy przekazaniu lub udostępnieniu podlegają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (zob. szerzej Rozdział 9). Ponadto podmiot zobowiązany będący muzeum państwowym, muzeum samorządowym, biblioteką publiczną, biblioteką naukową lub archiwum może dodatkowo określać inne niestandardowe warunki ponownego wykorzystywania ograniczające wykorzystywanie informacji sektora publicznego ze względu na specyfikę konkretnej informacji sektora publicznego (art. 14 ust. 2 UPW).

Obligatoryjne określenie warunków będzie miało miejsce, gdy przedmiotem ponownego wykorzystywania jest informacja sektora publicznego mająca cechy utworu lub przedmiotu praw pokrewnych w rozumieniu przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych lub stanowiących bazę danych w rozumieniu przepisów ustawy z dnia 27 lipca 2001 r. o ochronie baz danych, do których przysługują mu autorskie prawa majątkowe lub prawa pokrewne. W tej sytuacji podmiot zobowiązany jest zmuszony określić warunki ponownego wykorzystywania takiej informacji, w szczególności podmiot zobowiązany określa warunek dotyczący obowiązku poinformowania o nazwisku, imieniu lub pseudonimie twórcy lub artysty wykonawcy, jeżeli jest znany. W pozostałym zakresie ma pewną swobodę określenia warunków eksploatacji informacji sektora publicznego będących jednocześnie utworem, przedmiotem praw pokrewnych lub bazą danych, ale warunki te będą zdeterminowane zakresem uprawnień, którymi dysponuje, tj. autorskimi prawami majątkowymi lub prawem do bazy danych (np. dotyczących możliwych pól eksploatacji utworu)[462].

Należy podkreślić, że ogólną zasadą pozostaje bezwarunkowe ponowne wykorzystywanie informacji sektora publicznego, wyjątkiem jest odstąpienie od niej poprzez określenie warunków jej używania. Z tego powodu przepisy dopuszczające określenie warunków należy interpretować ściśle[463]. Określenie warunków – w myśl art. 15 UPW - ponownego wykorzystywania nie może w sposób nieuzasadniony ograniczać możliwości ponownego wykorzystywania. Zasada bezwarunkowego ponownego wykorzystywania oraz

[462] Zob szerzej *X. Konarski*, Prawa własności intelektualnej w kontekście ponownego wykorzystywania informacji sektora publicznego [w:] *E. Badura., M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń., M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 148 i nast. oraz *A. Piskorz-Ryń*, Zasady ponownego wykorzystywania informacji publicznej będącej utworem w rozumieniu ustawy z dnia 4 lipca 1994 r. o prawie autorskim i prawach pokrewnych, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2014 nr 1.
[463] *B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz*, Komentarz, 2017, s. 246.

ograniczenia warunków doznaje ograniczenia, gdy przedmiotem eksploatacji pozostają informacje spełniające cechy praw własności intelektualnej.

Po czwarte, podmiot zobowiązany musi rozstrzygnąć kwestię opłat za ponowne wykorzystywanie. Zasadą podstawową pozostaje przekazanie informacji sektora publicznego bezpłatnie. Podmiot zobowiązany nie ma swobody w nakładaniu opłaty za ponowne wykorzystywanie, ponieważ można ją nałożyć jedynie wyjątkowo, jeżeli przygotowanie i przekazanie informacji w sposób i w formie określonych we wniosku wymaga poniesienia dodatkowych kosztów (art. 17 ust. 1 i 2 UPW). Wyjątek dotyczy muzeów państwowych i samorządowych, które mogą ustalać dodatkowe opłaty, jeśli celem ponownego wykorzystywania jest inny niż niekomercyjny o charakterze badawczym, naukowym lub edukacyjnym (art. 18 UPW), przy czym jest to rozwiązanie fakultatywne.

Jeśli zatem nie występują przesłanki ograniczające prawo do ponownego wykorzystywania, a przedmiotem wniosku nie jest informacja sektora publicznego zawierające dane osobowe lub będąca utworem lub przedmiotem praw pokrewnych lub nie stanowi bazy danych, rozważyć powinien przekazanie informacji sektora publicznego w celu ponownego wykorzystywania bez określania warunków ponownego wykorzystywania i opłat. Sytuacja ta jest najkorzystniejsza z punktu widzenia użytkownika, pozwala mu bowiem na eksploatowanie informacji sektora publicznego bez dodatkowych wymogów i bez ograniczania odpowiedzialności podmiotu zobowiązanego za przekazywane informacje, jak również bez kosztów w postaci opłaty. Pod względem formalnym podmiot zobowiązany kończy postępowanie poprzez przekazanie wnioskodawcy informacji sektora publicznego w formie i w sposób określone we wniosku. Choć z przepisu art. 23 ust. 1 pkt 1 UPW wynika, że wystarczające pozostaje samo przekazanie informacji sektora publicznego wnioskodawcy z równoczesnym powstrzymaniem się od określania warunków ponownego wykorzystywania, jednak dla pewności obrotu rekomenduje się, aby jednocześnie poinformować wnioskodawcę, że nie określa się warunków ponownego wykorzystywania dla informacji sektora publicznego stanowiących przedmiot wniosku[464].

Jeśli wnioskodawca posiada informację sektora publicznego, ponieważ informacja została już udostępniona w systemie teleinformatycznym innym niż BIP lub CRIP lub została wnioskodawcy przekazana na podstawie przepisów szczególnych a przedmiotem wniosku jest jedynie rozstrzygniecie kwestii warunków ponownego wykorzystywania, podmiot zobowiązany zawiadamia o braku warunków ponownego wykorzystywania informacji sektora

[464] *M. Błachucki, G. Sibiga*, Postępowanie w sprawie ponownego wykorzystywania, s. 251.

publicznego. Pod względem formalnym podmiot zobowiązany kończy postępowanie poprzez przesłanie wnioskodawcy pisma, w którym informuje o braku warunków ponownego wykorzystywania dla ISP stanowiących przedmiot wniosku[465].

Kolejnym sposobem pozytywnego załatwienia wniosku jest przedstawienie wnioskodawcy oferty. Podmiot zobowiązany przedstawia wnioskodawcy ofertę zarówno w przypadku wniosku o przekazanie informacji sektora publicznego w celu ponownego wykorzystywania, jak i wniosku, którego przedmiotem jest rozstrzygniecie w przedmiocie warunków ponownego wykorzystywania. Podmiot zobowiązany obligatoryjnie przedstawia ofertę, gdy wniosek dotyczy informacji sektora publicznego będącej utworem lub przedmiotem praw pokrewnych lub stanowi bazę danych. W pozostałych przypadkach jest fakultatywne i ma miejsce, gdy podmiot zobowiązany nie zdecyduje o bezwarunkowym ponownym wykorzystywaniu. W tym miejscu warto dodać, że warunki ponownego wykorzystywania określone przez podmiot zobowiązany dla informacji sektora publicznego udostępnionej w systemie teleinformatycznym uważa się za ofertę.

Oferta zawiera warunki ponownego wykorzystywania ISP oraz wysokość opłaty za ponowne wykorzystywanie ISP. Pojęcie oferty należy rozumieć zgodnie z art. 66 i n. KC, z tym zastrzeżeniem, że przepisy UPW wprowadzają własne, szczególne rozwiązania dotyczące treści oferty oraz jej przyjęcia[466]. Przedstawienie oferty to czynność w postępowaniu w administracji. Jednak przede wszystkim oferta powoduje skutki cywilnoprawne, będąc oświadczeniem strony dążącej do zawarcia umowy (propozycją zawarcia umowy), które jest indywidualnie adresowane i zawiera istotne elementy umowy określone w UPW[467]. Skutkiem prawnym oferty jest powstanie stanu związania oferenta (podmiotu zobowiązanego) złożoną ofertą, w tym znaczeniu, że użytkownik (oblat) poprzez przyjęcie oferty zawiera umowę o określonej w ofercie treści, której postanowienia zdeterminowane są przepisami UPW, w tym w szczególności warunkami pod jakimi dozwolona będzie eksploatacja informacji przez użytkownika.

Zgodnie z art. 23 ust. 2 UPW wnioskodawca po otrzymaniu oferty ma trzy możliwości działania.

Po pierwsze, może przyjąć ofertę, przy czym powinien on zawiadomić podmiot zobowiązany o przyjęciu oferty w terminie 14 dni od jej otrzymania. Konsekwencją będzie

[465] *Ibidem*, s. 249.
[466] *Ibidem*, s. 252
[467] *Ibidem.*

doprowadzenie do zawarcia umowy o określonej w ofercie treści. Umowę poczytuje się za zawartą w chwili otrzymania przez podmiot zobowiązany zawiadomienia wnioskodawcy[468].

Po drugie, wnioskodawca może nie przyjąć oferty. Wystarczające jest samo milczenie wnioskodawcy. Brak zawiadomienia o przyjęciu oferty w terminie 14 dni od jej otrzymania jest równoznaczny z wycofaniem wniosku. Wywołuje podwójny skutek, tj. administracyjnoprawny, kończy bowiem postępowanie wszczęte na wniosek, do którego nie mają zastosowanie przepisy KPA oraz cywilnoprawny, nie dochodzi bowiem do zawarcia umowy o ponowne wykorzystywanie.

Po trzecie, może w terminie 14 dni od dnia otrzymania oferty złożyć sprzeciw wobec oferty z powodu naruszenia ustawy. Wnioskodawca, który otrzymał ofertę może złożyć sprzeciw z powodu naruszenia przepisów ustawy albo zawiadomić podmiot zobowiązany o przyjęciu oferty. W przypadku otrzymania sprzeciwu podmiot zobowiązany, w drodze decyzji, rozstrzyga o warunkach ponownego wykorzystywania lub o wysokości opłat za ponowne wykorzystywanie.

Złożenie sprzeciwu wszczyna zatem odrębne postępowanie administracyjne, którego stroną jest podmiot wnoszący sprzeciw[469]. Celem rozwiązania jest stworzenie podstaw do administracyjnej, a następnie sądowoadministracyjnej kontroli zgodności z prawem określonych w ofercie warunków lub opłat. Uruchamia to mechanizm samokontroli podmiotu zobowiązanego, który w decyzji musi ustalić warunki lub opłatę wraz z uzasadnieniem swojego rozstrzygnięcia[470]. Decyzja ta może podtrzymać pierwotnie ustalone warunki i wysokość opłaty albo też zmienić je w całości lub w części, co może również oznaczać całkowitą rezygnację z ich ustalania. Nawet w najkorzystniejszym dla wnioskodawcy rozwiązaniu, gdy podmiot zobowiązany ostatecznie podziela zarzuty zawarte w sprzeciwie, musi ostatecznie załatwić sprawę w drodze decyzji administracyjnej[471]. Decyzja podmiotu zobowiązanego może podlegać, na skutek wniesienia przez wnioskodawcę środka zaskarżenia, kontroli instancyjnej organu wyższego stopnia oraz kontroli sądu administracyjnego.

Problematyczną pozostaje kwestia ustalania charakteru odpowiedzialności użytkownika za nieprzestrzeganie warunków ponownego wykorzystywania. Co do zasady w przypadku zawarcia umowy o ponowne wykorzystywanie w trybie ofertowym nieprzestrzeganie warunków przyjętych przez użytkownika lub nieuiszczenie opłaty za ponowne

[468] *Ibidem*, s. 253.
[469] *M. Błachucki, G. Sibiga*, Przenikanie się cywilnoprawnych i administracyjnoprawnych elementów, s. 29.
[470] *M. Błachucki, G. Sibiga*, Postępowanie w sprawie ponownego wykorzystywania, s. 254.
[471] *B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz*, Komentarz, 2017, s. 344.

wykorzystywanie powinno być kwalifikowane jako niewykonanie lub nienależyte wykonanie zobowiązania w rozumieniu przepisów KC. Taka kwalifikacja wątpliwa będzie w przypadku określenia warunków lub opłat w drodze decyzji administracyjnej wydanej na skutek wniesienia sprzeciwu. Skoro nie doszło do zawarcia umowy, ponieważ wydano decyzję administracyjną, która pozostaje w sferze prawa publicznego należy rozważyć, czy w tym przypadku nie powinna zostać uruchomiona egzekucja administracyjna[472].

Odmiennie ustawodawca określił sposób rozpatrzenia wniosku o stały dostęp, o którym mowa w art. 21 ust. 2 UPW. W tym wypadku podmiot zobowiązany może:

1) złożyć ofertę zawierającą warunki ponownego wykorzystywania lub informację o wysokości opłat za ponowne wykorzystywanie, a wnioskodawca w terminie 14 dni od dnia jej otrzymania zawiadamia podmiot zobowiązany o przyjęciu oferty, przy czym od oferty tej nie przysługuje sprzeciw. Co istotne, opłata w tym wypadku może uwzględniać koszty wynikające z dostosowania systemu teleinformatycznego oraz warunków technicznych i organizacyjnych do realizacji wniosku o ponowne wykorzystywanie (art. 19 UPW);

2) poinformować wnioskodawcę o braku możliwości ponownego wykorzystywania w sposób wskazany we wniosku;

3) odmówić, w drodze decyzji, wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego, gdy zachodzą przesłanki ograniczające prawa do ponownego wykorzystywania informacji sektora publicznego.

Odrębności polegają zatem na pogorszeniu sytuacji wnioskodawcy względem wniosku zwykłego. Nie przewiduje się możliwości bezpośredniego zapewnienia dostępu do systemu teleinformatycznego po otrzymaniu wniosku przez podmiot zobowiązany i zawiadomienia o tym wnioskodawcy. Dopiero gdy wnioskodawca przyjmie ofertę, w wyniku czego nastąpi zawarcie umowy o ponowne wykorzystywanie, podmiot zobowiązany zapewnia dostęp do informacji sektora publicznego w systemie teleinformatycznym[473]. Wnioskodawca pozbawiony jest możliwości kwestionowania warunków lub opłat za ponowne wykorzystywanie informacji sektora publicznego w tym trybie, a w przypadku braku możliwości technicznej zapewnienia stałego dostępu podmiot zobowiązany informuje o tym wnioskodawcę zwykłym pismem.

[472] Zob. szerzej: *B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz*, op. cit., s. 346-345.

[473] *M. Błachucki, G. Sibiga*, Postępowanie w sprawie ponownego wykorzystywania, s. 265.

4.4. Zasady ogólne ponownego wykorzystywania informacji sektora publicznego

Podmioty zobowiązane, które udostępniają i przekazują informacje sektora publicznego w celu ponownego wykorzystywania, muszą respektować zasady, które swoje źródło mają w publicznym prawie podmiotowym do ponownego wykorzystywania informacji sektora publicznego, którego korelatem są poszczególne obowiązki po stronie podmiotu zobowiązanego[474].

Dyrektywy o ponownym wykorzystywaniu, jak i wykonujące je przepisy ustawy krajowej wymieniają podstawowe zasady, których adresatem jest podmiot udzielający informacji. Przepisy UPW transponują odpowiednie przepisy dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE. Przepisy nowej dyrektywy 2019/1024 nie wprowadziły w tym zakresie istotnych zmian. Dlatego też w dalszej części rozdziału omówione zostaną przepisy krajowe z uwzględnieniem wszelkich odrębności wykraczających poza minimum wyznaczone przepisami dyrektyw.

Zasady ponownego wykorzystywania można podzielić na zasady ogólne ujęte w rozdziale 2 UPW „Zasady udostępniania i przekazywania informacji sektora publicznego w celu ponownego wykorzystywania", tj. zasadę niedyskryminacji (równego traktowania), zasadę niewyłączności oraz zasadę przejrzystości (jawności lub transparentności) oraz otwartych formatów. Drugą grupę stanowią zasady szczegółowe doznające szeregu odrębności, tj. zasada bezpłatności oraz ograniczenia warunków ponownego wykorzystywania.

4.4.1. Przejrzystość

Jedną z podstawowych zasad ponownego wykorzystywania informacji sektora publicznego jest przejrzystość. Z reguły tej wynikają ściśle określone w ustawie obowiązki, które powinien spełnić podmiot zobowiązany do udostępnienia informacji sektora publicznego w celu ponownego wykorzystywania. Prawidłowa realizacja obowiązków informacyjnych ma istotne znaczenie zarówno z perspektywy potencjalnego użytkownika informacji, jak podmiotu udzielającego informację. Wpływa ona bowiem na pewność prawną korzystających z informacji, jak i może zredukować zapytania kierowane do podmiotów publicznych.

[474] Zob. *D. Sybilski*, Warunki ponownego wykorzystywania informacji sektora publicznego „Informacja w administracji publicznej" 2017, nr 4, s. 52-56.

Niewywiązanie się przez podmiot zobowiązany z obowiązków informacyjnych może rodzić skutki prawne[475].

Z brzmienia art. 11 ust. 1 wynika sposób realizacji zasady przejrzystości. Jest nim obowiązkowe wprowadzenie w menu przedmiotowym strony BIP zakładki o nazwie „ponowne wykorzystywanie". W zakładce tej bezwzględnie powinny być zamieszczone informacje dotyczące warunków i opłat za ponowne wykorzystywanie oraz środków prawnych przysługujących wnioskodawcy w przypadku odmowy wyrażenia zgody na ponowne wykorzystywanie oraz o prawie do sprzeciwu od oferty. Z kolei obowiązek publikacji tzw. umowy na wyłączność wraz z informacjami jej dotyczącymi uwarunkowany będzie faktem zawarcia przez dany organ tego rodzaju umowy.

W kontekście zasady przejrzystości należy przypomnieć, że brak poinformowania o warunkach rodzi skutki prawne. Brak bowiem informacji o warunkach ponownego wykorzystywania informacji udostępnionych w BIP (lub w centralnym repozytorium) należy w myśl art. 11 ust. 4 UPW uznać za domniemanie zgody na bezwarunkowe ponowne wykorzystywanie tak udostępnionych informacji przez każdego zainteresowanego niezależnie od celu dalszej eksploatacji.

Z kolei realizując zasadę przejrzystości w odniesieniu do opłat podmiot zobowiązany powinien w BIP podać informację o wysokości opłat za ponowne wykorzystywanie, a w tym:
– podstawie obliczania opłat;
– czynnikach, które będą brane pod uwagę przy rozpatrywaniu nietypowych wniosków o ponowne wykorzystywanie i które mogą mieć wpływ w szczególności na koszt lub czas przygotowania lub przekazania informacji.

Za dobrą praktykę można uznać podawanie przez podmiot zobowiązany w BIP kosztów nośnika na którym informacja może być przekazana (np. płyta CD, DVD, pamięć USB i in.). Użytkownik we wniosku zgodnie z art. 21 ust. 3 UPW powinien wskazać sposób i formę przekazania informacji, zatem wiedza na temat potencjalnych kosztów już na etapie formułowania wniosku pozwala użytkownikowi zracjonalizować swoje oczekiwania.

Odrębności dotyczą podmiotów zobowiązanych będących muzeami państwowymi lub samorządowymi. Instytucje te powinny podać informację o czynnikach, które są brane pod uwagę przy ustalaniu nakładanych opłat za ponowne wykorzystywanie. Wynika to z tego, że muzea zgodnie z art. 18 w przypadku udostępniania lub przekazywania ISP do ponownego

[475] Zob. *D. Sybilski*, Obowiązki informacyjne podmiotu zobowiązanego do udostępnienia informacji w celu ponownego wykorzystywania, „Informacja w administracji publicznej" 2018, nr 1, s. 48 i nast.

wykorzystywania w celach innych niż niekomercyjne o charakterze badawczym, naukowym lub edukacyjnym mogą nałożyć opłaty wyższe niż „standardowe". Maksymalne stawki opłat możliwe do nałożenia zostały określone w rozporządzeniu[476].

Obowiązek poinformowania o środkach prawnych należy uznać za spełniony, jeśli podmiot zobowiązany w BIP udostępni informacje o prawie do sprzeciwu oraz o środkach prawnych przysługujących w przypadku odmowy wyrażenia zgody na ponowne wykorzystywanie. W przypadku pierwszej kategorii chodzi o sytuację, w której wnioskodawca, który otrzymał ofertę zawierającą warunki ponownego wykorzystywania lub informację o wysokości opłat za ponowne wykorzystywanie, może w terminie 14 dni od dnia jej otrzymania złożyć sprzeciw z powodu naruszenia przepisów ustawy (art. 23 ust. 2 UPW). W przypadku otrzymania sprzeciwu podmiot zobowiązany, w drodze decyzji, rozstrzyga o warunkach ponownego wykorzystywania lub o wysokości opłat za ponowne wykorzystywanie (art. 23 ust. 3).

Druga kategoria informacji dotyczy środków prawnych po wydaniu decyzji o odmowie wyrażanie zgody na ponowne wykorzystywanie informacji sektora publicznego, czyli odwołania lub wniosku o ponowne rozpatrzenie sprawy (art. 127 KPA w zw. z art. 25 UPW). Zgodnie z obowiązującym od 1 czerwca 2017 r. stanem prawnym informacja o środkach prawnych przysługujących wnioskodawcy powinna również obejmować prawo do zrzeczenia się prawa do wniesienia odwołania wobec organu, który wydał decyzję (zgodnie z art. 127a KPA). W trakcie biegu terminu do wniesienia odwołania strona może zrzec się prawa do wniesienia odwołania wobec organu administracji publicznej, który wydał decyzję. Z dniem doręczenia organowi administracji publicznej oświadczenia o zrzeczeniu się prawa do wniesienia odwołania przez ostatnią ze stron postępowania, decyzja staje się ostateczna i prawomocna.

Zgodnie z wyrażoną w art. 9 zasadą niewyłączności podmiot zobowiązany, który udostępnia lub przekazuje ISP w celu ponownego wykorzystywania, nie może wprowadzać ograniczenia korzystania z tych informacji przez innych użytkowników. Jednak, gdy prawidłowe wykonywanie zadań publicznych wymaga ograniczenia korzystania z informacji sektora publicznego przez innych użytkowników, podmiot zobowiązany może zawrzeć z użytkownikiem umowę o udzielenie wyłącznego prawa do korzystania z tej informacji. Umowa taka podlega raz w roku ocenie przez podmiot zobowiązany co do dalszego istnienia

[476] Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego w sprawie maksymalnych stawek opłat za ponowne wykorzystywanie informacji sektora publicznego nakładanych przez muzea państwowe i muzea samorządowe z dnia 5 lipca 2016 r. (Dz.U. z 2016 r. poz. 1011).

powodów jej zawarcia. Jeżeli w wyniku oceny podmiot zobowiązany stwierdzi ustanie powodów jej zawarcia, niezwłocznie wypowiada umowę ze skutkiem natychmiastowym. Spełnienie obowiązku informacyjnego polegać będzie na publikacji w BIP w zakładacie „Ponowne wykorzystywanie" umowy o udzielenie wyłącznego prawa do korzystania z ISP (tj. jej odwzorowania cyfrowego) oraz informacji z nią związanych, tj. powody jej zawarcia oraz wyniki oceny zasadności obowiązywania umowy, o której mowa w art. 9 ust. 3 UPW.

4.4.2. Równe traktowanie

Ze wspomnianą powyżej zasadą jawności warunków ponownego wykorzystywania informacji (art. 11 UPW) koresponduje zasada niedyskryminacji (równego traktowania). Reguła ta stanowi, że udostępnienie lub przekazanie informacji sektora publicznego nie powinno odbywać się na warunkach, które wyeliminowałyby lub ograniczały konkurencję. Do takiego niekorzystnego zjawiska mogłoby dojść w przypadku oferowania przez podmiot zobowiązany zróżnicowanych warunków w podobnych okolicznościach wykorzystywania informacji. Dlatego też w art. 8 UPW sformułowano obowiązek stosowania jednolitych warunków ponownego wykorzystywania w porównywalnych sytuacjach. Przez porównywalne sytuacje należy rozumieć stany faktyczne lub prawne, które charakteryzują się takimi samymi okolicznościami, istotnymi z punktu widzenia stosowania danych norm prawnych. Zazwyczaj bowiem stany faktyczne lub prawne będą zróżnicowane do pewnego stopnia, jednakże z punktu widzenia zasady niedyskryminacji tylko niektóre różnice będą mogły stanowić podstawę dla różnego traktowania podmiotów uprawnionych w ramach dozwolonego różnicowania[477].

Zatem *a contrario* na gruncie art. 8 UPW możliwe będzie różnicowanie warunków wówczas, gdy sytuacje danych podmiotów uprawnionych nie będą porównywalne, a więc będą różnić się cechą istotną na tyle, że zasadne będzie odmienne ukształtowanie ich sytuacji[478]. Przepis nie precyzuje jednak, kiedy sytuacje podmiotów można uznać za porównywalne , jak i nieporównywalne. Pozostawienie podmiotom zobowiązanym luzu decyzyjnego w różnych kwestiach nie oznacza całkowitej dowolności w tym zakresie. Posiłkując się poglądem przyjętym w doktrynie prawa konstytucyjnego należy przyjąć, że konkretne odstępstwa od

[477] *M. Maciejewski*, Zasady udostępniania i przekazywania ISP w celu ponownego wykorzystywania [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 106.
[478] *Ibidem*, s. 107.

nakazu równego traktowania muszą zawsze znajdować podstawę w kryteriach racjonalności, proporcjonalności i sprawiedliwości dokonania takich zróżnicowań[479].

Ponadto, w przypadku gdy ponowne wykorzystywanie jest dokonywane przez użytkowników będących podmiotami wykonującymi zadania publiczne w ramach działalności wykraczającej poza realizację takich zadań, warunki ponownego wykorzystywania lub opłaty za ponowne wykorzystywanie określa się na takich samych zasadach jak w przypadku innych użytkowników.

4.4.3. Zakaz wyłączności

W art. 9 ust. 1 ustawy wprowadzono generalny zakaz zawierania umów na wyłączność, zgodnie z którym warunki ponownego wykorzystywania informacji sektora publicznego nie mogą wprowadzać ograniczenia korzystania z tej informacji przez innych użytkowników[480]. W myśl bowiem art. 12 dyrektywy 2019/1024 (art. 11 dyrektywy 2003/98/WE) ponowne wykorzystywanie jest otwarte dla wszystkich potencjalnych uczestników rynku, nawet jeżeli jeden lub kilku jego uczestników już wykorzystuje oparte na tych informacjach produkty o wartości dodanej. Umowy ani inne uzgodnienia między organami sektora publicznego lub przedsiębiorstwami publicznymi będącymi w posiadaniu dokumentów a stronami trzecimi nie mogą przyznawać praw wyłącznych.

Dzięki temu rozwiązaniu użytkownicy zainteresowani ponownym wykorzystywaniem mają co do zasady stale zagwarantowaną możliwość dostępu do informacji sektora publicznego. Celem zasady jest zatem zapewnienie konkurencyjności tworzonych produktów, usług czy aplikacji w oparciu o informacje sektora publicznego. Dzięki wyeliminowaniu konkurencji tylko jeden podmiot uprawniony mógłby oferować produkty oparte na danych informacjach. W efekcie maksymalizacja społecznej wartości uzyskiwanej z informacji sektora publicznego byłaby ograniczona przede wszystkim do korzyści jednego podmiotu[481].

Zasada nie ma jednak charakteru absolutnego. Zawarcie umowy wyłącznej jest jednak dopuszczalne wyjątkowo, w sytuacji gdy jest to niezbędne do prawidłowego wykonywania zadań publicznych; przy tym zaproponowano obowiązki informacyjne po stronie podmiotu zobowiązane związane w zawarciem umowy, która udziela wyłącznego prawa do korzystania

[479] *B. Banaszak,* Konstytucja Rzeczypospolitej Polskiej. Komentarz, Warszawa 2009, s. 184.
[480] Zakaz wyłączności bywa w literaturze nazywany również „zakazem monopolizacji" informacji. Zob. *M. Maciejewski*, Prawna regulacja ponownego wykorzystywania informacji publicznych [w:] *G. Sibiga (red.)*, Główne problemy prawa do informacji, s. 300-301.
[481] *M. Maciejewski,* Zasady udostępniania i przekazywania ISP, s. 109.

z tej informacji. Przez prawidłowe wykonywanie zadań publicznych należy rozumieć przede wszystkim skuteczność w wykonywaniu tych zadań, a więc możliwość osiągania określonego celu[482]. Przykładem takiego rodzaju sytuacji może być udzielenie prawa wyłącznego w związku z digitalizacją zasobów kulturowych[483].

4.4.4. Otwarte formaty

Zgodnie z art. 10 ust. 1 UPW podmioty zobowiązane, które udostępniają lub przekazują informacje sektora publicznego w celu ponownego wykorzystywania z użyciem systemów teleinformatycznych, są obowiązane do stosowania formatów danych oraz protokołów komunikacyjnych i szyfrujących określonych w przepisach wydanych na podstawie art. 18 pkt 1 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, jeżeli to możliwe w formacie przeznaczonym do odczytu maszynowego wraz z metadanymi. Przepisy te zapewniają jednolite formaty danych oraz protokoły komunikacyjne i szyfrujące dla informacji będących przedmiotem transferu.

Formaty danych, o których mowa w rozporządzeniu Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[484], spełniają kryteria określone dyrektywami o ponownym wykorzystywaniu, to jest „otwarty standard formalny" oraz „format otwarty".

„Format otwarty" oznacza format pliku, który nie jest powiązany z platformą oraz jest udostępniany obywatelom bez żadnych ograniczeń, które utrudniałyby ponowne wykorzystywanie dokumentów, zaś „otwarty standard formalny" oznacza standard określony w formie pisemnej, wyszczególniający specyfikacje wymogów dotyczących sposobu zapewnienia interoperacyjności oprogramowania[485].

Warto zauważyć, że dyrektywa 2019/1024 w art. 5 ust. 2 podkreśliła wagę otwartych formatów, formułując zasadą „otwartości w fazie projektowania" i „otwartości domyślnej".

Jak zostało udowodnione powyżej otwarty format jest warunkiem *sine qua non* uznania konkretnych zestawów informacji sektora publicznego za dane otwarte. Dlatego kluczowym dla realizacji prawa do ponownego wykorzystywania jest zapewnienie przez podmiot zobowiązany, że informacje udostępnianie do ponownego wykorzystywania spełniają kryteria

[482] *Ibidem.*
[483] Zob. art. 12 dyrektywy 2019/1024.
[484] Dz. U. poz. 526 oraz z 2014 r. poz. 1671.
[485] Art. 2 pkt 14 i 15 dyrektywy 2019/1024.

otwartości. W odniesieniu do formatu w jakim informacja jest utrwalona, a następnie udostępniona, chodzi w format umożliwiający automatyczne odczytywanie przez przeglądarkę lub system komputerowy. Przykładami takich formatów są XML, JSON, RDF, CSV. Formaty te ułatwiają dostęp i umożliwiają bardziej zaawansowane analizy dużej ilości informacji. Korzystanie w sposób zautomatyzowany z danych udostępnionych w formacie PDF, HTML czy w formie pliku tekstowego, jest utrudnione, ponieważ wymaga przetworzenia do ustrukturyzowanego formatu otwartego[486].

Z zasadą otwartych formatów koresponduje – wyrażone w art. 10 ust. 2 ustawy – wyłączenie obligatoryjności dodatkowego opracowania informacji sektora publicznego na potrzeby realizacji wniosku o ponowne wykorzystywanie. Dotyczy to wyłącznie sytuacji, w której dokonanie określonych we wniosku czynności wymaga podjęcia nieproporcjonalnych działań, przekraczającego proste operacje na informacji.

Zasada otwartych formatów została uznana przez *A. Piskorz-Ryń* jako element szerszej zasady dostępności informacji sektora publicznego do ponownego wykorzystywania. Zdaniem autorki z zasadą dostępności informacji związana jest z prowadzeniem przez organy sektora publicznego polityki proaktywnego dostępu dotyczącego dwóch aspektów: łatwego wyszukiwania i łatwego korzystania[487].

Łatwość wyszukiwania ma być zapewniona przez państwa członkowskie poprzez wprowadzenie wykazów najważniejszych zasobów dokumentacyjnych wraz z odpowiednimi metadanymi, dostępnych w Internecie i w formatach nadających się do odczytu maszynowego, oraz poprzez portale połączone z wykazami zasobów (art. 9 ust. 1 dyrektywy 2019/1024 oraz art. 9 dyrektywy 2003/98/WE). Ponadto Państwa członkowskie we współpracy z Komisją podejmują dalsze starania w celu uproszczenia dostępu do zbiorów danych, w szczególności przez stworzenie pojedynczego punktu dostępu oraz stopniowe udostępnianie odpowiednich zbiorów danych będących w posiadaniu organów sektora, jak również w odniesieniu do danych będących w posiadaniu instytucji unijnych, w formatach, które są dostępne, możliwe do znalezienia i możliwe do ponownego wykorzystywania za pomocą środków elektronicznych (ust. 2).

Z kolei łatwość wykorzystywania ma zostać zapewniona poprzez odpowiednią jakość danych, które powinny spełniać kryteria otwartości.

---

[486] Zob. Standardy otwartości danych. Standard prawny, Ministerstwo Cyfryzacji 2020, pkt 2.5., s. 26.

[487] *A. Piskorz-Ryń*, Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne, s. 235 i nast.

Na szczeblu krajowym zasada otwartych formatów, czy szerzej dostępności informacji sektora publicznego do ponownego wykorzystywania została zaadresowana Programie Otwierania Danych Publicznych, po drugie zaś poprzez prowadzenie portalu otwartych danych (CRIP).

4.4.5. Bezpłatność

W art. 16 ustawodawca sformułował generalną zasadę bezpłatnego udostępniania lub przekazywania informacji sektora publicznego w celu ich ponownego wykorzystywania[488]. Podmiot zobowiązany może jednak, zgodnie z art. 17 ustawy, nałożyć opłatę za ponowne wykorzystywanie, jeżeli przygotowanie lub przekazanie informacji w sposób lub w formie wskazanych we wniosku o ponowne wykorzystywanie wymaga poniesienia dodatkowych kosztów. Ustalając wysokość opłaty, o której uwzględnia się koszty przygotowania lub przekazania informacji w określony sposób i w określonej formie oraz inne czynniki, które będą brane pod uwagę przy rozpatrywaniu nietypowych wniosków o ponowne wykorzystywanie, które mogą mieć wpływ w szczególności na koszt lub czas przygotowania lub przekazania informacji. Łączna wysokość opłaty nie może przekroczyć sumy kosztów poniesionych bezpośrednio w celu przygotowania lub przekazania ISP w celu ponownego wykorzystywania w określony sposób i w określonej formie. Z treści tego przepisu wynika, że jedynie w przypadku przekazania informacji na wniosek możemy mieć do czynienia z ustaleniem przez podmiot zobowiązany opłaty. W przypadku udostępnienia informacji w trybie bezwnioskowym (BIP lub CRIP) będzie mieć zastosowanie ogólna zasada bezpłatności.

Odrębności od zasady kosztów bezpośrednich ustawodawca krajowy wprowadził dla szczególnej kategorii podmiotów zobowiązanych, tj. muzeów państwowych i samorządowych. Podmioty te w przypadku udostępniania lub przekazywania informacji sektora publicznego do ponownego wykorzystywania w celach innych niż niekomercyjne o charakterze badawczym, naukowym lub edukacyjnym mogą nałożyć opłaty wyższe niż ustalone na podstawie art. 17. Ustalając wysokość opłaty, o której mowa w ust. 1, uwzględnia się koszty gromadzenia, produkowania, reprodukowania, rozpowszechniania, ochrony i ustalania praw. Łączna wysokość opłaty nie może przekroczyć sumy tych kosztów wraz z rozsądnym zwrotem

[488] Szerzej na temat opłat zob. *A. Piskorz-Ryń*, Opłaty za ponowne wykorzystywanie informacji sektora publicznego w Unii Europejskiej [w:] *G. Szpor (red.),* Internet. Publiczne bazy danych i Big data, Warszawa 2014, s.149-170 oraz tej samej autorki: Opłaty za udostępnienie informacji publicznej do ponownego wykorzystywania, „Kwartalnik Prawa Publicznego" 2012, nr 3.

z inwestycji, jednak nie wyższym niż 5 punktów procentowych powyżej stopy referencyjnej Narodowego Banku Polskiego. Maksymalne stawki opłat za ponowne wykorzystywanie nakładanych przez muzea państwowe i muzea samorządowe, biorąc pod uwagę koszty oraz rozsądny zwrot z inwestycji, są określone rozporządzeniem Ministra Kultury i Dziedzictwa Narodowego[489]. Możliwość uwzględnienia rozsądnego zwrotu z inwestycji wynika wprost z art. 6 ust. 3 dyrektywy 2013/37/UE. Co istotne, krajowy prawodawca wprowadził w tym zakresie rozwiązanie korzystniejsze z perspektywy ponownego użytkownika, zrezygnował bowiem z możliwości uwzględnienia przedmiotowych kosztów dodatkowych również przez biblioteki i archiwa, do czego miał podstawy w przepisach dyrektywy. Z kolei definicja i sposób obliczania rozsądnego zwrotu z inwestycji został określony przez Komisję Europejską w Wytycznych w sprawie zalecanych licencji standardowych, zbiorów danych i opłat za ponowne wykorzystanie dokumentów (2014/C 240/01).

4.4.6. Ograniczenie warunków

Podmioty zobowiązane udostępniając informacje sektora publicznego za pośrednictwem systemów teleinformatycznych czy przekazując informacje na wniosek o ponowne wykorzystywanie mogą określić warunki dalszego korzystania z tych informacji. Nie mogą one jednak w nieuzasadniony sposób uniemożliwiać ponownego wykorzystywania. Precyzyjnie określone warunki chronią zarówno podmioty sektora publicznego udzielające informacji, jak i użytkownika informacji.

Podstawy prawne dla ustalania warunków ponownego wykorzystywania informacji zostały ujęte w rozdziale 3 UPW. Przepisy te mają zastosowanie przy udostępnianiu ISP za pośrednictwem systemów teleinformatycznych takich, jak BIP czy CRIP, jak i w sytuacji przekazywania ISP na wniosek o ponowne wykorzystywanie. Odstępstwa od ogólnych zasad dotyczących warunków będą mogły mieć miejsce w przypadku ponownego wykorzystywania zasobów bibliotek, archiwów i muzeów.

Podmiot zobowiązany udzielając informacji sektora publicznego tak w trybie wnioskowym jak i bezwnioskowym za pośrednictwem swojego systemu teleinformatycznego – zgodnie z art. 13 ust. 1 – może podjąć decyzję o nieokreślaniu warunków ponownego

[489] Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 5 lipca 2016 r. w sprawie maksymalnych stawek opłat za ponowne wykorzystywanie informacji sektora publicznego nakładanych przez muzea państwowe i muzea samorządowe (Dz.U. z 2016 r. poz. 1011).

wykorzystywania, wówczas użytkownik może wykorzystywać informację bez spełniania jakichkolwiek warunków.

Podjęcie takiej decyzji będzie uzależnione od rodzaju informacji. Udzielnie informacji sektora publicznego bez określenia warunków może dotyczyć tych informacji, które jednocześnie nie mają cech utworu lub przedmiotu praw pokrewnych w rozumieniu przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych lub stanowiących bazę danych w rozumieniu przepisów ustawy z dnia 27 lipca 2001 r. W praktyce mogą to być np. treści dokumentów, materiały urzędowe czy proste informacje dotyczące funkcjonowania urzędu czy wydatkowania środków publicznych.

W przypadku ISP dostępnych w BIP lub CRIP brak wyraźnej informacji o warunkach ponownego wykorzystywania należy uznać za zgodę podmiotu zobowiązanego na bezwarunkowe korzystanie (art. 11 ust. 4 UPW). W tym wypadku każdy zainteresowany wykorzystywaniem ISP nie musi składać wniosku do właściwego podmiotu zobowiązanego.

Artykuł 8 ust. 1 dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE stanowi, że organ sektora publicznego może zezwolić na ponowne wykorzystywanie dokumentów bez żadnych warunków lub może określić warunki, w uzasadnionych przypadkach w ramach licencji. Warunki te nie ograniczają niepotrzebnie możliwości ponownego wykorzystywania i nie są stosowane do ograniczania konkurencji. Motyw 26 preambuły dyrektywy 2013/37/UE podaje dwa przykłady tego rodzaju dopuszczalnych warunków: obowiązek podania źródła i wskazania, czy dokument został w jakikolwiek sposób zmieniony. Stanowi również, że wszelkie licencje powinny w każdym przypadku jak najmniej ograniczać ponowne wykorzystywanie, na przykład poprzez ograniczenie do wskazania źródła.

Polski ustawodawca transponując dyrektywę 2013/37/UE nie wprowadził w UPW podstawy dla stosowania standardowych otwartych licencji typu *Creative Commons* (CC). Nie ustanowił również – wzorem niektórych państw członkowskich UE – licencji krajowej. Powtórzono zaś z pewnymi modyfikacjami rozwiązanie funkcjonujące do 16 czerwca 2016 r. pod rządami dotychczasowych przepisów dotyczących ponownego wykorzystywania informacji publicznych zawartych w rozdziale 2a UDIP opierające się na koncepcji warunków ponownego wykorzystywania zawartych w ofercie.

W art. 14 ustawy określono katalog warunków ponownego wykorzystywania, jakie podmiot zobowiązany może ustanowić, udostępniając lub przekazując informację sektora publicznego do ponownego wykorzystywania.

Po pierwsze, warunek może dotyczyć obowiązku poinformowania o źródle, czasie wytworzenia i pozyskania informacji od podmiotu zobowiązanego. Ma on charakter

informacyjny, ponieważ jego spełnienie zapewnia potencjalnym użytkownikom i „dalszym użytkownikom" wiedzę co do statusu ponownie wykorzystywanych informacji[490]. Realizacja wymogu zapewnia możliwość sprawdzenia wiarygodności informacji oraz ich aktualności, a więc chroni końcowego użytkownika produktu, usługi czy jakiejkolwiek innej treści powstałej w wyniku ponownego wykorzystywania.

Kolejny warunek może obejmować obowiązek poinformowania o przetworzeniu informacji ponownie wykorzystywanej Spełnienie przez użytkownika drugiego obowiązku pozwala na zapewnienie wiarygodności informacji, którymi podmiot ten się posługuje. Jednocześnie ma na celu ochronę interesu podmiotu zobowiązanego, który udostępnia do ponownego wykorzystywania informację w określonej formie i o określonej treści, więc może oczekiwać, że przypisywane mu będzie wytworzenie takiej właśnie informacji[491].

Po trzecie, warunek może dotyczyć odpowiedzialności podmiotu zobowiązanego za udostępniane lub przekazywane informacje Zastrzeżenie tego warunku służy ograniczeniu odpowiedzialności podmiotu zobowiązanego. Chodzi o to, aby podmiot ten nie ponosił negatywnych konsekwencji wynikających z ponownego wykorzystywania pochodzących od niego zasobów informacyjnych[492].

Czwarty warunek dotyczący danych osobowych został wprowadzony ustawie w ramach nowelizacji służącej wykonaniu RODO. Ustawą z dnia 21 lutego 2019 r. zmieniającą sto sześćdziesiąt dwie ustawy w związku z zapewnieniem stosowania ogólnego rozporządzenia o ochronie danych znowelizowana również przepisy o ponownym wykorzystywaniu informacji sektora publicznego. Zmiana objęła również art. 14 polegającą na dodaniu w katalogu warunków ponownego wykorzystywania pkt 4 dotyczącego „informacji sektora publicznego zawierającej dane osobowe.".

Oznacza to, że podmiot zobowiązany określając warunki ponownego wykorzystywania informacji sektora publicznego, będzie mógł uwzględnić kwestie ochrony danych osobowych, przez co ochrona danych osobowych stanie się zobowiązaniem umownym (zagadnienie to szerzej omówiono w Rozdziale 9.3).

Zgodnie z art. 13 ust. 2 określenie przez podmiot zobowiązany warunków ponownego wykorzystywania jest obowiązkowe dla informacje sektora publicznego mających cechy utworu lub przedmiotu praw pokrewnych lub stanowiących bazę danych, do których

[490] *M. Sakowska-Baryła*, Warunki ponownego wykorzystywania ISP [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 130.
[491] *Ibidem*, s. 132.
[492] *Ibidem*, s. 133.

przysługują mu autorskie prawa majątkowe lub prawa pokrewne. W taki przypadku podmiot zobowiązany określa warunek dotyczący obowiązku poinformowania o nazwisku, imieniu lub pseudonimie twórcy lub artysty wykonawcy, jeżeli jest znany. Może również określić również inne warunki (ust. 3). Warunki te będą zdeterminowane zakresem praw przysługujących podmiotowi zobowiązanemu.

Odrębności w zakresie określenia warunków mogą dotyczyć zasobów, które są udostępniane lub przekazywane do ponownego wykorzystywania przez muzea państwowe lub samorządowe, biblioteki publiczne lub naukowe oraz archiwa tworzące państwową sieć archiwalną oraz innych jednostek organizacyjnych prowadzących działalność archiwalną w zakresie państwowego zasobu archiwalnego. Podmioty te, zgodnie z art. 14 ust. 2, mogą ustalić warunki ograniczające wykorzystywanie informacji:

1) w działalności komercyjnej lub na określonych polach eksploatacji, jeżeli dotyczą zbiorów o charakterze martyrologicznym oraz zawierają godło, barwy i hymn Rzeczypospolitej Polskiej, a także herby, reprodukcje orderów, odznaczeń lub odznak honorowych, odznak lub oznak wojskowych bądź innych odznaczeń;

2) do działalności niekomercyjnej, jeżeli są powiązane z obiektami objętymi roszczeniami osób trzecich lub niebędącymi własnością podmiotu zobowiązanego.

Przyjęcie takiego rozwiązania w pierwszym przypadku uzasadnione było ochroną zasobów, które stanowią część narodowego dziedzictwa kulturowego i często są ważnymi dla kraju symbolami[493]. W drugim wypadku, chodzi o zasoby o nieustalonym statusie, objętych roszczeniami prawno-własnościowymi osób trzecich, a także informacji sektora publicznego niebędących własnością podmiotu zobowiązanego, ale znajdujących się w czasowym depozycie.

Warto podkreślić, że odrębność przewidziana w przepisach UPW w możliwości określania dodatkowych warunków przez biblioteki, archiwa i muzea, jest wynikiem inicjatywy krajowego ustawodawcy i nie znajduje wprost zakotwiczenia w przepisach dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE.

Jak wskazano wyżej warunki ponownego wykorzystywania informacji sektora publicznego przekazanej na wniosek (art. 23 ust. 1 pkt 3 UPW), jak i udostępnionej w systemie teleinformatycznym stanowić będą (art. 12 ust. 1 i 2 UPW) ofertę. W przypadku przyjęcia przez wnioskodawcę oferty złożonej przez podmiot zobowiązany w odpowiedzi na wniosek albo

[493] *Ibidem*, s. 351.

rozpoczęcia ponownego wykorzystywania opatrzonej warunkami informacji udostępnionej w systemie teleinformatycznym, dochodzi do zawarcia umowy cywilnoprawnej.

Należy podkreślić, że w każdym przypadku bez względu na rodzaj informacji, formę jej udzielenia czy status podmiotu zobowiązanego określenie warunków nie może w sposób nieuzasadniony ograniczać możliwości ponownego wykorzystywania (art. 15 UPW). Z powodu posłużenia się przez ustawodawcę wyrażeniem nieostrym – tj. „w sposób nieuzasadniony" – każdy przypadek należy będzie rozpatrywać indywidualnie. Wydaje się, że zamysłem ustawodawcy było, aby określone warunki nie utrudniały czy wręcz uniemożliwiały w ogóle ponownego wykorzystywania danej informacji sektora publicznego poprzez zbyt restrykcyjne zastrzeżenia. Z jednej strony ustalenie warunków ma chronić interesy podmiotów uprawnionych oraz gwarantować pewność prawną dla użytkowników wykorzystujących dostępne informacje, z drugiej zaś nie może niweczyć celów ustawy, czyli jak najpełniejszego twórczego wykorzystania danych wytworzonych czy gromadzonych w sektorze publicznego w innowacyjnych produktach, usługach czy aplikacjach powstałych na ich podstawie.

Rozdział 5. Podstawowe zasady przetwarzania danych oraz wynikające z nich prawa i obowiązki

5.1. Podstawowe zasady przetwarzania danych osobowych - wprowadzenie

Przetwarzanie danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego musi odbywać się w zgodzie z zasadami przetwarzania danych osobowych wynikających z ogólnego rozporządzenia. Pomiędzy poszczególnymi zasadami zachodzą różnego rodzaju relacje i zależności, a żadnej z zasad nie należy analizować odrębnie w oderwaniu od pozostałych. Konieczne jest zatem opisanie podstawowych zasad przetwarzania danych osobowych i wynikających z nich uprawnień podmiotu danych, których korelatem są obowiązki administratora. Niemniej zagadnienie badania zgodności celów będące konsekwencję zasady ograniczenia celu ze względu na jego kluczowe znaczenie dla realizacji ponownego wykorzystywania informacji sektora publicznego zawierającej lub stanowiącej dane osobowe, zostanie szczegółowo omówiona w odrębnym poświęconym temu rozdziale.

Zasady przetwarzania danych osobowych zostały ujęte w art. 5 RODO. Wymienione w nim zasady mają charakter norm ogólnych zajmujących centralne miejsce w systemie norm ochrony danych osobowych, wyrażających podstawowe idee i założenia polityki europejskiej

wobec ochrony danych osobowych[494]. Zasadom tym przypisuje się nadrzędną moc w stosunku do pozostałych przepisów o ochronie danych osobowych, mają one charakter dyrektyw interpretacyjnych, zgodnie z którymi należy dokonywać wykładni poszczególnych przepisów[495]. Co istotne, zasady przetwarzania, nie są jedynie ogólnymi postulatami, ale mają charakter normatywny[496]. Statuują bowiem obowiązki, których adresatem jest administrator. Korelatem nałożonych z kolei na administratorów obowiązków zaliczanych do zasad przetwarzania danych osobowych są określone w rozporządzeniu sankcje za ich naruszenie, w tym administracyjne kary pieniężne[497].

Artykuł 5 RODO statuuje katalog następujących zasad dotyczących przetwarzania danych osobowych.

1) zasadę zgodności z prawem (legalności), rzetelności i przejrzystości;
2) zasadę ograniczenia celu;
3) zasadę minimalizacji danych;
4) zasadę prawidłowości (poprawności danych);
5) zasadę ograniczenia przechowywania;
6) zasadę integralności i poufności (bezpieczeństwa danych);
7) zasadę rozliczalności.

Zasady przetwarzania danych osobowych pełnią określone funkcje istotne z punktu widzenia praktyki stanowienia i stosowania prawa. Niewątpliwie zasady pełnią funkcję regulacyjną, ponieważ art. 5 określa zasady-normy, a również funkcję wytycznych legislacyjnych dla nowo projektowanych przepisów w zakresie ochrony danych osobowych, można je traktować zatem jako pewne idee przewodnie. Można również wskazać na funkcję dyrektyw interpretacyjnych, dokonując wykładni przepisów prawa– należy uwzględniać treść zasad, oraz funkcję dyrektyw kształtujących działalność organów władzy i administracji oraz podmiotów uczestniczących w obrocie gospodarczym w zakresie ochrony danych osobowych. Katalog zasad przetwarzania danych osobowych wraz z określeniem ich treści realizuje również funkcję systematyzującą, pozwalając na uporządkowanie nadrzędnych reguł rządzących przetwarzaniem danych[498].

---

[494] *A. Nerka*, Komentarz do art. 5, pkt 1 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie, Legalis/Wyd. 2018.
[495] *P. Fajgielski*, Zasady ogólne przetwarzania i ochrony danych osobowych [w:] *G. Goździewicz, M. Szabłowska (red.)*, Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych, Toruń 2008, s. 17.
[496] *P. Fajgielski*, op. cit., s. 17.
[497] Naruszenie podstawowych zasad przetwarzania danych zgodnie z art. 83 ust. 5 lit. a może skutkować administracyjną karą pieniężną w podwyższonej wysokości.
[498] *A. Nerka*, op. cit.

Porównując obecne brzmienie art. 5 ogólnego rozporządzenia z art. 6 dyrektywy 95/46/WE zatytułowanego „Zasady dotyczące jakości danych" wyznaczający ogólne zasady przetwarzania danych osobowych w porządku prawnym sprzed obowiązywania RODO[499] oraz wykonujące go polskie przepisy ustawy o ochronie danych osobowych z 1997 r. w art. 26, można zauważyć, że nowością w katalogu jest wprowadzenie zasady rozliczalności oraz wyraźne przyznanie zasadzie bezpieczeństwa danych rangi podstawowej zasady przetwarzania danych osobowych[500]. W pozostałym zakresie można podsumować, że w ogólnym rozporządzeniu w znacznej mierze przejęto rozwiązania znane z dyrektywy 95/46/WE. Treść motywów 9 i 10 RODO wprost wskazuje, iż zasady nakreślone w dyrektywie 95/46/WE pozostają aktualne, jednakże z uwagi na upowszechnianie się poglądu, iż ochrona praw związanych z przetwarzaniem danych osobowych jest znacznie zagrożona, należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie danych osobowych[501].

Zasady dotyczące przetwarzania danych osobowych nie mają charakteru bezwzględnego, mogą podlegać ograniczeniom określonym w art. 23 RODO w zakresie w jakim przepisy art. 5 odpowiadają prawom i obowiązkom przewidzianym w art. 12-22 rozporządzenia. Chodzi tu o: przejrzyste informowanie i przejrzystą komunikację oraz tryb wykonywania praw przez osobę, której dane dotyczą (art. 12 RODO); informacje podawane w przypadku zbierania danych od osoby, której dane dotyczą (art. 13 RODO); informacje podawane w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą (art. 14 RODO); prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO); prawo do sprostowania danych (art. 16 RODO); prawo do usunięcia danych ("prawo do bycia zapomnianym") (art. 17 RODO); prawo do ograniczenia przetwarzania (art. 18 RODO); obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania (art. 19 RODO); prawo do przenoszenia danych (art. 20 RODO); prawo do sprzeciwu (art. 21 RODO); zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie (art. 22 RODO). Zgodnie z art. 23 RODO, że wszelkie przewidziane w nim ograniczenia nie mogą naruszać istoty "podstawowych praw i wolności" oraz muszą być "w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym" służącym celom enumeratywnie wymienionym w art. 23 ust. 1 lit. a–j[502].

[499] W art. 6 prawodawca UE wymienił pięć zasad: rzetelność i legalność, celowość, proporcjonalność, prawidłowość oraz ograniczenie przechowywania, które państwa członkowskie powinny przestrzegać
[500] *P. Drobek* [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 326.
[501] *A. Nerka*, op. cit.
[502] Chodzi o następujące cele: a) bezpieczeństwo narodowe; b) obronę; c) bezpieczeństwo publiczne; d) zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych lub wykonywanie kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego

Należy podkreślić, że wszelkie odstępstwa od zasad ogólnych powinny być szczegółowo określone i jako wyjątki od nich interpretowane ścieśniająco[503].

Warto zauważyć, że art. 5 statuujący zasady przetwarzania danych osobowych, jednocześnie otwiera rozdział II ogólnego rozporządzenia zatytułowany „Zasady". Oznacza to, że zasady wymienione w art. 5 mają charakter podstawowy dla całej regulacji, lecz nie są jedynymi, które można odczytywać z przepisów rozporządzenia[504].

5.1.1. Legalność

W art. 5 ust. 1 lit. a RODO sformułowano zasadę zgodności z prawem (legalności). W myśl tego przepisu dane osobowe muszą być przetwarzane zgodnie z prawem. W doktrynie przyjmuje się, że nie chodzi jedynie o zgodność przetwarzania z przesłankami legalizującymi przetwarzanie wymienionymi w art. 6 i 9 RODO, jak i pozostałymi przepisami rozporządzenia, ale chodzi o całe *universum* norm prawnych (norm prawa materialnego i przepisów postępowania, przepisów rangi ustawowej i aktów wykonawczych)[505], w tym również zasad współżycia społecznego[506].

Stanowisko to potwierdza treść motywu 40 preambuły RODO, zgodnie z którym aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem: albo w niniejszym rozporządzeniu, albo w innym akcie prawnym Unii lub w prawie państwa członkowskiego, w tym musi się ono odbywać z poszanowaniem obowiązku prawnego, któremu podlega administrator, lub z poszanowaniem umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy. Jeśli chodzi o rodzaj aktu prawnego jako podstawy przetwarzania, niekoniecznie wymaga się przyjęcia aktu prawnego przez parlament. Taka podstawa prawna

i zapobieganiu takim zagrożeniom; e) inne ważne cele leżące w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważny interes gospodarczy lub finansowy Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu; f) ochronę niezależności sądów i postępowanie sądowe; g) zapobieganie naruszeniom zasad etyki w zawodach regulowanych, prowadzenie postępowań w takich sprawach, ich wykrywanie oraz ściganie; h) funkcje kontrolne, inspekcyjne lub regulacyjne związane nawet sporadycznie, ze sprawowaniem władzy publicznej w przypadkach, o których mowa w lit. a) – e) oraz g); i) ochronę osoby, której dane dotyczą, lub praw i wolności innych osób; j) egzekucję roszczeń cywilnoprawnych.

[503] *P. Fajgielski*, Zasady ogólne przetwarzania, s. 18.

[504] *P. Drobek* [w:] *E. Bielak-Jomaa, D. Lubasz (red.)*, RODO, s. 324.

[505] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 549.

[506] *A. Drozd*, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Warszawa 2007, s. 157.

lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających.

5.1.2. Rzetelność

Zasada ta, podobnie jak zasada legalności, została uregulowana w art. 5 ust. 1 lit. a. Wymaga ona, aby dane były przetwarzane rzetelnie, czyli uczciwie. Zasada rzetelności przy przetwarzaniu danych osobowych pełni podstawową funkcję, ponieważ stanowi punkt wyjścia dla sformułowania pozostałych zasad przetwarzania danych osobowych, jednocześnie obejmując je swoim zakresem[507]. Treść tej zasady jest bardzo pojemna, powinna być jednakże ujmowana jako nakaz uwzględniania przez administratorów interesów i uzasadnionych oczekiwań osób, których dane dotyczą, czyli w istocie wyważenia interesów stron[508]. Stąd też przyjmuje się, że zasada ta ma szerszy zakres od zgodności z prawem. Rzetelność przetwarzania danych osobowych rozumiana jest jako nakaz przetwarzania danych osobowych zgodnie z regułami uczciwości, rozumianymi jako poszanowanie interesów osób, których dane dotyczą, i niewykorzystywanie ich przymusowej sytuacji[509].

Zasada obejmuje również powinność dołożenia szczególnej staranności w procesie przetwarzania danych, mając przede wszystkim na uwadze ochronę interesów osób, których dane dotyczą[510]. Wymóg rzetelności przetwarzania można nadal odnosić do zasady szczególnej staranności w rozumieniu przepisów KC[511], bądź też do reguł staranności zawodowej[512].

Zasadę rzetelności przetwarzania danych osobowych należy interpretować dynamicznie, ponieważ ocena profesjonalnego podejścia do ochrony danych osobowych powinna uwzględniać zmiany technologiczne dotyczące stosowanych środków przetwarzania i zabezpieczania danych[513].

5.1.3. Przejrzystość

Treść w wyrażonej w art. 5 ust. 1 lit. a zasady przejrzystości można odczytać jako warunek dokonywania operacji przetwarzania danych osobowych w sposób transparentny dla

[507] *L.A. Bygrave*, Data Protection Law: Approaching Its Rationale Logic and Limit, Kluwer Law International 2002, s. 58.
[508] *A. Nerka*, op. cit., Komentarz do art. 5, pkt 3.
[509] *P. Litwiński (red.)*, op. cit., Komentarz do art. 5 pkt 4.
[510] *P. Fajgielski*, Zasady ogólne przetwarzania, s. 20 i n.
[511] *J. Barta, P. Fajgielski, R. Markiewicz*, Ochrona danych osobowych. Komentarz, Warszawa 2015, s. 468.
[512] *A. Drozd*, Ustawa, s. 152–153.
[513] *A. Nerka*, op. cit.

podmiotów danych[514]. Konsekwencją przedmiotowych wymogów jest rozszerzenie obowiązków informacyjnych, określonych w art. 12-15 (zob. Rozdział 5.2.2.).

Z zasady tej wynikają wymogi związane z zapewnieniem podmiotom danych jak najpełniejszej wiedzy na temat celu, zakresu i kontekstu przetwarzania danych, a także możliwości sprawowania kontroli nad własnymi danymi, co nie ogranicza się tylko do spełnienia obowiązków informacyjnych z art. 13 i 14 RODO, ale też zapewnienia świadomości w trakcie całego procesu przetwarzania. Zasada ta będzie stanowiła podstawę dla utrzymywania świadomości procesów przetwarzania po stronie osób, które dane dotyczą, aktualizacji informacji, formułowania zgód, instrukcji, procedur i polityk, a wreszcie realizacji praw podmiotów danych oraz wykonywania obowiązków notyfikacyjnych[515].

Wymóg przetwarzania danych osobowych w sposób przejrzysty szczególnie istotne znaczenie dla osoby, której dane dotyczą, jego korelatem są obowiązki informacyjne nałożonymi na administratora danych osobowych. Tylko wtedy można mówić o przejrzystości (transparentności) procesów przetwarzania danych, jeżeli osoba, której dane dotyczą, została należycie poinformowana o istotnych dla niej aspektach tego przetwarzania[516]. Na gruncie ogólnego rozporządzenia dyrektywa przejrzystego przetwarzania danych została skonkretyzowana w obowiązkach wynikających z art. 12 RODO, w szczególności poprzez wymóg przekazywania informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem (art. 12 ust. 1 RODO).

W doktrynie przyjmuje się, że obowiązki informacyjne wynikające z zasady przejrzystości mają dwa aspekty. Pierwszy ma charakter formalny i dotyczy wykonania obowiązku informacyjnego w odpowiednim czasie i formie, drugi zaś ma charakter materialny i wiąże się z podjęciem odpowiednich działań mających na celu zapewnienie, aby osoby których dane dotyczą, były poinformowane na tyle, by mogły zrozumieć istotne elementy i konsekwencje operacji przetwarzania danych osobowych[517].

Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku

[514] *A. Nerka*, op. cit., Komentarz do art. 5, pkt 4.
[515] *D. Lubasz*, Zasady dotyczące przetwarzania danych osobowych [w:] *D. Lubasz (red.)*, Meritum, s. 112.
[516] *P. Litwiński (red.)*, op. cit., Komentarz do art. 5, pkt 5.
[517] *P. Drobek*, Komentarz do art. 5 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 328.

do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem (motyw 39 preambuły RODO).

Wyjątkiem od zasady przejrzystości jest przetwarzanie danych w sposób niejawny, a więc nieinformowanie osób, których dane dotyczą o tym, że ich dane są przetwarzane. Jednak tego rodzaju działania, jako wyjątek od ogólnej zasady, powinny mieć wyraźną podstawę prawną i nie powinny być interpretowane rozszerzająco[518].

5.1.4. Ograniczenie celu

Artykuł 5 ust. 1 lit. b statuuje zasadę celowości, zwaną też zasadą związania celem. Jest to jedna z zasad zaliczanych do standardów ochrony danych osobowych oraz prywatności na poziomie międzynarodowym[519]. Zgodnie z jego brzmieniem dane osobowe musza 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 za niezgodne z pierwotnymi celami.

Przedmiotowy przepis należy odnieść do art. 6 ust. 1 lit. b dyrektywy 95/46/WE, zgodnie z którym państwa członkowskie zapewniają, aby dane osobowe były gromadzone do określonych, jednoznacznych i legalnych celów oraz nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem. Dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie jest uważane za niezgodne z przepisami (celami), pod warunkiem ustanowienia przez państwa członkowskie odpowiednich środków zabezpieczających.

Zasadzie celowości nadaje się znaczenie szczególne. Przyjmuje się, że jest ona pierwotna w stosunku do pozostałych zasad i wymogów określonych przepisami o ochronie danych osobowych, a także stanowi warunek wstępny ich realizacji. Zasada celowości jest bezpośrednio powiązana z zasadami państwa prawa i równoważenia władzy. W jej istotę jest

[518] *P. Fajgielski,* Komentarz, 2018, s. 146.
[519] Zob. art. 5 lit. b Konwencji Nr 108 Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2002 r. Nr 3, poz. 25), Zasada 9 Wytycznych Organizacji Współpracy Gospodarczej i Rozwoju (OECD) w zakresie ochrony prywatności i przepływu danych osobowych przez granice, art. 8 ust. 2 Karty Praw Podstawowych Unii Europejskiej z 26.10.2012 r. (Dz.Urz. C Nr 326 z 26.10.2012 r., s. 391–407).

wpisane zapobieganie nadużyciom spowodowanym wykorzystaniem danych w innych celach niż cel pierwotny, których z nim się nie da pogodzić, czyli tzw. *function creep* [520].

Z definicji administratora (art. 4 pkt 7 RODO) wynika, że co do zasady, o celu zbierania danych osobowych decyduje administrator danych. W doktrynie zauważa się, że jeżeli administrator danych jest podmiotem publicznym, wówczas cele przetwarzania danych osobowych wyznaczane są każdorazowo przepisami przyznającymi kompetencje do przetwarzania danych[521]. Jeżeli więc podmiot publiczny 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[522]. Zbierając natomiast dane osobowe bezpośrednio od osób, których dane dotyczą, administrator danych osobowych, w tym należący do sfery prawa publicznego, ma obowiązek zakomunikować cel zbierania danych osobom, których dane dotyczą.

W opinii Grupy Roboczej Art. 29 przyjmuje się, że zasada składa się z dwóch elementów: pierwszym jest zasada oznaczoności (określoności) celu wyrażona przez sformułowanie „dane osobowe muszą być zbierane dla określonych, jasnych i legalnych celów" (a w obecnie w myśl RODO: konkretnych, wyraźnych i prawnie uzasadnionych celach); drugim zaś zasada wykorzystania danych zgodnie z celem, czyi „nie były poddawane dalszemu przetwarzaniu w sposób niezgodny z tym celem"[523].

Zasada oznaczoności celu opiera się na założeniu, że zbieranie danych nie jest dopuszczalne, jeżeli nie zostały określone cele, dla których mają być one zebrane. Zakaz ten ma fundamentalne znaczenie dla zapewnienia zgodności operacji przetwarzania danych z pozostałymi zasadami ochrony danych osobowych, gdyż określenie celu lub celów zbierania danych w istocie determinuje możliwość zastosowania pozostałych zasad jakości danych, takich jak chociażby zasady adekwatności czy ograniczenia czasowego, ale także legalności[524]. Określenie celu stanowi też ramy, których nie mogą przekroczyć operacje przetwarzania danych osobowych. Konieczność określenia celu jest równoznaczna z zakazem zbierania danych na zapas dla przyszłych nieoznaczonych jeszcze celów, co wynika z założenia, że określenie celu może nastąpić najpóźniej w chwili zbierania danych[525].

[520] *P. Drobek*, Zasada celowości w dobie wielkich zbiorów danych (big data), „Monitor Prawniczy" 2014, nr 9 (dodatek), s. 22.
[521] *A. Drozd*, Ustawa, s. 150.
[522] *P. Litwiński* (red.), op. cit., Komentarz do art. 5 pkt 8.
[523] Zob. *Grupa Robocza Art. 29*, Opinion 03/2013 on purpose limitation, 02.04.2013, (WP 203), s. 4 i nast.
[524] *P. Drobek*, Zasada celowości, s. 24.
[525] *Ibidem*.

Cel zbierania danych powinien być zidentyfikowany w sposób jasny i konkretny, a także musi być wystarczająco szczegółowy, by można było określić, jakie operacje przetwarzania danych są nim objęte. Z tego względu należy unikać celów określonych zbyt ogólnie[526]. Stopień szczegółowości i konkretności będzie uzależniony od kontekstu zbierania danych[527]. W dużym stopniu to kontekst będzie determinował stopień szczegółowości celu[528]. Określenie celu wiąże się z zapewnieniem transparentności operacji przetwarzania danych osobowych i realizacji obowiązku informacyjnego wobec osób, których dane dotyczą[529].

Dane mogą być zbierane zarówno w jednym, jak i wielu celach, rodzi to zatem pytanie o sposób ich określenia. Niewątpliwie w odpowiedzi na nie pomocne będzie ustalenie, czy te cele są ze sobą powiązane, czy też nie. W przypadku celów powiązanych ze sobą wydaje się, że możliwe byłoby oznaczenie celu generalnego obejmującego je wszystkie[530].

Cel zbierania danych powinien być wyraźny, zatem musi być jednoznacznie wyrażony. Z tego względu nie jest dopuszczalne zbieranie danych dla celów ukrytych, zakamuflowanych bądź określonych jedynie w świadomości administratora[531].

Kolejnym elementem składowym zasady związania celem jest prawnie uzasadniony cel zbierania danych. Oznacza to zgodność celu zbierania danych z prawem rozumianym szeroko, nie tylko jako opartym na podstawie prawnej legalizującej przetwarzanie, ale całym systemie prawnym.

Z kolei zasada wykorzystania danych zgodnie z celem oznacza, że dane nie mogą być przetwarzane w sposób niezgodny z celami, dla których zostały zebrane. Co istotne, Grupa Robocza Art. 29 na gruncie art. 6 ust. 1 lit. b dyrektywy 95/46 wskazuje, że ustawodawca europejski nie posługuje się w nim rozróżnieniem na cele określone pierwotnie oraz wtórnie, lecz raczej odróżnia pierwszą operację przetwarzania danych, jaką jest ich zbieranie, od wszelkich innych następujących po niej. Prowadzi to do konkluzji, że każda operacja przetwarzania danych, następująca po ich zebraniu, bez względu na to, czy odbywa się w celach pierwotnie określonych, czy też w celach dodatkowych, będzie rozumiana jako dalsze przetwarzanie danych w rozumieniu art. 5 ust. 1 lit. b RODO. Oznacza to konieczność spełnienia testu zgodności przetwarzania takich danych z pierwotnie określonymi celami

[526] *Grupa Robocza Art. 29,* Opinion 03/2013, s. 12.
[527] *P. Drobek*, Zasada celowości, s. 24.
[528] *P. Drobek*, Komentarz do art. 5 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 331.
[529] *Grupa Robocza Art. 29,* Opinion 03/2013, s. 13.
[530] *P. Drobek*, Zasada celowości, s. 24.
[531] *Ibidem*, s. 25

zebrania danych, które zostały określone w art. 6 ust. 4 ogólnego rozporządzenia[532] (zob. Rozdział 8).

Niemniej w doktrynie przyjmuje się, że "pierwotny" cel przetwarzania danych to cel, który zakomunikowano osobie, od której pozyskano dane[533]. W motywie 33 preambuły do RODO wskazano sytuacje, w których w momencie zbierania danych nie da się w pełni zidentyfikować pierwotnego celu przetwarzania danych osobowych, jeżeli to przetwarzanie odbywa się na potrzeby badań naukowych. W takim przypadku osoby, których dane dotyczą, powinny móc wyrazić zgodę na przetwarzanie danych dla niektórych obszarów badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Osoby, których dane dotyczą, powinny móc wyrazić zgodę na przetwarzanie danych tylko na niektórych obszarach badań lub na pewne elementy projektów badawczych, o ile umożliwia to zamierzony cel.

Nie wyprzedzając dalszych rozważań poświęconych analizie testu zgodności celów, o którym mowa w art. 6 ust. 4 RODO, należy stwierdzić, że prawodawca unijny dopuścił dalsze („wtórne") przetwarzanie danych w dwóch przypadkach. Po pierwsze, dane mogą być przetwarzane dla tych samych celów, dla których zostały pierwotnie zebrane, po drugie zaś, dla innych celów, dla których nie są niezgodne z celami zebrania[534]. Powoduje to, że zasada wykorzystania danych zgodnie z celem nie może być rozumiana jako zakaz przetwarzania danych osobowych w innym celu niż cel, dla którego zostały zebrane, lecz jako zakaz przetwarzania danych w celu niezgodnym z pierwotnie określonym. Nie można zatem mówić o zasadzie niezmienności celu przetwarzania danych, ponieważ przepisy RODO nie zabraniają przetwarzania danych w celu innym niż cel, w którym dane zostały zebrane[535]. Zakaz dotyczy bowiem przetwarzania danych w celu niezgodnym z celem zebrania danych. Nieuprawnione również wydaje się przyjęcie, że administrator danych może przetwarzać dane osobowe jedynie w celu, dla którego zostały zgromadzone. Ogólne rozporządzenie nie formułuje bowiem zakazu przetwarzania danych w celach "innych", lecz jedynie zakaz przetwarzania danych w celach "niezgodnych" z pierwotnym celem przetwarzania[536]. Potwierdza to motyw 50 zd. pierwsze preambuły RODO, w którym stwierdzono, że przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, powinno być dozwolone wyłącznie w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały

[532] *P. Drobek*, Komentarz do art. 5 [w:] *E. Bielak-Jomaa, D. Lubasz,* RODO, s. 332-333.
[533] Zob. *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 551.
[534] *P. Drobek*, op. cit., s. 333.
[535] *P. Litwiński* (red.), op. cit., Komentarz do art. 5, pkt 9.
[536] *Ibidem.*

pierwotnie zebrane. Dla możliwości ponownego wykorzystywania danych osobowych istotne znaczenie może mieć zdanie kolejne motywu, „w takim przypadku nie jest wymagana odrębna podstawa prawna inna niż podstawa prawna, która umożliwiła zbieranie danych osobowych."

Z zasady ograniczenia celu przetwarzania danych osobowych wynika obowiązek administratora wykonania obowiązków informacyjnych wymienionych w art. 13 i 14 RODO obejmujących obowiązek przekazania informacji o celu przetwarzania danych, a także o podstawie prawnej w postaci zgody na przetwarzanie danych osoby, której dane dotyczą, i wymogiem, aby zgoda była oświadczeniem świadomym[537].

5.1.5. Minimalizacja danych

Z zagadnieniem celu przetwarzania danych osobowych nierozerwalnie związany jest problem określenia zakresu danych, które mogą być przetwarzane w określonym celu. Zasada ta, na gruncie art. 5 ust. 1 lit. c , przybiera postać zasady minimalizacji danych osobowych. W myśl zasady minimalizacji danych przetwarzanie danych osobowych powinno być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Stanowi to dalej idące ograniczenie w stosunku do zasady adekwatności danych osobowych – ograniczenie do danych niezbędnych oznacza takie ukształtowanie zakresu przetwarzania danych, aby przetwarzać tylko takie dane osobowe, bez których nie da się osiągnąć zamierzonego celu przetwarzania[538]. W literaturze prezentowany jest również pogląd, że wymóg niezbędności, należy odczytywać łącznie z wymogiem adekwatności i stosowności, który co powinno pozwolić na uwzględnienie okoliczności i dopuszczenie przetwarzania danych, które w istotny sposób mogą pomóc osiągnąć cele przetwarzania[539]. Zasada ta wprowadza kryteria limitacyjne ograniczające zbieranie i dalsze przetwarzanie danych osobowych, co prowadzi do ograniczenia zakresu przetwarzania danych opartego na kryterium niezbędności, czyli aby przetwarzać tylko takie dane osobowe, bez których nie da się osiągnąć zamierzonego celu przetwarzania[540]. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami (motyw 39 preambuły RODO).

[537] *Ibidem,* pkt 7.
[538] *P. Litwiński* (red.), op. cit., Komentarz do art. 5, pkt.
[539] Zob. *P. Fajgielski,* Komentarz, 2018, s. 148.
[540] *A. Nerka,* op. cit., komentarz do art. 5, pkt 6.

Realizacja zasady minimalizacji celu należy uwzględnić art. 11 RODO, zgodnie z którym jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają zidentyfikowania przez niego osoby, której dane dotyczą, administrator nie ma obowiązku zachowania, uzyskania ani przetworzenia dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do rozporządzenia. Jednakże ma to konsekwencje dla możliwości skorzystania przez osobę, której dane dotyczą, ze swoich praw, gdyż jeżeli administrator może wykazać, że nie jest w stanie zidentyfikować osoby, której dane dotyczą, to art. 15–20 nie mają zastosowania, chyba że osoba, której dane dotyczą, w celu wykonania przysługujących jej praw dostarczy dodatkowych informacji pozwalających ją zidentyfikować.

W doktrynie przyjmuje się, że zasada minimalizacji danych ma szczególne znaczenie nabiera dla przetwarzania danych osobowych w sektorze publicznym, zwłaszcza w toku prowadzonych postępowań administracyjnych. Zasadą na gruncie art. 51 Konstytucji RP jest bowiem niepozyskiwanie, niegromadzenie i nieudostępnianie informacji o obywatelach przez organy władzy publicznej. Przepisy rangi ustawy mogą wprowadzać wyjątki od tej zasady, przyznając organom władzy publicznej uprawnienie do gromadzenia informacji o obywatelach, ale wyłącznie w niezbędnym zakresie, a więc muszą spełniać wymóg proporcjonalności. Należy zatem uznać za spełniające zasadę minimalizacji danych przetwarzanie danych w toku postępowania administracyjnego, jeżeli zakres danych obejmuje dane, jakie są niezbędne dla rozstrzygnięcia sprawy, a jakie jednocześnie nie ingerują nadmiernie w prawo do prywatności informacyjnej osób, których dotyczą[541].

Realizacja zasady minimalizacji danych zakłada wdrożenie odpowiednich środków organizacyjnych i technicznych na każdym etapie przetwarzania danych, w tym w zakresie domyślnej ochrony danych, o którym mowa w art. 25 ust. 2 RODO. 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 ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.

[541] *P. Litwiński* (red.), op. cit., Komentarz do art. 5, pkt 15.

5.1.6. Prawidłowość

Artykuł 5 ust. 1 lit. d statuuje zasadę prawidłowości. Przepis stanowi, że dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

Wymóg zapewnienia prawidłowości danych osobowych wiąże się z obowiązkiem uwzględniania przez administratora danych znaczenia ewentualnej niedokładności danych z punktu widzenia osoby, której dane dotyczą, oceny wiarygodności źródła pozyskiwanych danych oraz stosowania trybu weryfikacji prawdziwości pozyskanych danych[542]. Naruszeniem tego nakazu jest zbieranie danych ze źródeł niewiadomego pochodzenia, które nie gwarantują poprawności danych osobowych[543].

W praktyce obowiązek ten oznacza, iż informacje wynikające z danych przetwarzanych przez administratora powinny być zgodne z prawdą, pełne (kompletne) oraz powinny odpowiadać aktualnemu (najnowszemu) stanowi rzeczy[544].

Merytorycznej poprawności danych nie można natomiast sprowadzać wyłącznie do nakazu regularnego przeglądu zbiorów danych pod względem ich aktualności[545]. Obowiązek ten przede wszystkim powinien znaleźć zastosowanie na etapie gromadzenia danych, a w jego wykonaniu, administrator zbierający dane powinien dołożyć szczególnej staranności celem zbierania danych merytorycznie poprawnych, a więc odpowiadających rzeczywistemu stanowi rzeczy[546].

W praktyce stosowania zasady pojawia się pytanie czy i w jakim zakresie obowiązek merytorycznej poprawności (prawidłowości) danych powinien być rozumiany jako obowiązek aktywnego działania administratora danych w celu zapewnienia poprawności przetwarzanych przez niego danych. RODO nie nakłada wprost tego rodzaju obowiązku na administratora danych osobowych, nie sposób go również wyprowadzić z ogólnego obowiązku rzetelności przetwarzania danych[547]. Administrator danych powinien wykonywać obowiązek prawidłowości danych w granicach „rozsądnych działań, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub

[542] *Ibidem,* pkt 16.
[543] *A. Drozd,* Ustawa, s. 153.
[544] Wyrok WSA w Warszawie z 02.04.2007 r., II SA/Wa 2328/06.
[545] *J. Barta, P. Fajgielski, R. Markiewicz,* Komentarz, 2004, s. 556.
[546] *P. Litwiński* (red.), op. cit., Komentarz do art. 5, pkt 16.
[547] *Ibidem,* pkt 17.

sprostowane”[548]. Przepisy nie konkretyzują kryteriów oceny rozsądnych działań administratora, jednakże można przypuszczać, że chodzi o podjęcie racjonalnych kroków w celu usunięcia lub sprostowania danych na wniosek osoby, której dane dotyczą, lub na podstawie posiadanych przez siebie informacji uzyskanych z wiarygodnych zewnętrznych źródeł[549].Odwołanie w tym kontekście do celów przetwarzania sprawia, że w istocie zasada ta dotyka nie kwestii treści danych rozumianej jako dane merytorycznie poprawne lub nie, ale zakresu danych rozumianego w kontekście zasady minimalizacji danych właśnie w odniesieniu do celu przetwarzania danych[550].

Korelatem zasady prawidłowości danych są uprawnienia osób, których dane są przetwarzane. W szczególności należy tu wymienić prawo do żądania niezwłocznego sprostowania nieprawidłowych danych oraz uzupełnienia danych niekompletnych (art. 16 RODO), a także prawo do usunięcia danych (art. 17 RODO).

5.1.7. Ograniczenie przechowywania danych

Zgodnie z art. 5 ust. 1 lit. e RODO dane powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą.

Zgodnie z motywem 39 preambuły RODO dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu.

[548] *Ibidem,* 5 pkt 18.
[549] *A. Nerka*, op. cit., komentarz do art. 5 pkt 7.
[550] *P. Litwiński* (red.), op. cit., Komentarz do art. 5, pkt 18.

Zasada ograniczenia przechowywania danych zabezpiecza osobę, której dane dotyczą, przed przetwarzaniem jej danych osobowych przez niczym nieograniczony okres ("w nieskończoność", a właściwie do śmierci osoby fizycznej). Punktem granicznym jest w takim przypadku osiągnięcie przez administratora danych zakładanego w chwili zbierania danych celu, w jakim pozyskał i przetwarzał dane osobowe[551].

Zasada wymaga zatem ustalenia okresów retencji danych lub dokonywania okresowego przeglądu danych pod względem ich niezbędności do osiągnięcia celu, dla którego są przetwarzane. Okres retencji należy bowiem ustalać w stosunku do każdego wyodrębnionego celu przetwarzania, który determinuje czas, w jakim dane mogą być przechowywane, a także dopuszczalny zakres danych przetwarzanych w danym okresie[552]. W tym kontekście trzeba mieć na uwadze art. 6 ust. 4 RODO, zgodnie z który może dojść do zmiany celu przetwarzania danych, okresy przechowywania mogą być określone w przepisach szczególnych[553].

5.1.8. Integralność i poufność

W myśl zasady integralności i poufności – wyrażonej w art. 5 ust. 1 lit. f – dane muszą 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.

Integralność danych oznacza właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany. Poufność danych to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom, zaś rozliczalność to właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi[554]. Poszukując wyjaśnienia i treści analizowanej zasady, należy wziąć pod uwagę motyw 39 wskazujący, że 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.

Zasada ta doznaje uszczegółowienia w art. 32 RODO, który w otwartym katalogu wymienia środki techniczne i organizacyjne, które wdrażają administrator i podmiot

[551] *P. Litwiński (red.)*, op. cit., Komentarz do art. 5, pkt 19.
[552] *A. Nerka*, op. cit., Komentarz do art. 5, pkt 8.
[553] *P. Drobek*, Komentarz do art. 5 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 340.
[554] *Ibidem*.

przetwarzający, aby zapewnić odpowiedni stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze, tj:

a) pseudonimizację i szyfrowanie danych osobowych;

b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;

d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

5.1.9. Rozliczalność

Zasada rozliczalności, o której mowa w art. 5 ust. 2 RODO, stanowi o tym, że administrator odpowiedzialny za przestrzeganie przepisów pozostałych zasad przetwarzania danych musi być w stanie to wykazać.

Przyjęty model regulacji w RODO oznacza to nową jakość w systemie ochrony danych osobowych, polegającą na proaktywnym podejściu administratorów do przetwarzania danych w celu wykazania realizacji zasady rozliczalności, czyli w gruncie rzeczy wszystkich zasad wyszczególnionych w art. 5 ust. 1. Prawodawca unijny kładzie nacisk na zmianę podejścia do ochrony praw i wolności podmiotów danych na podejście oparte na ryzyku (ang. *Risk-Based Approach*). Podejście umożliwia skoncentrowanie się na sytuacjach najwyższego ryzyka, przy jednoczesnym zapewnieniu odpowiedniego poziomu ochrony, a gdy to ryzyko jest niskie, nie wymaga wykorzystania wszystkich środków przewidzianych w RODO[555]. W praktyce oznacza to obowiązek wdrożenia i przestrzegania odpowiednich, a zarazem skutecznych środków w celu zapewnienia, że są realizowane obowiązki prawne w zakresie ochrony danych.

Prawodawca unijny statuując zasadę rozliczalności i przepisy ją wykonujące wzorował się na ustaleniach Grupy Roboczej, która w która wskazała, że zasada rozliczalności oznacza wdrożenie środków gwarantujących przestrzeganie przepisów o ochronie danych osobowych w związku z operacjami ich przetwarzania oraz sporządzenie dokumentacji, która wskazuje osobom, których dane dotyczą oraz organom nadzorczym, jakie środki podjęto, aby zapewnić

[555] *P. Drobek*, op. cit., s. 340.

przestrzeganie przepisów o ochronie danych osobowych[556]. Odpowiedzialność (*responsibility)* i rozliczalność (*accountability)* stanowią dwie strony tego samego medalu i są istotnymi składnikami dobrego zarządzania. Dostatecznie zaufanie można rozwinąć jedynie, gdy wykaże się, że odpowiedzialność skutecznie funkcjonuje w praktyce[557].

Zasada rozliczalności została uszczegółowiona w art. 24 RODO, który nakłada na administratora obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane. Administrator powinien uwzględnić charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Dla wykazania przez administratora przestrzegania ciążących na nim obowiązków mogą być stosowane zatwierdzone kodeksy postępowania, o których mowa w art. 40, lub zatwierdzone mechanizmy certyfikacji, o którym mowa w art. 42 RODO.

5.2. Prawa osoby, której dane dotyczą - wprowadzenie

W ogólnym rozporządzeniu – w stosunku do przepisów dyrektywy 95/46/WE – rozbudowany został katalog praw podmiotów danych, tj. uprawnień przysługujących osobom, których dane dotyczą, w związku z przetwarzaniem ich danych osobowych.

Na prawa podmiotów danych składają się:

1) uprawnienia informacyjne i dostępowe (art. 13–15),

2) korekcyjne, tj. prawo do sprostowania danych (art. 16),

3) zakazowe, tj.:

– prawo do usunięcia danych (prawo do bycia zapomnianym) (art. 17),

– prawo do ograniczenia przetwarzania (art. 18),

– prawo do przenoszenia danych (art. 20),

– prawo do sprzeciwu (art. 21) oraz

– prawo do niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa (art. 22).

Uprawnienia te można następnie podzielić w oparciu o kryterium aktywności podmiotu danych, tj. których realizacja jest uzależniona od zgłoszenia przez podmiot danych żądania, jak

[556] *Grupa Robocza Art. 29*, Opinia 03/2010 w sprawie rozliczalności, 13.07.2010 (WP 173), s. 9.
[557] *Ibidem, s. 8.*

i te, które muszą być realizowane przez administratora pomimo braku wniosku. W przeciwieństwie do określonego wprost w art. 13 lub 14 RODO obowiązku samodzielnego działania administratora, w realizacji którego następuje przekazanie podmiotowi danych informacji o przetwarzaniu jego danych osobowych, w przypadku praw określonych w art. 15–21 RODO osoba której dane dotyczą zmuszona jest do podjęcia działania i nawiązania kontaktu z administratorem lub podmiotem, co do którego przypuszcza, że jest on administratorem jego danych osobowych.

Istotną okolicznością realizacji uprawnień podmiotu danych osobowych wymienionych w rozdziale III RODO jest konieczność uprzedniej weryfikacji tożsamości żądającego realizacji przysługujących mu praw. Realizacja prawa podmiotu danych wobec osoby nieuprawnionej w każdym przypadku prowadzić będzie do naruszenia zasad ochrony danych osobowych oraz potencjalnego naruszenia praw i wolności podmiotów danych. Będzie tak z pewnością w każdym przypadku przekazania kopii danych osobowych w ramach realizacji prawa dostępu nieuprawnionemu. Jednak ryzyko wiąże się również z zastosowaniem się przez administratora na przykład do żądania ograniczenia przetwarzania danych osobowych złożonego przez podmiot inny niż osoba, której dane dotyczą. Realizacja żądania w zakresie usunięcia danych osobowych lub prawa do zapomnienia pochodzącego od osoby innej niż podmiot danych może z kolei prowadzić do naruszenia zasady integralności[558]. Jak wskazano powyżej obowiązek zachowania integralności danych osobowych oznacza ich ochronę przed m.in. przetwarzaniem polegającym na nieuprawnionym usunięciu danych. Z treści motywu 64 preambuły RODO wynika, że ciężar ustalenia, czy osoba żądająca dostępu jest do tego uprawniona, spoczywa na administratorze.

Podmiotowi danych – co do zasady – w procesie ponownego wykorzystywania jego danych osobowych przysługiwać będę wszystkie uprawnienia wymienione w rozdziale III RODO, choć możliwość skorzystania z każdego z praw uwarunkowana będzie podstawą legalizującą przetwarzanie danych, o której mowa w art. 6 ogólnego rozporządzenia. Pewne modyfikacje dotyczyć będą – na gruncie przepisów UPW – sposobu wykonania obowiązków informacyjnych przez administratora. Zagadnienie to zostanie omówione w Rozdziale 9. W dalszej części pracy – ze względu na zakres i przekrojowy charakter przepisów dotyczących uprawnień podmiotu danych – zostaną one przedstawione w zakresie w jakim jest to niezbędne dla tematyki pracy.

[558] *M. Susałko*, Realizacja żądań podmiotów danych – zagadnienia ogólne [w:] *D. Lubasz (red.)*, Meritum, s. 160.

5.2.1. Przejrzyste informowanie i przejrzysta komunikacja oraz tryb wykonywania praw przez osobę, której dane dotyczą

Artykuł 12 RODO wprowadza szczegółowe wymogi dotyczące przejrzystego informowania i przejrzystej komunikacji, nakładając na administratora obowiązek ułatwiania podmiotom danych realizacji przysługujących im praw. Stanowi on realizację zasady przejrzystości przetwarzania danych osobowych. Przepis ten reguluje proceduralne aspekty wykonywania praw osób, których dane dotyczą, o których mowa w rozdziale III RODO. Z tej perspektywy zwiększona przejrzystość w zakresie informacji przekazywanych osobom, których dane dotyczą, może doprowadzić do realnej i pozytywnej zmiany dla obywateli[559]. Znaczną część tego artykułu tworzą swoiste normy celowościowe czy wytyczne interpretacyjne, służące prawidłowej realizacji pozostałych przepisów rozdziału III oraz art. 34 RODO. Rolą art. 12 jest dookreślenie formy, trybu, kosztów, a zwłaszcza jakości działań podejmowanych przez administratora[560].

W przejrzystym informowaniu dostrzeżono remedium na dysparytet informacyjny pomiędzy administratorami i osobami, których dane są przetwarzane. Mechanizm ten ma służyć zapewnieniu osobom, których dane dotyczą, świadomości poprzez pełną, jasną i zrozumiałą wiedzę o relewantnych elementów dotyczących przetwarzania ich danych. Dzięki temu osoby, których dane dotyczą mogą dokonać oceny celu, zakresu i niezbędności przetwarzania ich danych osobowych i w konsekwencji podjąć świadomą decyzję w zakresie wyrażania zgody na takie przetwarzanie, czy też brak skorzystać z praw zakazowych[561].

Przekazywanie informacji osobie, której dane dotyczą, i prowadzenie z nią jakiejkolwiek komunikacji na podstawie art. 13–22 i art. 34 RODO powinno się odbywać w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Konieczność zapewnienia jasności przekazywanych informacji należy rozumieć jako konieczność posługiwania się, a więc niebudzącymi wątpliwości co do znaczenia. Z kolei wymóg zrozumiałości udzielonych informacji oznacza łatwość przyswojenia (zrozumienia) informacji. Wymóg używania prostego języka powinien skutkować nieużywaniem pojęć wywodzących się z języka technicznego, niezrozumiałych dla przeciętnego odbiorcy, nieposiadającego wiedzy specjalistycznej. Przejrzystość i łatwa dostępność w odniesieniu do

[559] *P. Litwiński* (red.), op. cit., Komentarz do art. 12, pkt 1.
[560] *K. Wygoda,* Komentarz do art. 12, pkt 1 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie, Legalis/Wyd. 2018.
[561] *D. Lubasz*, Prawa osób których dane dotyczą [w:] *D. Lubasz (red.)*, Meritum, s. 143.

formy przekazu to z kolei konieczność posługiwania się odpowiedniej wielkości czcionką, a także układem tekstu, który zapewnia szybki i łatwy dostęp do informacji (zakaz ukrywania informacji wśród innego rodzaju przekazu)[562].

Informacje mogą być przekazywane osobie, której dane dotyczą, zasadniczo w dowolnie wybranej formie – z wyjątkiem przekazania ich w formie ustnej. Przekazanie informacji w formie ustnej może bowiem nastąpić wyłącznie wtedy, gdy osoba, której dane dotyczą, tego zażąda i to wyłącznie pod takim warunkiem, że innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.

W art. 12 RODO wskazano również termin spełnienia przez administratora żądania podmiotu danych w zakresie realizacji przysługujących mu na mocy art. 15 – 22 ogólnego rozporządzenia. Powinno ono nastąpić bez zbędnej zwłoki, nie później jednak niż w terminie jednego miesiąca od dnia otrzymania żądania. Termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań pochodzących od tej samej osoby. W terminie miesiąca od otrzymania żądania administrator danych powinien poinformować osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeżeli natomiast administrator danych nie spełnia żądania pochodzącego od osoby, której dane dotyczą, powinien niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – poinformować o samym fakcie niespełnienia jej żądania, o powodach takiego stanu rzeczy oraz o możliwości wniesienia skargi do organu nadzorczego i o możliwości skorzystania z sądowej ochrony swoich praw (art. 12 ust. 3 i 4 RODO).

Przekazywanie informacji na podstawie art. 13 i 14 RODO, a także wszelkie działania podejmowane na podstawie art. 15–22 i art. 34 RODO, są wolne od opłat. Niemniej administrator ma możliwość pobierania opłat od osoby, której dane dotyczą, jeżeli pochodzące od niej żądania są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter. Mamy więc tutaj do czynienia ze swoistą konstrukcją nadużycia prawa do informacji[563]. Instrumentem służącym przeciwdziałaniu nadużycia prawa do informacji jest uprawnienie administratora do pobrania opłaty od osoby, której dane dotyczą, odmowa spełnienia żądania.

[562] *P. Litwiński* (red.), op. cit., Komentarz do art. 12, pkt 1.
[563] *Ibidem*, pkt. 9.

5.2.2. Uprawnienia informacyjne

Jednym z podstawowych obowiązków administratora danych, nałożonym przepisami o ochronie danych osobowych, jest obowiązek informowania osób, których dane dotyczą, o przetwarzaniu ich danych. Obowiązek ten nakłada na administratora danych tzw. obowiązek informacyjny, tj. obowiązek przekazania osobie, której dane dotyczą, pewnych informacji w sytuacji zbierania danych osobowych od osoby, której dane dotyczą (art. 13 RODO), jak i w sytuacji pozyskiwania danych osobowych nie od osoby, której dane dotyczą, czyli tzw. wtórnego zbierania danych (art. 14 RODO). Obowiązek informacyjny, polegający na konieczności przekazania osobie, której dane dotyczą, pewnych informacji istotnych z punktu widzenia procedury zbierania danych i ich dalszego przetwarzania, uznawany jest w doktrynie prawa za jedną z głównych gwarancji autonomii informacyjnej jednostki, w tym gwarancji dla wykonywania przyznanych jej uprawnień kontrolnych przetwarzania danych osobowych[564]. Obowiązek ten ma kluczowe znaczenie dla możliwości skorzystania z pozostałych uprawnień przez osoby, których dane dotyczą, ponieważ zazwyczaj tylko osoba poinformowana – mająca wiedzę na temat przetwarzania jej danych, może reagować na nieprawidłowości przy przetwarzaniu[565].

Obowiązkom informacyjnym po stronie administratora odpowiadają uprawnienia podmiotu danych. Mają one charakter niemajątkowy, osobisty, nie można ich zatem wyłączyć, ani też ograniczyć wolą stron, nie można się także ich zrzec czy przenieść na inną osobę[566].

Zakres obowiązków informacyjnych ciążących na administratorze danych osobowych w związku ze zbieraniem danych uregulowany został odmiennie w sytuacji zbierania danych od osób, których dane dotyczą, oraz w sytuacji, w której zbieranie danych następuje niebezpośrednio od tych osób. Istnieje jednak pewna grupa informacji, w stosunku do których obowiązek ich podania podmiotowi danych pozostaje wspólny w obydwu przypadkach (chodzi o analogiczne informacje wymienione w ust.1 art. 13 i 14 RODO). Do tej grupy należy zaliczyć:
1) informacje ujawniające tożsamość i dane kontaktowe administratora danych oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela,
2) gdy ma to zastosowanie – dane kontaktowe inspektora ochrony danych,
3) informacje o celach przetwarzania danych osobowych oraz podstawę prawną przetwarzania,

[564] *A. Drozd*, Ustawa, s. 133.
[565] *P. Fajgielski*, Obowiązek informacyjny w ogólnym rozporządzeniu o ochronie danych [w:] „Informacja w Administracji Publicznej" 2017, nr 1, s. 19.
[566] *P. Fajgielski*, Komentarz, 2018, s. 234.

4) informacje o prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią, jeżeli przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit. f RODO,
5) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
6) gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.

Nie jest jasne z jakich powodów prawodawca unijny informację o prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią, jeżeli przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit. f RODO, umieścił w pierwszej grupie informacji, podczas gdy na gruncie art. 14 RODO w drugiej grupie. Kolejną odrębnością jest występujący na gruncie art. 14 ust. 1 obowiązek poinformowania o kategoriach "odnośnych danych osobowych". Wydaje się, że sformułowanie to należy rozumieć jako informację o kategoriach danych osobowych zebranych przez administratora danych nie od podmiotu danych.

Dodatkowe obowiązki informacyjne właściwe dla zbierania danych w zależności od źródła pozyskania danych zostały nałożone na administratora danych w art. 13 ust. 2 oraz art. 14 ust. 2 ogólnego rozporządzenia. Przeanalizujmy obie sytuacje.

5.2.2.1. Informowanie przy gromadzeniu danych od osoby, której dane dotyczą

Obowiązek informacyjny przy zbieraniu danych osoby, której dane dotyczą, obejmuje także następujące kategorie informacji niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania:
a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
b) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych; c) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu

na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
d) informacje o prawie wniesienia skargi do organu nadzorczego;
e) informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
f) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Wymagane informacje powinny zostać przekazane osobie, której dane dotyczą, podczas zbierania danych osobowych. Przekazanie informacji powinno nastąpić przed zakończeniem zbierania danych osobowych, najpóźniej w chwili ich zebrania[567]. Jeżeli proces zbierania danych będzie rozciągnięty w czasie, tylko w wyjątkowych sytuacjach, do wykonania obowiązku informacyjnego może dochodzić wraz z zebraniem ostatnich kategorii danych[568]. Innymi słowy, obowiązek poinformowania ma charakter uprzedni w stosunku do pozyskania i utrwalenia danych[569].

Z punktu widzenia przedmiotu rozprawy szczególnie istotnego znaczenia nabiera art. 13 ust. 3 RODO, który przewiduje przypadek, w którym konieczne jest ponowienie obowiązku informacyjnego. Faktycznie nie mamy tu jednak do czynienia z informowaniem "podczas pozyskiwania danych osobowych". Z treści art. 13 ust. 3 RODO wynika, że obowiązek ten spełniany jest po akcie zbierania danych, czyli od momentu zbierania informowanie jest znacząco oddalone w czasie. Jeżeli bowiem administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, na gruncie analizowanego przepisu przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2. Oznacza to, że zmieniając lub rozszerzając cel przetwarzania danych osobowych, administrator musi liczyć się z koniecznością ponowienia obowiązku informacyjnego tyle tylko, że w zakresie ograniczonym do "stosowanych" informacji z art. 13 ust. 2. Oznacza to, że określenie, jakie informacje są stosowne, zależeć będzie od konkretnej sytuacji, a w zależności od tego administrator będzie tak komponował informację, aby spełniała

[567] *A. Drozd*, Ustawa, s. 146.
[568] *P. Litwiński* (red.), op. cit., Komentarz do art. 13, pkt 21.
[569] *J. Łuczak*, Komentarz do art. 13 [w:] *E. Bielak – Jomaa, Lubasz D. (red.)*, RODO, s. 485.

ona kryterium zapewnienia podmiotowi danych przejrzystego i rzetelnego przetwarzania oraz odpowiedniej wiedzy o tym, na jakich warunkach się ono odbywa[570]. Wydaje się, że w kontekście zmiany celu przetwarzania danych takimi informacjami będą: informacja o okresie, przez który dane osobowe będą przechowywane, informacja o prawie cofnięcia zgody, jeżeli przetwarzanie odbywa się na podstawie zgody, oraz informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, jeżeli takowe występuje[571].

Jedyny wyjątek od obowiązku informacyjnego dotyczy sytuacji, w której osoba, której dane dotyczą, dysponuje już informacjami, które miałyby być jej przekazane (art. 13 ust. 4 RODO). Zwolnienie dotyczy jednak wyłącznie takiego zakresu informacji, jakie dana osoba już posiada, co może powodować w pewnych sytuacjach ograniczenie tego obowiązku tylko do poszczególnych kategorii informacji. Całkowite wyłączenie obowiązku informacyjnego możliwe jest wyłącznie w przypadku posiadania przez osobę, której dane dotyczą, wszystkich informacji wymaganych zgodnie z art. 13 RODO[572].

5.2.2.2. Informowanie przy gromadzeniu danych z innych źródeł

Nie wyprzedzając dalszych rozważań dotyczących ujawnienia danych osobowych w ramach informacji sektora publicznego, to właśnie w związku z ponownym wykorzystywaniem może dochodzić do konieczności realizacji przez użytkownika obowiązku informacyjnego, o którym mowa w art. 14 RODO.

Jak wskazano powyżej przepis nakłada na administratora danych obowiązek informacyjny w sytuacji pozyskiwania danych osobowych nie od osoby, której dane dotyczą, czyli tzw. wtórnego zbierania danych. "Wtórny" obowiązek informacyjny z reguły nie jest wtórny dla administratora, ponieważ spełnia on go po raz pierwszy. Wtórność jest związana z ponownym zbieraniem tych samych danych osobowych, w sytuacji gdy pomiędzy podmiotem danych a administratorem, który dane pozyskał, jest jakiś pośrednik, a czasami i łańcuch pośredników, z których każdy powinien w swym zakresie spełnić obowiązek informacyjny przy zbieraniu danych[573]. Przypadki wtórnego gromadzenia danych to sytuacje, w których źródłem danych nie jest osoba, którą identyfikują zbierane dane osobowe – źródłem danych

[570] *M. Sakowska-Baryła*, Komentarz do art. 13, pkt 27 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie, Legalis/Wyd. 2018.
[571] *P. Litwiński* (red.), op. cit., Komentarz do art. 13, pkt 26.
[572] *Ibidem*, pkt 27.
[573] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 14, pkt 1.

będą więc w szczególności inne osoby lub dokumenty, w tym zbiory danych ogólnie dostępne (wykazy, rejestry, spisy, książki telefoniczne)[574], jak również przypadki nabycia baz danych od poprzedniego administratora, przejścia zakładu pracy na nowego pracodawcę[575].

Dodatkowy zakres informacji w tym wypadku – na mocy art. 14 ust. 2 RODO – obejmuje:

a) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

b) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią;

c) informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

d) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

e) informacje o prawie wniesienia skargi do organu nadzorczego;

f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;

g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Dla omawianej tematyki szczególnie istotny jest element wymieniony w lit. f. Źródło danych powinno być rozumiane jako wskazanie bądź innego administratora danych, który dane udostępnił, bądź też innego źródła danych, np. spisu lub rejestru. Konieczne jest takie określenie administratora, będącego źródłem danych, by możliwy był z nim kontakt. Jest to uzasadnione koniecznością umożliwienia osobie, której dane dotyczą, skorzystania z przysługujących jej uprawnień względem administratora danych osobowych, np. wycofania zgody lub wyrażenia sprzeciwu wobec przetwarzania danych[576]. Niezbędne jest więc podanie

[574] *P. Litwiński (red.)*, op. cit., Komentarz do art. 14, pkt 1.
[575] *J. Łuczak*, op. cit., komentarz do art. 13, s. 495.
[576] *P. Litwiński* (red.), op. cit., pkt. 2.

pełnej nazwy i adresu tego administratora danych[577]. Wydaje się, że wobec brzmienia art. 14 ust. 2 lit. f RODO, jeżeli dane osobowe zostały pozyskane ze źródeł publicznie dostępnych, należy tę okoliczność wyraźnie wskazać, z podaniem tego źródła. W literaturze przedmiotu wskazuje się, że przedmiotowy obowiązek należy wypełnić również w przypadku wtórnego pozyskania danych z rejestrów publicznych prowadzonych przez organy władzy publicznej, z których informacje są zgodnie z prawem udostępniane, w tym publikowane w Internecie, takich jak choćby KRS, elektroniczne księgi wieczyste, CEIDG. Zdaniem *M. Sakowskiej-Baryły* jeśli administrator pozyskuje dane z takich właśnie źródeł, nie może czuć się zwolniony z analizowanego tu obowiązku informacyjnego tylko z tej racji, że dane zostały upublicznione, a on je z tego publicznego źródła pozyskał. „Czym innym bowiem jest prowadzenie na warunkach określonych w przepisach prawa publicznych rejestrów, czym innym natomiast wtórne pozyskiwanie danych osobowych zawartych w tych rejestrach do celów niewiadomych podmiotowi danych[578]". Jednocześnie trzeba mieć na uwadze, że prawidłowa realizacja obowiązków informacyjnych oraz kontrola tego obowiązku może być skutecznym środkiem zapobieżenia niebezpieczeństwom związanym z profilowaniem osoby fizycznej, w tym tworzenia profili predykcyjnych w oparciu o źródła danych powszechnie dostępne[579].

W mojej opinii problem ten jest złożony w szczególności w kontekście faktycznych możliwości jego realizacji przez użytkownika ponownie wykorzystującego dane osobowe. Ponadto w kontekście modyfikacji sposobu i zakresu spełnienia przedmiotowego obowiązku informacyjnego w przepisach UPW kwestia ta zasługuje na rozwinięcie (zob. Rozdział 9).

W tym miejscu należy jedynie przytoczyć treść art. 14 ust. 5 RODO, który przewiduje okoliczności, w których pomimo pozyskania danych osobowych z innego źródła niż osoba, której dane dotyczą, administrator zwolniony jest z realizacji wtórnego obowiązku informacyjnego:

a) osoba, której dane dotyczą, dysponuje już tymi informacjami;

b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator

[577] Zob. wyr. NSA z 13.7.2004 r., OSK 507/04; por. też *A. Drozd*, Ustawa, s. 153–154.
[578] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 14, pkt 5.
[579] Zob. m.in. *W. R. Wiewiórowski*, Założenia wstępne dla zrównoważonego przetwarzania informacji, s. 33 i nast.

podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;
c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub
d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Przepisy RODO wskazują termin w jakim obowiązek informacyjny powinien zostać zrealizowany. Mianowicie w myśl art. 14 ust. 3 informacje, o których mowa w ust. 1 i 2, administrator podaje w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych; jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

Podobnie jak to miało miejsce w art. 13 ust. 3, także w przypadku wtórnego pozyskania danych, jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.

5.2.3. Prawo dostępu do danych

Źródłem prawa dostępu do danych osobowych jest wyrażona w art. 5 ust. 1 lit. a zasada przejrzystości. Poinformowanie o okolicznościach przetwarzania danych osobowych zmniejsza niepewność podmiotu danych co do tego, w jaki sposób konkretny administrator dysponuje jej sferą informacyjną, w jakim stopniu jest ona jemu znana, jakiemu celowi służy korzystanie z zasobu informacji dotyczących danej osoby, jak przetwarzanie może się kształtować w pewnej perspektywie czasowej, czy też jakie uprawnienia dla takiej osoby wiążą się z tym, że podmiot przetwarza jej dane osobowe[580]. Prawo dostępu do danych – zgodnie z art. 15 RODO – obejmuje uprawnienie do uzyskania od administratora potwierdzenia, czy

[580] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 15, pkt 2.

przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji:

a) cele przetwarzania;

b) kategorie odnośnych danych osobowych;

c) informacje o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;

d) w miarę możliwości planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

e) informacje o prawie do żądania od administratora sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;

f) informacje o prawie wniesienia skargi do organu nadzorczego;

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle;

h) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Rezultatem wykonania prawa dostępu do danych osobowych powinno być udzielenie osobie, której dane dotyczą, żądanych przez nią informacji. Zgodnie z art. 12 ust. 3 RODO udzielenie informacji powinno nastąpić bez zbędnej zwłoki, nie później niż w terminie miesiąca od otrzymania żądania.

Elementem prawa dostępu do danych osobowych jest uprawnienie osoby, której dane dotyczą, do otrzymania od administratora danych kopii danych osobowych. Uprawnienie to należy odróżnić od tzw. prawa do przenoszenia danych osobowych. Treścią prawa do przenoszenia danych osobowych jest bowiem prawo do otrzymania danych w ustrukturyzowanym, powszechnie używanym formacie, nadającym się do odczytu maszynowego oraz prawo przesłania tych danych innemu administratorowi, podczas gdy prawo dostępu do danych ogranicza się do otrzymania danych przez osobę, której dane dotyczą.

W wyniku realizacji prawa dostępu do danych osobowych, podmiot danych, może uzyskać kopię danych osobowych we wskazanym przez siebie formacie. Jeżeli jednak zwraca się ona o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną. Jak się wydaje, w takim przypadku dane powinny

zostać przesłane przy użyciu tego samego środka porozumiewania się, przy użyciu którego osoba, której dane dotyczą, skierowała swoje żądanie do administratora danych (art. 15 ust. 4).

5.2.4. Prawo do sprostowania danych

Na mocy art. 16 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia. Uprawnienie to znajduje swoje zakotwiczenie w zasadzie prawidłowości i minimalizacji danych. Prawo to zalicza się do uprawnień korekcyjnych, jego istotą są dwa uprawnienia podmiotu danych: sprostowania nieprawidłowych danych osobowych oraz uzupełnienia niekompletnych danych osobowych.

Administrator danych zobowiązany jest do spełnienia żądań tej osoby wyłącznie w sytuacji, gdy wnioskodawca wykaże, że dane osobowe dotyczące jego osoby są nieprawidłowe lub niekompletne. Stan wykazania zaistnienia okoliczności wymienionych w art. 16 RODO powinien istnieć pomiędzy administratorem danych a podmiotem danych, podmiot osoba, której dane dotyczą powinna udowodnić administratorowi danych, że ten przetwarza dane nieprawidłowe lub niekompletne[581].

Co istotne, prawo do sprostowania nie jest wykonywane w wyniku obowiązku prawnego nałożonego na podmiot danych, a dobrowolnie – w przypadku prawnie występującego nakazu spoczywającego na osobie, której danej dotyczą, mielibyśmy do czynienia z realizacją obowiązku uaktualnienia, uzupełnienia czy nawet poprawienia danych błędnych, a nie sprostowaniem danych, w rozumieniu art. 16 RODO[582].

Niezbędną przesłanką realizacji prawa do sprostowania danych jest ich nieprawidłowość. Za dane nieprawidłowe uważa się dane, które nie odpowiadają rzeczywistemu stanowi rzeczy. Dane nieprawidłowe to inaczej dane nieprawdziwe. Prawidłowość danych osobowych powinno się oceniać z perspektywy osoby, której dane dotyczą, i badać zgodność tych danych z rzeczywistością, którą opisują. Stan prawidłowości lub nieprawidłowości danych osobowych podlega ocenie obiektywnej w odniesieniu do osoby, której dane dotyczą[583].

[581] *P. Litwiński (red.)*, op. cit., Komentarz do art. 16, pkt 3.
[582] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 16, pkt 1.
[583] *P. Litwiński (red.)*, op. cit., pkt 4.

Z kolei, osoba, której dane dotyczą, może wystąpić z żądaniem uzupełnienia danych wtedy, kiedy są one niekompletne. Dane niekompletne to dane prawidłowe, ale niepełne co do swojego zakresu. Kompletność danych osobowych powinno się oceniać z punktu widzenia celu przetwarzania danych, który w oparciu o zasadę minimalizacji danych osobowych wyznacza zakres przetwarzania danych. Stan kompletności lub niekompletności danych podlega ocenie obiektywnej, w odniesieniu do celu, w którym dane są przetwarzane[584].

5.2.5. Prawo do usunięcia danych (prawo do bycia zapomnianym)

Genezy prawa do bycia zapomnianym rozumianego jako zapewnienie użytkownikom Internetu skutecznego prawa do bycia zapomnianym w Internecie, tj. prawa do usunięcia swoich danych przez osoby fizyczne, jeśli wycofają swoją zgodę i nie ma innych zasadnych podstaw do zachowania tych danych[585], należy upatrywać m.in. wyroku TSUE z 13.5.2014 r. w sprawie C-113/12 *Google Spain SL v. Agencia de Proteccion de Datos*[586] oraz w wyroku z 9.3.2017 r w sprawie Manni, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*[587]. Zdaniem TSUE na gruncie sprawy C-113/12 osoba, której dane dotyczą, ma prawo do tego, aby dotycząca jej dana informacja nie była już powiązana z jej imieniem i nazwiskiem poprzez listę wyświetlającą wyniki wyszukiwania mającego za punkt wyjścia to imię i nazwisko. Osoba, której dane dotyczą, jest uprawniona do żądania od operatora wyszukiwarki internetowej, aby ten zablokował możliwość wyszukiwania określonych informacji dotyczących tej osoby. W ocenie Trybunału, to swoiste prawo do bycia zapomnianym ma swoje źródło w art. 7 i 8 KPP. Jednocześnie TSUE podkreślił, że w niektórych przypadkach, ze względu na rolę odgrywaną przez daną osobę w życiu publicznym, ingerencja w prawa podstawowe tej osoby jest uzasadniona nadrzędnym interesem osób korzystających z wyszukiwarek internetowych, polegającym na posiadaniu dostępu do danej informacji dzięki działaniu wyszukiwarki (zob. pkt 4 sentencji wyroku). W wyroku tym Trybunał stwierdził, że operator wyszukiwarki internetowej ma status administratora danych

[584] *Ibidem*, pkt 5.
[585] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów "Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku", s. 6
[586] Zob. m.in. *M. Czerniawski*, Glosa do wyroku TS z 13.5.2014 r., C-131/12, LEX 2015; *M. Wróbel*, Prawo do „bycia zapomnianym" – glosa – C-131/12, Monitor Prawniczy" 2017, nr 2, s. 107-112.
[587] Zob. *M. Romanowski, A.M. Weber-Elżanowska*, Prawo członka organu spółki kapitałowej do „bycia zapomnianym" - glosa do wyroku Trybunału Sprawiedliwości z dnia 9 marca 2017 r., C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatore Manniemu, „Europejski Przegląd Sądowy" 2017, nr 8, s. 40-45.

osobowych w stosunku do informacji zawierających dane osobowe, które to informacje są przez operatora wyszukiwarki lokalizowane, indeksowane w sposób automatyczny, czasowo przechowywane i udostępniane internautom w sposób uporządkowany zgodnie z określonymi preferencjami. Na gruncie tego wyroku prawo do bycia zapomnianym, jest uprawnieniem, które może być wykonywane w stosunku do wyszukiwarek internetowych. Prawo to nie dotyczy informacji źródłowej, której usunięcie lub nieusunięcie nie ma wpływu na problem ingerencji w wyniki wyszukiwania[588].

Z kolei w drugiej przytoczonej sprawie C-398/15 TSUE stwierdził, że w przypadku przetwarzania danych osobowych w rejestrze spółek pierwszeństwo w stosunku do ochrony prywatności i danych osobowych ma konieczność ochrony interesów osób trzecich względem spółek akcyjnych i spółek z ograniczoną odpowiedzialnością oraz zapewnienia pewności prawa, uczciwości transakcji handlowych, a więc i sprawnego funkcjonowania rynku wewnętrznego. Zadaniem Trybunału prawo Unii nie przyznaje osobom, których dane są przetwarzane w rejestrze spółek, swoistego prawa do bycia zapomnianym rozumianego jako możliwość domagania się ograniczenia dostępu do figurujących w rejestrze i dotyczących tych osób danych osobowych.

Zgodnie z art. 17 ust. 1 RODO osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe.

Uprawnienie to można traktować jako rozwinięcie prawa do usunięcia danych, na podstawie art. 12 lit. b dyrektywy 95/46/WE, którego odpowiednikiem w prawie krajowym stanowił art. 32 ust. 1 pkt 6 UODO1997. Pewną nowością może z kolei być obowiązek informacyjny (prawo do bycia zapominanym) sformułowany w art. 17 ust. 2 RODO, zgodnie z którym 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. Mamy tu zatem do czynienia ze sformułowanym wprost obowiązkiem powiadomienia przez administratora nie tylko osób trzecich, którym dane zostały ujawnione, ale także administratorów, którzy uzyskali dane w inny sposób (tj. z innego źródła niż administrator, na którym ciąży obowiązek poinformowania)[589].

[588] *P. Litwiński (red.)*, op. cit., Komentarz do art. 17 pkt 3.
[589] *M. Czerniawski*, Komentarz do art. 17 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 524.

Korelatem przedmiotowego uprawnienia jest zatem obowiązek usunięcia danych przez administratora oraz obowiązek poinformowania innych administratorów o żądaniu usunięcia danych.

Co istotne, na gruncie RODO nie zdefiniowano pojęcia usunięcia danych osobowych. Przepisy też nie rozwiewają również wątpliwości co do sposobu usunięcia danych ani nie zawierają wskazówek niezbędnych do rozwiązania problemów mogących pojawiać się w praktyce, np. dotyczących zgłoszenia żądania przez osobę o popularnym imieniu i nazwisku. Na gruncie UODO1997 przez usunięcie danych osobowych rozumiano zniszczenie danych osobowych (usunięcie bezpowrotne danych, jak również fizyczne unicestwienie nośników danych, tak by odtworzenie informacji na nich zapisanych nie było możliwe) oraz modyfikację danych osobowych, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Efektem pierwszego działania powinien być brak możliwości dalszego dokonywania jakichkolwiek operacji na tych informacjach, druga zaś czynność w praktyce odpowiada ona dokonaniu takich operacji na danych (np. usunięcie części informacji o charakterze osobowym, umożliwiających połączenie pozostałych informacji z konkretną osobą fizyczną), które spowodują ich anonimizację[590].

Po drugie, art. 17 ust. 2 RODO zobowiązuje administratora do przekazania innym administratorom informacji o żądaniu podmiotu danych, a więc stawia go w roli „aktywnego pośrednika", bowiem nakłada na niego obowiązek czynnego odszukania administratorów przetwarzających dane, których dotyczy żądanie usunięcia[591]. Co istotne w myśl motywu 66 preambuły RODO, aby wzmocnić prawo do "bycia zapomnianym" w Internecie, należy rozszerzyć prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o usunięciu wszelkich łączy do tych danych, w tym kopii tych danych, czyli kopii zapasowych.

Zakres obowiązku poinformowania innych administratorów jest ograniczony przez dostępną technologię, koszt realizacji obowiązku poinformowania, odwołanie do podejmowania rozsądnych działań w wykonaniu tego obowiązku.

Warunkiem skorzystania przez podmiot danych osobowych z przedmiotowego uprawnienia jest wystąpienie przynajmniej jednej z następujących okoliczności:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

---

[590] *P. Litwiński (red.)*, op. cit., Komentarz do art. 17 pkt 12.

[591] *M. Czerniawski*, Komentarz do art. 17 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 527.

b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;
c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;
d) dane osobowe były przetwarzane niezgodnie z prawem;
e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1.

W ust. 3 art. 17 sformułowano wyłączenia od obowiązku realizacji prawa do usunięcia danych i prawa do bycia zapomnianym, tj. nie mają one zastosowania, w zakresie w jakim przetwarzanie jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji; do wywiązania się z prawnego obowiązku wymagającego przetwarzania z mocy przepisów, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; ze względu interesu publicznego w dziedzinie zdrowia publicznego; do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (o ile prawdopodobne jest, uniemożliwi to lub poważnie utrudni realizację celów takiego przetwarzania) lub do ustalenia, dochodzenia lub obrony roszczeń.

Z punktu widzenia przedmiotu rozprawy szczególnego znaczenia nabiera pierwsza przesłanka. Administrator danych, który przetwarza dane osobowe upublicznione przez pierwotnego administratora tych danych, będzie więc mógł dane przetwarzać dalej, jeżeli otrzyma on informację o żądaniu usunięcia danych osobowych, ale w konkretnym przypadku będzie mógł wykazać, że przetwarzanie tych danych jest niezbędne do korzystania z prawa do wolności wypowiedzi i informacji[592]. Przepis ten znajduje oparcie w przywołanym wyroku w sprawie C-131/12, w którym Trybunał uznał, że "usunięcie linków z listy wyników może, w zależności od rodzaju wyszukiwanej informacji, oddziaływać na uzasadniony interes potencjalnie zainteresowanych uzyskaniem dostępu do tej informacji internautów, (…) należy dążyć do znalezienia punktu równowagi pomiędzy tym interesem a prawami podstawowymi, które przysługują tej osobie na podstawie art. 7 i 8 Karty. Choć niewątpliwie chronione na mocy

[592] *P. Litwiński (red.)*, op. cit., Komentarz do art. 20, pkt 12.

tych postanowień prawa osoby, której dotyczą dane, są również co do zasady nadrzędne wobec tego interesu internautów, to jednak równowaga ta może, w szczególnych przypadkach, zależeć od charakteru rozpatrywanych informacji i od tego, jak istotne są one dla prywatności osoby, której dane dotyczą, oraz dla publicznego interesu w dysponowaniu tą informacją, który to z kolei interes może być uzależniony w szczególności od roli odgrywanej przez tę osobę w życiu publicznym". W tym wypadku konieczne jest więc wzajemne wyważenie prawa do ochrony danych osobowych oraz prawa do wolności wypowiedzi i informacji[593].

5.2.6. Prawo do ograniczenia przetwarzania

Kolejnym uprawnieniem osoby, której dane dotyczą jest – sformułowane w art. 18 RODO – prawo do ograniczenia przetwarzania. Dla określenia jego zakresu kluczowym jest odwołanie się do definicji samego ograniczenia przetwarzania, które zgodnie z art. 4 pkt 3 ogólnego rozporządzenia oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania. Zatem ograniczenie przetwarzania danych osobowych polega na konieczności ograniczenia przetwarzania danych wyłącznie do ich przechowywania. Uprawnienie to polega na możliwości złożenia przez osobę, której dane dotyczą w stosunku do administratora żądania przechowywania danych osobowych w stanie niezmienionym i niewykonywania innych niż przechowywanie operacji przetwarzania. Prawo to rozpatrywane na tle pozostałych uprawnień podmiotu danych określonych w rozdziale III RODO traktować należy jako ich uzupełninie stanowiące gwarancję dla podmiotu danych, że administrator nie tylko czasowo nie będzie przetwarzał jego danych osobowych w ustalonych przez siebie celach, ale również nie dokona na danych żadnej operacji, która mogłaby zniweczyć możliwość wykonania innych praw podmiotu danych, np. prawa do przenoszenia danych, lub zniweczyć możliwość dochodzenia roszczeń przez podmiot danych w przypadku, gdy przetwarzanie dokonywane jest przez administratora niezgodnie z ogólnym rozporządzeniem[594].

Przetwarzanie danych wykraczające poza ich przechowywanie jest możliwe wyłącznie, jeżeli osoba, której dane dotyczą, wyraziła na to zgodę; w celu ustalenia, dochodzenia lub obrony roszczeń; w celu ochrony praw innej osoby fizycznej lub prawnej; z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego (art. 18 ust. 3 RODO).

[593] *Ibidem*.
[594] *M. Susałko* [w:] *D. Lubasz*, Meritum, s. 192.

Administrator danych osobowych jest zobowiązany do ograniczenia przetwarzania danych, jeżeli osoba, której dane dotyczą: kwestionuje prawidłowość danych osobowych, zgodnie z art. 16 RODO (w takim przypadku ograniczenie przetwarzania następuje automatycznie, na okres pozwalający administratorowi sprawdzić prawidłowość tych danych); sprzeciwia się usunięciu danych osobowych przetwarzanych niezgodnie z prawem, żądając w zamian ograniczenia ich wykorzystywania; zażąda od administratora danych zastosowania ograniczenia przetwarzania w stosunku do danych, które zgodnie z zasadą ograniczenia przechowywania danych powinny zostać usunięte (ale które są potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń przysługujących tej osobie lub wobec niej) lub został wniesiony sprzeciw wobec przetwarzania danych osobowych zgodnie z art. 21 ust. 1 RODO (w takim przypadku ograniczenie przetwarzania następuje automatycznie, na okres pozwalający administratorowi stwierdzić, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą, tj. na czas potrzebny do ustalenia, czy sprzeciw jest zasadny).

Jeżeli administrator danych ma zamiar uchylić ograniczenie przetwarzania danych, powinien przed tą czynnością poinformować o swoim zamiarze osobę, której dane dotyczą (art. 18 ust. 3 RODO).

5.2.7. Prawo do przenoszenia danych

Uprawnieniem osoby, której danej dotyczą uzupełniającym prawo dostępu do danych jest prawo do przenoszenia danych. Zgodnie z brzmieniem art. 20 ust. 1 RODO na prawo to w istocie składają się dwa uprawnienia podmiotu danych, tj.

- prawo otrzymania przez osobę, której dane dotyczą, w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, danych osobowych jej dotyczących, które dostarczyła administratorowi,
- prawo przesłania przez osobę, której dane dotyczą, danych osobowych jej dotyczących, które dostarczyła administratorowi, innemu administratorowi, bez przeszkód ze strony administratora danych.

Warunkiem skorzystania przez osobę, której dane dotyczą, z przedmiotowych uwapnień jest łączne spełnienie dwóch przesłanek:

- przetwarzanie danych odbywa się na podstawie zgody (art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO) lub w celu wykonania umowy (art. 6 ust. 1 lit. b RODO) oraz
- przetwarzanie danych odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe (art. 20 ust. 2).

W literaturze przedmiotu wskazuje się, że możliwość przeniesienia danych osobowych od jednego dostawcy usług do drugiego staje się szczególnie istotna w przypadku usług świadczonych w modelu tzw. chmury obliczeniowej (*cloud computing*). W takim przypadku prawo samego dostępu do treści danych wykazuje niewielką przydatność z punktu widzenia postulatu umożliwienia klientowi usług chmurowych zmiany dostawcy takich usług. Powstaje natomiast konieczność zapewnienia możliwości przeniesienia (migracji) danych przetwarzanych w ramach usługi od jednego dostawcy do drugiego, bo tylko w ten sposób można w praktyce umożliwić zmianę dostawcy usług[595]. Jednym z powodów, dla których podjęto inicjatywę reformy europejskiego prawa ochrony danych osobowych, było właśnie zagwarantowanie podmiotom danych łatwego dostępu do danych ich dotyczących oraz prawa do przenoszenia danych rozumianych jako prawo do otrzymania kopii przechowywanych danych od administratora oraz swoboda przenoszenia ich od jednego usługodawcy do innego, bez utrudnień[596]. W rezultacie zmiana usługodawcy może stać się dużo łatwiejsza, zwiększając konkurencję na rynku.

Istotnym praktycznym elementem jest uprawnienie do otrzymania danych w odpowiednim ustrukturyzowanym formacie nadającym się do odczytu maszynowego. Zgodnie z dyrektywą 2019/1024 dane zawarte w plikach ustrukturyzowanych w formacie nadającym się do odczytu maszynowego należy uznać za dane nadające się do odczytu maszynowego. Format nadający się do odczytu maszynowego może być otwarty lub zastrzeżony, może też mieć formę standardów formalnych. Dokumentów zakodowanych w formacie pliku ograniczającym przetwarzanie automatyczne nie należy uznawać za sporządzone w formacie nadającym się do odczytu maszynowego, gdyż pozyskanie danych z tych dokumentów jest niemożliwe lub utrudnione. Państwa członkowskie powinny w miarę możliwości i stosownie do przypadku zachęcać do korzystania z unijnego lub uznanego na szczeblu międzynarodowym formatu otwartego nadającego się do odczytu maszynowego (motyw 35 preambuły dyrektywy 2019/1024). Za format plików spełniający ten standard uznaje się m.in. plik XML, JSON, CSV.

---

[595] *P. Litwiński (red.)*, op. cit., Komentarz do art. 20, pkt 2.

[596] Zob. Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów "Ochrona prywatności w połączonym świecie – europejskie ramy ochrony danych w XXI wieku", COM(2012) 9.

W art. 20 ust. 3 zastrzeżono, że wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa do usunięcia danych („prawa do bycia zapomnianym") uregulowanego w art. 17 RODO, jak również nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi.

Pierwsze ograniczenie prawa do przenoszenia danych dotyczy realizacji prawa do usunięcia danych; są to dwa uprawnienia zasadniczo od siebie niezależne, choć ze sobą powiązane. Posługując się potocznym rozumieniem pojęcia „przenoszenie" można byłoby twierdzić, że administrator, który przesłał dane realizując to żądanie, powinien niejako automatycznie usunąć dane, gdyż przenoszenie polega zazwyczaj na zabraniu czegoś z jednego miejsca i umieszczeniu w innym miejscu (danych od jednego administratora do drugiego). Skorzystanie z uprawnienia do przenoszenia danych nie pociąga za sobą automatycznie konsekwencji w postaci usunięcia danych przez administratora, który realizuje uprawnienie do przeniesienia danych. Przedmiotem prawa do przenoszenia danych, jest otrzymanie (przesłanie) danych, a nie ich usunięcie, a administrator może nadal przetwarzać dane przez okres niezbędny do realizacji celów przetwarzania. Oznacza to, że osoba korzystająca z prawa do przenoszenia swoich danych może domagać się usunięcia jej danych, jednak administrator nie będzie zobowiązany do realizacji żądania usunięcia danych, jeżeli zostaną spełnione przesłanki wskazujące na to, że dane nie powinny zostać usunięte (na podstawie art. 17 ust. 3 RODO)[597].

W kontekście ponownego wykorzystywania informacji sektora publicznego istotne jest, że prawo do przenoszenia danych nie obejmuje danych przetwarzanych na innej podstawie legalizującej niż zgoda czy umowa. Z tego względu prawo do przenoszenia danych nie przysługuje w stosunku do danych osobowych przetwarzanych w ramach wykonywania obowiązków publicznych, 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 (motyw 68 preambuły RODO). Tym samym uprawnienie to nie będzie również przysługiwać w przypadku oparciu przetwarzania danych, o podstawę wymienioną w art. 6 ust. 1 lit. f.

[597] *P. Fajgielski,* Prawo do przenoszenia danych, „Informacja w administracji publicznej" 2017, nr 4, s. 29.

5.2.8. Prawo do sprzeciwu

Prawo do sprzeciwu stanowi jedno z uprawnień zakazowych – zmierzających do wyeliminowania możliwości przetwarzania danych osobowych przez administratora w ogóle albo wyłączenia możliwości przetwarzania danych osobowych w celu marketingu bezpośredniego, co zwykle prowadzi do całkowitego zaprzestania przetwarzania danych. Uprawnienie to powiązane jest z prawem do usunięcia danych, prawem do niepodlegania decyzjom zautomatyzowanym, w tym profilowania, prawem do ograniczenia przetwarzania, a także uprawnieniami informacyjnymi z art. 13–15 RODO, ponieważ skutkiem jego wykonania może być usunięcie przetwarzanych danych osobowych, zaprzestanie profilowania, czasowe ograniczenie przetwarzania, a informacja o prawie do sprzeciwu ma być obligatoryjnie przekazywana osobie, której dane dotyczą, już przy zbieraniu danych niezależnie od tego, czy w konkretnym przypadku rzeczywiście będą podstawy do jego realizacji[598].

Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e lub f RODO; jeśli przetwarzanie jest związane z marketingiem bezpośrednim; do celów badań naukowych lub historycznych lub do celów statystycznych.

Należy zwrócić uwagę na pierwszą z przesłanek umożliwiających podmiotowi danych wniesienie sprzeciwu w sytuacji, gdy jego dane osobowe są przetwarzane w oparciu o niezbędność przetwarzania do celów wynikających z prawnie z uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią (art. 6 ust. 1 lit. f). Nie wyprzedzając dalszych rozważać (zagadnienie podstaw legalizujących przetwarzanie danych omówione zostało w kolejnym rozdziale), już w tym miejscu należy zauważyć, że sam art. 6 ust. 1 lit. f wymaga *a priori* dokonania testu ważenia interesów osoby, której dane dotyczą i administratora, który przedmiotowe ważenie musi przeprowadzić przed rozpoczęciem przetwarzania. Natomiast art. 21 ust. 1 wprowadza niejako kolejny obowiązek ważenia interesów przez administratora *a posteriori*, w odniesieniu do danych przetwarzanych zgodnie z prawem, i na wniosek podmiotu danych[599].

Przesłanką wniesienia sprzeciwu jest zatem wykazanie istnienia po stronie wnioskodawcy szczególnej sytuacji, która uzasadnia wniesienie sprzeciwu. Przepisy RODO nie wyjaśniają pojęcia "szczególnej sytuacji". Za taką okoliczność należy uznać każdy stan

[598] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 21, pkt 2.
[599] *M. Czerniawski*, Komentarz do art. 21 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 558.

faktyczny, który nie istniał w chwili zbierania danych osobowych, jeżeli dane były zbierane bezpośrednio od osoby, której dotyczą, lub który co prawda istniał w chwili zbierania danych, lecz nie był wiadomy administratorowi danych, jeżeli dane osobowe były zbierane nie bezpośrednio od osoby, której dane dotyczą. Szczególna sytuacja podmiotu danych, powinna wpływać na przetwarzanie jej danych osobowych w ten sposób, że dojdzie do zachwiania równowagi interesów tej osoby oraz administratora danych – w wyniku tego interes osoby, której dane dotyczą, powinien przeważyć nad interesem administratora danych. Potrzeba ochrony prywatności podmiotu danych powinna przeważyć nad potrzebą przetwarzania tych danych przez administratora [600].

Prawo do sprzeciwu w sposób szczególny na tle innych praw wynikających z rozdziału III RODO ma być komunikowane podmiotom danych, tj. najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa sprzeciwu oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji (art. 21 ust. 4 RODO).

W związku z korzystaniem z usług społeczeństwa informacyjnego osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne (art. 21 ust. 5 RODO). Niemniej sprzeciw, podobnie jak i żądania realizacji innych praw osoby, której dane dotyczą, może być wniesiony w dowolniej formie.

Skutkiem wniesienia sprzeciwu jest niezwłoczne zaprzestać przetwarzania danych przez administratora, jeżeli uzna wniosek za zasadny. Jeżeli jednak w ocenie administratora danych istnieją ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń, administrator może nadal przetwarzać dane objęte sprzeciwem[601]. Jeżeli osoba, której dane dotyczą, nie zgadza się z taką oceną zaistniałej sytuacji, może skorzystać z prawa do wniesienia skargi do organu nadzorczego.

Artykuł 21 RODO nie wymienia zgody, jako podstawy przetwarzania wobec której przysługuje podmiotowi danych wniesienie sprzeciwu. Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać zgodę na przetwarzanie. Nie sposób jednak uznać, że oświadczenie osoby, której dane dotyczą, jest równoznaczne ze sprzeciwem wobec

[600] *P. Litwiński (red.)*, op. cit., Komentarz do art. 21, pkt 4.
[601] *Ibidem*, pkt 7.

przetwarzania jej danych w celu marketingu bezpośredniego, choć ich skutki są w części podobne, ale nie identyczne[602].

5.2.9. Zakaz podejmowania zautomatyzowanych decyzji, w tym profilowania

Na podstawie art. 22 RODO osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Zakaz podejmowania automatycznych decyzji wobec osób, których dane dotyczą, opartych wyłącznie na przetwarzaniu danych osobowych, ma neutralizować niebezpieczeństwa wynikające z rozwoju nowych technologii (np. *big data*, Internet rzecz czy sztuczna inteligencja), a w szczególności zagrożenia dla praw jednostki, wynikające z podejmowania decyzji wyłącznie na podstawie zautomatyzowanego przetwarzania danych osobowych[603]). Jako typowy przykład tego rodzaju decyzji podaje się sytuacje, w których w bazie danych zawierającej dane osobowe zapisane zostały pewne kategorie informacji. Następnie oprogramowanie, w oparciu o algorytm przetwarzania informacji, wykonuje operacje na danych osobowych, wynikiem których jest w każdym przypadku podjęcie decyzji odnoszącej się do osób, których dane są przetwarzane. Decyzje takie podejmuje się, przetwarzając nie tylko dane podane bezpośrednio przez podmiot danych, ale także przez dane uzyskane w związku ze śledzeniem użytkowników w Internecie (np. na potrzeby reklamy behawioralnej) dane o lokalizacji, dane z kart kredytowych, dane z programów lojalnościowych itd.[604] W praktyce tego rodzaju sytuacje występować mogą np. w związku z analizą zdolności kredytowej osób fizycznych w oparciu o podane informacje[605].

W ogólnym rozporządzeniu nie wyjaśniono pojęcia "zautomatyzowanego przetwarzania". Można uznać, że zautomatyzowane przetwarzanie to takie, które w całości – na każdym etapie – dokonywane jest bez udziału czynnika ludzkiego[606]. Pojęcie bliskoznaczne "automatyczne przetwarzanie" zdefiniowane zostało w art. 2 lit. c konwencji Nr 108 Rady Europy z 28.1.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych

[602] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 21, pkt 11.
[603] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 562.
[604] *M. Czerniawski*, op. cit., Komentarz do art. 22, s. 562.
[605] *P. Litwiński* (red.), op. cit., Komentarz do art. 22, pkt 2.
[606] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 22, pkt 3.

osobowych[607]. Zgodnie z tym przepisem "automatyczne przetwarzanie" oznacza następujące operacje wykonane w całości lub częściowo za pomocą procedur zautomatyzowanych: gromadzenie danych, stosowanie do nich operacji logicznych lub arytmetycznych, ich modyfikowanie, usuwanie, wybieranie lub rozpowszechnianie. Zautomatyzowana decyzja stanowi rodzaj rozstrzygnięcia wobec osoby fizycznej, a jej zautomatyzowany charakter polega na tym, że rozstrzygnięcie wobec jednostki jest podejmowane bez udziału czynnika ludzkiego. Decyzja jest podejmowana automatycznie i jest wynikiem przetwarzania danych w systemie informatycznym, przy czym właśnie skutkiem, który warunkuje uznanie decyzji za "zautomatyzowaną", jest skutek w sferze prawnej jednostki lub podobny istotny skutek[608]. Decyzje podejmowane zatem z udziałem człowieka nie podlegają zakazowi wynikającemu z art. 22 RODO. Jednocześnie w ocenie Grupy Roboczej Art. 29 za niedopuszczalne należy uznać sytuacje, w których udział człowieka w procesie podejmowania decyzji byłby kreowany sztucznie, np. ograniczając się do prostego zatwierdzania profili przygotowanych w sposób automatyczny, bez wpływu na ich treść[609].

Z kolei pojęcie profilowania zostało zdefiniowane w art. 4 pkt 4 RODO zgodnie z którym oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się[610].

Profilowanie podlega regulacji art. 22 RODO, jeżeli prowadzi do zautomatyzowanego podejmowania decyzji wobec osób, których dane dotyczą. Nie każdy więc przykład profilowania będzie objęty dyspozycją art. 22 RODO, a wyłącznie taki, który prowadzi do podejmowania automatycznych decyzji ze skutkiem, o którym mowa w art. 22 ust. 1 RODO *in fine*. Regulacja profilowania w komentowanym przepisie RODO jest więc oparta na skutku: jeżeli profilowanie prowadzi do zautomatyzowanego podejmowania decyzji, wówczas jego dopuszczalność należy oceniać na gruncie art. 22; jeżeli nie, wówczas przepis ten nie znajdzie zastosowania do tego rodzaju profilowania[611].

---

[607] Dz.U. z 2003 r. Nr 3, poz. 25.
[608] *M. Sakowska-Baryła*, op. cit.
[609] *Grupa Robocza Art. 29*, Guidelines on automated individual decision-making and Profiling for the purpose of Regulation 2016/679, 03.10.2017 r. (WP 251), s. 10.
[610] Na temat profilowania zob. m.in. *M. Chomiczewski*, Profilowanie w ogólnym rozporządzeniu o ochronie danych [w:] *E. Bielak – Jomaa, D. Lubasz (red.)*, Polska i europejska reforma danych osobowych, Warszawa 2016; *M. Ciechomska*, Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych, „Europejski Przegląd Sądowy" 2017, nr 5.
[611] *P. Litwiński (red.)*, op. cit., Komentarz do art. 22, pkt 4.

Kolejnymi przesłankami uprawnienia, które należy rozstrzygnąć, są skutki prawne lub inny podobny sposób, który istotnie wpływa na podmiot danych. Pojęcie wywołania skutków prawnych w kontekście przedmiotowego przepisu powinno być rozumiane jako powstanie, zmiana lub ustanie stosunku prawnego. Przykładem tego rodzaju sytuacji może być zautomatyzowane podejmowanie decyzji dotyczących zawarcia, rozwiązania lub zmiany umowy z osobą, której dane dotyczą[612]. Grupa Robocza Art. 29 zdaje się jednak rozumieć to pojęcie znacznie szerzej, bo jako każdy przypadek wpływu na prawa przysługujące osobie fizycznej, np. takie jak: wolność zrzeszania się, prawo do głosowania, czy możliwość pozywania. Skutek prawny w opinii Grupy Roboczej Art. 29 to także wpływ na sytuację prawną osoby lub jej uprawnienia wynikające z umowy[613]. Z kolei istotny wpływ na osobę, której dane dotyczą, w sposób podobny do skutków prawnych, oznacza sytuację, w której automatycznie podjęta decyzja wpływa na osobę, której dane dotyczą, ale nie poprzez powstanie, zmianę lub ustanie stosunku prawnego, a wpływ ten jest istotny i podobny do powstania, zmiany lub ustania stosunku prawnego[614].

Przykłady decyzji opierających się wyłącznie na przetwarzaniu zautomatyzowanym, które wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa, zostały wymienione w motywie 71 preambuły RODO, tj. automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej.

Przepisy ogólnego rozporządzenia (art. 22 ust. 3) dopuszczają jednocześnie podejmowanie decyzji opartych wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, i wywołujących wobec osoby skutki prawne lub w podobny sposób istotnie na nią wpływających, o ile:

1) jest to niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem danych,

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

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

Wyjątkowo, decyzje wymienione wyżej oparte wyłącznie na zautomatyzowanym przetwarzaniu danych osobowych, w tym profilowaniu, i wywołujących wobec osoby skutki

[612] *W. Chomiczewski*, Profilowanie, s. 131
[613] *Grupa Robocza Art. 29*, Guidelines on automated individual decision-making, s. 10.
[614] *P. Litwiński (red.)*, op. cit., Komentarz do art. 22, pkt 8.

prawne lub w podobny sposób istotnie na nią wpływających, nie jest jednak dopuszczalne, jeżeli taka operacja przetwarzania miałaby się opierać na przetwarzaniu szczególnych kategorii danych osobowych. Ograniczenie to nie znajdzie jednak zastosowania, jeżeli podstawą przetwarzania danych osobowych należących do szczególnych kategorii byłby art. 9 ust. 2 lit. a (przetwarzanie za wyraźną zgodą osoby, której dane dotyczą) lub lit. g RODO (przetwarzanie niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego) i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą (art. 22 ust. 4 RODO).

Rozdział 6. Relacja przepisów o ochronie danych osobowych i o ponownym wykorzystywaniu informacji sekatora publicznego

Przed wejściem w życie ogólnego rozporządzenia relację ochrony danych osobowych i ponownego wykorzystywania informacji sektora publicznego wyznaczały przepisy dyrektywy 2003/98/WE w jej pierwotnym i zmienionym dyrektywą 2013/37/UE brzmieniu oraz implementujące je przepisy prawa krajowego. Dla ustalenia tej relacji konieczne było również odniesienie się do występującej w prawie krajowym przesłanki ograniczającej dostęp do informacji ze względu na prywatność osoby fizycznej oraz wyłączonych ze sfery poufności informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji.

Ponadto w sposób pośredni, odnosząc prawo do ponownego wykorzystywania jako pochodne prawu dostępu do informacji publicznej (dokumentów urzędowych) a ochrony danych osobowych do szerszej kategorii prywatności stosunek obu uprawnień kształtujących sferę informacyjną jednostki, można było rekonstruować w oparciu a akty wyższego szczebla w hierarchii źródeł prawa, jak Konstytucja RP czy traktaty międzynarodowe.

Od 25 maja 2018 r. relację obu praw należy oprzeć na trzeciej płaszczyźnie. Przepis art. 86 RODO wprost stanowi o konieczności pogodzenia prawa do ochrony danych osobowych z prawem do dostępu do dokumentów urzędowych (i ponownym wykorzystywaniem) oraz przewiduje konieczność uwzględnienia ochrony danych osobowych w przepisach o ponownym wykorzystywaniu informacji sektora publicznego. W sposób pośredni relację tę można odczytać również z przepisów dotyczących podstaw przetwarzania danych osobowych. Przepisy ogólnego rozporządzenia zostały – z zastrzeżeniami, o których będzie mowa dalej – wykonane w UPW. Przepisy polskiej ustawy będą musiały jednak zostać gruntownie znowelizowane w związku z przyjęciem w 20 czerwca 2019 r. nowej dyrektywa o otwartych

danych i ponownym wykorzystywaniu informacji sektora publicznego. Dyrektywa 2019/1024 nie wnosi wprawdzie zdecydowanego przełomu z punktu widzenia ochrony danych osobowych i opiera się na znanych z poprzedniej dyrektywy rozwiązaniach, przewiduje jednak nowe odwołania do aktualnego – wyznaczonego przepisami RODO – standardu ochrony danych osobowych.

Biorąc pod uwagę wymienione poziomy regulacyjne pomocne dla zrozumienia relacji ochrony danych osobowych i ponownego wykorzystywania jest odwołanie się do wypracowanej w doktrynie pod rządami ustawy o dostępie do informacji publicznej i nieobowiązującej już ustawy o ochronie danych osobowych koncepcji współstosowania i komplementarności obu unormowań. Jak zostanie udowodnione podglądy te pozostają aktualne również dla porządku regulacyjnego wyznaczonego przez ogólne rozporządzenie oraz obowiązujące przepisy o ponownym wykorzystywaniu. Przepisy te mają wspólne obszary regulacji przez co ich zakresy się krzyżują, w konsekwencji dochodzi do ich równoległego stosowania.

6.1. Przepisy o ochronie danych osobowych w dyrektywach o ponownym wykorzystywaniu informacji sektora publicznego i ich implementacja w prawie krajowym

Prawo do ponownego wykorzystywania podlega licznym ograniczeniom. Jedną z przesłanek ograniczających ponowne wykorzystywanie informacji sektora publicznego na gruncie dyrektyw jest konieczność zapewnienia ochrony danych osobowych.

Zgodnie z art. 1 ust. 4 dyrektywy 2003/98/WE akt ten w żaden sposób nie wpływa na poziom ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych zgodnie z przepisami Unii i prawa krajowego, w szczególności nie zmienia zobowiązań i praw określonych w dyrektywie 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych. Norma ta oznaczała, że przepisy o ponownym wykorzystywaniu powinny być stosowane w pełnej zgodności z regułami odnoszącymi się do ochrony danych osobowych zgodnie z dyrektywą 95/46/WE i przepisami państw członkowskich, czyli na gruncie prawa polskiego ówczesną UODO1997.

Dyrektywa 2013/37/UE zmieniająca dyrektywę 2003/98/WE dodała w art. 1 w ust. 4 lit. cc. W przepisie tym wymieniono trzy rodzaje dokumentów, w odniesieniu do których

przepisy dyrektywy 2003/98/WE nie mają zastosowania, a tym samym nie podlegają ponownemu wykorzystywaniu. Są to:

– dokumenty wyłączone z dostępu na podstawie systemów dostępu z powodu ochrony danych osobowych;

– dokumenty, do których dostęp jest ograniczony na podstawie systemów dostępu z powodu ochrony danych osobowych;

– części dokumentów dostępne na podstawie tych systemów, które to części zawierają dane osobowe, których ponowne wykorzystywanie zostało określone w przepisach jako niezgodne z prawem dotyczącym ochrony osób fizycznych w zakresie przetwarzania danych osobowych.

Uzupełnieniem regulacji jest motyw 11 preambuły dyrektywy, który stanowi, że zgodnie z dyrektywą 95/46/WE państwa członkowskie powinny określić warunki, pod którymi przetwarzanie danych osobowych jest zgodne z prawem. Ponadto wyeksponowano zasadę związania celem przetwarzania danych osobowych, odwołując się do postanowienia dyrektywy 95/46/WE przewidującego, że nie można dalej przetwarzać danych osobowych po to, by gromadzić je w sposób sprzeczny z określonymi, jednoznacznymi i uzasadnionymi celami, dla których te dane były gromadzone[615].

Znacznie szerzej prawodawca UE odniósł się do prawa do ochrony danych osobowych w dyrektywie 2019/1024 przyjętej już po wejściu w życie RODO. W art. 1 ust. 1 lit. h wyłączono poza zakres stosowania dyrektywy dokumenty wyłączone z dostępu lub do których dostęp jest ograniczony na podstawie systemów dostępu ze względu na ochronę danych osobowych, a także części dokumentów dostępnych na podstawie tych systemów, które to części zawierają dane osobowe, których ponowne wykorzystywanie zostało określone w przepisach jako niezgodne z przepisami dotyczącymi ochrony osób fizycznych w zakresie przetwarzania danych osobowych lub jako naruszające ochronę prywatności i integralności osoby fizycznej, w szczególności zgodnie z unijnymi lub krajowymi przepisami dotyczącymi ochrony danych osobowych. Przedmiotowa norma kolizyjna nie wprowadza nowych rozwiązań, opierając się dotychczasowej treści przywołanego wyżej art.1 w ust. 4 lit. cc dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE.

Co oczywiste, przepisy dyrektywy 2019/1024 odwołują się już do przepisów ogólnego rozporządzenia. W myśl bowiem art. 1 ust. 4 niniejsza dyrektywa pozostaje bez uszczerbku dla krajowego i unijnych przepisów dotyczących ochrony danych osobowych, w szczególności

[615] Art. 6 ust. 1 lit. b) dyrektywy 95/46/WE.

ogólnego rozporządzenia i dyrektywy 2002/58/WE, a także odpowiadających im przepisów prawa krajowego.

Uzupełnieniem tych przepisów są motywy preambuły dyrektywy, w które szerzej, niż to miało miejsce pod rządami dyrektywy 2003/98/WE, uwzględniają konieczność zapewnienia ochrony danych osobowych w związku z ponownym wykorzystywaniem. Po pierwsze, państwa członkowskie realizując zasadę „otwartości w fazie projektowania i otwartości domyślnej" powinny zapewnić ochronę danych osobowych, w tym w przypadkach gdy informacje zawarte w indywidualnym zbiorze danych samodzielnie nie stwarzają ryzyka identyfikacji lub wskazania osoby fizycznej, natomiast mogą stwarzać takie ryzyko gdy informacje te są połączone z innymi dostępnymi informacjami (motyw 16). Po drugie, w myśl motywu 44 licencja określająca warunki ponownego wykorzystywania może obejmować kwestie związane z ochroną danych osobowych. Po trzecie, ponowne wykorzystywanie danych osobowych jest dopuszczalne jedynie, gdy jest ono zgodne z zasadą celowości, jak określono w art. 5 ust. 1 lit. b i art. 6 RODO (motyw 52). Po czwarte, przy podejmowaniu decyzji w sprawie zakresu i warunków ponownego wykorzystywania dokumentów sektora publicznego zawierających danych osobowe, na przykład w sektorze zdrowia, wymagane może być przeprowadzenie oceny skutków dla ochrony danych zgodnie z art. 35 rozporządzenia (UE) 2016/679 (motyw 53).

Co ważne, dyrektywa 2019/1024 wprowadziła definicję anonimizacji, które nie występuje w przepisach ogólnego rozporządzenia. „Anonimizacja" oznacza proces zmiany dokumentów w informacje anonimowe, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, lub dane osobowe zanonimizowane w taki sposób, że identyfikacja osoby, której dane dotyczą, nie jest możliwa (art. 2 pkt 7). Zgodnie z motywem 52 proces anonimizacja informacji jest sposobem pogodzenia względów przemawiających za umożliwieniem ponownego wykorzystywania informacji sektora publicznego, w jak najszerszym zakresie, z obowiązkami wynikającymi z przepisów o ochronie danych. Istotną zmianą jest możliwość uwzględnienia kosztów anonimizacji w opłatach za ponowne wykorzystywanie informacji sektora publicznego (art. 6 ust. 1 dyrektywy 2019/1024).

Implementując dyrektywę 2003/98/WE, krajowy ustawodawca nie zdecydował o wprowadzeniu przesłanki ograniczającej prawo do ponownego wykorzystywania ze względu na ochronę danych osobowych. W ówczesnym rozdziale 2a UDIP[616], w którym ujęto przepisy o ponownym wykorzystywaniu informacji publicznej, w ogóle nie odniesiono się do kategorii

[616] Dz.U. z 2014 r. poz. 782.

danych osobowych. Oczywiście nie oznacza to, że relacje pomiędzy prawem do ochrony danych osobowych a prawem do ponownego wykorzystywania informacji nie występowały, ale należało je oceniać w oparciu o przesłankę ochrony prywatności, o której stanowił art. 5 ust. 2 w związku z art. 23g ust. 8, a dopiero następnie rozwiązanie to odnieść do ówczesnych przepisów o ochronie danych osobowych, których zakres wyznaczała UODO1997.

Dopiero ustawodawca implementując dyrektywę 2013/37/UE podjął próbę określenia relacji pomiędzy prawem do ponownego wykorzystywania a ochroną danych osobowych.

Przepisy UPW w pierwotnie uchwalonym brzmieniu[617] określały relację między prawem do ponownego wykorzystywania oraz ochroną danych osobowych pośrednio oraz bezpośrednio.

Po pierwsze, zgodnie z art. 6 ust. 2 UPW prawo do ponownego wykorzystywania podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy (symetryczne ograniczenie znajdziemy w art. 5 ust. 2 ustawie o dostępie do informacji publicznej). Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Przesłanką ograniczającą ponowne wykorzystywanie była ochrona prywatności, z której następczo wywodzono konieczność zapewnienia ochrony danych osobowych zawartych w informacji sektora publicznego.

Po drugie, w myśl art. 7 ust. 2 UPW w jej pierwotnym brzmieniu, przepisy ustawy nie naruszały przepisów ustawy o ochronie danych osobowych[618].

Współistnienie w jednej ustawie, z jednej strony ograniczenia ponownego wykorzystywania w oparciu o kryterium niezdefiniowanego pojęcia prywatności, a z drugiej normy *quasi* kolizyjnej odwołującej się do ówczesnych przepisów o ochronie danych osobowych, niewątpliwie nie spełniało kryteriów określoności przepisów składającej się na zasadę prawidłowej legislacji. Relacja obu praw w oparciu o brzmienie aktualnie obowiązujących przepisów UPW zostanie omówiona w Rozdziale 6.3.

[617] Dz. U. 2016 poz. 352.
[618] Chodziło o nieobowiązującą ustawę z 29.08. 1997 r. o ochronie danych osobowych.

6.2. Ponowne wykorzystywanie informacji sektora publicznego w przepisach ogólnego rozporządzenia o ochronie danych osobowych

Przepisy ogólnego rozporządzenia w jego części normatywnej wprost nie odwołują się do ponownego wykorzystywania informacji sektora publicznego. Nowością natomiast jest ustalenie relacji pomiędzy prawem do ochrony danych osobowych a dostępem do informacji (dostępem do dokumentów urzędowych). Należy przypomnieć, że w poprzednio obowiązującym stanie prawnym pod rządami dyrektywy 95/46/WE nie określono relacji pomiędzy tymi prawami. Na gruncie przepisów ogólnego rozporządzenia – co zostanie dalej udowodnione – relację ponownego wykorzystywania informacji sektora publicznego i ochrony danych osobowych należy dokonywać w oparciu o przepisy odwołujące się do dostępu do dokumentów urzędowych. W tym kontekście stosunek obu praw można zrekonstruować bezpośrednio w oparciu o normę wyrażoną w art. 86 RODO i dopełniającym go motywie 154 preambuły rozporządzenia oraz pośrednio w oparciu o przepisy dotyczące podstaw przetwarzania danych osobowych, tj. art. 6 ust. 1 lit. e oraz ust. 2 i 3 RODO. Nie wyprzedzając dalszych rozważań poświęconych przesłankom legalności przetwarzania danych w związku ponownym wykorzystywaniem, którym poświęcony jest kolejny rozdział pracy, w tym podrozdziale omówiona zostanie relacja bezpośrednia wyznaczona art. 86 RODO.

Zgodnie z art. 86 RODO dane osobowe zawarte w dokumentach urzędowych, które posiada organ albo podmiot publiczny lub podmiot prywatny, w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych.

Przepis ten z jednej strony zawiera wyraźne zamanifestowanie, iż ochrona danych osobowych wynikająca z RODO nie stoi na przeszkodzie realizacji prawa dostępu do dokumentów urzędowych, z drugiej – określa granice tego dostępu. Wyznacza ją konieczność realizacji prawa do ochrony danych osobowych na zasadach określonych w tym akcie[619].

Co istotne, art. 86 RODO został umieszczony w rozdziale IX rozporządzenia zatytułowanym: „Przepisy dotyczące szczególnych sytuacji związanych z przetwarzaniem". W rozdziale tym nie zawarto typowych zasad dotyczących przetwarzania i ochrony danych osobowych, jak w innych częściach RODO. Wskazano w nim szczególne przypadki, które muszą lub mogą być regulowane w przepisach krajowych państw członkowskich UE, ale

[619] *M. Sakowska – Baryła*, op. cit., Komentarz do art. 86, pkt.

jednocześnie określono warunki dla tej regulacji krajowej i jej odniesienie do zasad określonych w RODO[620]. Artykuł 86 RODO należy zaliczyć do tej kategorii przepisów ogólnego rozporządzenia, które – zdaniem *G. Sibigi* – powinny być obligatoryjnie przyjęte w prawie krajowym[621]. Wprawdzie nie służy on bezpośrednio wdrożeniu postanowień rozporządzenia, ale zachowaniu równowagi między prawem ochrony danych osobowych oraz prawem do informacji, które może być w różnorodny sposób ujęte w prawie krajowym[622]. Z tego powodu jego głównym adresatem jest ustawodawca krajowy.

W literaturze przedmiotu podnosi się także, że art. 86 RODO jest również bezpośrednio skierowany do podmiotów wymienionych wprost w jego treści, a więc posiadających dokumenty urzędowe organów, podmiotów publicznych lub podmiotów prywatnych w celu wykonywania zadań realizowanych w interesie publicznym, jak również do sądów orzekających w sprawach dotyczących realizacji uprawnień dostępowych, a praktyce może okazać się, że przepis ten będzie miał duże znaczenie właśnie dla tej ostatniej grupy podmiotów, a zasady przetwarzania danych osobowych wynikające z RODO mogą bardzo istotnie wpłynąć na zakres informacji o osobach fizycznych udostępnianych jako informacje publiczne lub informacje sektora publicznego[623].

Wykładnia językowa art. 86 RODO nie pozwala na przesądzenie, że ma on zastosowanie do ponownego wykorzystywania informacji sektora publicznego. Podstawowym celem omawianego przepisu jest określenie relacji pomiędzy prawem do ochrony danych osobowych a prawem dostępu do dokumentów urzędowych. Zestawienie zakresu przedmiotowego i podmiotowego stosowania art. 86 RODO prowadzi do wniosku, że chodzi w nim o przepisy krajowe dotyczące powszechnego dostępu do informacji będących w posiadaniu (utrwalonych) przez organy władzy publicznej lub inne podmioty wykonujące zadania publiczne w państwie członkowskim, które zostały objęte mocą tych przepisów[624]. Na gruncie prawa polskiego jest prawo dostępu do informacji realizowane jest w oparciu o art. 61 Konstytucji i przepisy UDIP.

W literaturze prezentowane jest również stanowisko, że art. 86 RODO przesądza, że podmiot ujawniający informacje publiczne zawierające dane osobowe, czy to w trybie określonym w prawie Unii Europejskiej, czy w trybie określonym w przepisach krajowych, nie

[620] *G. Sibiga, I. Małobęcka-Szwast,* Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych osobowych (RODO), „Monitor Prawniczy" 2019, nr 22 (dodatek), s. 60.
[621] *G. Sibiga,* Dopuszczalny zakres, s. 19.
[622] *Ibidem.*
[623] *M. Sakowska – Baryła,* op. cit., pkt 2.
[624] Zob. szerzej: *G. Sibiga, I. Małobęcka-Szwast,* Relacje, s. 60 i nast.

narusza w ten sposób przepisów RODO. Po stronie podmiotu udostępniającego informację zawierającą dane osobowe istnieje więc podstawa prawna dla przetwarzania danych osobowych w ten właśnie sposób. Jednocześnie przepisy prawa krajowego mogą przewidywać pewne ograniczenia w ujawnianiu informacji ze względu na ochronę danych osobowych[625].

Dopełnieniem art. 86 RODO dostarczającym wytycznych interpretacyjnych jest motyw 154 preambuły, który już wprost odnosi się do ponownego wykorzystywania informacji sektora publicznego. Jego analiza jest zatem kluczowa dla omawianego zagadnienia. Motyw ten pozwala uwzględnić przy stosowaniu przepisów rozporządzenia zasadę publicznego dostępu do dokumentów urzędowych. Publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny. Organ publiczny lub podmiot publiczny powinny móc publicznie ujawniać dane osobowe z dokumentów przez siebie przechowywanych, jeżeli takie ujawnienie jest przewidziane przepisami prawa Unii lub prawa państwa członkowskiego, któremu organ ten lub podmiot podlegają. Przepisy takie powinny godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych, i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie niniejszego rozporządzenia. Wzmianka o organach i podmiotach publicznych powinna w tym kontekście dotyczyć wszystkich organów lub innych podmiotów objętych prawem państwa członkowskiego dotyczącym publicznego dostępu do dokumentów. Dyrektywa 2003/98/WE nie narusza ani w żaden sposób nie wpływa na stopień ochrony osób fizycznych w związku z przetwarzaniem danych osobowych wynikający z przepisów prawa Unii i prawa państwa członkowskiego, a w szczególności nie zmienia obowiązków i praw przewidzianych w niniejszym rozporządzeniu. Dyrektywa ta nie powinna mieć zastosowania w szczególności do dokumentów, do których – w ramach systemów dostępu – dostęp jest wykluczony lub ograniczony z powodu ochrony danych osobowych, ani do fragmentów dokumentów dostępnych w ramach tych systemów, ale zawierających dane osobowe, których ponowne wykorzystanie zostało określone w prawie jako niezgodne z prawem o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych.

Odwołanie się przez unijnego prawodawcę w motywie 154 do dyrektywy 2003/98/WE w istocie nie niesie żadnej nowej treści normatywnej, bowiem w tym zakresie stanowi jedynie powtórzenie art. 2 lit. cc) tejże dyrektywy (w brzmieniu nadanym dyrektywą 2013/37/UE). Nowością, którą należy przeanalizować, jest wymóg „pogodzenia" praw oraz klauzula interesu publicznego. Wydaje się zatem, że celem powtórzenia w części nienormatywnej

[625] Zob. *P. Litwiński (red.)*, op. cit., Komentarz do art. 86.

rozporządzenia tej dyspozycji była próba podkreślenia, że gdy organ powołuje się na ochronę danych w celu odmowy publicznego dostępu do dokumentów, nie powinno się „obchodzić" tego ograniczenia, stosując przepisy dotyczące ponownego wykorzystywania[626].

Zestawiając art. 86 z motywem 154, choć na gruncie samego RODO nie zdefiniowano dokumentu urzędowego, nie ma wątpliwości, że chodzi o dokument urzędowy w rozumieniu przepisów dyrektywy 2003/98/WE, którego definicja wyznacza zakres pojęcia informacji sektora publicznego. Jeśli chodzi zaś o jego zakres podmiotowy, to obejmuje on zarówno organy i podmioty publiczne, jak i podmioty prywatne wykonujący zadania w interesie publicznym (motyw 154 stanowi o „innych podmiotach objętych prawem państwa członkowskiego dotyczącym publicznego dostępu do dokumentów"). RODO – w przeciwieństwie do dyrektywy 2003/98/WE – również nie definiuje tych podmiotów. Te trzy kategorie adresatów normy z art. 86 i motywu 154 należy więc odnieść podmiotów objętych zakresem stosowania przepisów o ponownym wykorzystywaniu, które na gruncie krajowym zwane są podmiotami zobowiązanymi (zgodnie z art. 3 UPW).

Co ciekawe, na gruncie art. 86 i motywu 154 RODO można zaobserwować pewną niespójność. W art. 86 pojawia się kategoria interesu publicznego jako wyznacznik celu, dla którego dane osobowe zawarte w dokumentach urzędowych posiadają organ lub podmiot publiczny lub podmiot prywatny. Chodzi tutaj o dokumenty urzędowe, które posiadają te podmioty w celu wykonywania zadania realizowanego w interesie publicznym. Z kolei w motywie 154 RODO, nie wiąże się interesu publicznego z wykonywanym zadaniem, ale wskazuje wprost, że „publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny". Jak wskazuje *M. Sakowska – Baryła*, to znacząco odmienny sens obu przepisów, „bo czym innym jest posiadać dokument w celu wykonania zadania realizowanego w interesie publicznym, a czym innym udostępniać go w interesie publicznym"[627].

Pojęcie "interes publiczny" nie zostało zdefiniowane ani w RODO, ani w przepisach prawa krajowego. W literaturze wskazuje się, że w odniesieniu do polskiego porządku prawnego pojęcie to identyfikuje się z interesem ogółu, a w jeszcze szerszym znaczeniu z dobrem wspólnym, o którym mowa w art. 1 Konstytucji RP[628]. Pojęcie interesu publicznego było wielokrotnie przedmiotem wypowiedzi TK, ale orzecznictwo nie dokonało wykładni konkretyzującej jego zakresu znaczeniowego, ograniczając się głównej mierze do stwierdzeń,

[626] Zob. *H. Kranenborg*, Commentary on 86 of the General Data Protection Regulation [w:] *L. Bygrave, C. Kuner, C. Docksey* (red.), Commentary on the EU General Data Protection Regulation, Oxford University Press 2020, s.1221.
[627] *M. Sakowska – Baryła*, op. cit., pkt 3.
[628] *Ibidem*.

czy w określonej sprawie interes ów występuje czy nie, i czy jest naruszany czy też wymaga szczególnej ochrony[629]. Analiza orzecznictwa TK w kontekście interesu publicznego pokazuje, że można precyzyjnie wskazać te desygnaty pojęcia interesu publicznego, które nie wymienione zostały w art. 31 ust. 3 Konstytucji RP, z tym, że tworzą one katalog otwarty[630]. Wśród desygnatów przedmiotowego pojęcia wymienia się również jawność życia publicznego (np. wyrok TK z 5.3.2003 r., K 7/01). Wskazuje się, że interes publiczny w istotny sposób musi determinować wyważenie ochrony danych osobowych i uprawnień dostępowych w sytuacji, w której po jednej stronie stawiamy prywatność jednostki i jej ochronę, a po drugiej ów interes rozumiany szeroko i łączący się z poszanowaniem zasady jawności, transparentności działania państwa i jego organów oraz osób pełniących funkcje publiczne[631]. Wykonywanie prawa do informacji można sprowadzać do zaspokojenia indywidulanych potrzeb informacyjnych, ale równocześnie stanowi ono narzędzie troski o stan państwa oraz podmiotów wykonujących zadania publiczne w jego imieniu[632]. Konieczne może okazać się zatem swoiste wartościowanie informacji o osobie fizycznej w zależności od tego, do jakiej ze sfer jej działalności się one odnoszą, a co za tym idzie, czy przez wzgląd na interes publiczny powinny być ujawniane[633].

Kwestią zasadniczą pozostaje rozstrzygnięcie czy dyspozycja zawarta w art. 86 adresuje również ponowne wykorzystywanie informacji sektora publicznego, a następnie czy realizację prawa do ponownego wykorzystywania można uznać za interes publiczny jak to *expressis verbis* w zd. drugim motywu 154 stwierdzono w odniesieniu do publicznego dostępu do dokumentów. Nie są to zagadnienia o wyłącznie teoretycznym charakterze, dostarczają w istocie odpowiedzi na fundamentalne pytania, czy wymóg pogodzenia praw obejmuje również ponowne wykorzystywanie informacji sektora publicznego oraz na jakiej podstawie prawnej można dokonywać przetwarzania danych osobowych w ramach ponownego wykorzystywania informacji sektora publicznego.

Jak wskazywano ponowne wykorzystywanie informacji sektora publicznego jest nierozerwalnie związane prawem dostępu do dokumentów. Możliwość wykorzystywania informacji zawsze zależna jest od samej jej dostępności. Pierwotną regulacją prawną jest

---

[629] Zob. *A. Wilczyńska*, Interes publiczny w prawie stanowionym i orzecznictwie Trybunału Konstytucyjnego, „Przegląd Prawa Handlowego" 2009, nr 9, s. 49.
[630] *J. Chmielewski*, Pojęcie nadrzędnego interesu publicznego w prawie administracyjnym, Warszawa 2005, s. 238-247.
[631] *M. Jabłoński* [w:] *M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda*, Obowiązywanie i stosowanie postanowień ogólnego rozporządzenia o ochronie danych osobowych w polskim porządku prawnym, Wrocław 2017, s. 120–123.
[632] *M. Bernaczyk*, Prawo do informacji publicznej w Polsce i na świecie, Warszawa 2014, s. 257.
[633] *M. Sakowska – Baryła*, op. cit.

„system dostępu" (tj. przepisy o dostępie do dokumentów urzędowych/informacji publicznej), którego w żaden sposób nie modyfikują przepisy o ponownym wykorzystywaniu, ale jedynie z niego korzystają. W zakresie dostępności i ochrony poufności danych dla potrzeb eksploatacyjnych przepisy o ponownym wykorzystywaniu powinny opierać się na przepisach tworzących system dostępu, co nie wyklucza jednocześnie możliwości tworzenia odrębności, czyli np. ograniczeń czy zasad ponownego wykorzystywania nie znajdujących odzwierciedlenia w przepisach „dostępowych". Stanowi o tym generalna zasada przyjęta w art. 1 ust.3 dyrektywy 2019/1024/UE (dawny art. 1 ust. 3 dyrektywy 2003/98/WE), według której niniejsza dyrektywa opiera się na systemach dostępu obowiązujących w państwach członkowskich i pozostaje bez uszczerbku dla tych systemów. Można zatem skonkludować, że oba prawa łącznie konstytuują kompletne uprawnienie informacyjne przysługujące każdemu.

W mojej opinii należy zatem przyjąć w drodze wykładni systemowej, że dyspozycja zawarta w art. 86 ma również zastosowanie w odniesieniu do ponownego wykorzystywania informacji sektora publicznego. Za łącznym rozpatrywaniem dwóch praw przemawia sposób definiowania regulacji obu uprawnień dostępowych w przepisach prawa. Gwarantuje się w nich nie tylko prawo dostępu, ale i prawo ponownego wykorzystywania informacji, które w swej istocie stanowią ważne elementy składowe, a zarazem konsekwencje zasady otwartości i transparentności rządów wyrażonych w aktach prawa pierwotnego UE, jak art. 15 TFUE (każdy obywatel UE i każda osoba fizyczna lub prawna mająca miejsce zamieszkania lub siedzibę statutową w państwie członkowskim ma prawo dostępu do dokumentów instytucji, organów i jednostek organizacyjnych UE, niezależnie od ich formy, z zastrzeżeniem zasad i warunków określonych w tym przepisie) czy stanowiącym jego odzwierciedlenie art. 42 KPP, jak aktach prawa pochodnego, w tym rozporządzeniu 1049/2001 z 30.5.2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji[634]. Ponadto przemawia za tym także wykładania celowościowa, bowiem zd. 3 motywu 154 stanowi, że przepisy dotyczące dostępu do dokumentów urzędowych „powinny godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych, i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie niniejszego rozporządzenia". Fragment ten określa relację jaka ma zachodzić między publicznym dostępem do dokumentów urzędowych w powiązaniu z ponownym wykorzystaniem informacji sektora

[634] *M. Sakowska – Baryła*, op. cit., pkt 4.

publicznego z jednej strony, a prawem do ochrony danych osobowych z drugiej. RODO statuuje zatem oba te reżimy łącznie względem prawa do ochrony danych osobowych[635].

Te same argumenty przemawiają również za tym, aby uznać prawo do ponownego wykorzystywania za interes publiczny. Konsekwencją będzie zatem zastosowanie odpowiedniej przesłanki legalizującej przetwarzanie danych osobowych przez podmiot zobowiązany ujawniający dane osobowe w ramach informacji sektora publicznego, szczególności w kontekście zadania realizowanego w interesie publicznym, o którym mowa w art. 6 ust. 1 lit. e w związku z art. 6 ust. 2 i 3 RODO (zagadnienie to zostanie omówione w kolejnym rozdziale).

Po udzieleniu odpowiedzi na zasadnicze kwestie, można następnie przejeść do podjęcia próby ustalenia relacji prawa do ochrony danych osobowych z prawem do ponownego wykorzystywania informacji sektora publicznego na gruncie ogólnego rozporządzenia. Łączna interpretacja art. 86 i motywu 154 preambuły RODO pozwala na wyprowadzenie następujących wniosków.

Po pierwsze, RODO nie wyłącza możliwości ujawnienia danych osobowych stanowiących informacje sektora publicznego w ramach ponownego wykorzystywania[636]. Oznacza to, że krajowe organy publiczne lub podmioty publiczne (czyli na gruncie UPW podmioty zobowiązane), powinny mieć zapewnioną możliwość, aby w ramach informacji sektora publicznego przekazywanych lub udostępnianych do ponownego wykorzystywania znajdowały się dane osobowe, jeżeli takie ujawnienie przewidziane zostało przepisami prawa państwa członkowskiego[637].

Po drugie, państwa członkowskie UE powinny w prawie krajowym wykonać dyspozycję art. 86 i motywu 154 poprzez przyjęcie przepisów godzących publiczny dostęp do dokumentów i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych. Przepisy te powinny być tak skonstruowane, aby zagwarantować realizację uprawnień dostępowych, jednocześnie szanując gwarancje prawa do ochrony danych osobowych[638].

---

[635] *G. Sibiga, I. Małobęcka-Szwast*, Relacje, s. 65.

[636] *D. Sybilski*, Ponowne wykorzystywanie informacji sektora publicznego a ochrona danych osobowych według ogólnego rozporządzenia o ochronie danych oraz dyrektywy 2003/98/WE – wybrane zagadnienia, „Prawo Mediów Elektronicznych" 2017, nr 4, s. 34–39.

[637] Zob. podobnie na gruncie dostępu do informacji publicznej: *G. Sibiga, I. Małobęcka-Szwast*, Relacje, s. 66.

[638] zob. *M. Jabłoński* [w:] *M. Jabłoński, D. Kornobis-Romanowska, K. Wygoda*, Obowiązywanie i stosowanie, s. 123.

Po trzecie, konieczne jest uwzględnienie przepisów o ochronie danych w przepisach o ponownym wykorzystywaniu informacji sektora publicznego[639].

Ochrona danych osobowych z góry nie wyłącza zatem możliwości ponownego wykorzystywania danych osobowych w ramach informacji sektora publicznego. Należy przypomnieć, że Grupa Robocza Art. 29 jeszcze w poprzednim porządku prawnym wyznaczonym przepisami dyrektywy 95/46/WE rekomendowała, aby państwa członkowskie na poziomie przepisów krajowych jasno wskazały, które dane osobowe są udostępniane publicznie, do jakich celów oraz w jakim stopniu i na jakich warunkach ponowne wykorzystywanie jest dozwolone. Brak szczegółowych przepisów nie oznacza jednak, że dostępne publicznie dane osobowe mogą być zawsze ponownie wykorzystywane[640]. Kluczowe jest, aby przepisy krajowe, które przewidują możliwość ponownego wykorzystywania danych osobowych spełniały wymóg „pogodzenia" obu praw wynikający z RODO.

Owo pogodzenie (ang. *reconcile*) należy odnieść do znanego z doktryny i ustawodawstw niektórych państw członkowskich koncepcji wyważenia (ang. *balancing*) dwóch kolizyjnych względem siebie uprawnień[641], w tym wypadku prawa do ochrony danych osobowych z prawem do ponownego wykorzystywania informacji. Jego istotą podział ograniczeń dostępności informacji na przesłanki bezwzględne (absolutne) oraz względne (relatywne)[642]. Opierają się one na procesie ustalenia wystąpienia przesłanki ograniczającej ujawnienie informacji w oparciu o dwa mechanizmy badania: testu szkody (*harm test*) oraz testu ważenia interesów (*balancing of interest*). Testy przeprowadza się *casu ad casum*, a przepisy prawa, z góry nie przesądzają o niedostępności informacji[643]. Decyzję o ujawnieniu informacji podejmuje organ, który podlega w tym zakresie kontroli (najczęściej przez niezależny organ, np. Information Commissioner w Wielkiej Brytanii czy La Commission d'accès aux documents administratifs – CADA we Francji)[644]. W przypadku wystąpienia

[639] Zob. *D. Sybilski*, Ponowne wykorzystywanie informacji sektora publicznego a ochrona danych osobowych, s. 34–39.
[640] Opinia 06/2013 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (ISP), 5.6.2013 r. (WP 207).
[641] *R. Jay*, Guide to the General Data Protection Regulation, A Companion do Data Protection Law and Practice (4th edition), London 2017, pkt 16-025.
[642] Zob. *G. Sibiga*, Prawne ograniczenia dostępności informacji [w:] *G. Sibiga (red.)*, Główne problemy prawa do informacji, s. 97 i nast.
[643] Tamże, s. 97.
[644] Na temat niezależnego organu oraz modeli instytucjonalnych łączących kompetencje kontroli dostępu do informacji publicznej oraz ochrony danych osobowych zob. *A. Piskorz-Ryń*, Wyspecjalizowany organ do spraw dostępu do informacji o charakterze publicznym w wybranych krajach UW [w:] *G. Sibiga (red.)*, Główne problemy prawa do informacji, s. 149-239; *A. Piskorz-Ryń*, Kontrola ochrony danych osobowych i dostępu do informacji publicznej w jednym organie? – dylematy instytucjonalne [w:] *A. Mednis*, Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość, s. 193-203.

przesłanki bezwzględnej, organ jest zobowiązany ograniczyć dostęp do informacji, przy czym może on przeprowadzić test szkody, który polega na ustaleniu czy ujawnienie określonej informacji powoduje lub może spowodować negatywne konsekwencje dla określonego dobra chronionego (np. porządek publiczny)[645]. Z kolei właściwy test ważenia interesów przeprowadza się dla zbadania przesłanek względnych, których istota polega na tym, że pomimo tego, iż ujawnienie informacji może naruszać lub narusza określone wartości, to należy te wartości zestawić i wyważyć z interesem publicznym przemawiającym za udostępnieniem informacji[646]. Istotne jest, że należy brać pod uwagę te wartości, które mieszczą się w ramach interesu publicznego, nie zaś interesy indywidulane żądającego dostępu do informacji[647].

W tak ujętej konstrukcji ograniczającej ujawnienie informacji, ochrona danych osobowych może stanowić względną przesłankę ograniczającą dostęp do informacji czy ponowne jej wykorzystywanie. Jej stosowanie polegać zatem może na stosowaniu dwóch wspomnianych testów. Podstawowe założenie polegać zatem będzie na zaakceptowaniu, iż nawet pomimo wystąpienia negatywnych przesłanek udostępnienia (w tym wypadku ochrony danych osobowych), należy je odnieść do szerszej kategorii interesu publicznego, który uzasadnia ujawnienie informacji. W konkretnych przypadkach dopuszczalne jest zatem „poświęcenie określonych prawem wartości przemawiających za poufnością na rzecz korzyści, jakie może przynieść ujawnienie informacji"[648]. Kwestią, dyskusyjną pozostaje praktyczna możliwość zastosowania testu ważenia interesu w kontekście bezwnioskowego ponownego wykorzystywania informacji udostępnianych za pośrednictwem systemów teleinformatycznych, czy dopuszczalne jest „poświęcenie" prawa do ochrony danych osobowych na rzecz korzyści płynących z ponownego wykorzystywania danych osobowych, które zgodnie z definicją, może odbywać się w dowolnych celach, również komercyjnych, których nie sposób będzie z góry publikując informacje przewidzieć. Z tego powodu, w mojej opinii przeprowadzenie testu szkody i testu ważenia interesów jest możliwe, jedynie w sytuacji, w której znane są cele ponownego wykorzystywania, a więc w praktyce jedynie w trybie wnioskowym.

Jako przykład oparcia ograniczeń w dostępie do informacji o test ważenia interesu, można podać niemieckiej ustawy z 5 września 2005 r. o dostępie do informacji pozostających w posiadaniu Rządu Federalnego (Gesetz zur Regelung des Zugangs zu Informationen des

[645] *G. Sibiga*, Prawne ograniczenia, s. 98.
[646] *Ibidem*.
[647] *Ibidem*, s. 100.
[648] *Ibidem*, s. 99.

Bundes (Informationsfreiheitsgesetz – IFG[649]). W art. 5 IFG przewiduje test ważenia interesów, który polega na zbadaniu czy interes wnioskodawcy w uzyskaniu informacji zawierającej dane osobowe przeważa nad interesem osoby trzeciej, której dane dotyczą, uzasadniające wyłączenie dostępu do informacji lub gdy osoba trzecia wyraziła na to zgodę.

Innym przykładem wykorzystania w ustawodawstwie testu ważenia interesu jest regulacja słoweńska[650]. W art. 6 ustawy o dostępie do informacji publicznej (Zakon o dostopu do informacij javnega značaja – ZDIJZ[651]), wśród katalogu względnych przesłanek ograniczających dostęp i ponowne wykorzystywanie informacji publicznej wymieniono dane osobowe, których ujawnienie mogłoby stanowić naruszenie ochrony danych osobowych według właściwych przepisów. Podmiot publiczny będący w posiadaniu informacji może jednak zdecydować o ich udostępnieniu, o ile interes publiczny ujawnienia tych informacji przeważa nad interesem ich utajnienia, tak publicznym jak i prywatnym.

Przepisy ogólnego rozporządzenia nie dostarczają niestety wyczerpujących wskazówek, jak owo pogodzenie ponownego wykorzystywania informacji sektora publicznego z prawem do ochrony danych osobowych w prawie krajowym powinno nastąpić. Motyw 154 nie stanowi również wprost, o konieczności przeprowadzenia testu ważenia interesów. Jedyną wytyczną wymienioną w motywie 154 jest konieczność „niezbędnego uwzględnienia prawa do ochrony danych osobowych na podstawie niemniejszego rozporządzenia" w przepisach krajowych. Oznacza to przepisy wykonujące art. 86 RODO powinny uwzględniać konkretne zasady przewidziane w tym rozporządzeniu realizujące prawo do ochrony danych osobowych. W tym miejscu warto sięgnąć po ugruntowane stanowisko doktryny wypracowane na gruncie dostępu do informacji publicznej. Podkreśla się, że w aktach prawnych dotyczących publicznego dostępu do dokumentów urzędowych nie mogą znaleźć się odstępstwa od ogólnych zasad wynikających z RODO, a w prawie państw członkowskich dotyczących publicznego dostępu do dokumentów należy zachować co najmniej minimalny poziom ochrony danych osobowych, a w szczególności nie mogą być ograniczone prawa i obowiązki wynikające z ogólnego rozporządzenia[652].

Powyższe należy odnieść do przepisów krajowych o ponownym wykorzystywaniu informacji sektora publicznego. Potwierdza to zdanie 6 motywu 154, zgodnie z którym dyrektywa 2003/98/WE (a zatem również zastępująca ją dyrektywa 1024/2019) nie narusza,

[649] https://www.gesetze-im-internet.de/englisch_ifg/index.html
[650] Zob. szer. *D. Sybilski*, Ponowne wykorzystywanie w Słowenii [w:] *A. Piskorz-Ryń*, Jawność i jej ograniczenia. Dostęp i wykorzystywanie. Tom V, Warszawa 2016, s. 168-181.
[651] https://www.ip-rs.si/zakonodaja/zakon-o-dostopu-do-informacij-javnega-znacaja/
[652] *N. Zawadzka*, Komentarz do art. 86 pkt 4 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, S. 1084.

ani w żaden sposób nie wpływa na stopień ochrony osoby fizycznej w związku z przetwarzaniem danych osobowych, a w szczególności nie zmienia obowiązków i praw przewidzianych w niniejszym rozporządzeniu.

Treść motywu 154 potwierdza zatem wprost konieczność stosowania przepisów ogólnego rozporządzenia również przy realizacji prawa do ponownego wykorzystywania informacji sektora publicznego[653]. Mamy tu zatem do czynienia ze współstosowaniem dwóch porządków regulacyjnych, którego koncepcja zostanie opisana w dalszej części niniejszego rozdziału.

Na zakończenie tej części należy się zgodzić z konkluzjami Grupy Tematycznej ds. Prawnych Aspektów Informacji Sektora Publicznego - LAPSI powołanej przez Komisję Europejską. Próba pogodzenia prawa ochrony danych osobowych z ponownym wykorzystywanie informacji może być trudna do realizacji w praktyce[654]. Podnoszono, że częściowym rozwiązaniem tego problemu może być stosowanie organów sektora publicznego zasady domyślnej ochrony danych osobowych (*privacy by default*) i ochrony danych w fazie projektowania (*privacy by design*) oraz stosowanie oceny skutków dla ochrony danych. Czynności te poprzedzać każdorazowe udostępnienie danych osobowych do ponownego wykorzystywania. Jednocześnie autorzy Rekomendacji przyznając słuszność tych postulatów dla unikania nieumyślnego naruszenia ochrony danych osobowych, sami wskazują, że nie rozwiewa to wszystkich wątpliwości[655]. Informacje sektora publicznego zawierające dane osobowe, które są udostępnianie w celu ponownego wykorzystywania, a więc co do zasady w innym celu publicznym, niż dla którego zostały zebrane, jest wysoce problematyczne. Użycie danych osobowych w nieznanym celu lub w innym kontekście może naruszać zasadę określoności celów (Zob. Rozdział X).

W kontekście art. 86 i motywu 154 uprawnionym jest przesądzenie nadrzędności reguł ochrony danych osobowych przed prawem do ponownego wykorzystywania informacji[656]. Nie zmienia tego zasada, że publiczne ujawnianie danych osobowych jest dozwolone, o ile jest to przewidziane przepisami prawa krajowego lub prawa UE, które równoważą (godzą) prawo dostępu do informacji (i ponownego ich wykorzystywania) z prawem ochrony danych

[653] Podobnie *N. Zawadzka*, op. cit, s. 1082.
[654] *The European Thematic Network on Legal Aspects of Public Sector Information (LAPSI),* Privacy and Personal Data Protection, Policy Recommendation N. 4, 2012. https://ec.europa.eu/digital-single-market/en/news/legal-aspects-public-sector-information-lapsi-thematic-network-outputs (dostęp: 30.10.2020).
[655] *LAPSI 2.0*, Position paper access to data, 12.12.2014, s. 11. https://digital-strategy.ec.europa.eu/en/library/lapsi-position-paper-access-data (dostęp: 30.10.2020).
[656] *Ibidem*.

osobowych. Trudno wciąż też jednoznacznie przesądzić hierarchię norm w przypadku proaktywnego otwierania danych (np. w celu przejrzystości życia publicznego). Mankamentem przyjętego w ogólnym rozporządzeniu rozwiązania może być brak w ustawodawstwie wyraźnego obowiązku publikacji (a w konsekwencji możliwości ponownego wykorzystywania) danych osobowych. Przynajmniej teoretycznie – na gruncie art. 86 i motywu 154 RODO – możliwe jest przyjęcie, że przepisy prawa krajowego w ogóle nie przewidują lub przewidują – co bardziej prawdopodobne – jedynie w nielicznych okolicznościach ujawnienie danych osobowych, a tym bardziej ich ponowne wykorzystywanie. W takim wypadku potencjalne ujawnienie danych (w tym w celu ich ponownego wykorzystywania) mogłoby mieć miejsce jedynie na wniosek zainteresowanego (użytkownika), lecz wówczas pojawia się pytanie o podstawą prawną dla takiego przetwarzania (zob. Rozdział 7).

6.3. Relacja prawa do ochrony danych osobowych i prawa do ponownego wykorzystywania w ustawie o ponownym wykorzystywaniu informacji sektora publicznego

W ustawie o ponownym wykorzystywaniu informacji sektora publicznego stosunek prawa do ochrony danych osobowych i prawa do ponownego wykorzystywania informacji sektora publicznego można ustalić w oparciu o dwie grupy przepisów. Po pierwsze, w ustawie tej – w przeciwieństwie do UDIP – zawarto przepisy, które wprost odwołują się do ochrony danych osobowych i właściwych przepisów ogólnego rozporządzenia. Przepisy, które bezpośrednio określają relację między dwa porządkami regulacyjnymi, zostały wprowadzone dwukrotną nowelizacją UPW przeprowadzoną w ramach dostosowania przepisów krajowych do ogólnego rozporządzenia. Po drugie, relację tę można również pośrednio zrekonstruować w oparciu – o znane z przepisów UDIP – ograniczenie prawa do ponownego wykorzystywania informacji sektora publicznego ze względu na prywatność osoby fizycznej. Z uwagi na chronologię obowiązywania przepisów w pierwszej kolejności zostanie omówiona relacja pośrednia, a następnie relacja bezpośrednia w kontekście wykonania przepisów ogólnego rozporządzenia w UPW.

6.3.1. Prywatność jako przesłanka ograniczająca ponowne wykorzystywanie informacji sektora publicznego

W krajowym stanie prawnym dla wyznaczenia relacji pomiędzy dwoma prawami konieczne jest uwzględnienie art. 6 ust. 2 UPW, zgodnie z którym prawo do ponownego wykorzystywania podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Przepisy UPW – wzorem art. 5 ust. 2 UDIP – przewidują dwie przesłanki ograniczenia prawa do prywatności, które dotyczą informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji oraz rezygnacji osoby fizycznej ze swojego prawa do prywatności, przy czym w UPW nie zdefiniowano tych pojęć, ustawa ta nie zawiera w tym względzie także żadnych odesłań. Dla omawianego zagadnienia kluczowe jest zatem rozstrzygnięcie trzech kwestii, tj. prywatności osoby fizycznej jako jednego z ograniczeń prawa do ponownego wykorzystywania, pojęcia osoby pełniącej funkcje publiczne oraz informacji związanych z pełnieniem tej funkcji, jak również koncepcji rezygnacji z prawa do prywatności. W związku z tym, że przepisy UPW w tym zakresie stanowią odzwierciedlenie przepisów UDIP, przedmiotowe pojęcia na gruncie obu ustaw pozostają tożsame, uzasadnionym jest zatem odwołanie się do poglądów doktryny i orzecznictwa wypracowanych na gruncie prawa dostępu do informacji publicznej.

Pojęcie prywatności jest powszechnie używane i występuje w tekstach prawnych, to pozostaje ono trudne do zdefiniowania (zob. Rozdział 2.1.). Ponadto jest kategorią wspólną dla wielu dziedzin prawa i wartością chronioną na gruncie różnych gałęzi prawa oferujących następczą ochronę prywatności według przepisów KC o ochronie dóbr osobistych (art. 23 i 24) oraz ochronę prewencyjną wynikającą z przepisów o ochronie danych osobowych[657].

Jak wcześniej wykazano treść i zakres pojęcia prywatności można wyznaczyć w oparciu o regulację konstytucyjną. Konstytucja RP przewiduje w art. 47, że każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym, a jednocześnie w art. 51 gwarantuje jednostce prawo do ochrony danych osobowych, na które składa się kilka wyodrębnionych w jego treści uprawnień, w tym w ust. 1 autonomię informacyjną jednostki poprzez wskazanie, że nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby oraz – w ust. 2 – ustalenie ram ingerencji władz publicznych w sferę informacyjną jednostki. Władze

[657] *M. Sakowska-Baryła*, Dostęp do informacji publicznej a ochrona danych osobowych, s. 226-227.

publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.

W literaturze przedmiotu[658] najczęściej wskazuje się na obszary życia człowieka, które powinny zostać objęte prawem do prywatności. Za kryterium rozróżnienia poszczególnych sfer życia osobistego jednostki przyjmuje się stopień w jakim jednostka ma prawo odosobnienia od społeczeństwa w zakresie swojego życia. W tym kontekście część doktryny posługuje się pojęciem prywatności informacyjnej[659].

W ujęciu normatywnym prywatność odnoszona jest do stanu, w którym osoba fizyczna jest wolna od ingerencji innych pomiotów i dla nich niedostępna, w tym w sferze informacyjnej, decydując o tym, jakie informacje o niej, komu i na jakich zasadach są przekazywane, i jest w stanie przewidzieć, w jaki sposób będą wykorzystywane[660].

Prywatność postrzega się jako prawo do bycia pozostawionym w spokoju, prawo do autonomii, prawo do kontroli nad ujawnianiem informacji dotyczącej konkretnej osoby, prawo do poszanowania życia rodzinnego, tajemnicy, intymności[661]. Zasadniczo prywatność należy pojmować jako stan, w którym jednostka jest pozostawiona w spokoju i wolna od ingerencji zewnętrznych podmiotów tak publicznych, jak i prywatnych, także w sferze dysponowania informacjami o sobie w takim zakresie, jaki dotyczy jej życia osobistego[662]. Konieczność ochrony prywatności spowodowała ukształtowanie się prawa na podstawie którego każdy może domagać się, aby nieuprawnione osoby nie mieszały się w do jego życia prywatnego, zwłaszcza przez rozpowszechnianie wiadomości[663].

W zakresie przetwarzania informacji ochrona prywatności może mieć dwa różne znaczenia, tj. oznaczać sekret (*secrecy*) lub kontrolę jednostki nad jej indywidualnymi informacjami (*control over personal information*)[664]. Prawo jednostki będzie w szczególności

---

[658] Zob. m.in. *A. Kopff*, Koncepcja praw do intymności i do prywatności życia osobistego, „Studia cywilistyczne" t. XX, Kraków 1972; *M. Safjan*, Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym, „Państwo i prawo" 2002, nr 6; *K. Wygoda*, Ochrona danych osobowych i prawo do informacji o charakterze osobowym [w:] *B. Banaszak, A. Preisner (red.)*, Prawa i wolności obywatelskie, Warszawa 2002; *Sibiga G.*, Dostęp do informacji publicznej a prawa do prywatności jednostki i ochrony jej danych osobowych, „Samorząd Terytorialny" 2003, nr 11; *M. Braciak*, Prawo do prywatności, Warszawa 2004; *I. Lipowicz*, Konstytucyjne podstawy ochrony danych osobowych [w:] *P. Fajgileski (red.)* Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia; *Sobczyk P.*, Ochrona danych osobowych jako element prawa do prywatności, „Zeszyty prawnicze UKSW" 2009, nr 1.

[659] *M. Braciak*, Prawo do prywatności, , s. 41.

[660] *M. Sakowska – Baryła*, Ograniczenia prawa do ponownego wykorzystywania [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 63-64.

[661] *Ibidem*, s. 63.

[662] *Ibidem*, s. 64.

[663] *M. Sakowska – Baryła,* Dostęp do informacji publicznej a ochrona danych osobowych, s. 227.

[664] Zob. *D. J. Solove*, Understanding privacy, Harvard University Press 2008, str. 21 i n.

obejmowało gwarancję, że nikt, w tym władze publiczne, nie będzie ujawniał faktów dotyczących życia prywatnego i rodzinnego jednostki, czy manipulował taką informacją[665]. Przede wszystkim to sama jednostka, w ramach autonomii informacyjnej, kontroluje treść i obieg informacji na swój temat.

W orzecznictwie przyjmuje się pewną gradację dostępności informacji w zależności od tego, z jakiej sfery one pochodzą. Inaczej traktuje się informacje o jednostce dotyczące jej sfery zawodowej, wykonywania przez nią funkcji publicznych, podejmowania różnego rodzaju działań w sferze publicznej, inaczej zaś informacje dotyczące tego, co dla człowieka intymne, indywidualne, niedostępne dla szerszej publiczności. Zwykle wskazuje się, że do prywatności jednostki należą informacje dotyczące jej zdrowia, życia rodzinnego, towarzyskiego, seksualnego, sposobu spędzania wolnego czasu, sytuacji majątkowej[666].

Ze względu na to, że prywatność jest dobrem przynależnym konkretnej osobie fizycznej, informacje należące do tej sfery mogą stanowić dane osobowe. Ochrona danych osobowych służy ochronie prywatności. Zasady ochrony danych osobowych mają na celu zapewnienie poszanowania autonomii informacyjnej jednostki, w tym samodzielnego decydowania o ujawnianiu innym podmiotom informacji dotyczących własnej osoby, a także sprawowania kontroli nad tymi informacjami nawet jeśli znajdują się w posiadaniu innych osób[667].

Celem art. 6 ust. 2 UPW jest ochrona informacji ze sfery prywatności, natomiast autonomia informacyjna i zasady ochrony danych osobowych odnoszą się do wszelkich informacji dotyczących osoby fizycznej, zarówno prywatnych, jak i spoza sfery prywatności. W związku z tym przedmiotowe ograniczenie ponownego wykorzystywania będzie miało miejsce, gdy podmiot zobowiązany dysponuje informacjami ze sfery prywatności, które stanowią jednocześnie informacje sektora publicznego[668]. W pozostałych przypadkach, tj. gdy informacje nie dotyczą prywatności jednostki, o dopuszczalności ich ujawnienia do ponownego wykorzystywania będzie trzeba decydować na podstawie przepisów o ochronie danych osobowych. Procedury ochrony danych osobowych dotyczą wszystkich informacji będących danymi osobowymi[669].

---

[665] *J. Braciak*, op. cit., s. 41.

[666] *M. Sakowska – Baryła*, Ograniczenia prawa do ponownego wykorzystywania [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 64. Zob. wyroki NSA z dnia 30.09.2015 r., I OSK 2093/14; z 18.02.2015 r., I OSK 796/14; z 06.02. 2015 r., I OSK 650/14; wyrok SN z dnia 08.11.2012 r., I CSK 190/12.

[667] *B.Fischer, A.Piskorz-Ryń (red.), M.Sakowska-Baryła, J.Wyporska-Frankiewicz A. Piskorz-Ryń (red.)*, Komentarz, 2017, s. 97.

[668] *Ibidem*, s. 98.

[669] *Ibidem*.

Problem kolizji prawa do informacji publicznej z prawem do ochrony danych osobowych byłem przedmiotem licznego orzecznictwa sądowego. Przykładowo sądy przyznawały priorytet prawu do informacji publicznej w odniesieniu do kontrahentów podmiotów publicznych, uzasadniając, że w ramach gospodarki rynkowej nie istnieje przymus zawierania umów z podmiotami publicznymi. Dlatego podmiot (w tym osoba fizyczna) zawierając umowę cywilnoprawną z podmiotem publicznym nie może oczekiwać, że w zakresie takich danych jak imię i nazwisko lub firma, przedmiot umowy, wysokość wynagrodzenia, zachowa prawo do prywatności[670].

Zasada jawności relewantnych danych osobowych podmiotów będących stronami umów zawieranych z podmiotami publicznymi, korzystających z majątku publicznego – jest podkreślana w obecnie jednolitej linii orzeczniczej Naczelnego Sądu Administracyjnego[671]. W wyroku NSA z dnia 4 lutego 2015 r. (I OSK 531/15) stwierdzono, że dane o kontrahentach jednostki samorządu terytorialnego, takie jak ich imiona i nazwiska, podlegają udostępnieniu w trybie informacji publicznej - i nie podlegają wyłączeniu z uwagi na prywatność tych osób wskazaną art. 5 ust. 2 UDIP.

Do sfery prywatności orzecznictwo nie zalicza również informacji o przekazaniu konkretnej osobie fizycznej środków z majątku publicznego w ramach dofinansowania. Jak wskazał WSA w Warszawie „wykaz kręgu podmiotów, które otrzymały dofinansowanie od Polskiej Agencji Rozwoju Przedsiębiorczości w ramach realizacji prowadzonego przez nią programu, a więc podmiotów, które zostały zasilone majątkiem publicznym, jest informacją publiczną”[672]. Bez znaczenia dla określenia danych udostępnianych podmiotów ma okoliczność czy są to osoby fizyczne czy też inne podmioty prawa.

Co istotne, wydaje się, że linia orzecznicza wskazująca na jawność danych osobowych kontrahentów podmiotów publicznych zostanie podtrzymana również po rozpoczęciu stosowania ogólnego rozporządzenia. W wyroku WSA w Gdańsku z 13 lutego 2018 r. (II SA/Gd 665/18, wyrok nieprawomocny) w ocenie Sądu, udostępnieniu tych danych nie sprzeciwiają się przepisy RODO, a „podstawą udostępnienia danych osobowych w ramach dostępu do informacji publicznej jest art. 6 ust. 1 lit. e rozporządzenia (przetwarzanie jest

[670] Por. wyroki: SN z 08.11.2012 r., I CSK 190/12; NSA z 11.12.2014 r., I OSK 213/14; NSA z 04.02.2015 r., I OSK 531/14; WSA w Gorzowie Wielkopolskim z 19.05.2016 r., II SAB/Go 33/16; WSA w Gdańsku z 04.09.2013 r., II SA/Gd 447/13; WSA we Wrocławiu z 09.11.2016 r., IV SAB/Wr 183/16; WSA w Łodzi z 20.04.2017 r., II SA/Łd 100/17; WSA w Poznaniu z 06.04.2017 r., IV SA/Po 47/17, wyrok NSA z 05.01.2016 r., I OSK 3184/14.
[671] Por. wyroki NSA z: 22.03.2016 r., I OSK 2317/14; 13.04.2016 r., I OSK 2563/14; 15.06.2016 r., I OSK 3217/14; 25.11.2016 r., I OSK 2153/14.
[672] Wyrok WSA w Warszawie z dnia 2 listopada 2010 r., II SAB/WA 253/10. Zob. również wyrok WSA w Łodzi w wyrok z dnia 8 lutego 2012 r., II SAB/Łd 101/11.

niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi) w związku z określonymi przepisami prawa krajowego, które w naszym przypadku zawiera UDIP. W konsekwencji, ujawnienie imienia i nazwiska osób fizycznych zawierających umowy z podmiotem publicznym wykonującym zadania publiczne związane z obrotem mieniem publicznym, dokonane w zgodzie z art. 5 ust. 2 u.d.i.p. oraz art. 61 ust. 3 i art. 31 ust. 3 Konstytucji RP, nie mogłoby naruszać postanowień rozporządzenia".

Granicę ochrony prywatności na gruncie art. 6 ust. 2 UPW wyznacza informacja o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji.

Sądownictwo administracyjne i doktryna opowiada się za szerokim rozumiem pojęcia osoby pełniącej funkcje publiczne[673]. Przyjmuje się, że wymieniony w art. 115 § 13 i 19 KK katalog osób uznanych przez ustawodawcę za funkcjonariuszy publicznych ma charakter jedynie podstawowy i niewyczerpujący[674]. Podkreśla się, że pojęcie "osoby pełniącej funkcję publiczną" ma na gruncie UDIP autonomiczne i szersze znaczenie niż pojęcie funkcjonariusza publicznego, o którym mowa w Kodeksie karnym[675]. Najprostszym wyjaśnieniem pojęcia osoby pełniącej funkcję publiczną jest przyjęcie, że osoba, aby mogła być za taką uznana, musi

[673] Na temat pojęcia osoby pełniącej funkcje publiczne zob. m.in. *M. Sakowska-Baryła*, Dostęp do informacji publicznej a ochrona danych osobowych, s. 293-296 i tej autorki: Współstosowanie ustaw o dostępie do informacji publicznej i ochronie danych osobowych przy udostępnianiu informacji o osobie pełniącej funkcję, „Orzecznictwo Sądu Apelacyjnego w Łodzi" 2015, nr 2, s. 28 i nast. oraz Dostęp do informacji o osobach pełniących funkcje publiczne w świetle orzecznictwa i praktyki, „Informacja w Administracji Publicznej" 2016, nr 2, s. 11 i nast., *P. Sitniewski*, Kim jest osoba pełniąca funkcję publiczną?, „Informacja w Administracji Publicznej" 2017, nr 3, s. 47-55.

[674] W myśl art. 115 § 13 KK Funkcjonariuszem publicznym jest:
1) Prezydent Rzeczypospolitej Polskiej;
2) poseł, senator, radny;
2a) poseł do Parlamentu Europejskiego;
3) sędzia, ławnik, prokurator, funkcjonariusz finansowego organu postępowania przygotowawczego lub organu nadrzędnego nad finansowym organem postępowania przygotowawczego, notariusz, komornik, kurator sądowy, syndyk, nadzorca sądowy i zarządca, osoba orzekająca w organach dyscyplinarnych działających na podstawie ustawy;
4) osoba będąca pracownikiem administracji rządowej, innego organu państwowego lub samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe, a także inna osoba w zakresie, w którym uprawniona jest do wydawania decyzji administracyjnych;
5) osoba będąca pracownikiem organu kontroli państwowej lub organu kontroli samorządu terytorialnego, chyba że pełni wyłącznie czynności usługowe;
6) osoba zajmująca kierownicze stanowisko w innej instytucji państwowej;
7) funkcjonariusz organu powołanego do ochrony bezpieczeństwa publicznego albo funkcjonariusz Służby Więziennej;
8) osoba pełniąca czynną służbę wojskową, z wyjątkiem terytorialnej służby wojskowej pełnionej dyspozycyjnie;
9) pracownik międzynarodowego trybunału karnego, chyba że pełni wyłącznie czynności usługowe.
§ 19. Osobą pełniącą funkcję publiczną jest funkcjonariusz publiczny, członek organu samorządowego, osoba zatrudniona w jednostce organizacyjnej dysponującej środkami publicznymi, chyba że wykonuje wyłącznie czynności usługowe, a także inna osoba, której uprawnienia i obowiązki w zakresie działalności publicznej są określone lub uznane przez ustawę lub wiążącą Rzeczpospolitą Polską umowę międzynarodową.

[675] Wyrok NSA z 15.06.2015 r., I OSK 3217/14.

w ramach instytucji publicznej realizować w pewnym zakresie nałożone na tę instytucję zadania publiczne, z wyłączeniem stanowisk usługowych i technicznych.

Osobą pełniącą funkcję publiczną jest każdy, kto pełni funkcję w organach władzy publicznej lub też w strukturach osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej, jeżeli tylko funkcja ta ma związek z dysponowaniem majątkiem państwowym lub samorządowym albo zarządzaniem sprawami związanymi z wykonywaniem swych zadań przez władze publiczne, a także inne podmioty, które tę władzę realizują lub gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa[676].

Wykładni pojęcia funkcji publicznej dokonał Trybunał Konstytucyjny w wyroku z dnia 20 marca 2006 r. (K17/05). W ocenie TK, aby zdekodować to pojęcie należy badać czy określona osoba w ramach instytucji publicznej realizuje w pewnym zakresie nałożone na tę instytucję zadanie publiczne. Chodzi zatem o podmioty, którym przysługuje co najmniej wąski zakres kompetencji decyzyjnej w ramach instytucji publicznej. W tym kontekście Trybunał zaznaczył, że nie każdy pracownik takiej instytucji będzie tym funkcjonariuszem, którego sfera chronionej prywatności może być zawężona z perspektywy uzasadnionego interesu osób trzecich, realizującego się w ramach prawa do informacji. Nie można twierdzić, że w wypadku ustalenia kręgu osób, których życie prywatne może być przedmiotem uzasadnionego zainteresowania publiczności, istnieje jednolity mechanizm czy kryteria badania zakresu możliwej ingerencji. TK dostrzegł, że trudno byłoby stworzyć ogólny, abstrakcyjny, a tym bardziej zamknięty katalog tego rodzaju funkcji i stanowisk.

W orzecznictwie administracyjnym zaznacza się, że dana osoba może w pewnym okresie być ujmowana jako pełniąca funkcję publiczną i dla tego okresu informacja związana z pełnieniem tej funkcji będzie podlegać udostępnieniu, natomiast w późniejszym czasie może być pozbawiona tego przymiotu. Zaprzestanie pełnienia funkcji publicznej nie oznacza jednak, że informacje z okresu, gdy ta funkcja była pełniona, przestają podlegać udostępnieniu z ograniczeniem prywatności jednostki. Przeciwnie, wciąż będą one udostępniane osobom zainteresowanym, jednak tylko w tym relewantnym zakresie czasowym[677].

Należy zauważyć, że w orzecznictwie sądowym pomimo szczegółowego wyjaśnienia pojęcia „osoby pełniącej funkcję publiczną" oraz „informacje mające związek z pełnioną funkcją", zauważalne są jednak różnice poglądów w rozumieniu każdego z nich. W niektórych

[676] Zob. *I. Kamińska, M. Rozbicka-Ostrowska*, Ustawa o dostępie do informacji publicznej, 2012, s. 87; *M. Bidziński* [w:] *M. Bidziński, M. Chmaj, P. Szustakiewicz*, Ustawa o dostępie do informacji publicznej. Komentarz, Warszawa 2010, s. 73-74.
[677] Zob. wyrok NSA z 31.07.2013 r., I OSK 742/13

orzeczeniach rozumienie funkcji publicznej wykracza poza sferę związaną z realizacją określonych zadań w ramach wykonywania władzy publicznej, czy co najmniej działaniem w ramach struktur władzy publicznej. Przykładowo w postanowieniu NSA z dnia z dnia 13 stycznia 2016 r. (I OSK 2932/15) adwokata zakwalifikowano jako „osobę wykonującą zadania publiczne" i w związku z tym stwierdzono się, że „w zakresie tych wykonywanych przez niego zadań ochrona jego prywatności jest ograniczona zgodnie z art. 5 ust. 2 ustawy o dostępie do informacji publicznej" [678]. Można wręcz odnotować, iż ostatnimi laty, w orzecznictwie NSA pojawia się tendencja do rozszerzania kręgu osób, traktowanych jako osoby pełniące funkcje publiczne, której przykładem jest m.in. wyrok NSA z 19 grudnia 2016 r. wydany w sprawie I OSK 2060/16 gdzie stwierdzono, iż osoba kupująca nieruchomość od Skarbu Państwa, co prowadzi wszak do zubożenia zasobu nieruchomości w jego własności, wpływa na sprawę publiczną, tj. gospodarkę nieruchomościami publicznymi. W tym zatem aspekcie jest "osobą pełniącą funkcję publiczną", o której mowa w art. 5 ust. 2 UDIP[679].

W innej sprawie wyrokiem z dnia 21 czerwca 2018 r. (SA/Wa 735/17) NSA uznał, że nazwiska ekspertów przygotowujących podstawę programową dla szkół są jawne i podlegają udostępnieniu w trybie ustawy o dostępie do informacji publicznej. Zdaniem sądu osoby wchodzące w skład zespołów tworzących dla Ministerstwa Edukacji Narodowej założenia do podstawy programowej kształcenia ogólnego dzieci wpłynęły na kształt przyjętej podstawy programowej a więc na treść decyzji o charakterze ogólnospołecznym. Tym samym, w ocenie Sądu zasadnym jest traktowanie tych osób, jako pełniących funkcje publiczne. Dane o osobach współpracujących w szczególności z organami administracji publicznej, a więc o osobach mających choćby minimalny wpływ na kształtowanie się sposobu funkcjonowania tychże organów, jak też dane o kontrahentach tych podmiotów publicznych, takie jak imiona i nazwiska, podlegają udostępnieniu w trybie dostępu do informacji publicznej[680].

Przywołane orzeczenie dotyka zatem innego istotnego zagadnienia, ochroną przed ujawnieniem – ze względu na prywatność osoby fizycznej - nie są także objęte dane innych osób niż osób pełniących funkcje publiczne. Tylko stwierdzenie istnienia adekwatnego związku między żądaną informacją o osobie a pełnieniem przez tę osobę funkcji publicznej – uzasadnia danie prymatu dyspozycji art. 61 ust. 1 Konstytucji RP przed art. 51 ust. 1 i art. 47 ustawy zasadniczej. To właśnie w prawidłowym i precyzyjnym ustaleniu istnienia granic tego związku,

[678] Zob. wyrok WSA w Szczecinie z 22 czerwca 2016 r., II SA/Sz 428/16.
[679] Zob. wyrok NSA z dnia 21 czerwca 2018 r., I OSK 166/18.
[680] Zob. *D. Sybilski*, Jawne dane osobowe ekspertów przygotowujących podstawę programową dla szkół, „Informacja w Administracji Publicznej" 2019, nr 1, s. 31-34.

należy upatrywać właściwej ochrony prawa do prywatności jednostek, w tym osób pełniących funkcje publiczne[681]. W ocenie NSA, ingerencja w prywatność polegająca na ujawnieniu nazwiska osoby pełniącej funkcje publiczną nie przekracza granicy intymności oraz życia rodzinnego wyznaczonej przepisami art. 47 i art. 61 ust. 3 Konstytucji RP oraz art. 8 i art. 10 Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności[682]. Mieści się w ramach wyjątku sformułowanego w art. 5 ust. 2 zdanie drugie UDIP odczytywanego w kontekście równoważnych norm konstytucyjnych ustanawiających prawo do dostępu do informacji publicznej oraz ochronę prywatności[683].

W wyroku z 19 października 2018 r. wydanym już po wejściu w życie RODO WSA w Olsztynie z 19 października 2018 r. (II SA/Ol 542/18, wyrok nieprawomocny) z kolei uznał, że lekarze, niebędący funkcjonariuszami publicznymi, ale podlegający wpisowi do właściwego rejestru, nie mogą korzystać z ochrony danych w rejestrze tym zawartych – w szczególności dotyczy to ich imion i nazwisk. Lekarze wykonują zawód zaufania publicznego i szczególnej odpowiedzialności, stąd też winni być podmiotami możliwymi do pełnej identyfikacji na płaszczyźnie zawodowej. Przepisy: art. 5 ust. 1 pkt b), art. 6 ust. 1 pkt c) RODO, art. 23 i art. 24 KC oraz art. 5 ust. 2 UDIP „nie wykluczały możliwości uwzględnienia wniosku skarżącego w zakresie udostępnienia imion i nazwisk lekarzy legitymujących się specjalizacją z onkologii klinicznej, świadczących usługi medyczne finansowane ze środków publicznych w poszczególne dni i godziny, którzy zostali sprawozdani przez Ośrodek. Powołane (…) przepisy RODO dotyczą bowiem zbierania i przetwarzania danych osobowych osób fizycznych, a nie ich udostępniania w ramach dostępu do informacji publicznej. Te kwestie regulują bowiem przepisy UDIP".

Podsumowując tę część rozważań, należy mieć na uwadze, że choć zakres podlegających ujawnieniu informacji o osobie pełniącej funkcje publiczne jest znacznie szerszy, niż ma to miejsce w przypadku osób nienależących do tej grupy podmiotowej, podmiot zobowiązany za każdym razem musi rozważyć, czy konkretna informacja nie dotyczy chronionej prawem prywatności. Pełnienie funkcji publicznej nie może prowadzić do pozbawienia danej osoby sfery, w której pozostaje ona wolna od zewnętrznego zainteresowania[684]. Jako przykładowe informacje, które nie dotyczą pełnienia funkcji

[681] Zob. wyrok NSA z dnia 18 lutego 2015 r., sygn. akt I OSK 695/14.
[682] Dz. U. z 1993 r. Nr 61, poz. 284 ze zm.
[683] Wyrok NSA z dnia 21 czerwca 2018 r., SA/Wa 735/17.
[684] *M. Sakowska-Baryła*, Ograniczenia prawa do ponownego wykorzystywania ISP [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska,* op. cit., s. 73.

publicznej i nie są z nią związane można wymienić, informacje dotyczące korzystania z zakładowego funduszu świadczeń socjalnych, informacje o hobby, zainteresowaniach, sposobie spędzania wolnego czasu, przynależności wyznaniowej, stanie zdrowia, stanie rodzinnym, prywatnym numerze telefonu, prywatnym adresie mailowym, adresie zamieszkania[685].

Ostatnim elementem ograniczenia, o którym mowa w art. 6 ust. 2 UPW jest zagadnienie rezygnacji z ochrony prywatności, czyli drugiej przesłanki ograniczającej prawo do prywatności. Przedmiotem „rezygnacji" mogą być wszelkie informacje o osobie fizycznej mieszczące się w jej sferze prywatności omówionej powyżej. W UPW (podobnie zresztą jak i w UDIP), nie określono formy rezygnacji z prywatności, niewątpliwie musi ona być wyraźna. Konsekwencją jej złożenia jest rezygnacja z ochrony prawa do prywatności przez osobę, której informacja dotyczy, wyłącza bezprawność naruszenia jej prawa do prywatności[686].

Należy zauważyć, że na gruncie ogólnego rozporządzenia niejasna pozostanie relacja rezygnacji osoby fizycznej ze swojego prawa do prywatności w stosunku do instytucji zgody na przetwarzanie danych w rozumieniu art. 7 RODO. Należy uznać, że oświadczenie w przedmiocie rezygnacji z prawa ze względu na swoje konsekwencje w postaci udostępnienia danych osobowych ma porównywalny charakter do zgody i może znaleźć w takiej sytuacji zastosowanie przepis art. 7 RODO (zagadnienie to zostanie omówione w Rozdziale 7.5).

6.3.2. Wykonanie wymogów z ogólnego rozporządzenia w krajowych przepisach o ponownym wykorzystywaniu informacji sektora publicznego

Jak wskazano powyżej, artykuł 86 RODO, powinien być wykonany w prawie krajowym. Konsekwencją uznania ponownego wykorzystywania za interes publiczny jest również konieczność wykonania art. 6 ust. 2 i 3 w związku z ust. 1 lit. e RODO. Oznacza to potrzebę uwzględnienia przepisów o ochronie danych osobowych w krajowych przepisach regulujących nie tylko ponowne wykorzystywanie informacji sektora publicznego, ale przede wszystkim dostęp do dokumentów urzędów (informacji publicznej). Analiza zaniechania polskiego ustawodawcy w tym zakresie i jego konsekwencje dla realizacji prawa dostępu do informacji publicznej zawierającej dane osobowe wykracza poza zakres niniejszej pracy. W związku z tym, że regulacja ponownego wykorzystywania opiera się na unijnych i krajowych systemach dostępu do dokumentów (informacji) i pozostaje dla nich bez

[685] *Ibidem.*
[686] *B. Fischer, A. Piskorz-Ryń (red.), M. Sakowska-Baryła, J. Wyporska-Frankiewicz*, Komentarz, 2017, s. 98.

uszczerbku, brak wykonania art. 86 RODO w UDIP miałby konsekwencje dla przepisów o ponownym wykorzystywaniu, gdyby te ostanie nie przewidywały w swoim zakresie kwestii ochrony danych osobowych. Z tego powodu kwestia zastosowania przepisów RODO dla ponownego wykorzystywania informacji sektora publicznego nie budzi kontrowersji, jak stosowanie przepisów ogólnego rozporządzenia w kontekście udostępniania informacji publicznej zawierającej dane osobowe[687].

Dostosowanie przepisów UPW do wymagań ogólnego rozporządzenia o ochronie danych osobowych odbyło się w dwóch etapach[688].

W pierwszej kolejności przepisami UODO2018 nadano nowe brzmienie art. 7 ust. 2 UPW zgodnie z którym „przepisy ustawy nie naruszają przepisów o ochronie danych osobowych". Była to w istocie jedynie zmiana porządkująca, bowiem w poprzednim brzmieniu art. 7 ust. 2 stanowił o tym, że przepisy niniejszej ustawy nie naruszają przepisów ustawy z 29.8.1997 r. o ochronie danych osobowych, która została uchylona nową ustawą o ochronie danych osobowych służącej stosowaniu RODO.

W mojej opinii nie sposób uznać art. 7 ust. 2 za skuteczną próbę określenia relacji pomiędzy prawem do ponownego wykorzystywania a ochroną danych osobowych spełniającej wymóg art. 86 RODO. Przepis ten zarówno w pierwotnym – jak i zresztą aktualnym brzmieniu nadanym UWprowRODO – nie wnosi żadnej treści normatywnej. W tekście prawnym nie należy zamieszczać przepisów zawierających formułę „nie narusza" . Zgodnie bowiem z § 11 Zasad techniki prawodawczej w ustawie nie zamieszcza się wypowiedzi, które nie służą wyrażaniu norm prawnych. Tekst prawny powinien zawierać wyłącznie te wypowiedzi, które służą wyrażeniu norm postępowania lub dokonaniu aktów konwencjonalnych. Zatem zamieszczanie w tekście prawnym jakichkolwiek wypowiedzi, które służą innemu celowi, jest tym bardziej niebezpieczne, że takiej wypowiedzi może być i jest nadawana treść normatywna. O ile zatem art. 7 ust. 2 UPW nie można uznać za klasyczną normę kolizyjną, o tyle ma on walor informacyjny, w szczególności dla podmiotu zobowiązanego, który podejmując decyzję o ujawnieniu danych osobowych w ramach informacji sektora publicznego, powinien wziąć pod uwagę przepisy o ochronie danych osobowych[689]. W doktrynie zauważa się, że przepis ten

[687] Zdaniem niektórych autorów udostępnianie w ramach dostępu do informacji publicznej danych osobowych nie jest objęte zakresem prawa UE i w konsekwencji RODO nie znajduje w tym zakresie zastosowania. Zob. *P. Litwiński*, Unia nie wtrąca się do przepisów o informacji publicznej, Rzeczypospolita z 13.8.2019 r., https://www.rp.pl/Opinie/308139983-RODO-a-listy-poparcia-do-KRS-Unia-nie-wtraca-sie-do-przepisow-o-informacji-publicznej.html (dostęp: 13.08.2020 r.). Inaczej m.in. *G. Sibiga, I. Małobęcka-Szwast*, Relacje, s. 63.

[688] Zob. *D. Sybilski*, Nowelizacja ustawy o ponownym wykorzystywaniu informacji sektora publicznego dostosowująca do przepisów ogólnego rozporządzenia o ochronie danych osobowych, „Prawo Mediów Elektronicznych"2019, nr 4, s. 74–79.

[689] *Ibidem*, s. 75.

potwierdza konieczność stosowania przepisów o ochronie danych osobowych do ponownego wykorzystywania informacji sektora publicznego i można w tym wypadku mówić o współstosowaniu tych dwóch porządków regulacyjnych, ale w taki sposób, aby zapewnić brak naruszenia zasad ochrony danych wynikających z przepisów o ochronie danych osobowych[690]. Należy zwrócić uwagę, że przepis stanowi powtórzenie równie ogólnego rozwiązania zawartego w art. 1 ust. 4 dyrektywy 2019/1024/UE[691]. Nie można zatem uznać, że art. 7 ust. 2 UPW stanowi wystarczającą podstawą „pogodzenia" dwóch różnych uprawnień, ponieważ przenosi cały ciężar wyważenia tych uprawnień na poziom interpretatora, czyli w praktyce na podmiot zobowiązany przekazujący lub udostępniający informacje do ponownego wykorzystywania, podczas gdy istotą rozwiązania przewidzianego w art. 86 RODO jest to, aby jego dyspozycję wykonać w prawie krajowym. Unormowanie to nie jest zatem skutecznym środkiem dla ustalenia wzajemnych relacji pomiędzy ochroną danych osobowych a ponownym wykorzystywaniem informacji sektora publicznego. W konsekwencji stosującym ten przepis podmiotom zobowiązanym nie pozwala na jednoznaczne ustalenie, co norma ta ma oznaczać w praktyce[692].

Projektodawca uznał, że konieczne jest jednak szersze uwzględnienie przepisów RODO w UPW, dlatego też w ramach UWprowRODO zmieniono również przepisy o ponownym wykorzystywaniu informacji sektora publicznego. Nowelizacja objęła zmianę art. 7 ustawy polegającą na ograniczeniu wykonania obowiązków informacyjnych, o których mowa w art. 13, 14 i 19 RODO w związku z realizacją prawa do ponownego wykorzystywania informacji stanowiących lub zawierających dane osobowe. Ponadto dodano w – wymienionym w art. 14 ust. 4 UPW – katalogu warunków ponownego wykorzystywania pkt 4 dotyczący „informacji sektora publicznego zawierającej dane osobowe". Tym samym przesądzono w sposób nie budzący wątpliwości, że możliwe jest ponowne wykorzystywanie danych osobowych w ramach informacji sektora publicznego. Zagadnieniom tym poświęcono rozdział 9.

Jednocześnie ustawodawca pozostawił w niezmienionym brzmieniu art. 6 ust. 2 UPW ograniczającym ponowne wykorzystywanie ze względu na prywatność osoby fizycznej. Należy podkreślić, że poza wymienionymi wyżej przepisami służącymi wykonaniu RODO, ustawodawca nie zdecydował o wprowadzaniu odrębnej przesłanki ograniczającej ponowne wykorzystywanie ze względu na ochronę danych osobowych. Trzeba jednak zauważyć, że

[690] *B.Fischer, A.Piskorz-Ryń (red.), M.Sakowska-Baryła, J.Wyporska-Frankiewicz,* Komentarz, 2017, s. 198 i n.
[691] Niniejsza dyrektywa pozostaje bez uszczerbku dla krajowego i unijnych przepisów dotyczących ochrony danych osobowych, w szczególności rozporządzenia (UE) 2016/679 i dyrektywy 2002/58/WE, a także odpowiadających im przepisów prawa krajowego.
[692] *M. Sakowska-Baryła*, Komentarz do art. 86, pkt 7 [w:] *M. Sakowska-Baryła (red.),* Ogólne rozporządzenie.

prywatność i ochrona danych osobowych nie są kategoriami tożsamymi pod względem przedmiotowym, a nawet podmiotowym (dopuszczalna jest bowiem ochrona sfery prywatnej osoby zmarłej), tymczasem z art. 86 RODO wynika obowiązek odniesienia się w przepisach do prawa do ochrony danych osobowych w rozumieniu RODO[693].

Pomimo wprowadzonych zmian w UPW wątpliwości budzi pełne wykonanie art. 86 RODO w zakresie „pogodzenia" ochrony danych osobowych z ponownym wykorzystywaniem informacji sektora publicznego[694], jak i realizacji rekomendacji Grupy Roboczej art. 29 w odniesieniu do określenia kategorii danych osobowych, które mogą być ponownie wykorzystywane. Pomimo że art. 6 ust. 2 RODO umożliwia przyjęcie bardziej szczegółowych przepisów regulujących relację ponownego wykorzystywania i przepisów o ochronie danych osobowych, a tym samym dostosowania przepisów RODO do tej szczególnej sytuacji przetwarzania danych osobowych, to krajowy ustawodawca zdecydował się nie doregulować stosunku konkurencyjnych uprawnień. Przepisy UPW – pomimo wprowadzonych zmian w obszarze modyfikacji sposobu spełnienia obowiązku informacyjnego oraz uwzględnienia kwestii danych osobowych w warunkach ponownego wykorzystywania, nie określają szczegółowych wymogów przetwarzania i innych środków w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności (art. 6 ust. 2 RODO). W UPW nie określono precyzyjnie zakresu danych osobowych, które mogą zostać ujawnione w ramach ponownego wykorzystywania informacji sektora publicznego i sytuacji z tym związanych, ani przesłanek, w przypadku zaistnienia których należałoby przekazać lub odmówić przekazania danych osobowych do ponownego wykorzystywania, poza sytuacją danych o osobach pełniących funkcje publiczne. Tym samym wydaje się, że przepisy UPW spełniają wymóg niezbędności (konieczności), o którym mowa w art. 6 ust. 3 zd. 2 RODO, jedynie w ograniczonym zakresie. Zagadnienie to zostanie szerzej omówione w kolejnym rozdziale.

6.4. Koncepcja współstosowania i komplementarności przepisów o ochronie danych osobowych i o ponownym wykorzystywaniu informacji sektora publicznego

Po przeprowadzeniu analizy obowiązujących przepisów pozwalających na wyznaczenie relacji pomiędzy prawem do ochrony danych osobowych oraz prawem do ponownego

[693] *G. Sibiga*, *I. Małobęcka-Szwast*, Relacje, s. 63
[694] Zob. *D. Sybilski*, Nowelizacja, s. 79 i *N. Zawadzka*, Komentarz do art. 86 pkt 6 [w:] *E. Bielak-Jomaa*, *D. Lubasz*, RODO, s. 1085.

wykorzystywania zasadnym jest odwołanie się do koncepcji współstosowania i komplementarności przepisów obu porządków regulacyjnych[695]. Dostarczają one bowiem doktrynalnych podstaw dla podsumowania wzajemnego stosunku między dwoma regulacjami. W mojej opinii koncepcje te wypracowane jeszcze na gruncie UODO1997 dla określenia wzajemnego stosunku ochrony danych osobowych z prawem dostępu do informacji publicznej pozostają wciąż aktualne również w obecnym stanie prawnym i mają zastosowanie przy realizacji do prawa do ponownego wykorzystywania informacji sektora publicznego po wejściu w życie ogólnego rozporządzenia.

Prawo do ponownego wykorzystywania informacji sektora publicznego oraz prawo do ochrony danych osobowych często postrzegane są jako uprawnienia przeciwstawne sobie lub ze sobą konkurujące. Prawo do informacji oraz ochrona danych osobowych to odrębne prawa jednostki, ale mające w pewnym zakresie „wspólną przestrzeń informacyjną"[696]. Wszelkie regulacje dotyczące prawnej ochrony informacji potencjalnie ograniczają zakres prawa do informacji. Prawo do ochrony danych osobowych powinno być rozpatrywane jako ograniczenie dostępu do informacji, bowiem wyraża ono w zakresie ochrony prywatności konkurencyjne uprawnienie, która wymaga wyważenia z prawem do informacji i to niezależnie od tego czy uważa się je za sprzeczne, czy też komplementarne, ale wymagające ustalenia granic między nimi[697].

W literaturze prezentowany jest pogląd komplementarności obu porządków regulacyjnych[698]. Komplementarność unormowań wynika wprost z przepisów Konstytucji RP, ponieważ prawo do ochrony danych osobowych (art. 51) i gwarancja prawa do prywatności (art. 47) z jednej strony a prawo do ponownego wykorzystywania informacji sektora publicznego, które można zakotwiczyć w prawie dostępu do informacji publicznej (art. 61), wolności pozyskiwania i rozpowszechniania informacji (art. 54 ust. 1), czy też prawa do informacji o stanie i ochronie środowiska (art. 74 ust. 3) z drugiej strony, kształtują sferę informacyjnych uprawnień jednostki, wzmacnianych przez wiele innych konstytucyjnych wolności i praw[699]. Biorąc pod uwagę zakres tych uprawnień, jednostka ma prawo dostępu do

[695] Koncepcja opracowana i rozwijana na gruncie UDIP i UODO1997 przez *M. Sakowską-Baryłę*. Zob. tej autorki: Prawo do ochrony danych osobowych, Wrocław 2015, s. 326; Dostęp do informacji publicznej a ochrona danych osobowych, s. 37-49, 76-103; Problem współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych [w:] *A. Mednis* (red.), Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość, s. 173-193. Na temat problematyki komplementarności zob. *G. Sibiga*, Komplementarność czy kolizja? Prawna ochrona danych osobowych a dostęp do informacji publicznych oraz o informacji o środowisku i jego ochronie [w:] *P. Fajgielski*, Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia.
[696] *G. Sibiga*, Komplementarność czy kolizja?, s. 153.
[697] *M. Sakowska – Baryła*, Prawo do ochrony danych osobowych, s. 326.
[698] Zob. *M. Sakowska - Baryła*, Dostęp do informacji publicznej a ochrona danych osobowych, s. 211.
[699] *Ibidem*, s. 39.

informacji o sprawach publicznych i prawo do dalszej dowolnej jej eksploatacji, a jednocześnie autonomię informacyjną w odniesieniu do informacji dotyczących jej osoby, z równoczesną gwarancją niedysponowania tymi informacjami przez władze publiczne bez podstawy określonej w ustawie[700]. Z drugiej strony, w doktrynie na gruncie przywołanych norm konstytucyjnych, prezentuje się również opinię, że kolizja pomiędzy dwoma uprawnieniami jest nieunikniona, czego konsekwencją będzie potrzeba wyważenia racji związanych z interesem publicznym oraz interesem jednostki[701]. Kolizja praw i zasad na poziomie konstytucyjnym nie może prowadzić w ostatecznym wyniku do pełnej eliminacji jednego z praw pozostających w konflikcie. Problemem wymagającym rozstrzygnięcia jest zawsze w takim wypadku znalezienie pewnego punktu równowagi, balansu dla wartości chronionych przez Konstytucję i wyznaczenie obszaru stosowania każdego z praw[702].

Po drugie, wzajemne relacje aktów prawnych regulujących ochronę danych osobowych oraz ponowne wykorzystywanie i ich wzajemne oddziaływanie w procesie stosowania prawa pokazują, że właściwie powinno się mówić o współstosowaniu obu porządków regulacyjnych, które wprawdzie posiadają pewien wspólny obszar wpływów, ale zasadniczo służą realizacji innych celów i gwarancji.

W poprzednim stanie prawnym wyznaczonym przepisami krajowymi implementującymi odpowiednio dyrektywy 95/46/WE oraz dyrektywy 2003/98/WE współstosowanie UODO1997 oraz UDIP (nie tylko w zakresie dostępu do informacji publicznej, ale i ponownego jej wykorzystywania, które do wejścia w życie UPW było unormowane w rozdziale 2a UDIP) było tym bardziej wyraźne, że wówczas obowiązywały dwa równorzędne akty prawne, regulujące wprawdzie różne zagadnienia, ale wzajemnie się krzyżujące. Relacji pomiędzy UODO1997 oraz UDIP nie wyznaczała reguła kolizyjna: *lex specialis derogat legi generali*, ponieważ pomimo pewnych wspólnych obszarów zdeterminowanych wspólnym dla tych aktów ogólnym pojęciem – „informacja", obie te ustawy miały inny zakres regulacji i służyły ochronie odmiennych dóbr i wartości, nie zawsze będących względem siebie w opozycji[703]. Wprawdzie jednoczesna realizacja wymogów stawianych przez te ustawy mogła rodzić – z uwagi na specyfikę obu regulacji – pewne trudności w praktyce, ponieważ zazwyczaj ten sam podmiot występował w roli zobowiązanego do udostępniania informacji publicznej oraz do udostępniania informacji publicznej w celu ponownego

[700] *Ibidem.*
[701] *G. Sibiga,* Komplementarność czy kolizja?, 155.
[702] Zob. wyrok TK z dnia 20 marca 2006 r., K 17/50.
[703] Zob. *M. Sakowska - Baryła*, op. cit., s. 77.

wykorzystywania, jak również w roli administratora danych, jednak trudności w stosowaniu przepisów tych ustaw nie oznaczały, że wzajemnie się one wykluczają, czy też, że nie stanowią aktów równorzędnych[704]. Teza znalazła swe potwierdzenie w orzecznictwie sądów administracyjnych, choć należy zaznaczyć, że nie jest to stanowisko jednolite[705]. Sądy statuując UDIP i UODO1997 jako akty równorzędne, nie przyznając żadnej z ustaw pierwszeństwa, jednocześnie podkreślały konieczność wyważenia prawa do informacji publicznej w sytuacji, gdy w tej informacji zawarte są jednocześnie dane osobowe. Z przepisów tych ustaw nie można wyprowadzić generalnego zakazu udostępnienia informacji publicznej, w treści której figurują określone dane osobowe. Jednocześnie brak też takiej regulacji, która byłaby podstawą legalizującą co do zasady uzyskanie dostępu do danych osobowych w ramach realizowanego prawa do informacji publicznej[706].

Choć ogólne rozporządzenie oraz UPW, jak i niewdrożona jeszcze do krajowego porządku prawnego dyrektywa 2019/1024 nie są aktami równorzędnymi w hierarchii źródeł prawa, to jednak w dalszym ciągu za aktualny uznawać należy pogląd o konieczności współstosowania zasad określających odpowiednio dostęp do informacji publicznej i ponownego wykorzystywania informacji sektora publicznego oraz zasad ochrony danych osobowych wszędzie tam, gdzie udostępniana, czy przekazywana informacja obejmuje dane osobowe oraz w obszarze organizacyjno-administracyjnym[707]. O ile zatem nie po wejściu w życie ogólnego rozporządzenia nie można już mówić o równorzędności obu porządków normatywnych, o tyle wciąż nie sposób uznać, że przepisy ogólnego rozporządzenia stanowią *lex specialis* dla regulacji ponownego wykorzystywania.

Jak wykazano, realizacja prawa do ponownego wykorzystywania wymaga jednocześnie respektowania zasad i procedur postępowania z danymi osobowymi określonymi przede wszystkim w RODO i przepisach prawa krajowego służącymi jego stosowaniu. W procesie udostępniania lub przekazywania informacji sektora publicznego zawierającej lub stanowiącej dane osobowe w celu ponownego wykorzystywania, jak i ponownego wykorzystywania danych osobowych przez użytkownika, oba porządki regulacyjne należy stosować jednocześnie, ponieważ służą one unormowaniu innych zagadnień i co do zasady

[704] *M. Sakowska - Baryła*, Problem współstosowania ustawy o odstępie do informacji publicznej i ustawy o ochronie danych osobowych, s. 175 i nast.
[705] Niektóre sądy przyjmowały tezę o „pierwszeństwie" UODO1997 przed przepisami UDIP, wskazując, że ma ona charakter *lex specialis*, a „odmienna wykładnia prowadziłaby do tego, że w oparciu o ustawę o dostępie do informacji publicznej legalnie można byłoby uzyskać dostęp do danych chronionych ustawą o ochronie danych osobowych". Zob. np. wyrok WSA w Warszawie z 20 kwietnia 2006 r. o sygn. akt II SA/Wa 2227/05.
[706] Zob. Wyroki NSA z:05.03.2013 r., I OSK 2872/12; z 25.4.2014 r., I OSK 2499/13.
[707] *M. Sakowska – Baryła*, Komentarz do art. 86 pkt 7 [w:] *M. Sakowska – Baryła (red.)*, Ogólne rozporządzenie.

zawarte w nich postanowienia nie pozostają ze sobą w sprzeczności, choć mogą mieć wspólny obszar regulacji, co opisano w Rozdziale 3.3. W praktyce oznacza to konieczność równoległej realizacji uprawnień i obowiązków wynikających z ogólnego rozporządzenia i UPW.

Celem przepisów o ponownym wykorzystywaniu nie jest ochrona danych osobowych, przepisy te mają przede wszystkim służyć możliwości eksploatacji informacji sektora publicznego zapewniając jednocześnie pełne poszanowanie prawa do ochrony danych osobowych, gdy dochodzi do ujawnienia danych osobowych w ramach realizacji prawa do ponownego wykorzystywania informacji sektora publicznego. Z kolei RODO nie jest regulacją „dostępową", a jej przepisy będą miały zastosowanie dopiero wtedy, gdy w ramach informacji sektora publicznego będą mogły być ujawnione dane osobowe, a następnie będzie możliwe ponowne ich wykorzystywanie.

Jeśli przy realizacji prawa do ponownego wykorzystywania informacji sektora publicznego pojawia się problem przetwarzania danych, kwestia ta ma charakter incydentalny i nie stanowi meritum regulacji UPW[708]. Oba unormowania, choć służą realizacji zgoła odmiennych celów, posiadają wspólne obszary regulacji, które sprawiają, że mamy do czynienia z krzyżowaniem się dwóch porządków regulacyjnych. Obszar wspólny, w którym spotykają się obie regulacje, pojawia się wtedy gdy ujawnieniu podlegać mają dane osobowe w ramach informacji sektora publicznego. Nawet jeśli w ramach ponownego wykorzystywania przekazuje się lub udostępnia się informacje sektora publicznego będące danymi osobowymi lub informacje, w których skład wchodzą dane osobowe, ujawnienie to nie następuje dlatego, że informacje te należą do „danych osobowych" w rozumieniu art. 4 pkt 1 RODO, ale dlatego, że stanowią one informację sektora publicznego, w stosunku do której, zasady i warunki wykorzystywania oraz tryb przekazania lub udostępniania określa UPW. Udostępnianie lub przekazanie informacji sektora publicznego w celu ponownego wykorzystywania, w której zakres wchodzą dane osobowe, następuje zatem według zasad, warunków i w trybie UPW, z jednoczesnym uwzględnieniem zasad ochrony danych osobowych wynikających z RODO i właściwych przepisów krajowych. Oznacza to, że sposób realizacji ponownego wykorzystywania informacji sektora publicznego zawierającej dane osobowe wynika z UPW, ale o dopuszczalności (przesłankach) i zasadach przetwarzania danych osobowych decydują przepisy o ochronie danych osobowych. Podmioty zobowiązane do przekazywania lub udostępniania informacji sektora publicznego do ponownego wykorzystywania powinny realizować zatem przewidziane w UPW uprawnienia dostępowe (eksploatacyjne),

[708] Tak na gruncie UODO1997 oraz UDIP *M. Sakowska – Baryła*, Problem współstosowania, s. 176.

przestrzegając jednocześnie zasad ochrony danych uregulowanych poprzez ocenę dopuszczalności przetwarzania danych, wprowadzenie odpowiednich zabezpieczeń, powołanie inspektora ochrony danych, prowadzenie odpowiedniej dokumentacji pozwalającej wykazać zgodność działania z RODO, czy realizowanie uprawnień osób, których dane dotyczą[709].

Czy można zatem stwierdzić, że zakres stosowania przepisów o ponownym wykorzystywaniu kończy się wtedy, gdy zaczyna się stosowanie przepisów o ochronie danych osobowych? Może wydawać się to logiczną konsekwencją ujawnienia danych osobowych w ramach informacji sektora publicznego, zasady ich przetwarzania wyznaczają bowiem już przepisy o ochronie danych osobowych.

W istocie, w dalszym ciągu dochodzić będzie do współstosowania przepisów obu reżimów prawnych. Z jednej strony, zasady i podstawy przetwarzania danych osobowych, uprawnienia osób których dane dotyczą oraz obowiązki administratora danych będące korelatem tych uprawnień pozostają wyznaczone przepisami ogólnego rozporządzenia, z drugiej wciąż zastosowanie mają ogólne zasady oraz warunki ponownego wykorzystywania, jakie określono dla danej informacji sektora publicznego na podstawie UPW.

Co istotne zatem, do współstosowania przepisów będzie dochodzić na dwóch etapach. Po pierwsze równoległe stosowanie przepisów UPW i RODO będzie miało miejsce przed ujawnieniem danych osobowych do ponownego wykorzystywania. Na tym etapie można wyodrębnić z kolei dwa poziomy wyznaczone dwoma odrębnymi trybami udzielenia informacji sektora publicznego, tj. trybu wnioskowego i trybu bezwnioskowego. Do odpowiedniego równoczesnego stosowania przepisów o ochronie danych osobowych i przepisów UPW dojdzie przy rozpatrywaniu wniosku o przekazanie informacji sektora publicznego zawierającej lub stanowiącej dane osobowe albo na poziomie udostępnienia przez podmiot zobowiązany danych osobowych w ramach informacji sektora publicznego w centralnym repozytorium informacji publicznej, stronie podmiotowej BIP lub w innym systemie teleinformatycznym (z własnej inicjatywy lub w wyniku obowiązku prawnego wynikającego z przepisów szczegółowych). Na tym poziomie konieczne będzie przynajmniej ustalenie, czy informacje sektora publicznego stanowią lub zawierają dane osobowe, a następnie rozstrzygnięcie, czy ze względu na zasady i przesłanki dopuszczalności przetwarzania danych osobowych, określone w art. 5, 6 oraz art. 9 RODO, dane te podlegają ujawnieniu. Równocześnie podmiot zobowiązany stosował będzie odpowiednie przepisy UPW dotyczące wyłączeń i ograniczeń ponownego wykorzystywania, zasad ogólnych, trybu

[709] *M. Sakowska – Baryła*, Komentarz do art. 86, pkt 7 [w:] *M. Sakowska – Baryła (red.),* Ogólne rozporządzenie.

udostępniania lub przekazywania informacji sektora publicznego, warunków ponownego wykorzystywania czy zasad ustalania opłat. Stosującym równolegle przepisy na tym etapie będzie zatem podmiot zobowiązany.

Drugi etap współstosowania przepisów będzie miał miejsce po ujawnieniu danych osobowych w ramach informacji sektora publicznego. Wówczas konieczne będzie przestrzeganie procedur postępowania z danymi osobowymi[710]. Respektowanie zasad wynikających z ogólnego rozporządzenia, w tym realizacja uprawnień osób których dane dotyczą, adresowane będzie na tym etapie nie tylko do podmiotów zobowiązanych na gruncie UPW, ale również (ponownych) użytkowników, którzy będą musieli brać pod uwagę równocześnie przepisy UPW, jak zasady ogólne czy określone przez podmiot zobowiązany warunki ponownego wykorzystywania.

Rozdział 7. Przesłanki legalności przetwarzania danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego

Udostepnienie i przekazanie danych osobowych w ramach informacji sektora publicznego, jak i samo ponowne wykorzystywanie informacji sektora publicznego zawierających dane osobowe stanowi przetwarzanie w rozumieniu art. 4 pkt 2 RODO i dla swojej zgodności z prawem wymaga spełnienia jednej z przesłanek dopuszczalności przetwarzania danych.

Przepisy o zgodności przetwarzania z prawem uszczegółowiają i nadają skonkretyzowaną normatywną treść podstawowej zasadzie legalności przetwarzania sformułowanej w art. 5 ust. 1 RODO[711]. Ogólne rozporządzenie przewiduje dwie grupy przesłanek, których spełnienie warunkuje zgodne z prawem przetwarzanie danych, w zależności od tego, czy przetwarzaniu poddane będą dane zwykłe, czy też szczególne kategorie danych (dane wrażliwe), statuując dwie zasady:

- ogólnego dopuszczenia przetwarzania danych zwykłych, gdy spełniona jest co najmniej jedna z przesłanek wymienionych w art. 6 ust. 1 RODO, oraz

- ogólnego zakazu przetwarzania danych wrażliwych, chyba że zachodzi którykolwiek z wyjątków pozwalających na takie przetwarzanie, którym mowa w art. 9 ust. 2 RODO[712].

[710] *M. Sakowska-Baryła*, Dostęp do informacji publicznej, s. 76 i n.; *M. Sakowska-Baryła*, Problem współstosowania, s. 173 i n.; *A. Piskorz-Ryń* (red.) Ustawa o ponownym wykorzystywaniu, s. 206–207; *P. Drobek, A. Piskorz-Ryń*, Prawne problemy ponownego wykorzystania, s. 222.
[711] *D. Lubasz*, Komentarz do art. 6 [w:] *D. Lubasz (red.)*, RODO, s. 346.
[712] *D. Lubasz*, Komentarz do art. 6 [w:] *D. Lubasz, E. Bielak-Jomaa* (red.), RODO, s. 347.

Należy zatem uznać, że podstawy wymienione w art. 6 RODO, stanowią ogólne materialne przesłanki przetwarzania danych osobowych, jednak ujmowane od strony pozytywnej, nie zaś od strony negatywnej, jak to ma miejsce w przypadku danych osobowych zaliczonych do szczególnych kategorii, zgodnie z art. 9 RODO. Innymi słowy, w przypadku art. 6 RODO nie mamy do czynienia z negatywnie ujętymi wyjątkami od ogólnej zasady zakazu przetwarzania danych osobowych, lecz z pozytywnie wskazanymi przesłankami legalności przetwarzania danych osobowych[713]. Tak ujęty dychotomiczny podział podstaw przetwarzania ze względu na rodzaj danych osobowych determinuje kierunek wykładni wspomnianych przepisów, w szczególności nakazuje wąską interpretację wyjątków od zakazu przetwarzania danych wrażliwych, wymienionych w art. 9 ust. 2, zgodnie z zasadą *exceptiones non sunt extendendae*, która to dyrektywa wykładni przepisów nie będzie miała zastosowania do przesłanek legalizujących przetwarzanie zwykłych danych osobowych[714].

Dozwolone jest przetwarzanie zwykłych danych osobowych jeśli spełniony jest co najmniej jeden z warunków wymienionych w art. 6 ust. 1, tj.

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) 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;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę ,trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

[713] *P. Litwiński (red.),* op. cit., Komentarz do art. 6, pkt 2.
[714] *D. Lubasz,* op. cit., s. 347.

Generalny zaś zakaz przetwarzania szczególnych kategorii danych osobowych został wyrażony wprost w art. 9 ust. 1, zgodnie z którym zabrania się przetwarzania 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.

Prawodawca unijny przewidział zatem dla tych danych wyższy stopień ochrony prawnej niż w stosunku do pozostałych danych osobowych. Szczególne kategorie danych 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 (motyw 51 preambuły do RODO). W doktrynie zwraca się uwagę, że kryterium wyróżnienia tych informacji jako danych objętych szczególną ochroną należy upatrywać w okoliczności, że dotyczą one bezpośrednio sfer należących do prywatności czy nawet intymności osoby fizycznej, jak również znacznie większym poczuciem zagrożenia oraz niebezpieczeństwem wywołania na różnych polach (zatrudnienie, ubezpieczenie, kredytowanie itd.) decyzji dyskryminujących[715]. Stąd wyższy reżim prawny zabezpieczający interesy jednostki w zakresie przetwarzania danych zaliczanych do powyższej kategorii oraz wynikający stąd intensywniejszy poziom ochrony[716].

Niemniej prawodawca UE sformułował jednocześnie przesłanki, które uchylają ogólny zakaz przetwarzania tych danych. Podstawą legalizacją przetwarzanie szczególnych kategorii danych osobowych, zgodnie z art. 9 ust. 2 RODO, jest:

a) zgoda osoby, której dane dotyczą na przetwarzanie w jednym lub kilku konkretnych celach (chyba że przepisy przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania szczególnych kategorii danych)

b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (o ile jest to dozwolone przepisami prawa lub porozumieniem zbiorowym przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów podmiotu danych);

c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody);

[715] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 569
[716] *M. Sakowska-Baryła*, Komentarz do art. 9 pkt 1 [w:] *M. Sakowska-Baryła (red.),* Ogólne rozporządzenie.

d) przetwarzania dokonuje fundacja, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych (o ile przetwarzanie dotyczy wyłącznie aktualnych lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami, a dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą);

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie przepisów prawa, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie przepisów prawa lub zgodnie z umową;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego (jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych) na podstawie przepisów prawa, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową);

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie przepisów prawa, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Katalog podstaw przetwarzania danych zarówno zwykłych, jak i szczególnych kategorii danych ma charakter zamknięty. Nie należy jednak zapominać, że ów dwupodział jest podziałem sztucznym i nie jest podziałem doskonałym, gdyż opiera się na uogólnieniu[717].

[717] *P. Litwiński (red.)*, op. cit., Komentarz do art. 9, pkt 3.

O ile wymieniony katalog ma charakter zamknięty, to w myśl motywu 10 preambuły i art. 9 ust. 4 RODO na gruncie krajowym może to ulec modyfikacji. Państwom członkowskim przysługuje prawo doprecyzowania kwestii przetwarzania danych wrażliwych, w tym RODO nie wyklucza możliwości określenia w prawie krajowym okoliczności dotyczących konkretnych sytuacji związanych z przetwarzaniem danych, w tym dookreślenia warunków, które decydują o zgodności przetwarzania z prawem (motyw 10 zdanie ostatnie). Ponadto w zakresie danych biometrycznych, genetycznych lub dotyczących zdrowia, zgodnie z art. 9 ust. 4 RODO, ustawodawca krajowy może zachować lub wprowadzić dalsze warunki, w tym ograniczenia przetwarzania.

Zarówno dyrektywa 2003/98/WE, jak i dyrektywa 2019/1024 oraz przepisy UPW nie zawierają wyrażonego wprost zakazu ponownego wykorzystywania informacji sektora publicznego zawierających szczególne kategorie danych, to w mojej opinii dane te co do zasady nie będą podlegały ujawnieniu w celu ponownego wykorzystywania. W art. 1 ust. 2 lit. d dyrektywy 2019/1024 wprowadzono wprawdzie wyłączenie stosowania przepisów o ponownym wykorzystywaniu w odniesieniu do dokumentów takich jak „dane wrażliwe, które są wyłączone z dostępu na podstawie systemów dostępu państwa członkowskiego", jednak po pierwsze, jako przykłady okoliczności wyłączenia „danych wrażliwych" wymieniono ochronę bezpieczeństwa narodowego (to jest bezpieczeństwa państwa), obronę lub bezpieczeństwo publiczne; tajemnicę statystyczną; poufność informacji handlowych (w tym tajemnicę handlową, zawodową lub przedsiębiorstwa), po drugie zaś, dyrektywa 2019/1024 została przyjęta w okresie obowiązywania ogólnego rozporządzenia, więc jeśli miała odnosić się do pojęcia danych wrażliwych w rozumieniu RODO, powinna posługiwać się terminem szczególnej kategorii danych osobowych.

Przetwarzanie szczególnych kategorii danych osobowych w ramach ich ujawniania w informacji sektora publicznego nie będzie możliwe bez wyraźnej podstawy, w tym zakresie w prawie krajowym lub UE. Spośród wymienionych w art. 9 ust. 2 RODO przesłanek legalizujących przetwarzanie danych wrażliwych w ramach realizacji prawa do ponownego wykorzystywania, którą potencjalnie należy rozważyć, może stanowić zgoda wymieniona w lit. a) tego przepisu. Przesłanka zgody na przetwarzanie szczególnych kategorii danych osobowych co do zasady odpowiada wymogom wyrażenia zgody na przetwarzanie zwykłych danych osobowych. Podstawowym elementem odróżniającym jednak oświadczenie o wyrażeniu zgody na przetwarzanie szczególnych kategorii danych od oświadczenia zgody na przetwarzanie danych zwykłych jest wymóg, aby zgoda na przetwarzanie danych wrażliwych

była "wyraźna"[718]. Już na gruncie dyrektywy 95/46/WE istniała dokładnie tak samo sformułowana przesłanka przetwarzania danych wrażliwych (*explicit consent*).

Przy wskazaniu zgody jako przesłanki dopuszczalności przetwarzania szczególnej kategorii danych osobowych prawodawca unijny przewidział dodatkowo możliwość, aby w prawie (unijnym bądź krajowym) zostało zawarte zastrzeżenie, że osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania tych danych. Wprowadzenie w przepisach tego rodzaju postanowienia oznaczałoby brak możliwości oparcia przetwarzania szczególnych kategorii danych na zgodzie osoby, której dane dotyczą. Z uwagi na brzmienie art. 9 ust. 4 RODO wydaje się, że w szczególności takie ograniczenia mogą dotyczyć przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia[719].

Biorąc powyższe pod uwagę, poczynione w dalszej części rozprawy ustalenia dotyczące podstawy przetwarzania wymienionej w art. 6 ust. 1 lit. a RODO będzie można również odnieść do przetwarzania danych wrażliwych w oparciu o zgodę wyrażoną przez osobę, której te dane dotyczą.

7.1. Rodzaje przesłanek i ich podział ze względu na kategorię administratora

Kluczowym zagadnieniem dla ponownego wykorzystywania danych osobowych jest ustalenie na jakiej podstawie prawnej możliwe będzie przetwarzanie danych. W procesie stosowania przepisów o ponownym wykorzystywaniu, kiedy potencjalnie może dojść do ujawnienia danych osobowych, a następnie ich wykorzystywania, konieczne jest oparcie przetwarzania danych osobowych zawartych w informacji sektora publicznego o jedną z podstaw prawnych wymienionych w art. 6 ust. 1 RODO.

W literaturze przedmiotu podnosi się, że zamknięty katalog przesłanek legalizujących przetwarzanie danych ma charakter autonomiczny i niezależny[720]. Oznacza to, że określone operacje przetwarzania danych osobowych będą legalizowane przez więcej niż jedną przesłankę, co nie ma jednak znaczenia prawnego, z zastrzeżeniem sytuacji, w której po wygaśnięciu jednej z przesłanek administrator danych może powoływać się na drugą (z uwzględnieniem oczywiście możliwości odmiennego zakresu danych, których przetwarzanie jest dopuszczalne na podstawie drugiej przesłanki, zgodnie z zasadą minimalizacji danych)[721].

[718] *P. Litwiński (red.)*, op. cit., pkt 10.
[719] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 9, pkt 12.
[720] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 472–473.
[721] *P. Litwiński (red.)*, op. cit., Komentarz do art. 6, pkt 5.

Natomiast dla przesądzenia o tym, czy przetwarzanie jest dopuszczalne, wystarczy wykazanie istnienia jednej z nich. W przypadku jednak udzielonej zgody jako podstawy przetwarzania, w celu zachowania elementu dobrowolności, nie jest co do zasady dopuszczalne dodatkowe jej wykorzystywanie do legalizacji przetwarzania, w sytuacji gdy administrator dysponuje inną odrębną przesłanką przetwarzania danych w tym samy celu i zakresie (np. w związku z realizacją umowy lub realizacją obowiązku wynikającego z przepisu prawa)[722].

Kolejną cechą zestawu przesłanek legalizujących przetwarzanie jest ich równoprawność czy też równoważność, oznaczająca brak formalnego uprzywilejowania którejkolwiek z podstaw legalności oraz brak ich hierarchicznego uporządkowania[723]. W literaturze można jednak spotkać pogląd ukształtowany jeszcze na gruncie UODO1997, który przesłankę niezbędności przetwarzania dla celu realizacji obowiązku wynikającego z przepisu prawa należy stosować jednak przed innymi przesłankami[724].

Co istotne, również w związku z ponownym wykorzystywaniem, wybór przesłanki legalizacyjnej, w oparciu o którą administrator będzie przetwarzał dane, musi mieć charakter uprzedni w stosunku do procesu przetwarzania. Jest to uzasadnione tym, że jedną z informacji jaką administrator zobowiązany jest przekazać osobie, której dane dotyczą w ramach realizacji obowiązku informacyjnego (na podstawie art. 13 i 15 RODO) jest konieczność wskazania uzasadnionych interesów w przypadku oparcia legalności przetwarzania o art. 6 ust. 1 lit. f. już na etapie pozyskiwania danych (art. 13 ust. 1 lit. d i art. 14 ust. 2 lit. b)[725].

Równoprawność przesłanek nie oznacza, że konsekwencje oparcia przetwarzania o którąkolwiek podstawę będą takie same tak dla praw podmiotów danych i będących ich korelatem obowiązków administratora. Skutki prawne będą zasadniczo różnić się w zależności od zastosowanej przesłanki. Jako przykład można wymienić prawo przenoszenia danych, o którym mowa w art. 20 RODO, które przysługuje osobie, której dane dotyczą jedynie w przypadku, gdy podstawą po przetwarzania danych była zgoda lub niezbędność dla wykonania umowy. Innym przykładem relewantnym z punktu widzenia ponownego wykorzystywania danych osobowych będzie prawo wniesienia sprzeciwu – zgodnie z art. 21 RODO – które podmiot danych może zrealizować wyłącznie wtedy, gdy przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. e lub f.

---

[722] *D. Lubasz*, op. cit., komentarz do art. 6, s. 348.
[723] *Ibidem.*
[724] *W. Zimny*, Przesłanki legalizujące przetwarzanie, „Biuletyn Administratorów Bezpieczeństwa Informacji" 2000, nr 4, s. 5 i 7. Zob. wyrok WSA w Warszawie z 03.06.2004 r., II SA/Wa 328/04. Na gruncie RODO pogląd podzielany m.in. przez *D. Lubasz*, Komentarz do art. 6 [w:] *D. Lubasz, E. Bielak-Jomaa (red.)*, RODO, s. 350 czy *M. Sakowska-Baryła*, Komentarz do art. 6 pkt 3 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie.
[725] *D. Lubasz*, op. cit., s. 349.

Wreszcie możliwość oparcia przetwarzania o daną przesłankę zależeć będzie od kategorii administratora. Podział ten ma zasadnicze znaczenia z punku widzenia realizacji prawa do ponownego wykorzystywania informacji sektora publicznego zawierającej lub stanowiącej dane osobowe. Zgodnie z brzmieniem art. 6 ust. 1 akapit drugi, organy publicznie w ramach realizacji swoich zadań zostały wykluczone z możliwości wykorzystania przesłanki wymienionej w art. 6 ust. 1 lit. f. Nie wyprzedzając dalszych rozważań już w tym miejscu można zatem nadmienić, że w przypadku udostępnienia lub przekazania danych osobowych do ponownego wykorzystywania z przesłanki prawnie uzasadnionych interesów administratora nie będzie mógł zatem skorzystać podmiot zobowiązany.

Ostatnim aspektem, który należy wziąć pod uwagę dokonując rozróżnia przesłanek legalizujących przetwarzanie, stanowi kryterium niezbędności. Pojęcie to występuje wprost w treści podstaw prawnych przetwarzania danych, wymienionych w art. 6 ust. 1 lit. b–f (nie ma zastosowania do przesłanki zgody), a zatem ściśle ogranicza okoliczności, w jakich mogą one mieć zastosowanie. W odniesieniu do przetwarzania danych nieznajdującego oparcia w przesłance zgody kryterium niezbędności oznacza, że administrator powinien stwierdzić rzeczywistą i racjonalną potrzebę przetwarzania danych, uzasadniającą ingerencję w sferę prywatności osoby w oparciu o badanie niezbędności przetwarzania danych na podstawie wybranej przesłanki[726]. Przesłanka niezbędności nie ma zatem charakteru absolutnego i należy ją każdorazowo badać pod kątem zasady proporcjonalności wynikającej z art. 52 ust. 1 KPP, art. 8 ust. 2 EKPC oraz art. 31 Konstytucji RP, jak również zasadami przetwarzania danych osobowych wymienionych w art. 5 RODO[727]. Wkraczanie w sferę prywatności osoby fizycznej powinno zatem pozostawać w odpowiedniej proporcji do celów, których ochrona uzasadnia dokonane ograniczenie. Kryterium niezbędności, należy ustalać w każdym konkretnym przypadku, z uwzględnieniem celu, potrzeb i kontekstu przetwarzania danych osobowych[728].

W mojej opinii przesłankami legalizującymi przewarzanie danych osobowych, które należy rozważyć w związku z realizacją prawa do ponownego wykorzystywania będą: wypełnienie obowiązku prawnego ciążącego na administratorze (art. 6 ust. 1 lit. c), wykonanie zadania realizowanego w interesie publicznym lub w ramach władzy sprawowanej w interesie publicznym (art. 6 ust. 1 lit. e) oraz prawnie uzasadnione interesy (art. 6 ust. 1 lit. f). Przesłanką legalizującą przetwarzanie danych, która – przynajmniej teoretycznie – będzie mogła również wystąpić, jest zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a). W dalszej części pracy

[726] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 6, pkt 2.
[727] *D. Lubasz*, op. cit., s. 350.
[728] *M. Sakowska-Baryła*, op. cit.

zostaną szerzej omówione te podstawy prawne przetwarzania danych osobowych, które będą miały zastosowanie w związku z realizacją prawa do ponownego wykorzystywania. Przyjęcie odpowiedniej podstawy przetwarzania danych osobowych, będzie związane z kategorią osób i danych, których może dotyczyć ponowne wykorzystanie oraz podmiotu, który dane będzie przetwarzał. Należy zwrócić uwagę, że nawet w przypadku, gdy ostatecznie nie dojdzie do udostępnienia lub przekazania danych osobowych w trybie ponownego wykorzystywania (udzielone zostaną dane zanonimizowane lub nastąpi odmowa przekazania danych osobowych w ramach ponownego wykorzystywania), to już na etapie poprzedzającym udzielenie informacji sektora publicznego zawierających dane osobowe również może dochodzić do przetwarzania danych osobowych, np. w związku rozpatrzeniem wniosku o ponowne wykorzystywanie przez podmiot zobowiązany czy też podjęcia decyzji w sprawie udostępnienia danych w ogólnodostępnym systemie teleinformatycznym (np. strona BIP urzędu czy portal otwartych danych). Zatem także taka czynność przetwarzania powinna mieć swoją podstawę prawną.

W wielu przypadkach zasoby informacyjne przechowywane przez organy publiczne zawierają dane osobowe związane z tożsamością użytkowników usług publicznych. Ponadto publicznie dostępne rejestry mogą zawierać dane osobowe obywateli, jaki i osób fizycznych wykonujących funkcje publiczne, osób wykonujących zawody lub działalność regulowaną czy osób prowadzących działalność gospodarczą lub wchodzących w skład organów osób prawnych. Wreszcie na oficjalnych stronach internetowych podmiotów zobowiązanych będących stronami BIP czy portalami informacyjnymi udostępnia się dane osobowe osób pełniących funkcje publiczne, jak i innych osób nie pełniących tych funkcji, jak chociażby dane kontrahentów ujawnione w wykazach umów.

W tym wypadku organy władzy publicznej, gromadzą a więc przetwarzają dane osobowe, na podstawie art. 6 ust. 1 lit. c) lub na podstawie art. 6 ust. 1 lit. e). Taką też podstawę prawną należy przyjąć dla udostępniania lub przekazywania danych osobowych w ramach informacji sektora publicznego przez podmioty zobowiązane. Z kolei inną przesłankę legalizującą należy przyjąć dla przetwarzania danych osobowych przez użytkowników ponownie wykorzystujących informacji. Wówczas podstawę dla takiego przetwarzania należy oprzeć na art. 6 ust. 1 lit. f). Rozważyć również można przesłankę zgody, o której mowa w art. 6 ust. 1 lit. a (względnie art. 9 ust. 2 lit. a RODO), która potencjalnie może być zastosowana zarówno przez podmiot zobowiązany, jak i użytkownika.

Dla przetwarzania danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego nie będą miały zastosowania przesłanki legalizujące

przetwarzanie związane z zawarciem i wykonaniem umowy (art. 6 ust. 1 lit. b) oraz ochrona żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej (art. 6 ust. 1 lit. d).

Istota pierwszej z nich polega na założeniu, że ochrona danych osobowych nie może stanowić przeszkody dla zawierania i wykonywania umów. Przesłanka ta przesądza dwa przypadki, kiedy przetwarzanie jest dopuszczalne w związku z szeroko rozumianym kontraktowaniem. Chodzi o przetwarzanie niezbędne do podjęcia działań przed zawarciem umowy, jeżeli odbywa się na żądanie podmiotu danych lub wykonania umowy, której podmiot danych jest stroną[729]. Oczywiście podmiot zobowiązany może posiadać dane osobowe, które pozyskał w ramach zawieranych kontraktów, np. umów cywilnoprawnych. Jako przykład danych osobowych ujawnianych w ramach informacji sektora publicznego czy w trybie dostępu do informacji publicznej można podać dane identyfikacje kontrahentów podmiotów publicznych. Podstawą legalizującą jednak ich przekazanie lub udostępnienie w celu ponownego wykorzystywania nie będzie stanowił art. 6 ust. 1 lit. b, bowiem realizacja prawa do ponownego wykorzystywania nie jest związana z wykonaniem umowy, a wykonaniem zadania w interesie publicznym.

Istota drugiej zaś przesłanki irrelewantnej dla przedmiotu rozprawy, o której mowa w art. 6 ust. 1 lit. d, polega na możliwości przetwarzania danych z uwagi na żywotne interesy podmiotu danych lub innej osoby fizycznej. Stanowi ona swoisty bufor bezpieczeństwa, który pozwala na dokonywanie czynności na danych osobowych, gdy wymagają tego ważne z punktu widzenia życia innych osób powody. Chodzi zatem o sytuacje, kiedy spełnienie innej przesłanki legalizującej przetwarzanie danych nie byłoby możliwe lub byłoby możliwe do zrealizowania, ale ze względu na konieczność szybkiego działania, np. dla ochrony życia lub majątku, uzyskiwanie zgody byłoby niecelowe albo wręcz nieuzasadnione[730]. Oczywistym zatem jest, że podstawa ta nie będzie miała z zastosowania w przypadku ponownego wykorzystywania informacji.

[729] *M. Chomiczewski*, Niezbędność do wykonania umowy lub podjęcia działań przez zawarciem umowy [w:] *D. Lubasz (red.)*, Meritum, s. 131.
[730] *Ibidem*, s. 133.

7.2. Podstawy przetwarzania danych osobowych przez podmiot zobowiązany

7.2.1. Obowiązek prawny ciążący na administratorze

Zgodnie z art. 6 ust. 1 lit. c RODO, przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy jest to niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze. Takie ujęcie tej właśnie podstawy przetwarzania danych stanowi istotną zmianę w stosunku do przepisów UODO1997 w brzmieniu nadanym nowelizacją z 2014 r.[731], której art. 23 ust. 1 pkt 2 zezwalał na przetwarzanie danych osobowych wtedy, gdy jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa. Przedmiotowa podstawa prawna przetwarzania w brzmieniu RODO nie odnosi się więc do kategorii uprawnienia, a poprzestaje wyłącznie na kategorii obowiązku prawnego[732].

W pierwotnym brzmieniu art. 23 ust. 1 pkt 2 UODO1997 legalizował przetwarzanie danych osobowych wtedy, gdy "zezwalają na to przepisy prawa". Na kanwie tego przepisu w orzecznictwie sądowym wyrażony został pogląd, zgodnie z którym przesłanka ta mogła zostać uznana za spełnioną wyłącznie wtedy, gdy przepis prawa wyraźnie mówi o przetwarzaniu danych osobowych[733]. Jest to o tyle istotne, że w poszczególnych ustawach odnoszących się do problematyki przetwarzania danych osobowych zastosowane zostały różne rozwiązania – w części z nich wprost przyznana została kompetencja do przetwarzania danych osobowych, w części natomiast wyznaczono jedynie prawa i obowiązki, dla realizacji których niezbędne jest przetwarzanie danych osobowych[734].

W obecnym stanie prawnym należy zatem przyjąć za *P. Fajgielskim*, że jeżeli przepisy nakładają obowiązek, do realizacji którego konieczne jest przetwarzanie danych, to nawet w przypadku, gdy przepisy wyraźnie wskazują na uprawnienie do przetwarzania danych, należy przyjąć, że przetwarzanie to służy realizacji obowiązku nałożonego przepisami, a zatem spełniona jest przesłanka, o której mowa w art. 6 ust. 1 lit. c[735].

W poglądach doktryny wypracowanych na gruncie przepisów sprzed obowiązywania ogólnego rozporządzenia prezentowano opinię, że jeśli okoliczności przetwarzania danych osobowych regulowane są bezpośrednio przepisami prawa, to tę podstawę przetwarzania

[731] Ustawa z 22.01.2004 r. o zmianie ustawy o ochronie danych osobowych oraz ustawy o wynagrodzeniu osób zajmujących kierownicze stanowiska państwowe (Dz. U. poz. 285).
[732] *P. Litwiński (red.)*, op. cit., pkt 42.
[733] Wyr. WSA w Warszawie z 11.3.2004 r., II SA 1974/03.
[734] *X. Konarski, G. Sibiga*, Zmiany w ustawie o ochronie danych osobowych w świetle dyrektywy 95/46/WE, „Monitor Prawniczy" 2004, nr 12, s. 550.
[735] *P. Fajgielski*, Komentarz, 2018, s. 169.

danych osobowych, należy stosować przed innymi przesłankami[736]. Zauważono również, że gdy administrator danych osobowych przetwarza dane dla spełnienia obowiązku wynikającego z przepisów prawa, określenie celu przetwarzania danych osobowych powinno nastąpić przez odwołanie się do okoliczności konkretnej sprawy, z którą związane jest przetwarzanie danych[737].

Jeżeli przetwarzanie danych jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze, nie powinno się występować o zgodę osoby, której dane dotyczą, na przetwarzanie jej danych osobowych. Może to bowiem prowadzić m.in. do mylnego przekonania o swobodzie w zakresie podania danych, w sytuacji gdy obowiązek ich podania wynika z powszechnie obowiązujących przepisów prawa[738].

Brzmienie art. 6 ust. 1 lit. c wskazuje dwa warunki, jakie muszą zostać spełnione łączne dla oparcia przetwarzania zgodnego z prawem o omawianą przesłankę, tj. przetwarzanie danych osobowych jest dopuszczalne, o ile istnieje przepis prawa, który nakłada na administratora danych obowiązek prawny oraz przetwarzanie danych jest niezbędne dla realizacji tego obowiązku prawnego[739]. Oznacza to, że art. 6 ust. 1 lit. c RODO nie stanowi samodzielnej podstawy przetwarzania danych osobowych, ale jedynie w połączeniu z odpowiednim przepisem prawa obowiązującego w państwie, któremu podlega administrator lub też w połączeniu z odpowiednim przepisem prawa UE, o treści zgodnej z wymogami określonymi w art. 6 ust. 3 RODO[740].

Kryterium niezbędności dla realizacji obowiązku prawnego należy odróżnić, od wymogu niezbędności wymienionego w pozostałych podstawach przetwarzania wymienionych w art. 6 ust. 1 lit. b, d i f[741]. Można przyjąć, że obowiązek wykazania przez administratora kryterium niezbędności przetwarzania będzie tu łatwiejszy do wykonania, ponieważ w tym wypadku konkretny przepis często będzie wyznaczał zakres niezbędności przetwarzania. W konsekwencji przetwarzanie dokonywane z naruszeniem ram wyznaczonych przez treść takiego przepisu zasadniczo nie będzie spełniało waloru niezbędności[742]. Niezbędność zatem

[736] Por. *W. Zimny*, Przesłanki, s. 5–7.
[737] Zob. *A. Drozd*, Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy, Warszawa 2007, s. 150.
[738] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 505. Podobnie *P. Litwiński (red.)*, op. cit., Komentarz do art. 6, pkt 44.
[739] *P. Litwiński (red.)*, op. cit., pkt 44.
[740] *D. Lubasz*, op. cit., komentarz do art. 6 ust. 1 lit. c, s. 368.
[741] *Ibidem.*
[742] *M. Sakowska-Baryła*, op. cit., pkt 22.

będzie w tym wypadku rozumiana węziej, co wynika z ustanowienia ustawowego obowiązku przetwarzania[743].

Istnienie przepisu prawa należy oceniać z uwzględnieniem katalogu źródeł prawa wynikającego z art. 87 ust. 1 Konstytucji RP, z zastrzeżeniem, że nie dotyczy to rozporządzeń, gdyż zgodnie z zasadą wyrażoną w art. 31 ust. 3 Konstytucji RP, że ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw (a więc również prawa do decydowania o ujawnieniu swoich danych – art. 51 ust. 1 Konstytucji RP) mogą być ustanawiane tylko w ustawie[744]. Mogą one wynikać również z ratyfikowanej, po uprzedniej zgodzie wyrażonej w ustawie, umowy międzynarodowej – zgodnie z art. 89 ust. 1 pkt 2 Konstytucji RP. Nie mogą natomiast być same w sobie podstawą uprawniającą do przetwarzania danych osobowych w szczególności przepisy niższej rangi, w tym także zawarte w aktach prawa miejscowego czy inne przepisy nie mające charakteru źródeł prawa powszechnie obowiązującego, jak np. statuty spółdzielni czy stowarzyszeń [745]. Poza tym *in abstracto* nie stanowią podstawy przetwarzania danych osobowych akty stosowania prawa (decyzje, postanowienia itp.)[746].

Co istotne, zgodnie z art. 6 ust. 2 RODO państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy, aby dostosować stosowanie przepisów niniejszego rozporządzenia w odniesieniu do przetwarzania służącego wypełnieniu warunków określonych w ust. 1 lit. c i e; w tym celu mogą dokładniej określić szczegółowe wymogi przetwarzania i inne środki w celu zapewnienia zgodności przetwarzania z prawem i jego rzetelności, także w innych szczególnych sytuacjach związanych z przetwarzaniem przewidzianych w rozdziale IX. Dyspozycja tego przepisu *in fine* wprost zatem wskazuje, że dotyczy on również podstawy prawnej służącej pogodzeniu prawa do ochrony danych osobowych z prawem dostępu do dokumentów urzędowych, o której mowa w art. 86 RODO.

Dla omawianej przesłanki szczególnego znaczenia nabiera sposób spełnienia wymogów podstawy prawnej przetwarzania, o której mowa w art. 6 ust. 1 lit. c. Podstawa prawna, ustanowiona w prawie krajowym lub prawie Unii musi – zgodnie z art. 6 ust. 3 – określać przynajmniej cel przetwarzania. Ponadto podstawa prawna może zawierać elementy fakultatywne dostosowujące stosowanie przepisów RODO, w tym: ogólne warunki zgodności z prawem przetwarzania przez administratora; rodzaj danych podlegających przetwarzaniu; osoby, których dane dotyczą; podmioty, którym można ujawnić dane osobowe; cele, w których

[743] *D. Lubasz,* op. cit., s. 368.
[744] *P. Litwiński (red.),* op. cit., pkt 46. Podobnie: *D. Lubasz,* op. cit., s. 373.
[745] *Ibidem.*
[746] *M. Sakowska-Baryła*, op. cit., pkt 21.

można je ujawnić; ograniczenia celu; okresy przechowywania; oraz operacje i procedury przetwarzania, w tym środki zapewniające zgodność z prawem i rzetelność przetwarzania, w tym w innych szczególnych sytuacjach związanych z przetwarzaniem, o których mowa w rozdziale IX. Prawo Unii lub prawo państwa członkowskiego muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu.

W tym kontekście kluczowym wydaje się motyw 45 preambuły do RODO, zgodnie z którym RODO nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne – wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Jak więc się wydaje, nie istnieje bezwzględny obowiązek regulowania w przepisach prawa każdej operacji wykonywanej na danych osobowych – wystarczy, że przepisy regulują obowiązek prawny ciążący na administratorze danych i nie ma możliwości realizacji tego obowiązku bez przetwarzania danych osobowych[747]. W konsekwencji administrator będzie zobowiązany do ustalenia związku między zakresem przetwarzania danych a realizacją obowiązku wynikającego z przepisu[748]. Brak szczegółowego określenia w przepisie prawa, do którego odsyła art. 6 ust. 1 lit. c zakresu przetwarzania każe weryfikować *ad casum* istnienie takiego związku kształtowanego przesłanką niezbędności[749]. W doktrynie zauważa się, że wymóg istnienia obowiązku prawnego ciążącego na konkretnym administratorze nie musi każdorazowo implikować powiązanego z nim obowiązku podania danych osobowych przez osobę, której dane podlegać mają przetwarzaniu. Zwłaszcza w przypadku istnienia zobowiązania nałożonego na organ lub podmiot publiczny może on dysponować innymi sposobami pozyskiwania informacji o podmiotach danych, wykorzystywanymi priorytetowo w procesie ich przetwarzania, dającymi dodatkowo pewność co do poprawności użytych w procesie przetwarzania informacji[750].

Adresatem obowiązków określonych w przepisach prawa musi być administrator, przy czym nie jest istotne czy jest nim podmiot prawa prywatnego czy prawa publicznego, przepis

[747] *P. Litwiński (red.),* op. cit., pkt 46.
[748] *M. Sakowska-Baryła*, op. cit., pkt 22.
[749] *D. Lubasz,* op. cit., s. 369.
[750] *K. Wygoda*, Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych w oparciu o art. 6 RODO a działania podmiotów sektora publicznego, [w:] *M. Jabłoński, K. Flaga-Gieruszyńska, K. Wygoda (red.),* Reforma ochrony danych osobowych a jawność dostępu do informacji sądowej: aspekty proceduralne, Wrocław 2017, s. 39. Dostęp online: http://www.bibliotekacyfrowa.pl/publication/92803 (dostęp: 20.11.2020).

art. 6 ust. 1 lit. c może bowiem znaleźć zastosowanie, tak do organów publicznych, jak i prywatnych[751]. Motyw 45 preambuły RODO wskazuje na możliwość realizacji zadań podmiotów publicznych nawet przez osoby fizyczne: "Prawo Unii lub prawo państwa członkowskiego powinno określać także, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu (…)". Jako przykład tego typu przypadku można wskazać realizowanie zadań związanych z ochroną zdrowia publicznego przez lekarzy i to nawet wtedy, gdy nie korzystają oni ze środków publicznych (np. w ramach realizacji obowiązków określonych w ustawie z 5.12.2008 r. o zapobieganiu oraz zwalczaniu zakażeń i chorób zakaźnych u ludzi)[752].

W literaturze przedmiotu zauważa się jednocześnie, że przedmiotowa podstawa prawna przetwarzania będzie miała jednak w szczególności zastosowanie do organów administracji publicznej. Są one zobowiązane do działania na podstawie i w granicach prawa (art. 7 Konstytucji RP), a więc zbierając informacje i dane osobowe o obywatelach, powinny legitymować się stosowną podstawą prawną do takiego działania, o czym przesądza art. 51 ust. 1 i 2 Konstytucji RP[753].

Zasada ta odnosi się do wszelkich form przetwarzania danych osobowych, zarówno ich zbierania, jak i udostępniania. W przypadku udostępniania danych osobowych przepisy RODO nie określają bowiem szczególnych wymogów w tym zakresie. W pierwszej kolejności odwołać się więc należy do przepisów prawa, na podstawie których dany zbiór danych jest prowadzony[754]. Zdaniem *P. Litwińskiego*, „jeżeli jednak przepisy powszechnie obowiązującego prawa, stanowiące podstawę do gromadzenia danych osobowych, nie przewidują odrębnej procedury udostępniania danych, która mogłaby znaleźć zastosowanie w przypadku udostępniania danych, udostępnianie takie powinno zostać uznane za niedopuszczalne. Jeżeli bowiem organy administracji publicznej działają na podstawie i w granicach prawa, a ani przepisy RODO, ani ustawy szczególne nie przewidują możliwości udostępnienia danych, wówczas dane osobowe zgromadzone przez organy administracji z wykorzystaniem ich władczych kompetencji nie powinny być swobodnie udostępniane”[755].

[751] *D. Lubasz,* op. cit., s. 368.
[752] *K. Wygoda*, Modyfikacja przesłanek dopuszczalności przetwarzania danych zwykłych, s. 38. Autor jako przykład podaje dostęp do zasobów zawartych w Systemie Rejestrów Państwowych poprzez aplikację ŹRÓDŁO.
[753] *P. Litwiński (red),* op. cit., pkt. 47.
[754] *Ibidem.*
[755] *Ibidem.*

W kontekście realizacji prawa do ponownego wykorzystywania w związku z przetwarzaniem danych osobowych w celu wypełnienia obowiązku prawnego ciążącego na administratorze – w mojej opinii - należy wziąć pod uwagę następujące podstawy prawne.

Podstawa prawna dla przetwarzania danych osobowych wymieniona w art. 6 ust. 1 lit. c RODO będzie miała zastosowanie w przypadku przekazania lub udostępnienia danych o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, o których mowa w art. 6 ust. 2 UPW. Co do zasady należy założyć, że wskazany art. 6 ust. 2 UPW nie dotyczy przetwarzania danych szczególnych kategorii danych i informacji o karalności. W tym zakresie potrzebna byłaby (odrębna) wyraźna podstawa prawna, wynikająca odpowiednio z treści art. 9 ust. 2 lub 10 RODO (jak wskazano powyżej należy w tym wypadku potencjalnie rozważyć przesłankę zgody). Pojawia się natomiast wątpliwość czy te informacje, które można uznać za związane z pełnieniem funkcji publicznych, a które jednocześnie kwalifikują się jako szczególne kategorie danych osobowych (np. poglądy polityczne prezydenta miasta) lub dane osobowe dotyczące wyroków skazujących czy naruszeń prawa (np. informacja o wyroku skazującym za przestępstwo, którego konsekwencją może być pozbawienie osoby pełnienia danej funkcji publicznej), stanowią dane, o których mowa w art. 6 ust. 2 UPW. Co istotne, przyjęcie takiej podstawy prawnej dla przetwarzania danych osobowych osób pełniących funkcje publiczne, oznacza, że osoba której dane dotyczą nie może w tym wypadku skorzystać z prawa do sprzeciwu w myśl art. 21 ust. 1 RODO.

Poza danymi osób pełniących funkcje publiczne nie wskazano *expressis verbis* w UPW w sposób niebudzący wątpliwości, jakie inne dane osobowe są objęte zakresem przepisów o ponownym wykorzystywaniu, niejasność tę potęguje szeroki zakres definicji informacji sektora publicznego.

Niemniej, w mojej opinii należy również rozważyć podstawę z art. 5 pkt 1 w związku z art. 11 ust. 4 UPW oraz przepisami szczególnymi przewidującymi obowiązek prawny ciążący na podmiocie zobowiązanym do publikacji danych w BIP lub centralnym repozytorium informacji publicznej. Pierwszy z wymienionych przepisów, jak zostało wykazane, statuuje publiczne prawo podmiotowe do ponownego wykorzystywania informacji sektora publicznego udostępnionych w systemie teleinformatycznym, a w szczególności na stronie podmiotowej BIP podmiotu zobowiązanego lub w centralnym repozytorium informacji publicznej lub w innym systemie teleinformatycznym podmiotu zobowiązanego. Drugi ze wspomnianych przepisów stanowi o tym, że brak informacji o warunkach ponownego wykorzystywania informacji sektora publicznego udostępnionych w BIP lub w centralnym repozytorium uważa się za udostępnienie informacji sektora publicznego w celu ponownego wykorzystywania bez

warunków, a więc statuuje zasadę domniemanej zgody na ponowne wykorzystywanie tak upublicznionych informacji.

W związku z tym, podstawę dla przetwarzania danych osobowych w ramach realizacji prawa do ponownego wykorzystywania można odszukać zarówno w przepisach samej UDIP w zakresie w jakim na mocy art. 8 ust. 3 ustawy podmioty, o których mowa w art. 4 ust. 1 i 2, obowiązane są do udostępniania w BIP informacji publicznych, o których mowa w art. 6 ust. 1 pkt 1–3, pkt 4 lit. a tiret drugie, lit. c i d i pkt 5 UDIP. Chodzi tu o następujące podmioty:

- organy władzy publicznej;
- organy samorządów gospodarczych i zawodowych;
- podmioty reprezentujące zgodnie z odrębnymi przepisami Skarb Państwa;
- podmioty reprezentujące państwowe osoby prawne albo osoby prawne samorządu terytorialnego oraz podmioty reprezentujące inne państwowe jednostki organizacyjne albo jednostki organizacyjne samorządu terytorialnego;
- podmioty reprezentujące inne osoby lub jednostki organizacyjne, które wykonują zadania publiczne lub dysponują majątkiem publicznym, oraz osoby prawne, w których Skarb Państwa, jednostki samorządu terytorialnego lub samorządu gospodarczego albo zawodowego mają pozycję dominującą w rozumieniu przepisów o ochronie konkurencji i konsumentów;
- organizacje związkowe i pracodawców, reprezentatywne w rozumieniu ustawy z dnia 24 lipca 2015 r. o Radzie Dialogu Społecznego i innych instytucjach dialogu społecznego oraz partie polityczne.

Podmioty obowiązane do publikacji określonych informacji publicznych w BIP – pomimo tego, iż katalog ten został odmiennie skonstruowany – mieszczą się jednocześnie w zakresie podmiotowym UPW, o którym mowa w art. 3 tej ustawy.

Z kolei, w katalogu informacji publicznych, które obligatoryjne podlegają publikacji w BIP na gruncie UPW w zakresie w jakim mogą one stanowić dane osobowe lub je zawierać można wskazać w szczególności informacje o: organach i osobach sprawujących w nich funkcje i ich kompetencjach (art. 6 ust. 1 pkt 2 lit. d) czy naborze kandydatów do zatrudnienia na wolne stanowiska, w zakresie określonym w przepisach odrębnych (art. 6 ust. 1 pkt 3 lit. g).

Należy zwrócić uwagę, że również obowiązki publikacyjne na BIP wynikają z samego rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji Publicznej[756]. W myśl § 11 ust. 1 pkt 3 strona podmiotowa BIP

[756] Dz.U. 2007 nr 10 poz. 68.

zawiera imię i nazwisko, numer telefonu, numer telefaksu i adres poczty elektronicznej co najmniej jednej z osób redagujących stronę podmiotową BIP.

Innym przykładem obowiązku publikacji informacji, które zawierać mogą dane osobowe, sformułowanym w akcie wykonawczym, jest rozporządzenie Ministra Cyfryzacji z 23 sierpnia 2018 r. w sprawie zasobu informacyjnego przeznaczonego do udostępniania w centralnym repozytorium informacji publicznej[757]. Delegacja ustawowa do wydania przedmiotowego aktu wykonawczego zawarta jest wprawdzie w przepisach UDIP (art. 9a ust. 3 i 4), ale rozporządzenie ma to szczególne znaczenie dla ponownego wykorzystywania. Wymienia się w nim bowiem podmioty i konkretne zestawy danych będące w ich posiadaniu, które podlegają udostępnieniu na portalu dane.gov.pl (pełniącym funkcje centralnego repozytorium). Portal ten wraz ze stronami podmiotowymi BIP stanowi, jak zostało to już wspomniane, bezwnioskowy tryb dostępu do informacji publicznej, jak i ponownego wykorzystywania. W rozporządzeniu tym, a w konsekwencji na portalu dane.gov.pl, zostały ujęte zasoby informacyjne zawierające dane osobowe, jak m.in. lista rzeczoznawców majątkowych[758]. Wykaz ten zawiera m.in. imię i nazwisko osoby wykonującej zawód rzeczoznawcy, imiona jego rodziców, jak i adres wykonywania działalności.

Jednak, jak wskazano wyżej, art. 6 ust. 1 lit c RODO nie obejmuje swoim zakresem aktów o randze podustawowej, zatem wydaje się, że przetwarzanie danych osobowych przez podmiot zobowiązany wynikające zarówno z rozporządzenia w sprawie BIP, jak i w sprawie zasobów informacyjnych do udostępnienia w CRIP, należy oprzeć o art. 6 ust. 1 lit. e RODO.

Obowiązek publikacyjny w BIP rozproszony jest również w innych ustawach szczególnych. W kontekście publikacji danych osobowych tytułem przykładu wymienić można oświadczenia majątkowe, do których złożenia obowiązani są wymienieni w ustawach „branżowych" funkcjonariusze publiczni, z jednoczesnym wskazaniem obowiązku ich ujawnienia w BIP, np. zgodnie z art. 24i ust. 1 i 3 ustawy z 8 marca 1990 r. o samorządzie gminnym[759], art. 25d ust. 1 i 3 ustawy z 5 czerwca 1998 r. o samorządzie powiatowym[760] oraz art. 27d ust. 1 i 3 ustawy z 5 czerwca 1998 r. o samorządzie województwa[761]: informacja o stanie majątkowym osób zobowiązanych do składania oświadczeń majątkowych podlega udostępnieniu w BIP. Wyłączeniem od ustanowionej zasady jawności

[757] Dz.U. z 2018 r. poz. 1790.
[758] Zob. Załącznik nr 1 do rozporządzenia oraz zasób na: https://dane.gov.pl/dataset/1161,centralny-rejestr-rzeczoznawcow-majatkowych-1/resource/1378/table?page=1&per_page=20&q=&sort=
[759] t.j. Dz. U. z 2020 r. poz. 713, 1378.
[760] t.j. Dz. U. z 2020 r. poz. 920.
[761] t.j. Dz. U. z 2020 r. poz. 1668.

objęto informacje dotyczące adresów zamieszkania osób składających oświadczenia oraz miejsca położenia nieruchomości.

Przykładem przepisów o publikacji danych osobowych w innym systemie teleinformatycznym podmiotu zobowiązanego („strona internetowa") jest ustawa 11 lipca 2014 r. o petycjach[762]. Zgodnie z art. 8, który realizuje zasadę jawności petycji, na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego niezwłocznie zamieszcza się informację zawierającą odwzorowanie cyfrowe (skan) petycji, datę jej złożenia oraz – w przypadku wyrażenia zgody – imię i nazwisko albo nazwę podmiotu wnoszącego petycję lub podmiotu, w interesie którego petycja jest składana[763], choć w tym wydaje się, że przesłanką przetwarzania danych, którą również w tym wypadku należy rozważyć będzie zgoda.

Analiza powyższych przepisów krajowych, które w związku z art. 6 ust. 1 lit. c RODO, stawia pod znakiem zapytania, czy przedmiotowe podstawy prawne przetwarzania danych osobowych spełniają wymagania określone w art. 6 ust. 3 ogólnego rozporządzenia. Należy zauważyć, że poza nowelizacją przepisów UPW, która zostanie omówiona w dalszej części niniejszego rozdziału, ustawodawca krajowy nie zdecydował się na zmianę przedmiotowych przepisów, w tym UDIP, mających na celu dostosowanie do wymogów ogólnego rozporządzenia.

7.2.2. Wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej

Kolejną przesłanką legalizującą przetwarzanie danych osobowych przez podmiot zobowiązany, którą należy rozważyć w związku realizacją prawa do ponownego wykorzystywania jest niezbędność przetwarzania do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

Przesłanka określona w art. 6 ust. 1 lit. e. daje potencjalnie szerokie możliwości wykazania legalności przetwarzania, nieskierowane bezpośrednio na ustanowienie kompetencji organu lub podmiotu powołującego się na ich istnienie jako uzasadnienie występowania interesu publicznego[764].

[762] t.j. Dz.U. 2018 poz. 870.
[763] Zob. szerz. *D. Sybilski*, Zagadnienie jawności i dostęp do akt w sprawach skarg, wniosków i petycji [w:] *M. Błachucki, G. Sibiga*, Skargi, wnioski i petycje – powszechne środki ochrony prawnej, Wrocław 2017, s. 75-99.
[764] *M. Sakowska-Baryła*, op. cit., pkt 25.

Konstrukcja podstawy prawnej zakłada dwie alternatywne przesłanki przetwarzania wtedy, gdy jest ono niezbędne do wykonania zadania realizowanego w interesie publicznym lub wtedy, gdy jest niezbędne dla w ramach sprawowania władzy w publicznej powierzonej administratorowi. Mamy tu zatem do czynienia z dwoma w istocie niezależnymi elementami, tj. interesu publicznego oraz władzy publicznej. Przesłanka ta odpowiada podstawie prawnej zawartej w dyrektywie 95/46/WE, która z kolei w sposób odmienny została transponowana w przepisach UODO1997 stanowiących o niezbędności do wykonania określonych prawem zadań realizowanych dla dobra publicznego.

Na gruncie przepisów UODO1997 pojęcie zadań realizowanych w interesie publicznym (dla dobra publicznego) było powszechnie utożsamiane w nauce prawa z pojęciem zadań publicznych[765]. Przesłanka ta, dotyczyła sytuacji, gdy brak było odpowiednich przepisów wprost upoważniających do przetwarzania danych osobowych[766]. Ze względu jednak na brzmienie art. 23 ust. 1 pkt 2 UODO1997 przyjmowano, że art. 23 ust. 1 lit. 4 UODO1997 nie mógł stanowić podstawy prawnej do przetwarzania danych osobowych w związku z działalnością organów władzy publicznej o charakterze władczym[767]. Chodzi zatem o działania prowadzone w interesie publicznym przy użyciu form niewładczych, np. świadczenie pomocy socjalnej, pomocy ofiarom klęsk żywiołowych, walka z terroryzmem, przeciwdziałanie praniu brudnych pieniędzy itp. Choć w art. 6 ust. 1 lit. e mowa o przetwarzaniu danych "w ramach sprawowania władzy publicznej", w tym przypadku owego sprawowania władzy nie należy utożsamiać z takimi aktami władztwa publicznego, jak decyzje administracyjne, wyroki sądowe czy innego rodzaju akty indywidualno-konkretne stanowiące przejawy władztwa publicznego wobec osób fizycznych czy podmiotów prywatnych, z którymi wiąże się przetwarzanie danych osobowych[768].

Przesłanka ma charakter otwarty; nie sposób z góry bowiem określić katalogu zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej w przypadku jakiegokolwiek administratora[769]. Katalogu takich administratorów także nie można w sposób wyczerpujący określić. Chodzi o zadania, które zostały zlecone przez prawo temu podmiotowi, który dane przetwarza, oraz że mogą to być zadania z zakresu bezpieczeństwa publicznego, walki z przestępczością, udzielania pomocy ofiarom klęsk

[765] *A. Drozd*, Ustawa o ochronie danych osobowych, 2006, s. 123; *A. Mednis*, Ustawa o ochronie danych osobowych, s. 67
[766] *E. Kulesza*, Istotne rozróżnienie, „Rzeczpospolita" z 14.2.2000 r. za: *P. Litwiński (red.)*, op. cit., pkt. 53.
[767] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 509.
[768] *M. Sakowska-Baryła*, op. cit..
[769] *Ibidem*, pkt 26.

żywiołowych itd., a podmiotami wykonującymi zadania publiczne mogą zaś być organy państwowe, samorządowe lub komunalne jednostki organizacyjne, a także inne podmioty wykonujące zadania publiczne, w tym podmioty niepubliczne[770]. Bez wątpienia natomiast chodzi tu o takie zadania, które administrator wykonuje – nawiązując do tradycyjnego podziału obszarów działalności podmiotów publicznych – w sferze *imperium*, a nie sferze *dominium*, a więc tam, gdzie realizuje swoje kompetencje z zakresu przyznanej mu władzy, nie zaś z zakresu działalności ściśle cywilnoprawnej, w tym zwłaszcza właścicielskiej w odniesieniu do majątku, którym dysponuje, czy też w sferze prawnopracowniczej wobec członków swojego personelu[771].

Przesłanki tej nie można zatem rozumieć jako generalne zezwolenie na przetwarzanie danych osobowych przez organy władzy publicznej, w oderwaniu od norm kompetencyjnych regulujących funkcjonowanie tychże organów. Przeciwnie, w dalszym ciągu aktualna pozostaje zasada działania władzy publicznej – także w sferze informacyjnej – na podstawie i w granicach prawa[772]. W odniesieniu do organów władzy publicznej, podstawy przetwarzania danych osobowych zawarte w art. 6 ust. 1 lit. c i e RODO wzajemnie się więc uzupełniają, regulując sytuacje, w których w przepisach prawa Unii lub prawa krajowego wprost wskazano obowiązek przetwarzania określonych danych lub też wskazano zadania, do realizacji których niezbędnym jest przetwarzanie danych osobowych[773].

Jako przykład typu zadań mogą być zadania publiczne wyszczególnione w każdej z ustaw samorządowych (art. 7 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, art. 4 ustawy z dnia 5 czerwca 1998 r. o samorządzie powiatowym o oraz art. 14 ustawy z dnia 5 czerwca 1998 r. o samorządzie województwa). W każdym z tych przypadków zadania określone zostały w taki sposób, że w zależności od konkretnej sytuacji, stanu prawnego w danym czasie, kontekstu realizacyjnego mogą one wymagać przetwarzania danych osobowych bądź nie, a jeżeli tak, na warunkach określonych w RODO potencjalnie można poszukiwać dla nich oparcia w treści art. 6 ust. 1 lit. e.[774] Przesłanka ta dostarcza podstawy legalizacyjnej dla przetwarzania danych osobowych tam, gdzie to niezbędne dla realizacji zadania publicznego, ale niewysłowione wprost w przepisie prawa kreującym takie zadanie[775].

[770] Wyrok NSA z 5.2.2008 r., I OSK 37/07.
[771] *M. Sakowska-Baryła*, op. cit., pkt 26.
[772] *P. Litwiński (red.)*, op. cit., pkt. 54.
[773] *Ibidem.*
[774] *M. Sakowska-Baryła*, op. cit.
[775] *Ibidem.*

Wymienione w przesłance kryterium niezbędności należy odnieść do symetrycznego wymogu określonego dla podstawy z art. 6 ust. 1 lit. c. Podstawowe relewantne dla kształtowania kryterium, czyli kryterium konieczności nie oznacza, że przetwarzanie ma następować wyłącznie w przypadkach absolutnie koniecznych do realizacji obowiązku. Ocena ta powinna brać pod uwagę istnienie związku pomiędzy przetwarzaniem a wykonaniem zadania w interesie publicznym lub w ramach sprawowania władzy publicznej. Związek ten powinien być oceniany pod względem proporcjonalności oraz podstawowych zasad przetwarzania danych, w tym przede wszystkim zasady celowości i minimalizacji danych[776].

Podobnie jak w przypadku podstawy z art. 6 ust. 1 lit. c, także tutaj konieczne jest, aby podstawa prawna takiego przetwarzania była określona w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator (art. 6 ust. 3), przy czym RODO nie wymaga określenia w tej podstawie celu przetwarzania, jak to ma miejsce w ramach art. 6 ust. 1 lit. c. Przesłanka z art. 6 ust. 1 lit. e z kolei wymaga określenia w przepisach niezbędności przetwarzania do wykonania zadania realizowanego w interesie publicznym bądź niezbędności przetwarzania w ramach sprawowania władzy publicznej powierzonej administratorowi oraz fakultatywnie może zawierać pozostałe elementy wymienione w art. 6 ust. 3 RODO. Także w odniesieniu do tej przesłanki, przepisy statuujące podstawę prawną przetwarzania podlegają ograniczeniom wynikającym z zasady proporcjonalności. Wymóg ten będzie spełniony wtedy, gdy wprowadzona regulacja ustawodawcza jest w stanie doprowadzić do zamierzonych przez nią skutków (zasada przydatności); regulacja ta jest niezbędna dla ochrony interesu publicznego, z którym jest powiązana (zasada konieczności); a ponadto jej efekty pozostają w proporcji do ciężarów nakładanych przez nią na obywatela (zasada proporcjonalności w ścisłym tego słowa znaczeniu[777].

Zgodnie z motywem 154 zd. 2 preambuły RODO publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny, a zatem prawodawca UE wprost uznał publiczny dostęp do dokumentów za zadanie w zakresie interesu publicznego, do którego odnosi się przesłanka z art. 6 ust. 1 lit. e RODO, a przepisy uzupełniające mogą dostosować prawo krajowe do wypełnienia warunków z tej przesłanki[778]. Jak wykazano w poprzednim rozdziale, ponowne wykorzystywanie informacji sektora publicznego można uznać za interes publiczny, z tego też powodu art. 6 ust. 1 lit. e RODO również stanowić będzie podstawę dla przetwarzania danych osobowych przez podmiot obowiązany do przekazania lub udostępnienia

[776] *D. Lubasz*, op. cit., Komentarz do art. 6 ust. 1 lit. e, s. 384.
[777] Wyrok TK z 11.4.2000 r., K 15/98.
[778] *G. Sibiga, I. Małobęcka-Szwast*, Relacje, s. 67.

informacji sektora publicznego do ponownego wykorzystywania. Należy zatem uznać, że art. 6 ust. 1 lit. e w związku z ust. 2 i 3 RODO wyznacza relację pośrednią prawa do ochrony danych osobowych i ponownego wykorzystywania informacji sektora publicznego, dlatego też łącznie z art. 86 RODO powinien zostać wykonany w prawie krajowym.

Jednocześnie w art. 6 ust. 2 RODO bezpośrednio wskazano, że przepisy prawa krajowego przyjmowane w oparciu o art. 6 ust. 1 lit. e RODO służą dokładniejszemu określeniu szczegółowych wymogów przetwarzania i innych środków w celu zapewnienia zgodności przetwarzania danych i jego rzetelności w sytuacjach przewidzianych w Rozdziale IX, a zatem również w art. 86 i co z tym związane w odniesieniu do ponownego wykorzystywania. W szczególności art. 6 ust. 2 RODO nawiązuje do zasady wyrażonej w art. 5 ust. 1 lit. a RODO, czyli zgodności przetwarzania z prawem, rzetelność i przejrzystości. W tym kontekście należy stwierdzić, że prawodawca krajowy może uszczegółowić zasadę zgodności z prawem i rzetelności, natomiast jeśli tego nie uczyni, stosuje się generalną zasadę wyrażoną w art. 5 ust. 1 lit. a RODO[779].

Przyjęcie podstawy przetwarzania danych z art. 6 ust. 1 lit. e RODO, dla ponownego wykorzystywania danych osobowych osób innych niż pełniące funkcje publiczne w związku z pełnieniem tych funkcji oraz w pozostałych przypadkach niewynikających już wprost z przepisów UPW (opisanych powyżej) wzmacnia ochronę podmiotów danych. Osoby te mają możliwość zgłoszenia umotywowanego sprzeciwu, o którym mowa w art. 21 ust. 1 RODO. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e lub f, w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

W jakich zatem okolicznościach przetwarzania danych osobowych w ramach ponownego wykorzystywania informacji będzie miał zastosowanie art. 6 ust. 1 lit. e? W mojej opinii można przyjąć, że w zakresie realizacji przez podmiot zobowiązany prawa do ponownego wykorzystywania informacji sektora publicznego zasadą pozostaje właśnie powoływanie się na omawianą przesłankę. Nie wyklucza to jednak szczególnych regulacji, które będą nakładały prawny obowiązek ciążący na administratorze do ujawnienia danych

[779] *Ibidem*.

w ramach informacji sektora publicznego (art. 6 ust. 1 lit. c RODO), jak w odniesieniu do danych osób pełniących funkcje publiczne czy danych ujawnionych oświadczeniach majątkowych z mocy prawa publikowanych w BIP.

Jakie potencjalnie dane osobowe będą mogły być ujawnione w ramach informacji sektora publicznego do ponownego wykorzystywania w oparciu o przedmiotową przesłankę? W mojej opinii podstawa ta będzie miała m.in. zastosowanie w przypadku udostępnienia do ponownego wykorzystywania danych osobowych wymienionych w art. 7 ust. 4 UPW. Zgodnie z tym przepisem do przetwarzania przez użytkownika, w celu ponownego wykorzystywania, danych osobowych: 1) osób pełniących funkcje publiczne mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania tych funkcji, 2) osób fizycznych reprezentujących osoby prawne, w tym ich dane kontaktowe, 3) obejmujących nazwę (firmę), numer identyfikacji podatkowej (NIP) albo imię i nazwisko kontrahenta podmiotu zobowiązanego nie stosuje się przepisów art. 14 ust. 1–4 RODO. Należy zatem uznać, że celem art. 7 ust. 4 jest ułatwienie ponownego wykorzystywania wymienionych kategorii informacji obejmujących dane osobowe, poprzez zwolnienie użytkownika z wypełniania wtórnego obowiązku informacyjnego w sytuacji, w której bądź uzyskał przedmiotowe informacje od podmiotu zobowiązanego w trybie wnioskowym bądź dane są powszechnie dostępne na stronie podmiotowej BIP, portalu otwartych danych lub innym systemie teleinformatycznym podmiotu zobowiązanego (zob. szerz. Rozdział 10.3). Nie można natomiast uznać art. 7 ust. 4 UPW za samodzielną podstawę legalizującą przetwarzanie określonych danych osobowych. Celowościowo należy przyjąć taką wykładnię tego przepisu, że skoro racjonalny ustawodawca wyłączył konieczność spełnienia obowiązku informacyjnego przez użytkownika w związku z przetwarzaniem danych wymienionych w art. 7 ust. 4 pkt 2 i 3 (pkt 1 dla tych rozważań jest irrelewantny, możliwość przetwarzania danych osobowych osób pełniących funkcje publiczne mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania tych funkcji wynika wprost w z art. 6 ust. 2) , to jednocześnie dopuścił legalność przetwarzania tych danych. Przyjęcie przeciwnej interpretacji oznaczałoby, że art. 7 ust. 4 jest bezprzedmiotowy. W związku z powyższym podstawą prawną dla podmiotu zobowiązanego ujawniającego przedmiotowe dane do ponownego wykorzystywania będzie stanowił właśnie art. 6 ust. 1 lit. e, natomiast użytkownik będzie przetwarzał te dane w oparciu o przesłankę art. 6 ust. 1 lit. f.

7.2.3. Zgoda

Potencjalnie jako podstawę przetwarzania danych osobowych w ramach informacji sektora publicznego przez administratora będącego podmiotem zobowiązanym należy rozważyć również zgodę. W art. 6 ust. 1 lit. a wskazano jedną z podstawowych przesłanek legalizujących przetwarzanie danych osobowych, którą jest zgoda osoby, której dane dotyczą. Zgodnie z art. 4 pkt 11 RODO, zgoda na przetwarzanie danych osobowych to okazanie woli przez osobę, której dane dotyczą, którego treścią jest przyzwolenie na przetwarzanie danych osobowych. Okazanie woli może mieć przy tym postać oświadczenia lub wyraźnego działania potwierdzającego, a także charakteryzować się następującymi cechami: być dobrowolne, konkretne, świadome i jednoznaczne.

W art. 7 RODO prawodawca UE określił z kolei warunki wyrażenia zgody:

- jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych (ust. 1);
- jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca (ust. 2);
- osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie (ust. 3);
- oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy (ust. 4).

Zgoda jest w doktrynie postrzegana jako najsilniejszy przejaw autonomii informacyjnej osoby, ponieważ pozwala jednostce na samodzielną decyzję dotyczącą określenia sfery

dostępności dla innych informacji o sobie[780]. Przyznaje się podstawowego znaczenie przesłance zgody osoby zainteresowanej na udostępnianie informacji[781].

Przepisy ogólnego rozporządzenia nie wymagają dochowania żadnej szczególnej formy wyrażenia zgody na przetwarzanie danych osobowych. Brak wymogu formy powoduje, że w praktyce zgoda może zostać udzielona w dowolny sposób i za pośrednictwem dowolnych mediów (telefon, poczta elektroniczna, formularz umieszczony na stronie internetowej)[782]. Niedochowanie więc formy pisemnej może mieć tylko znaczenie dla udowodnienia faktu złożenia takiego oświadczenia[783]. Wprowadzanie zatem pewnych wymagań dotyczących formy lub sposobu wyrażenia zgody może być wynikiem związania zasadą rozliczalności (art. 5 ust. 2), która niesie obowiązek wykazania, że zgoda została wyrażona, oraz konsekwencją rozłożenia ciężaru dowodu, który zgodnie z art. 7 ust. 1 spoczywa na administratorze[784].

Z formą wyrażenia zgody związany jest wymóg jej jednoznaczności, który oznacza, że nie może pozostawać wątpliwości co do zamiaru wyrażenia zgody przez osobę, której dane dotyczą. Innymi słowy, wskazanie przez podmiot danych, na to, że wyraża przyzwolenie, musi niedwuznacznie określać jej zamiar[785].

Zgoda powinna zostać udzielona dobrowolnie. Nie spełnia tego wymogu takie ukształtowanie sytuacji osoby, której dane dotyczą, że nie ma ona rzeczywistego i wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji (motyw 42 preambuły do RODO). Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna (motyw 43 preambuły RODO).

Kolejną konstytutywną cechą zgody na przetwarzanie danych osobowych jest konkretność i świadomość. Wymóg konkretności ma na celu zapewnienie przez administratora,

[780] *M. Sakowska-Baryła*, op. cit., pkt 5.
[781] Zob. wyrok TK z 20.11.2002 r., K 41/02.
[782] *P. Litwiński (red.)*, op. cit., pkt 8.
[783] *Ibidem*.
[784] *M. Sakowska-Baryła*, op. cit., pkt 7.
[785] *D. Lubasz*, op. cit., komentarz do art. 4 pkt 11, s. 255.

aby zgoda w sposób zrozumiały, wyraźny i precyzyjny oznaczała cel oraz zakres przetwarzania[786]. Tym samym cel przetwarzania nie może zostać podany w sposób blankietowy, ogólny czy odnosić się do otwartego zbioru czynności przetwarzania[787]. Kryterium konkretności nie odnosi się tylko do celu przetwarzania, ale dotyczy innych aspektów powiązanych z celem, w szczególności zakresu przetwarzania i zakresu danych, i pod tym względem związany jest z przesłanką świadomości zgody obejmującej m.in. skonkretyzowanie ram przetwarzania[788]. Celem wymogu świadomości zgody jest zapewnienie podmiotowi danych jak najpełniejszej kontroli nad jego danymi poprzez wyposażenie go w wiedzę na temat celu, zakresu i kontekstu przetwarzania danych, na które ma wyrazić zgodę, jak również powinien on znać tożsamość administratora. Wymóg ten jest zatem skorelowany z koniecznością realizacji zasady przejrzystości (art. 5 ust. 1 lit. a RODO) i związanych z nią obowiązków informacyjnych[789]. Wykonanie obowiązków informacyjnych nie daje jednak gwarancji pełnej świadomości, zwłaszcza w przypadkach, gdy administrator występuje o zgodę w związku z rozszerzeniem celów przetwarzania, a pozostałych obowiązków już nie realizuje[790].

Prawidłowe wyrażenie zgody na przetwarzanie danych osobowych wymaga zatem wskazania celu lub celów przetwarzania. Określenie celu jest nie tylko elementem zgody, ale przede wszystkim realizacją sformułowanej art. 5 ust. 1 lit. b RODO zasady związania celem. W motywie 32 wyjaśniono, że zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach, jeżeli przetwarzanie zaś służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Przepis posługuje się pojęciem "czynności przetwarzania", które nie zostało wyjaśnione na gruncie RODO. Na gruncie analizowanego przepisu wydaje się, że chodzi o konkretne działania podejmowane na danych w ramach każdego z celów[791]. Zgodnie w powołanym przepisem w ramach jednego celu możliwe jest podejmowanie kilku czynności przetwarzania[792].

Co istotne, wymóg ten rozciąga się także na udostępnianie danych osobowych, a więc ten rodzaj przetwarzania danych, który będzie miał szczególne znaczenie z perspektywy ponownego wykorzystywania. Osoba, której dane dotyczą, musi zostać poinformowana

[786] Zob. *Grupa Robocza Art. 29*, Wytyczne dotyczące zgody na mocy rozporządzenia 2016/679 z 28.11.2017 r., (WP259), s. 13.
[787] *D. Lubasz,* op. cit., s. 249.
[788] *D. Lubasz,* Zgoda [w:] *D. Lubasz (red.)*, Meritum, s. 122.
[789] *Ibidem*, s. 123.
[790] *A. Mednis*, Cechy zgody na przetwarzanie danych osobowych w opinii Grupy Roboczej Art. 29 dyrektywy 95/46 Nr 15/2011 (WP 187), „Monitor Prawniczy" 2012, nr 7 (dodatek), s. 27.
[791] *M. Sakowska-Baryła*, op. cit., pkt 6.
[792] *P. Litwiński (red.)*, op. cit., pkt 13.

o odbiorcach danych (art. 13 ust. 1 lit. e RODO). Jeżeli więc to właśnie zgoda ma stanowić podstawę prawną do udostępniania danych osobowych, udostępnianie będzie dopuszczalne wyłącznie na rzecz takich odbiorców danych, o jakich informacje zostały zakomunikowane osobie, której dane dotyczą, w chwili zbierania danych osobowych, a przed udzieleniem stosownej zgody[793].

Stąd zgoda powinna być rozumiana tak, jak rozumiała ją osoba, której dane dotyczą, w chwili udzielania zgody. Należy więc ustalić, czy zwrot "udostępnianie danych osobowych" był rozumiany wyłącznie jako przekazywanie tych danych innym podmiotom, czy też również jako przetwarzanie tych danych przez odbiorców danych (np. użytkownika na gruncie UPW, zob. Rozdział 7.3.2). W tym drugim przypadku zgoda na "udostępnianie" danych będzie wywierała także taki skutek, że odbiorcy danych będą mogli przetwarzać otrzymane dane z powołaniem się na zgodę osoby, której dane dotyczą, jako na podstawę prawną przetwarzania danych[794]. Zdaniem *P. Litwińskiego* "udostępnianie danych osobowych" odbiega w sposób istotny od znaczenia wyrażeń "ujawnianie danych" czy "podawanie do publicznej wiadomości". "<Udostępnianie danych osobowych> wskazuje bowiem nie tylko na element ich upublicznienia (jak to ma miejsce w przypadku ujawniania danych), lecz także na przejmowanie tych danych przez inne podmioty (odbiorców danych). Jeżeli dodatkowo zestawimy zwrot <udostępnianie danych osobowych> z podaniem – w wykonaniu obowiązku informacyjnego z art. 13 ust. 1 lit. e RODO – informacji o odbiorcach danych, wówczas nie ulega wątpliwości, że treścią oświadczenia o wyrażeniu zgody na udostępnianie danych osobowych jest zgoda na fizyczne przekazanie danych oraz na ich przetwarzanie przez odbiorców danych"[795].

Zgoda może zostać cofnięta przez osobę, która jej udzieliła. Uprawnienie to należy do istotnych komponentów autonomii informacyjnej podmiotu danych. Skoro przesłance zgody podmiotu danych na udostępnienie informacji przypisuje się podstawowe znaczenie jako warunkującej możliwość decydowania o swoich danych, to wycofanie zgody stanowi instrument zapewniający realne korzystanie z tego uprawnienia[796]. Odwoływalność zgody powinna zapobiegać zjawisku zbierania zgód "na zapas", zwłaszcza gdy administrator dysponuje inną przesłanką legalizującą przetwarzanie danych w określonym celu[797].

[793] *P. Litwiński (red.),* op. cit., pkt. 29.
[794] *Ibidem.*
[795] *Ibidem.*
[796] *M. Sakowska-Baryła*, op. cit., Komentarz do art. 9, pkt 4.
[797] *Ibidem.*

Skutkiem cofnięcia zgody na przetwarzanie danych osobowych będzie brak możliwości powołania się na tę właśnie podstawę przetwarzania danych (skutek *ex nunc),* co oznacza, że nie wpływa ono na legalność przetwarzania danych do momentu cofnięcia zgody[798]. Odwołanie zgody skutkuje zatem brakiem możliwości przetwarzania danych osobowych na tej podstawie w przyszłości. Jednocześnie podmiot danych powinien zostać o tym informowany zanim wyrazi zgodę, stąd wydaje się zasadne uwzględnienie tej informacji w klauzuli zgody[799]. Na administratorze danych osobowych ciąży prawny obowiązek poinformowania osoby, której dane dotyczą, o możliwości odwołania zgody jeszcze przed jej wyrażeniem, co wynika z zakresu obowiązków informacyjnych towarzyszących gromadzeniu danych osobowych na podstawie art. 13 ust. 2 lit. c RODO.

Przyznając zgodzie osoby, której dane dotyczą, podstawowe znaczenia w świetle przysługującego jej prawa do prywatności informacyjnej, należałoby więc przyjąć, że jeżeli udzielono zgody na przetwarzanie danych osobowych, a następnie zgodę wycofano, wówczas przetwarzanie danych osobowych stałoby się na przyszłość niedopuszczalne, jako stojące w sprzeczności z zasadą autonomii informacyjnej. Za niedopuszczalną należałoby więc uznać sytuację, w której administrator danych osobowych, który zebrał dane osobowe na podstawie zgody osoby zainteresowanej, kontynuuje przetwarzanie tych danych z powołaniem się na inną podstawę prawną ich przetwarzania, podczas gdy osoba, której dane dotyczą, wycofała zgodę lub w inny sposób zamanifestowała swoją wolę zaprzestania przetwarzania jej danych osobowych[800].

Na gruncie przepisów krajowych pojawia się natomiast wątpliwość jaka jest podstawa przetwarzania danych osobowych w przypadku, gdy osoba fizyczna – zgodnie z art. 6 ust. 2 UPW - rezygnuje z przysługującego jej prawa. Jest to rozwiązanie, które swoje źródło znajduje w przepisach ustawy o dostępie do informacji publicznej. Zgodnie z art. 5 ust. 2 UDIP prawo do informacji publicznej podlega ograniczeniu ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy. Ograniczenie to nie dotyczy informacji o osobach pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji, oraz przypadku, gdy osoba fizyczna lub przedsiębiorca rezygnują z przysługującego im prawa. Ustawodawca wyodrębniając przepisy o ponownym

[798] *Ibidem.* Podobnie: *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2004, s. 487 oraz *P. Litwiński (red.)*, op. cit., Komentarz do art. 9, pkt 8.
[799] *Ibidem.*
[800] *P. Litwiński (red.)*, op. cit.

wykorzystywaniu do UPW stworzył symetryczne ograniczenie – oczywiście - odnosząc je przedmiotowo do prawa do ponownego wykorzystywania informacji sektora publicznego.

Przepisy o ponownym wykorzystywaniu nie przewidują obowiązku każdorazowego występowania przez podmiot zobowiązany do osoby fizycznej, której dane mogą zostać ujawnione w ramach informacji sektora publicznego z pytaniem, czy rezygnuje ona z przysługującego jej prawa do ochrony prywatności i wskazywania konsekwencji takiego oświadczenia polegającego o możliwości dowolnego ponownego wykorzystywania (czyli przetwarzania) jej danych osobowych przez każdego zainteresowanego w dowolnym nieoznaczonym z góry celu (w przypadku podjęcia decyzji o udostępnieniu informacji sektora publicznego w systemie teleinformatycznym podmiotu zobowiązanego), jak i wykorzystywania przez konkretnego użytkownika w danym celu wskazanym we wniosku o ponowne wykorzystywanie[801].

Należy podkreślić, że przepisy ogólnego rozporządzenia nie znają instytucji rezygnacji z ochrony danych osobowych, tym bardziej rezygnacji z prawa do prywatności. Podobnego rozwiązania nie przewidują również przepisy dyrektyw o ponownym wykorzystywaniu. Kluczowe jest zatem odpowiedzenie na pytanie czy rezygnacja z prawa do prywatności na gruncie UPW jest tożsama ze zgodą, o której mowa w art. 6 ust. 1 lit. a) RODO[802].

W kontekście ochrony praw lub wolności osób fizycznych oczywiście korzystniejsze z perspektywy podmiotu danych byłoby uznanie, że „rezygnacja z przysługujących praw" jest tożsama ze zgodą wg RODO[803]. Po pierwsze, wówczas należałoby przyjąć, że „rezygnację z prawa do prywatności" również można cofnąć, wzorem art. 7 ust. 3 RODO. Po drugie, należy zauważyć, art. 6 ust. 2 UPW nie obejmuje wyłącznie przetwarzania zwykłych danych osobowych. Można zatem przyjąć, że uzyskanie wyraźnej zgody zalegalizuje przetwarzanie także danych szczególnych kategorii w oparciu o art. 9 ust. 2 lit. a) RODO, w myśl którego nie zabrania się przetwarzania szczególnych kategorii danych osobowych, jeżeli osoba której dane dotyczą wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku

[801] Zob. *M. Sakowska-Baryła*, Ograniczenia prawa do ponownego wykorzystywania ISP [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska,* op. cit., s. 65-66.

[802] Na gruncie przepisów UDIP oraz UODO1997 *M. Sakowska-Baryła* przyznaje, że zgoda na przetwarzanie danych osobowych i rezygnacja z prawa do prywatności nie są pojęciami tożsamymi, rezygnacja jest pojęciem szerszym, ale przez zgodę może być wyrażona rezygnacja, a co za tym idzie otwiera się możliwość udostępnienia danych osobowych tą zgodą objętych, zob. tej autorki: Dostęp do informacji publicznej a ochrona danych osobowych, s. 394.

[803] Zob. *M. Gumularz*, Ekspertyza s. 38 oraz *P. Sitniewski*, Komentarz do art. 6, pkt 4, Ustawa o ponownym, Legalis/Wyd.2017, choć autor nie pisze o zgodzie w ogólności, nie odnosząc jej wprost do zgody w rozumieniu RODO.

konkretnych celach. Jednakże w praktyce realizowania prawa ponownego wykorzystywania informacji sektora publicznego taka okoliczność wydaje się mało prawdopodobna.

Kończąc powyższe rozważania trzeba przypomnieć, że konstrukcja „rezygnacji z prawa do prywatności" swoim zakresem podmiotowym nie obejmuje jedynie osób pełniących funkcje publiczne. Z możliwości „rezygnacji" może skorzystać każda osoba fizyczna, której dane osobowe mogą potencjalne zostać przekazane lub udostępnione do ponownego wykorzystywania. W mojej opinii taka sytuacja jest teoretycznie możliwa, lecz może mieć znikome znaczenie w praktyce ponownego wykorzystywania informacji sektora publicznego.

7.3. Podstawy przetwarzania danych osobowych przez użytkownika

7.3.1. Prawnie uzasadniony interes

Podstawową przesłanką legalizującą przetwarzanie danych osobowych przez użytkownika w ramach ponownego wykorzystywania informacji sektora publicznego stanowi art. 6 ust. 1 lit. f RODO. W myśl tego przepisu przetwarzanie danych osobowych jest dopuszczalne, gdy jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem. Przepis ten stanowi odpowiednik tzw. klauzuli prawnie usprawiedliwionego celu administratora danych osobowych, unormowany w art. 23 ust. 1 pkt 5 UODO1997[804].

Posłużenie się przez prawodawcę UE klauzulą generalną zwiększa elastyczność katalogu wymienionego w art. 6 ust. 1 RODO. Umożliwia dopuszczenie przetwarzania danych osobowych w przypadkach, które pojawią się dopiero w przyszłości wraz z postępem technologicznym raz rozwojem nowych modeli biznesowych[805]. W doktrynie zauważa się, że gdyby przepisy RODO nie przewidywały przedmiotowej przesłanki, to mogłoby dojść do sytuacji, gdy nawet w uzasadnionych przypadkach administratorzy, inni niż organy publiczne, nie mieliby podstawy prawnej do przetwarzania danych osobowych. Mogłoby to

[804] Przetwarzanie danych jest dopuszczalne tylko wtedy, gdy: jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.
[805] *W. Chomiczewski,* Komentarz do art. 6 ust. 1 lit. f [w:] *E. Bielak-Jomaa, D. Lubasz,* RODO s. 389.

w konsekwencji uniemożliwić w przyszłości rozwój niektórych usług, postęp technologiczny lub przeciwdziałać rozwojowi nowych modeli biznesowych[806].

Podstawa wprowadza klauzulę o charakterze ogólnym, w ramach której przyjęcie, że przetwarzanie danych bez zgody osoby, której dane dotyczą, jest dopuszczalne, wymaga łącznego spełnienia dwóch przesłanek:

- przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią,
- nie zachodzą sytuacje, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych[807].

Zatem *a contrario*, jeśli występują w danym stanie faktycznym interesy lub podstawowe prawa i wolności podmiotu danych, przewarzające nad prawnie uzasadnionymi interesami administratora lub strony trzeciej, powołanie się na przedmiotową przesłankę legalizującą przetwarzanie danych osobowych będzie niemożliwe.

Konieczne będzie zatem wyważenie dwóch dóbr, prawnie uzasadnionego interesu administratora lub strony trzeciej z interesem, podstawowymi prawami i wolnościami osoby, której dane dotyczą. Punkt ciężkości omawianej podstawy przetwarzania danych powinien więc być poszukiwany w dążeniu do wyważenia interesów podmiotów uczestniczących w procesie przetwarzania danych, nie zaś do poszukiwania takich interesów związanych z przetwarzaniem danych, jakie mogą zostać uznane za uzasadnione prawnie[808]. Wynika to z koncepcji ochrony danych osobowych, która opiera się na balansowaniu interesów[809]. Zgodnie z motywem 47 administrator przy ważeniu dóbr powinien wziąć pod uwagę rozsądne oczekiwania osób, których dane dotyczą, oparte na ich powiązaniach z administratorem, czyli np. uwzględnić pozostawanie w relacji z klientem administratora lub gdy osoba działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji,

[806] *Ibidem*, s. 390.
[807] *P. Litwiński (red.)*, op. cit., Komentarz do art. 6, pkt 58.
[808] *P. Litwińsk(red.)*, op. cit., pkt 66.
[809] *M. Safjan*, Ochrona danych osobowych – granice autonomii informacyjnej [w:] *M. Wyrzykowski*, Ochrona danych osobowych, Instytut Spraw Publicznych, Warszawa 1999 r., s. 14.

w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania.

Elementem składowym testu ważenia interesu, który wymaga wyjaśnienia jest prawnie uzasadniony interes. Należy go odnieść do terminu, usprawiedliwionego celu występującego na gruncie UODO1997. W orzecznictwie sądowym wskazuje się, że termin ten jest zwrotem niedookreślonym i stanowi klauzulę generalną w znaczeniu funkcjonalnym. Daje w szczególności pewnego rodzaju luz decyzyjny, dzięki któremu organ stosujący prawo może przy podejmowaniu decyzji kierować się ocenami indywidualnymi konkretnej sytuacji, a także pewnymi zasadami postępowania niesformułowanymi w przepisach prawa[810].

Interesy realizowane przez administratora lub przez stronę trzecią przy przetwarzaniu danych muszą być uzasadnione prawnie. W doktrynie przyjmuje się, że nie można jednak sformułowania "prawnie", w tym wypadku odnosić do uprawnienia do przetwarzania danych, które miałoby wynikać z jakiegoś szczególnego przepisu prawa. Takie podejście prowadziłoby do przyjęcia, że takie przetwarzanie powinno mieć swoje źródło w uprawnieniach wynikających ze szczególnych przepisów prawa, co prowadziłoby do powstania konkurencyjnej podstawy przetwarzania danych w stosunku do art. 6 ust. 1 lit. c lub lit. e RODO[811].

Nie można również prawnie uzasadnionego interesu utożsamiać z interesem prawnym w rozumieniu przepisów o postępowaniu administracyjnym. Interes prawny powinien bowiem znajdować oparcie w przepisach prawa materialnego, co znów niebezpiecznie zbliżałoby tę przesłankę przetwarzania danych do przesłanek z art. 6 ust. 1 lit. c lub lit. e RODO[812].

W tym kontekście zachowują swoją aktualność poglądy sformułowane na gruncie UODO1997. Ocenie powinna podlegać okoliczność, czy interes (cel), który zamierza osiągnąć (administrator danych lub podmiot trzeci), jest uzasadniony (usprawiedliwiony), tzn. czy znajduje swoje gospodarcze i prawne uzasadnienie, jak również jest zgodny z przedmiotem działalności konkretnego administratora danych (np. czy jest zgodny z przedmiotem działalności spółki)[813]. Również działalność "pomocnicza" w stosunku do działalności zasadniczej (wpisanej m.in. do przedmiotu działalności) może być uznana za interes (cel) uzasadniający wykorzystanie danych osobowych[814]. Zatem prawnie uzasadniony interes trzeba

[810] Zob. wyrok NSA z 19.11.2001 r., II SA 2702/00.
[811] *P. Litwiński (red.)*, op. cit., pkt 59. Podobne stanowisko na gruncie UODO1997 *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2015, s. 468 i n.
[812] *P. Litwiński (red.)*, op. cit., pkt 58.
[813] Zob. *A. Mednis*, Ustawa o ochronie danych osobowych. Komentarz, Warszawa 2001, s. 68-69, *A. Drozd*, Ustawa, s. 128.
[814] *A. Mednis*, Ustawa, 2001, s. 69.

rozumieć nie jako interes wynikający z przepisów prawa, lecz jako interes, który jest zgodny z prawem[815].

Prawodawca unijny, wprowadzając kategorię "uzasadnionego interesu administratora", ustanowił szerszą przesłankę przetwarzania danych osobowych. Pojęcie "interesu" będzie kategorią szerszą niż pojęcie "celu". Interes administratora może być określany jako pewna relacja między jakimś stanem obiektywnym a oceną tego stanu z punktu widzenia korzyści, jaką on przynosi lub może przynieść administratorowi, przy czym musi być uzasadniony[816]. Kategoria interesu jest zróżnicowana, zależna od potrzeb powstałych w związku z prowadzoną działalnością przez administratora, czyli w konsekwencji i dynamiczna, co oznacza, że nie powinno się go w sposób jednoznaczny ustalić i zdefiniować. Nie przesądzając z góry, co stanowi *interes* administratora, prawodawca UE stworzył możliwość określania go przez samych zainteresowanych z uwzględnieniem okoliczności każdego konkretnego przypadku, pod warunkiem spełnienia pozostałych kryteriów określonych w przepisie oraz przy respektowaniu wymagań art. 5 RODO[817].

Wykładnia pojęcia prawnie uzasadnionego interesu powinna być zatem szeroka i obejmować różne interesy: gospodarcze, faktyczne, prawne i inne. W przypadku podmiotów innych niż biznesowe, interesem takim mogą być interesy oparte na celach statutowych działania, np. fundacji czy stowarzyszeń[818].

W rekonstrukcji pojęcia prawnie uzasadnionego interesu pomocna jest treść motywów 47-49 preambuły RODO. Zawierają one przykłady takich interesów, zaliczając do nich m.in. cele marketingu bezpośredniego, przesyłanie danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, przetwarzanie danych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji.

Prawnie uzasadniony interes administratora lub osoby trzeciej, należy odróżnić od interesu osoby, której dane dotyczą. Chodzi o interes wymagający ochrony jego danych osobowych. Z jego istoty będzie miał on zawsze subiektywny charakter i trzeba go będzie odnosić do sytuacji danego człowieka[819]. Natomiast obiektywny charakter ma kategoria ochrony podstawowych praw i wolności podmiotu danych. Ich źródłem niewątpliwie będzie

[815] Zob. *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2015, s. 468 i n., *M. Sakowska-Baryła*, Komentarz do art. 6, pkt 28 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie, *W. Chomiczewski*, Komentarz do art. 6 ust. 1 lit. f [w:] *E. Bielak –Jomaa, D. Lubasz (red.)*, RODO, s. 392.
[816] *M. Sakowska-Baryła*, op. cit., pkt 28.
[817] *Ibidem*.
[818] *W. Chomiczewski*, Komentarz do art. 6 ust. 1 lit. f [w:] *E. Bielak –Jomaa, D. Lubasz (red.)*, RODO, s. 392.
[819] *Ibidem*, s. 395.

KPP oraz EKPC. Na gruncie prawa krajowego natomiast należałoby podczas wykładni tego pojęcia odwoływać do gwarancji praw i wolności, które znajdują swoje podstawy w normach konstytucyjnych. Wydaje się, że podstawowym instrumentem przysługującym podmiotowi danych w celu ochrony jego interesów, praw i wolności, na gruncie RODO będzie prawo do wniesienia sprzeciwu, o którym mowa w art. 21.

Na zakończenie tej części trzeba przypomnieć, że zgodnie z art. 6 ust. 1 lit. f zd. drugie RODO klauzula prawnie uzasadnionych interesów nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. W przypadku podmiotów z sektora publicznego podstaw przetwarzania danych osobowych należy poszukiwać w art. 6 ust. 1 lit. c i e RODO.

Bezwzględnie nie wyklucza się jednak stosowania tej przesłanki w związku z przetwarzaniem w innych celach niż te, które łączą się bezpośrednio z realizacją zadań organów publicznych[820]. Organy publiczne mogą korzystać z przedmiotowej przesłanki poza zadaniami realizowanymi w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, np. gdy podmiot publiczny występuje w obrocie jako strona stosunków prywatnoprawnych[821].

Dla realizacji prawa do ponownego wykorzystywania oznacza to, że na przedmiotową przesłankę może powoływać się jedynie użytkownik w rozumieniu przepisów UPW, nie będzie miała ona zatem zastosowania dla podmiotów zobowiązanych przekazujących lub udostępniających dane osobowe do ponownego wykorzystywania.

Na gruncie realizacji prawa do ponownego wykorzystywania informacji sektora publicznego istota przesłanki prawnie uzasadnionego interesu zakładać będzie konieczność każdorazowego wyważenia interesów użytkownika danych osobowych zawartych w informacji sektora publicznego oraz osoby, której dane dotyczą, związanych z jednej strony z realizacją prawnie uzasadnionych interesów użytkownika, z drugiej natomiast – z ochroną interesów lub podstawowych praw i wolności osoby, podmiotu danych. Interes użytkownika może polegać np. na wykorzystaniu danych osobowych pochodzących z publiczne dostępnych źródeł państwowych do budowy serwisu internetowego służącemu zapewnieniu transparentności oświadczeń majątkowych osób wykonujących funkcje publiczne.

Jako przykład przetwarzania danych osobowych w oparciu o prawnie uzasadniony interes administratora – na kanwie decyzji Prezesa Urzędu Ochrony Danych Osobowych

[820] *M. Sakowska-Baryła*, op. cit., pkt 26.
[821] *M. Gumularz*, Uzasadniony interes w sektorze publicznym – na przykładzie monitoringu, „ABI Expert" 2018, nr 2, s. 18.

z 15.03.2019 r . (ZSPR.421.3.2018)[822] – można podać wykorzystywanie danych przez podmioty komercyjne świadczące szeroko pojęte usługi wywiadu gospodarczego (np. wywiadownie gospodarcze, które poprzez tzw. biały wywiad gromadzą informacje z ogólnie dostępnych źródeł na temat innych przedsiębiorców) pochodzące z rejestrów państwowych (jak np. KRS czy REGON). Takim prawnie uzasadnionym interesem w przypadku wywiadowni gospodarczych może być np. możliwość zbierania i udostępniania innym uczestnikom obrotu gospodarczego poprawnych i rzetelnych informacji dotyczących prowadzonej działalności gospodarczej i sytuacji przedsiębiorców, które służą zapewnieniu bezpieczeństwa, przejrzystości i pewności tego obrotu. Podstawowym celem udostępniania danych w publicznie dostępnych rejestrach jest możliwość ich dalszego wykorzystywania w celu identyfikacji i weryfikacji uczestników obrotu gospodarczego (zarówno reprezentantów spółek prawa handlowego, jak i osób fizycznych prowadzących działalność gospodarczą)[823].

7.3.2. Zgoda

Podobnie jak w przypadku podmiotu zobowiązanego, również wobec administratora będącego użytkownikiem w rozumieniu przepisów UPW, należy wziąć pod uwagę możliwość oparcia przetwarzania danych osobowych w ramach ponownego wykorzystywania informacji sektora publicznego o zgodę, o której mowa w art. 6 ust. 1 lit. a RODO. Uwagi poczynione wcześniej dotyczące cech konstytutywnych oraz podstawowych wymogów zgody, jako przesłanki legalizującej przetwarzanie danych osobowych, należy również odnieść do okoliczności przetwarzania danych przez użytkownika.

Jak wyjaśniłem (zob. Rozdział 7.2.3) osoba, której dane dotyczą, musi zostać poinformowana o odbiorcach danych (art. 13 ust. 1 lit. e RODO). Przyjęcie zgody za podstawę prawną do udostępniania lub przekazania danych osobowych do ponownego wykorzystywania będzie dopuszczalne wyłącznie wtedy, kiedy osobie, której dane dotyczą zostanie ten fakt zakomunikowany przed udzieleniem stosownej zgody. Udzielenie zgody na udostępnianie danych osobowych wywołuje taki skutek, że odbiorcy danych – pod warunkiem, że udostępnianie następuje na rzecz podmiotów, o których osoba, której dane dotyczą, została należycie poinformowana – mogą powołać się na tę właśnie zgodę jako na podstawę prawną

[822] Szerzej na ten temat: Rozdział 9.
[823] *J. Byrski, H. Hozer*, Nałożenie administracyjnej kary pieniężnej za niezrealizowanie obowiązku informacyjnego przy pozyskiwaniu danych z publicznie dostępnych źródeł – glosa do ostatecznej decyzji Prezesa Urzędu Ochrony Danych Osobowych z 15.03.2019 r . (ZSPR.421.3.2018), „Palestra" 2019, nr 5, s. 81.

przetwarzania przez siebie otrzymanych danych[824]. W takiej sytuacji miałoby to znaczenie dla odbiorcy danych będącego użytkownikiem w rozumieniu UPW. W przypadku bowiem uzyskania zgody przez podmiot zobowiązany od podmiotu danych na ponowne wykorzystywanie jego danych osobowych przez użytkownika podstawą prawną przetwarzania danych osobowych przez tego użytkownika (odbiorcę danych) wydaje się, że nie będzie stanowił art. 6 ust. lit. f, a właśnie art. 6 ust.1 lit. a.

Na szczególną uwagą zasługuje kwestia zbadania okoliczności, w których użytkownik może powołać się na przedmiotową przesłankę. Jak wyjaśniono wyżej, nie jest dopuszczalne zbieranie zgód „na zapas", w szczególności gdy administrator dysponuje inną przesłanką legalizującą przetwarzanie danych w określonym celu. Z tego względu, w przypadku użytkownika, w pierwszej kolejności, należy rozważyć podstawę przetwarzania danych, o której mowa w art. 6 ust. 1 lit. f. Wątpliwości mogą pojawić się w sytuacji, w której użytkownik nie jest w stanie wykazać spełnienia wymogów prawnie uzasadnionego interesu, a podmiot zobowiązany zbierając dane od osoby, której dane dotyczą nie poinformował o odbiorcach danych. Przyjmując, że użytkownik będzie dążył do uzyskania zgody podmiotu danych na ponowne wykorzystywanie danych osobowych, a nie będzie dysponował żadnymi informacjami umożliwiającymi skuteczne uzyskanie zgody od osoby, której dane dotyczą, pojawia się pytanie o dopuszczalną aktywność podmiotu zobowiązanego w uzyskaniu takiej zgody. Tego rodzaju pośredniczenie pomiędzy osobą, której danej dotyczą, a potencjalnym użytkownikiem zainteresowanym przetwarzaniem danych osobowych, w ogóle na gruncie UPW, jak i dyrektyw o ponownym wykorzystywaniu nie jest przedmiotem regulacji. W mojej ocenie nie jest również zasadne, może bowiem prowadzić do dyskusyjnego wniosku, że w przypadku każdego wniosku o przekazanie informacji sektora publicznego zawierającej dane osobowe, gdy brak jest wyraźnej podstawy dla ujawnienia danych osobowych w ramach realizacji prawa do ponownego wykorzystywania, podmiot zobowiązany każdorazowo będzie występował do podmiotu danych o zgodę na takie przetwarzanie danych[825]. Z tego powodu

[824] *P. Litwiński (red.)*, op. cit., pkt. 29.

[825] Tego rodzaju sytuacja jest adresowana przez projektowany akt o zarządzaniu danymi (zob. Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act) 25.11.2020 COM(2020) 767). Skoro sam projektodawca unijny uznał za zasadne doregulowanie kwestii pośrednictwa „wymiany" danych osobowych, w dodatku w drodze rozporządzenia, które będzie obowiązywało wprost, należy przyjąć, że jest niedopuszczalne na gruncie dyrektyw o ponownym wykorzystywaniu informacji sektora publicznego. Na marginesie należy dodać, że kwestia ta, jak i inne rozwiązania zawarte w projekcie aktu o zarządzaniu danymi, budzi wątpliwości z punktu widzenia zgodności z RODO, w tym zgodności przetwarzania danych osobowych z prawem. Zob. EDPB-EDPS Joint Opinion 03/2021 on the Proposal for a regulation of the European Parliament and of the Council on European data governance (Data Governance Act) https://edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-032021-proposal_pl

w mojej opinii przesłanki zgody legalizującej przetwarzanie danych przez użytkownika nie można wykluczyć, jednak w praktyce stosowania przepisów będzie miała znikome znaczenie.

7.4. Ocena podstawy prawnej przetwarzania danych w krajowych przepisach o ponownym wykorzystywaniu. Podsumowanie przesłanek legalizujących przetwarzanie

Podsumowując ten rozdział, należy podkreślić, że do przetwarzania danych osobowych w ramach realizacji prawa do ponownego wykorzystywania dochodzi, z jednej strony w ramach udostępnienia lub przekazania informacji sektora publicznego zawierającej dane osobowe przez podmiot zobowiązany, z drugiej zaś w ramach jej ponownego wykorzystywania przez użytkownika. Mamy zatem w ramach stosowania przepisów UPW do czynienia z przetwarzaniem danych po obydwu stronach tej operacji, dlatego też oba podmioty zaangażowane w takie przetwarzanie danych (pierwotny administrator - podmiot zobowiązany i odbiorca danych - użytkownik) powinny legitymować się stosowną podstawą prawną do takiego działania. Oznacza to, że podmiot zobowiązany przed ujawnieniem danych osobowych w ramach informacji sektora publicznego na wniosek zainteresowanego ich ponownym wykorzystywaniem użytkownika musi zbadać podstawę prawną z art. 6 RODO zarówno dla czynności przetwarzania po swojej stronie, jak i przesłankę legalizującą przetwarzanie w sposób opisany we wniosku po stronie użytkownika. W przypadku zaś udostępnienia informacji sektora publicznego zawierającej lub stanowiącej danej osobowe w BIP, CRIP czy winnym systemie teleinformatycznym podmiot zobowiązany, jak wykazano, co do zasady realizuje obowiązek prawny na nim ciążący z mocy przepisów prawa. Brak stosownej podstawy prawnej dla przetwarzania danych skutkować będzie bądź odmową przekazania informacji sektora publicznego zawierającej lub stanowiącej dane osobowe do ponownego wykorzystywania lub decyzją o nieudostępnieniu danych osobowych w BIP, CRIP lub innym systemie teleinformatycznym.

Jak wykazano, oparcie przetwarzania danych osobowych w ramach realizacji prawa do ponownego wykorzystywania przez podmiot zobowiązany opierać się będzie o art. 6 ust. 1 lit. c lub e. Prawo do ponownego wykorzystywania można uznać za interes publiczny. Zatem co do zasady przesłanką legalizującą przetwarzanie danych osobowych w ramach realizacji prawa do ponownego wykorzystywania przez podmiot zobowiązany będzie wykonanie zadania w interesie publicznym (sprawowania władzy publicznej). Nie wyklucza to możliwości

ponownego wykorzystywania w szczególnych sytuacjach (np. dane osób wykonujących funkcje publiczne pozostające w związku z ich wykonywaniem) w oparciu o przesłankę obowiązku prawnego ciążącego na administratorze. Podstawa prawna takiego przetwarzania powinna spełniać podstawowe wymogi stawiane krajowym podstawom prawnym przetwarzania danych osobowych, o których mowa w art. 6 ust. 2 i 3 RODO. Niesie to za sobą określone konsekwencję na gruncie RODO, spróbujmy je podsumować.

Po pierwsze, przesłanka obowiązku prawnego, jaki i interesu publicznego (władzy publicznej), jak wskazano we wstępie tego rozdziału, stanowią samodzielną przesłankę dopuszczalności przetwarzania danych osobowych. Oznacza to, że skuteczne powołanie się na którąś z przedmiotowych przesłanek przez podmiot zobowiązany gwarantuje zgodność z prawem przetwarzania (w tym udostępniania lub przekazywania) danych osobowych[826].

Po drugie, obie przesłanki odnoszą się do właściwego przepisu prawa krajowego (lub prawa unijnego). Podstawa przetwarzania w oparciu o te przesłanki musi być określona w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator. Co istotne, w myśl motywu 45 preambuły RODO – podobnie jak w przypadku przesłanki obowiązku prawnego - rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Oznacza to, że przedmiotowa podstawa przetwarzania danych osobowych nie jest przesłanką samoistną, ale uzupełniana innymi przepisami. Zgodnie z art. 6 ust. 2 RODO państwa członkowskie mogą zachować już obowiązujące przepisy w tym zakresie albo wprowadzić odrębne przepisy krajowe dostosowujące do RODO. Również z zasady praworządności wynika, że realizacja władzy publicznej, ale także konstrukcja wykonywania zadań publicznych, następuje na podstawie i w granicach prawa. Przesłanki obowiązku prawnego oraz interesu publicznego (władzy publicznej) nie występują samoistnie, a jest związana z dalszymi przepisami prawa krajowego lub prawa unijnego, które stanowią podstawę wykonywania władzy publicznej lub zadania publicznego (zadania w interesie publicznym).

Po trzecie, przepis prawa krajowego realizujący przesłankę interesu publicznego (władzy publicznej) powinien spełniać wytyczne określone w art. 6 ust. 3. Przepis ten wyznacza obligatoryjne elementy, które musi zawierać prawidłowa podstawa prawna, oraz elementy fakultatywne. Przetwarzanie danych, o którym mowa w art. 6 ust. 1 lit. c i e RODO musi,

[826] Por. *G. Sibiga, I. Małobęcka-Szwast,* Relacje, s. 67.

w pierwszym przypadku być zgodne ze wskazanym w podstawie prawnej celem przetwarzania, w drugim przypadku, być niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Kryterium konieczności nie oznacza, że przetwarzanie ma następować wyłącznie w przypadkach absolutnie niezbędnych do realizacji obowiązku prawnego lub wykonania zadania w interesie publicznym (władzy publicznej). Ocena niezbędności powinna być relatywizowana i uwzględniać istnienie związku pomiędzy przetwarzaniem a realizacją tych obowiązków czy wykonywaniem zadania w interesie publicznym lub sprawowania władzy publicznej powierzonej administratorowi. Na gruncie ponownego wykorzystywania, przepisy UPW powinny spełnić wymóg niezbędności, o którym mowa w art. 6 ust. 3 zd. 2 RODO.

Ponadto przepisy krajowe muszą służyć realizacji celu leżącego w interesie publicznym, oraz być proporcjonalne do wyznaczonego, prawnie uzasadnionego celu. Państwa członkowskie mogą zatem tworzyć szczególne regulacje w zakresie ponownego wykorzystywania danych osobowych, jednak regulacje te muszą spełniać wytyczne zawarte w art. 6 ust. 2 i 3 RODO.

Poza wskazanymi wyżej elementami obligatoryjnymi, ustawodawca krajowy lub prawodawca unijny powinien rozważyć w uwzględnienie w podstawie prawnej elementy fakultatywne, wymienione w art. 6 ust. 3, których katalog jest otwarty.

Przepisy UPW spełniają wymóg niezbędności, o którym mowa w art. 6 ust. 3 zd. 2 RODO, jedynie w ograniczonym zakresie, nie wskazują również ogólnych warunki zgodności z prawem przetwarzania przez administratora ani rodzaju danych podlegających przetwarzaniu w ramach ponownego wykorzystywania.

Generalnie, szczególne regulacje prawa krajowego muszą mieścić się w ramach ogólnego rozporządzenia oraz następować w jego duchu i zgodnie z wyrażonymi w nim zasadami, w szczególności wymienionymi w art. 5. Ponadto przepisy te nie mogą formułować kolejnych – po tych wymienionych w art. 6 RODO – przesłanek przetwarzania danych, a jedynie ograniczać się do doszczegółowienia tych, które są wskazane w przepisie kompetencyjnym, tj. art. 6 ust. 1 lit. c i e[827].

Wątpliwość budzi, czy przepisy UPW są proporcjonalne do wyznaczonego, prawnie uzasadnionego celu, o czym stanowi art. 6 ust. 3 zd. 4 RODO. Niewątpliwie przepisy UPW służą realizacji celu leżącego w interesie publicznym, którym jest ponowne wykorzystywanie informacji sektora publicznego. Opierając ograniczenie ponownego wykorzystywania danych

[827] *D. Lubasz*, Komentarz do art. 6 ust. 1 lit. e [w:] *D. Lubasz, E. Bielak-Jomaa (red.)*, RODO, s. 388.

osobowych o ochronę prywatności osoby fizycznej (art. 6 ust. 2 UPW), nie wydaje się możliwe dokonanie oceny, ze względu nieostrość kryterium prywatności, czy przepis ten jest proporcjonalny do prawnie uzasadnionego celu jakim jest ponowne wykorzystywanie informacji sektora publicznego[828].

Ponadto, UPW zawiera tylko niektóre elementy podstawy prawnej przetwarzania danych osobowych, o których mowa w art. 6 ust. 3 zd. 3 RODO. Wskazuje kategorie osób, których dane mogą zostać udostępnione i rodzaje danych (*expressis verbis* jedynie osoby pełniące funkcje publiczne i informacje związane pełnieniem tych funkcji, pośrednio podmioty i dane wymienione w art. 7 ust. 4 pkt 2 i 3), podmioty, którym można ujawnić dane osobowe (art. 2 ust. 2 UPW - użytkownik). Można również uznać, że po stronie podmiotu zobowiązanego wskazuje również cel, jest nim realizacja prawa do ponownego wykorzystywania informacji sektora publicznego. Krajowa ustawa nie wskazuje jednak środków zapewniających zgodność z prawem i rzetelność przetwarzania oraz innych elementów, o których mowa w art. 6 ust. 3 zd. 3 RODO, lub określa je w sposób nieprecyzyjny.

W mojej opinii można zatem uznać, że ustawodawca wypełnił jedynie minimalny obowiązek uwzględnienia ochrony danych osobowych w regulacji ponownego wykorzystywania informacji sektora publicznego bez jednoczesnego „pogodzenia" obu praw oraz wyczerpującego wykonania wymogów dla podstawy prawnej przetwarzania wymienionych w art. 6 ust. 2 i 3 RODO.

Stan niepełnego wykonania przepisów ogólnego rozporządzenia rodzi określone konsekwencje prawne, zarówno dla podmiotów zobowiązanych i użytkowników, jako administratorów, jak i osób których dane dotyczą. Należy uznać, że obowiązują w zakresie ustalonym w samym RODO wszystkie główne zasady ochrony danych osobowych (art. 5–10 RODO) oraz uprawnienia osób, których dane dotyczą (art. 12–22 RODO), z tym zastrzeżeniem, że w zakresie obowiązków informacyjnych wymienionych w art. 13 ust. 3, 14 ust. 1-4 oraz art. 19 RODO przepisy UPW dokonały pewnych modyfikacji. W szczególności znajdą zastosowanie wszystkie podstawowe zasady przetwarzania danych osobowych określone w art. 5 RODO, w tym zasada zgodności z prawem, rzetelności i przejrzystości, co do której polski prawodawca nie zdecydował się na przyjęcie środków, o których mowa w art. 6 ust. 2 i 3 RODO. Mamy zatem do czynienia z równoczesnym stosowaniem przepisów RODO z przepisami UPW, tym jej art. 6 ust. 2, czyli ograniczenia prawa do ponownego wykorzystywania ze względu na prywatność osoby fizycznej.

[828] Tak na gruncie analogicznej normy w UDIP *G. Sibiga, I. Małobęcka-Szwast*, Relacje, s. 67.

Osobie, której dane dotyczą przysługują jej uprawnienia wynikające z ogólnego rozporządzenia. Jednym z określonych w RODO uprawnień jest prawo do sprzeciwu wobec przetwarzania danych osobowych przez administratora, z przyczyn związanych ze szczególną sytuacją podmiotu danych (art. 21 ust. 1 RODO). Prawo sprzeciwu przysługuje osobie fizycznej, gdy podstawą przetwarzania danych jest wykonanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. e RODO) oraz gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora (art. 6 ust. 1 lit. f RODO), a jak wykazano takie właśnie przesłanki legalizujące przetwarzanie danych osobowych należy zastosować w ramach ponownego wykorzystywania. Przypomnieć należy, że prawo do sprzeciwu nie obejmie sytuacji, gdy podstawą dla przetwarzania będzie przesłanka obowiązku prawnego ciążącego na administratorze. Wniesienie sprzeciwu nie oznacza jego automatycznego uwzględnienia, ale obowiązek rozpatrzenia przez administratora, co jest następnie kontrolowane – z inicjatywy osoby, której dane dotyczą – przez organ nadzorczy (art. 77 RODO) oraz sąd (art. 79 RODO)[829].

W prawie polskim nie ograniczono, ani też nie zmodyfikowano kompetencji organu nadzorczego do: kontrolowania (art. 58 ust. 1 RODO), nakładania środków naprawczych (art. 58 ust. 2) oraz nakładania administracyjnych kar pieniężnych (art. 83) w przypadku naruszenia przepisów o ochronie danych osobowych w ramach realizacji ponownego wykorzystywania informacji sektora publicznego. W szczególności osoby fizyczne, których dane są ujawniane (jako informacja sektora publicznego) mogą korzystać z uprawnień procesowych przewidzianych w RODO, w tym skargi do niezależnego organu nadzorczego (art. 77 RODO), jeżeli uznają, że przyznane im w RODO prawa zostały naruszone[830]. Obowiązkiem organu nadzoru jest rozpatrzenie wniesionego środka prawnego poprzez rozstrzygnięcie w przedmiocie realizacji praw określonych w RODO, a w przypadku ich naruszenia co najmniej zastosowanie środka naprawczego[831].

Brak skonkretyzowania w UPW w jakich przypadkach szczególne kategorie danych, o których mowa w art. 9 RODO, będą mogły zostać ujawnione w ramach informacji sektora publicznego (jako wyjątku od zasady ich nieprzetwarzania) i wyłączenia w tym zakresie

[829] *G. Sibiga*, *I. Małobęcka-Szwast*, Relacje, s. 72.
[830] *Ibidem*.
[831] Zob. *G. Sibiga*, Skarga do organu nadzorczego oraz jej rozpatrzenie według ogólnego rozporządzenia o ochronie danych. Postępowanie w przedmiocie skargi osoby, której dane dotyczą, „Prawo Mediów Elektronicznych" 2017, nr 4, s. 6 i n.

stosowania art. 9 RODO, spowodowało niedopuszczalność ujawniania takich danych w ramach realizacji prawa do ponownego wykorzystywania informacji sektora publicznego.

Po stronie użytkownika podstawą przetwarzania danych osobowych w ramach ponownego wykorzystywania będzie stanowiła przesłanka prawnie uzasadnionego interesu.

Potencjalnie należy również jako podstawę przetwarzania wziąć pod uwagę zgodę podmiotu danych. Wydaje się, że bez względu czy będzie miała zastosowanie zgoda w rozumieniu RODO czy „rezygnacja z prawa do prywatności" w rozumieniu art. 6 ust. 2 UPW - podstawa te będzie miała mniejsze znaczenie praktyczne, aczkolwiek wciąż *de lege lata* możliwe.

Praktyczna różnica pomiędzy omówionymi przesłankami przetwarzania danych, o których mowa w art. 6 ust. 1 lit. a, c, e i f RODO - z perspektywy osób, których dane są przetwarzane – jest taka, że w przypadku przetwarzania danych osobowych w oparciu o art. 6 ust. 1 lit. c podmiotowi danych nie przysługuje prawo sprzeciwu. Prawo sprzeciwu z kolei przysługiwać będzie w przypadku oparcia przetwarzania danych na art. 6 ust. 1 lit. e i f. Z kolei przypadku oparcia przetwarzania o zgodę, osoba może w każdym momencie ją wycofać.

Rozdział 8. Zmiana celu przetwarzania danych osobowych a ponowne wykorzystywanie informacji sektora publicznego

Ponowne wykorzystywanie informacji sektora publicznego z samej definicji oznacza zmianę pierwotnego celu dla, którego dane zostały zebrane. Skuteczne zastosowanie zasady celowości w przypadku ponownego wykorzystywania stanowi znaczące wyzwanie. Z jednej strony sama koncepcja i siła napędowa innowacyjności stojąca za pojęciem „otwartych danych" i ponownym wykorzystywaniem informacji sprowadza się do tego, aby dane mogłyby być szeroko dostępne dla ich użycia w nowych, innowacyjnych produktach i usługach, a tym samym w celach, które nie zostały wcześniej określone i nie sposób ich wyraźne przewidzieć. Dyrektywy o ponownym wykorzystywaniu również wymagają takiego określenia warunków licencjonowania informacji, które niepotrzebnie nie ograniczają ponownego wykorzystania danych[832].

Z drugiej strony, zasada celowości jest kluczową zasadą ochrony danych, wymagającą, by dane osobowe, które zgromadzono do konkretnego celu, nie zostały następnie wykorzystane do innego celu niezgodnego z celem pierwotnym. Zasada ta ma również zastosowanie do

[832] *Grupa Robocza Art. 29*, Opinia 06/2013, s. 38.

danych osobowych, które są publicznie dostępne. Sam fakt, że dane osobowe są publicznie dostępne w konkretnym celu, nie oznacza, iż takie dane osobowe są otwarte do ponownego wykorzystania w jakimkolwiek innym celu[833].

Grupa Robocza Art. 29 zaleca, by przepisy przewidujące publiczny dostęp do danych, jasno określały cele udostępniania danych osobowych. Jeżeli tak się nie stanie albo cele te będą określone w sposób nieprecyzyjny i szeroki, ucierpi na tym pewność i przewidywalność prawa. W szczególności w odniesieniu do każdego wniosku o ponowne wykorzystanie danych organowi sektora publicznego i potencjalnym ponownym użytkownikom będzie bardzo trudno ustalić, jakie były zamierzone pierwotne cele upublicznienia, a tym samym, jakie dalsze cele byłyby zgodne z tymi pierwotnymi celami. Jak już wspomniano, nawet jeżeli dane osobowe zostały opublikowane w Internecie, nie należy zakładać, że można je dalej przetwarzać w jakichkolwiek możliwych celach[834].

Zgodnie z art. 6 ust. 4 RODO możliwa jest zmiana celu przetwarzania danych osobowych względem celu, w którym dane osobowe zostały pierwotnie zebrane. Zmiana celu – w myśl omawianego przepisu – może mieć swoją podstawę w zgodzie osoby, której dane dotyczą lub w przepisach prawa Unii lub prawa członkowskiego. Jednocześnie – jak stanowi art. 6 ust.4 RODO – przepisy prawa krajowego lub prawa Unii muszą stanowić niezbędny i proporcjonalny środek w demokratycznym społeczeństwie, który służy zagwarantowaniu celów, o których mowa w art. 23 ust. 1 RODO. Państwa członkowskie nie mają zatem pełnej swobody w kreowaniu przepisów zmieniających cele przetwarzania danych osobowych, a każdy przypadek przyjęcia takiej regulacji musi być oceniany z puntu widzenia dopuszczalności ograniczania prawa i obowiązków wynikających z RODO[835]. Cele wymienione w art. 23 ust. 1 obejmują bezpieczeństwo narodowe, obronę, bezpieczeństwo publiczne, zapobieganie przestępczości i prowadzenie postępowań, ogólny interes publiczny UE lub państwa członkowskiego, ochronę niezależności sądów i postępowania sądowego, zapobiegania naruszeniom etyki w zawodach regulowanych, funkcjom kontrolnym, inspekcyjnym lub regulacyjnym, ochronie osoby, której dane dotyczą, lub praw i wolności innych osób czy egzekucji roszczeń cywilnoprawnych. W związku z powyższym przepisy prawa o ponownym wykorzystywaniu informacji sektora publicznego *in genere* nie mogą stanowić samodzielnie podstawy prawnej zmiany celu przetwarzania danych, ponieważ nie mogą być uznane za niezbędny i proporcjonalny środek służący w demokratycznym

[833] *Ibidem.*
[834] *Ibidem*, s. 23.
[835] *P. Litwiński (red.)*, op. cit., Komentarz do art. 6, pkt.

społeczeństwie zagwarantowaniu celów, o których mowa w art. 23 ust. 1 RODO. Katalog celów (wartości) wymieniony w art. 23 ust. 1 ma charakter zamknięty

Co do zasady przetwarzanie danych osobowych w celu niezgodnym z pierwotnym celem zebrania danych jest zawsze niedopuszczalne. Nie oznacza to jednak samo w sobie zakazu przetwarzania danych osobowych w celu innym, niż cel pierwotny[836]. W sytuacji, w której ani przepis prawa UE ani prawa krajowego, jak i zgoda osoby, której dane dotyczą, nie przewidują wprost zmiany celu przetwarzania danych w stosunku do celu pierwotnego, konieczne jest zbadanie czy istnieje zgodność miedzy tym pierwotnym celem zebrania danych a nowymi celami (test zgodności). Służą temu przesłanki dopuszczalności zmiany celu wymienione w art. 6 ust. 4 RODO. Taka sytuacja może mieć miejsce w ramach realizacji prawa do ponownego wykorzystywania informacji sektora publicznego zawierającej dane osobowe.

A contrario, jeżeli osoba, której dane dotyczą, wyraziła zgodę lub jeżeli przetwarzanie ma podstawę w prawie UE lub w prawie państwa członkowskiego stanowiącego w demokratycznym społeczeństwie niezbędny i proporcjonalny środek, który zapewnia w szczególności realizację ważnych celów leżących w ogólnym interesie publicznym, administrator może dokonać dalszego przetwarzania bez względu na jego zgodność z pierwotnymi celami[837].

Należy zauważyć, że przepis art. 6 ust. 4 nie stanowi nowej przesłanki legalizującej przetwarzanie danych osobowych, która uzupełniałaby katalog wymieniony w ust. 1 tego artykułu[838]. Jak słusznie zauważa *W. Chomiczewski,* gdyby art. 6 ust. 4 miałby pełnić funkcję przesłanki legalizującej przetwarzanie, wówczas znalazłby się w przepisie ust. 1[839]. Dlatego też art. 6 ust. 4 służy zbadaniu czy w ogóle dopuszczalna jest zmiana celu przetwarzania danych osobowych. Natomiast, żeby w ogóle do takiego przetwarzania w nowym celu mogło dojść, konieczne jest spełnienie jednej z przesłanek legalizujących przetwarzanie danych, o których mowa w art. 6 ust. 1 RODO[840].

Jak wskazano w Rozdziale 5.1.4., zgodnie z zasadą wyrażoną w art. 5 ust. 1 lit. b), dane osobowe można zbierać w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie

[836] Zob. *Grupa Robocza Art. 29*, Opinia 03/2013, s. 21. Opinia choć wydana w nieobowiązującym już stanie prawnym pozostaje w znacznej mierze aktualna po wejściu w życie RODO, merytoryczna treść zasady celowości nie uległa bowiem zmianie
[837] Zob. motyw 50 preambuły RODO.
[838] *W. Chomiczewski,* Komentarz do art. 6 ust. 4, s. 404.
[839] *Ibidem.*
[840] *Ibidem.*.

można przetwarzać niezgodnie z tymi celami. Z tego powodu art. 6 ust. 4 należy uznać za wyjątek od ogólnej zasady ograniczenia celu[841].

8.2. Test zgodności

Przeprowadzenie testu zgodności celu pierwotnego zebrania danych z celem nowym przetwarzania danych osobowych będzie konieczne w przypadku braku zgody podmiotu danych i braku podstawy prawnej wyrażonej przepisami prawa UE lub prawa krajowego. Zgodnie z wytycznymi Grupy roboczej art. 29 administrator danych podejmując decyzje o zmianie celów, może kierować się albo ściśle formalnymi kryteriami (*formal assessment)*, bazując na informacji przekazanej osobie, której dane dotyczą, albo oceniać także kwestie merytoryczne (*substantive assessment*), takie jak sposób rozumienia informacji o celu przetwarzania danych przez osobę, której dane dotyczą, czy kontekst przetwarzania[842]. Należy zwrócić uwagę, że zgodność dalszego przetwarzania danych z celem pierwotnym ich zebrania, nie wymaga aby te nowe, dodatkowe cele przetwarzania stanowiły swojego rodzaju „podcele" (*sub-purpose*) celu pierwotnego. Zgodność celów zaistnieje nawet wtedy, kiedy nowy cel jest inny od pierwotnego, ale jest z nim skorelowany w sensie kontekstowym, czasowym lub logicznym[843].

Badanie zgodności celów powinno zostać przeprowadzone przez administratora w oparciu o wymienione w art. 6 ust. 4 kryteria. Administrator, aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem, w którym dane osobowe zostały pierwotnie zebrane, bierze pod uwagę między innymi:

a) wszelkie związki między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania;

b) kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem;

c) charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10;

d) ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą;

---

[841] *Ibidem*, s. 405.
[842] *Grupa Robocza Art. 29*, op. cit.
[843] *W. Kotschy* Commentary on art. 6 (4) of the General Data Protection Regulation [w:] *L. Bygrave, C. Kuner, C. Docksey* (red.), Commentary on the EU General Data Protection Regulation, s. 341.

e) istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji.

Należy zwrócić uwagę, że prawodawca unijny formułując przepis posłużyć się zwrotem „(administrator) bierze pod uwagę między innymi", otworzył przedmiotowy katalog kryteriów, przesądzając jednocześnie, że ma on jedynie charakter przykładowy. Oznacza to, że w toku oceny na gruncie konkretnego stanu faktycznego, administrator może wziąć pod uwagę również inne kryteria oceny zgodności celów, niż te wymienione w lit. a) -e)[844].

Kryteria wymienione w art. 6 ust. 4 RODO co do zasady opierają się na rekomendacjach Grupy Roboczej Art. 29 zawartych w Opinii 03/2013, a następnie powtórzonych w Opinii 06/2013. Jedyną nową przesłanką dodaną przez unijnego prawodawcę stanowi kryterium wymienione w lit. d) dotyczące konieczności wzięcia pod uwagę potencjalnych konsekwencji dalszego przetwarzania dla podmiotów danych.

Zgodnie z art. 6 ust. 4 lit. a) administrator, aby ustalić, czy przetwarzanie w innym celu jest zgodne z celem pierwotnym bierze pod uwagę, wszelkie związki między celami, w których zebrano dane osobowe, z celami dalszego przetwarzania. Badanie związków między celami, w których zebrano dane osobowe, a celami zamierzonego dalszego przetwarzania nie powinno być sprowadzane do warstwy językowej. Należy uwzględnić sytuacje, gdy pierwotny cel przetwarzania zawierał już w sobie zamierzone nowe cele (dalsze przetwarzanie było „dorozumiane" w celu pierwotnym) oraz czy przetwarzanie danych osobowych w nowym celu jest logiczną konsekwencją wcześniejszego przetwarzania ich w celu, w jakim zostały zebrane[845]. W pewnych sytuacjach można uznać, że nowe cele niejako domyślnie mieszczą się w zakresie pierwotnego celu lub są naturalną konsekwencją celu pierwotnego, czy też można zidentyfikować między nimi związek. Przy czym im ten związek jest mniejszy, tym mniejsze prawdopodobieństwo stwierdzenia zgodności pomiędzy tymi celami[846].

W myśl art. 6 ust. 4 lit. b) administrator powinien wziąć pod uwagę kontekst, w którym zebrano dane osobowe, w szczególności relację między osobami, których dane dotyczą, a administratorem. Należy zatem wziąć pod rozwagę to, czy osoba, której dane dotyczą, spodziewałaby się, że jej dane zostaną wykorzystane w oparciu o kontekst gromadzenia danych[847]. W myśl motywu 50 preambuły RODO, administrator powinien uwzględnić rozsądne przesłanki pozwalające osobom, których dane dotyczą, oczekiwać, że dalsze wykorzystanie

[844] *W. Chomiczewski* op. cit.,, s. 404.
[845] *Grupa Robocza Art. 29,* op. cit., s. 24.
[846] *P. Drobek,* Zasada celowości, s. 24.
[847] *Grupa Robocza Art. 29,* op. cit..

danych będzie oparte na rodzaju ich powiązaniu z administratorem. Istotny jest zatem rodzaj relacji łączących administratora z podmiotem danych. Ocena charakteru tego związku powinna również obejmować badanie równowagi sił między osobą, której dane dotyczą, a administratorem danych. W szczególności należy rozważyć, czy podmiot danych był zobowiązany do przekazania danych zgodnie z przepisami prawa. W przypadku gromadzenia danych na podstawie umowy, należy zbadać charakter umowy i równowagę pozycji między osobą, której dane dotyczą, a administratorem danych (na przykład, jak łatwo osoba, której dane dotyczą, mogła rozwiązać umowę i szukać alternatywnego usługodawcy). Jeśli dalsze przetwarzanie opierało się na zgodzie, należy ocenić, w jakim zakresie zgoda została udzielona swobodnie i na podstawie precyzji jej warunków[848]. Bez względu na źródło tych relacji, należy uwzględnić uzasadnione oczekiwania podmiotu danych co do zachowania ściślejszej poufności czy surowszych ograniczeń dalszego przetwarzania danych osobowych.

Kolejne kryteria wymienione w lit. c – e sprowadzają się do konieczności rozważenia dodatkowego ryzyka dalszego przetwarzania dla podmiotu danych. Oznacza to, że badanie zgodności celów obejmuje także przeprowadzanie oceny ryzyka zamierzonych czynności przetwarzania. Dalsze cele przetwarzania nie mogą powodować istotnie wyższego ryzyka od przetwarzania w celach pierwotnych, jeśli mają być uznane za zgodne [849].

Kryterium wymienionym w art. 6 ust. 4 lit. c jest charakter danych osobowych, w szczególności czy przetwarzane są szczególne kategorie danych osobowych zgodnie z art. 9 lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa zgodnie z art. 10. Przesłanka ta nie będzie miała znaczenia dla badania zgodności celów w związku z ponownym wykorzystywaniem informacji sektora publicznego. Jak wykazano bowiem wcześniej, ponowne wykorzystywanie – co do zasady – nie obejmuje danych osobowych „wrażliwych." Niemniej uwzględniając przedmiotowe kryterium – bez względu czy chodzi o szczególne kategorie danych – istotny wpływ może mieć sposób dalszego przetwarzania danych, np. czy dane są przetwarzane przez innego administratora w innym kontekście z nieznanymi konsekwencjami, czy dane są ujawniane publicznie lub w inny sposób udostępniane dużej liczbie osób lub czy duże ilości danych osobowych są przetwarzane lub łączone z innymi danymi (np. w przypadku profilowania, w celach komercyjnych, w celu egzekwowania prawa lub w innych celach), szczególnie jeśli takich operacji nie można było przewidzieć w momencie ich gromadzenia[850].

[848] *Ibidem.*
[849] *W. Kotschy,* op.cit., s. 342.
[850] *Ibidem,* s. 26.

Administrator następnie bierze pod uwagę – zgodnie z art. 6 ust. 4 lit. d) – ewentualne konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą. Oczywiście należy rozważyć konsekwencje negatywne dla podmiotu danych uzasadniające brak zgodności celów, jak i skutki pozytywne przeważające za uznaniem celów jako zgodnych.

Ostatnim wymienionym w art. 6 ust. 4 lit. e) kryterium jest istnienie odpowiednich zabezpieczeń, w tym ewentualnie szyfrowania lub pseudonimizacji. Wydaje się zatem, że kryterium to ma znaczenie wówczas, gdy uznano dopuszczalność przetwarzania danych w nowym celu. Wówczas administrator danych stosuje odpowiednie środki zabezpieczania danych. Pseudonimizacja – zgodnie z art. 4 pkt 4 RODO – oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, 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. Dane poddane pseudonimizacji wciąż mogą być poddane ochronie przepisów RODO w przeciwieństwie do danych zanonimizowanych.

Podsumowując powyższe kryteria, należy zaznaczyć, że nie są one przesłankami decydującymi o istnieniu zgodności celów. Jeśli na gruncie jednego lub więcej kryteriów przeważa wniosek o występowaniu zgodności między celami, to negatywna ocena pozostałych kryteriów może przesądzić o braku zgodności celów[851]. Po drugie, z uwagi na otwarty katalog kryteriów wymieniony w art. 6 ust. 4 administrator powinien wziąć pod uwagę wszelkie inne okoliczności w danym stanie faktycznym.

8.3. Test zgodności a realizacja prawa do ponownego wykorzystywanie informacji sektora publicznego

8.3.1. Obowiązek przeprowadzania testu zgodności

Aby rozwiązać dylemat wpływu omawianej zasady na możliwość ponownego wykorzystywania informacji zawierającej dane osobowe, w pierwszej kolejności trzeba jednak odpowiedzieć na pytanie czy przeprowadzenie testu zgodności w związku z ponownym wykorzystywaniem jest zawsze obligatoryjne.

[851] *W. Chomiczewski*, op. cit., s. 406.

Jak ustalono powyżej, badania zgodności celów nie przeprowadza się w przypadku przetwarzania danych w innym celu niż cel w którym zebrano pierwotnie dane w oparciu o zgodę osoby, której dane dotyczą oraz wyraźną podstawę prawną.

W pierwszym przypadku przyjęto, że za zgodę w rozumieniu RODO można uznać „rezygnację z prawa do prywatności" na gruncie UPW. „Rezygnacja" osoby, której dane dotyczą musi zatem obejmować zmianę celu, dla którego pierwotnie zebrano jej dane osobowe. Pojawia się zatem wątpliwość o określenie tego następczego celu ponownego wykorzystywania danych osobowych. Podmiot danych musi być poinformowany o tym, że jego dane osobowe będą przetwarzane w ramach ponownego wykorzystywania informacji sektora publicznego oraz musi poznać cel ponownego wykorzystywania, który jak wynika z definicji, może być dowolny (komercyjny lub niekomercyjny). Wydaje się, że w praktyce wymóg ten nie będzie mógł zostać zrealizowany. Po pierwsze, w mojej opinii nie jest prawnie dozwolone blankietowe zbierania „rezygnacji z prawa do prywatności" przez podmiot zobowiązany od osób, których dane dotyczą niejako na wypadek możliwości ponownego wykorzystywania jego danych osobowych w ramach informacji sektora publicznego. Wynika to również z istoty przesłanki zgody, w której mowa w art. 6 ust. 1 lit. a RODO. Prawidłowe wyrażenie zgody na przetwarzanie danych osobowych wymaga wskazania celu lub celów przetwarzania. Konkretyzacja celu jest nie tylko warunkiem zgody, ale przede wszystkim realizacją sformułowanej art. 5 ust. 1 lit. b zasady związania celem. Zatem, o ile hipotetycznie można założyć, że podmiot zobowiązany będzie informował podmiot danych na etapie pozyskiwania (zbierania danych), o tym, że jego dane mogą następnie zostać przekazana lub udostępnione do ponownego wykorzystywania, jednakże taka zgoda obejmowałaby jedynie wtórny (inny) cel po stronie podmiotu zobowiązanego. Nie jest jedocześnie możliwe z góry określenie możliwych celów przyszłego ponownego wykorzystywania przez każdego potencjalnego użytkownika. Po drugie, jedynie w przypadku ponownego wykorzystywania w trybie wnioskowym podmiot zobowiązany zna cel następczego wykorzystywania danych. Zgodnie bowiem z art. 21 ust. 3 pkt 4 UPW wnioskodawca jest zobowiązany do wskazania celu ponownego wykorzystywania (komercyjny albo niekomercyjny), w tym określenie rodzaju działalności, w której informacje sektora publicznego będą ponownie wykorzystywane, w szczególności wskazanie dóbr, produktów lub usług. Niemniej w tym wypadku podmiot zobowiązany, który rozpatruje wniosek o ponowne wykorzystywanie informacji sektora publicznego zawierającej dane osobowe musiałby wystąpić do podmiotu danych o rezygnację z prawa do prywatności, czyli zgodę na przetwarzanie jego danych osobowych w tym następczym celu wskazanym przez wnioskodawcę. Z tego też powodu, przesłanka zgody na

przetwarzanie danych osobowych w kontekście zwolnienia z konieczności przeprowadzania testu zgodności celu nie będzie miała zastosowania.

Należy zatem rozstrzygnąć drugą przesłankę, czyli brak wymogu przeprowadzania testu zgodności celów ze względu na przepis prawa. Na gruncie przepisów UPW *per analogiam* można przyjąć stanowisko prezentowane w literaturze dotyczące udostępniania danych osobowych podmiotom uprawnionym, nie doznaje ono ograniczenia w postaci stosowania zasady związania celem przetwarzania danych osobowych „dane mogą być udostępniane podmiotom, które dysponują stosowną podstawą prawną do swojego żądania także wtedy, gdy następujące w wyniku udostępnienia przetwarzanie danych odbywać się będzie w celu niezgodnym z celem, dla którego dane zostały zebrane. W przeciwnym bowiem razie dochodziłoby do praktycznego zniweczenia obowiązku udostępniania danych osobowych podmiotom uprawnionym do ich otrzymania"[852]. W tym kontekście zasadne wydaje się przyjęcie, że w przypadku przetwarzania danych osobowych osób pełniących funkcje publiczne pozostających w związku z ich pełnieniem (art. 6 ust. 1 lit. c RODO w zw. z art. 6 ust. 2 UPW). stanowi podstawę (zawartą w prawie krajowym) zmiany celu przetwarzania danych[853]. Przyjęcie odmiennej interpretacji podważyłoby sens wprowadzenia w przepisach UPW przesłanki ograniczającej prawo do prywatności.

8.3.2. Podmiot obowiązany do przeprowadzenia testu zgodności

Przeprowadzenie testu zgodności powinno poprzedzać ujawnienie danych osobowych w ramach informacji sektora publicznego w oparciu o art. 6 ust. 1 lit. e i f RODO. Trzeba zatem odpowiedzieć na pytania, który podmiot w ramach ponownego wykorzystywania informacji zawierającej dane osobowe jest obowiązany do przeprowadzenia testu zgodności i na jakim etapie.

Grupa Robocza Art. 29 wskazywała, że ocena zgodności celu ujawnienia danych do ponownego wykorzystywania oraz pierwotnego celu ich zebrania należy zarówno do podmiotu ujawniający informację, jak i użytkownika, który ma te dane wykorzystywać. Przeanalizujmy obydwa scenariusze.

Niewątpliwie na etapie podjęcia decyzji o ujawnieniu danych osobowych z własnej inicjatywy (np. na publicznie dostępnej stronie internetowej) czy na wniosek zainteresowanego użytkownika podmiot zobowiązany – jednocześnie administrator danych osobowych –

[852] *P. Litwiński (red.)*, op. cit., Komentarz do art. 6, pkt 22.
[853] *M. Gumularz*, Ekspertyza, teza 121, s. 42.

dokonuje oceny zgodności celu ujawnienia danych w ramach informacji sektora publicznego w celu ponownego wykorzystywania i pierwotnego celu ich zebrania. Innymi słowy konieczne jest uwzględnienie pierwotnego celu zebrania danych oraz cel ujawnienia (cel podmiotu zobowiązanego na gruncie UPW). Weryfikację celów może przeprowadzić w ramach oceny skutków dla ochrony danych osobowych, o której mowa w art. 35 RODO. Należy zauważyć, że w pierwszym wypadku ocena potencjalnych celów ponownego wykorzystywania leży po stronie podmiotu zobowiązanego, które jak pamiętamy mogą być dowolne. Musi on zatem niejako antycypować *in abstracto* potencjalne wtórne cele przetwarzania ujawnianych danych osobowych, pamiętając, że po opublikowaniu danych osobowych w otwartym systemie teleinformatycznym traci kontrolę nad ich przetwarzaniem. Może w tym wypadku określić – na podstawie art. 14 ust. 1 pkt 4) UPW – z góry warunki ponownego wykorzystywania informacji sektora publicznego zawierającej dane osobowe, które uznaje za zgodnie z pierwotnym celem ich zebrania (szerzej na ten temat zob. Rozdział 9). W drugim wypadku – przekazując informacje na wniosek – podmiot zobowiązany *in concreto* rozstrzyga możliwość przetwarzania danych osobowych w ramach informacji sektora publicznego w celu wskazanym we wniosku zainteresowanego użytkownika (zgodnie z art. 21 ust. 3 pkt 4), zatem dokonuje testu zgodności celu pierwotnego ze wskazanym przez wnioskodawcę celu ponownego wykorzystywania.

Bardziej problematycznym zagadnieniem jest konieczność dokonywania badania zgodności celów przez użytkownika. Użytkownik, który uzyskał dane osobowe w ramach realizacji wniosku o ponowne wykorzystywanie, co do zasady nie dokonuje testu zgodności. Jak wskazano obowiązek ten leży po stronie podmiotu zobowiązanego. W mojej opinii podmiot zobowiązany powinien określić możliwe cele ponownego wykorzystywania w warunkach, choć *de lege lata* jest to rozwiązane fakultatywne. Użytkownik zaś musi wskazać we wniosku cel ponownego wykorzystywania (w tym wypadku cel przetwarzania danych osobowych w ramach ISP), w tym określić rodzaj działalności, w której informacje sektora publicznego będą ponownie wykorzystywane, w szczególności wskazać dobra, produkty lub usługi. W oparciu o cel wskazany we wniosku podmiot zobowiązany powinien dokonać testu zgodności celów przed przekazaniem informacji sektora publicznego.

Drugą sytuacją, w której użytkownik nie będzie musiał dokonywać testu zgodności celów, jest udostępnienie w BIP, CRIP lub w inny sposób do ponownego wykorzystywania informacji sektora publicznego zawierających dane osobowe z jednoczesnym określeniem przez podmiot zobowiązany warunków ponownego wykorzystywania, w tym wskazanie dopuszczalnych celów przetwarzania takich danych. W tym wypadku, użytkownik z góry zna

dopuszczalne następcze cele przetwarzania danych osobowych. Jeżeli użytkownik chciałby jednak wykorzystać dane osobowe w innym celu, wówczas – zgodnie z art. 21 ust. 1 pkt 3 UPW – powinien wnieść wniosek o określenie innych niż pierwotnie dopuszczono warunków ponownego wykorzystywania. Podmiot zobowiązany rozpatrując taki wniosek będzie zatem obowiązany do dokonania oceny zgodności celu pierwotnego zebrania danych z wtórnym celem wskazanym we wniosku w tym trybie. W przypadku, gdy test zgodności da odpowiedź negatywną, podmiot zobowiązany odmawia zgody na ponowne wykorzystywanie danych osobowych na warunkach (obejmujących cel przetwarzania wskazanych we wniosku) żądanych przez wnioskodawcę. Pojawia się tutaj ciekawe zagadnienie proceduralne o formę załatwienia sprawy. Rozpatrywać w tym wypadku można zwykłe poinformowanie wnioskodawcy lub rozstrzygnięcie sprawy w drodze decyzji. Wydaje się jednak, że odmowa powinna nastąpić w drodze decyzji, podstawą do jej wydania stanowiłby art. 23 ust. 4 pkt 3 UPW.

Sytuacja komplikuje się, gdy użytkownik zamierza wykorzystywać dane osobowe z powszechnie dostępnych źródeł takich, jak strony internetowe podmiotów publicznych, dla których podmiot zobowiązany w ogóle nie określił warunków ponownego wykorzystywania (przetwarzania danych osobowych). W tym wypadku na gruncie przepisów UPW należy rozgraniczyć dwie sytuacje – w zależności od źródła pozyskania danych – na strony podmiotowe BIP oraz centralne repozytorium informacji publicznej oraz pozostałe systemy teleinformatyczne (jak np. rejestry publiczne czy strony informacyjne urzędów).

W pierwszej sytuacji mamy do czynienia z domyślną akceptacją ponownego wykorzystywanie informacji sektora publicznego bez konieczności spełnienia jakichkolwiek warunków, gdy tych warunków nie określono. Zgodnie bowiem z art. 11 ust. 4 brak informacji o warunkach ponownego wykorzystywania informacji sektora publicznego udostępnionych w BIP lub w centralnym repozytorium uważa się za udostępnienie informacji sektora publicznego w celu ponownego wykorzystywania bez warunków. Oznacza to, że użytkownik bez konieczności wystąpienia z wnioskiem o ustalenie warunków może dowolnie wykorzystywać informacje dostępne na stronach BIP oraz portalu otwartych danych, jeśli warunków ponownego wykorzystywania w ogóle nie określono. Co to oznacza dla możliwości wykorzystywania danych osobowych udostępnianych na tych portalach, np. danych osobowych osób pełniących funkcje publiczne?

W mojej opinii należy przyjąć, że publikacja danych osobowych w BIP lub portalu otwartych danych oznacza dopuszczalność ich przetwarzania w ramach ponownego wykorzystywania, odbywa się bowiem na konkretnej podstawie prawnej (Zob. Rozdział 7).

Przepisy jednocześnie *expressis verbis* stanowią, że tak opublikowane dane bez wskazania jakichkolwiek warunków mogą być dowolnie wykorzystywane. Czy udostępnienie informacji sektora publicznego w celu ponownego wykorzystywania bez warunków oznacza również brak konieczności spełnienia zasad przetwarzania danych osobowych wynikających z RODO? Niewątpliwie nie. Prowadzi to zatem do konkluzji, że pomimo zasady domniemanej dopuszczalności ponownego wykorzystywania wyrażonej w art. 11 ust. 4 UPW, użytkownik pozyskując dane osobowe z tych źródeł powinien samodzielnie dokonać testu zgodności pierwotnego celu opublikowania danych na stronie BIP lub w centralnym repozytorium z następczym celem użycia danych, np. w budowie aplikacji na urządzenia mobilne czy wykorzystania w serwisie internetowym. W praktyce może się to okazać niemożliwe do zrealizowania, ponieważ brak określenia warunków ponownego wykorzystywania danych osobowych dostępnych w tych serwisach, powoduje, że użytkownik może mieć trudności z ustaleniem nawet pierwotnego celu ujawnienia tych danych przez podmiot zobowiązany, w oparciu o który samodzielnie ma ocenić dopuszczalność przetwarzania w następczym celu przez niego zdefiniowanym. Postulowanym rozwiązaniem – podnoszonym zresztą przez Grupę Roboczą art. 29 – jest to, aby użytkownicy z góry znali warunki przetwarzania danych osobowych[854]. Skoro zatem użytkownik ma uwzględnić pierwotny cel zebrania danych[855], minimalnym warunkiem jaki powinien określić podmiot zobowiązany, powinno być poinformowanie odbiorcy danych (użytkownika) o pierwotnym celu zebrania danych, dzięki czemu użytkownik będzie mógł ocenić zgodność zamierzonego wykorzystania danych z tym celem[856]. W przeciwnym razie, konieczne będzie wystąpienie z wnioskiem o ustalenie warunków ponownego wykorzystywania obejmujących zasady przetwarzania danych osobowych, co powoduje, że zasada „domniemanej zgody" w rozumieniu art. 11 ust. 4 UPW staje się bezprzedmiotowa w odniesieniu do informacji sektora publicznego zawierających dane osobowe.

Inaczej wygląda sytuacja użytkownika pozyskującego dane osobowe z innych publicznie dostępnych źródeł. W tym wypadku, gdy podmiot zobowiązany prowadzący dany system teleinformatyczny, nie określił warunków ponownego wykorzystywania danych osobowych nie obowiązuje zasada „domniemanej zgody" na ponowne wykorzystywanie bez spełnienia jakichkolwiek warunków. W tym wypadku – zgodnie z art. 21 ust. 1 pkt 2 UPW – użytkownik powinien wystąpić z wnioskiem o określenie zasad przetwarzania danych

[854] *Grupa Robocza Art. 29*, Opinia 6/2013, s. 10.
[855] Zob. *J. Andraško, M. Mesarčík*, Quo Vadis Open Data? s. 200.
[856] Podobnie *M. Gumularz*, Ekspertyza, teza 121, s. 42.

osobowych. W tym miejscu należy nadmienić, że większość rejestrów państwowych zawierających dane osobowe, np. KRS czy CEIDG w ogóle nie przewiduje warunków wykorzystywania danych. Oznacza to, że zgodnie z przepisami UPW każde wtórne użycie danych, np. serwisach czy aplikacjach, powinno być poprzedzone uzyskaniem warunków ponownego wykorzystywania danych. Także w tym wypadku, optymalnym rozwiązaniem byłoby określenie z góry warunków ponownego wykorzystywania obejmujących zasady przetwarzania danych osobowych.

Podsumowując, weryfikacja zgodności celów przetwarzania danych dotyczyć będzie innych przypadków niż wskazane w art. 6 ust. 2 UPW („rezygnacja z prawa do prywatności" oraz dane osób pełniących funkcje publiczne). W pozostałych okolicznościach negatywny wynik testu zgodności celów może prowadzić do konieczności przeprowadzenia anonimizacji całości lub części danych osobowych zawartych w informacji sektora publicznego, których ujawnienie do ponownego wykorzystania byłoby niezgodne z pierwotnym celem zebrania danych. Przeprowadzenie testu zgodności celów nie byłoby konieczne, gdyby UPW lub przepisy szczególne wprost dopuszczały możliwość przetwarzania wskazanych kategorii danych osobowych w ramach UPW. Przyjęcie, że podmiot zobowiązany nie musi przeprowadzać testu zgodności celów, nie oznacza, że użytkownik jest także zwolniony z tego obowiązku.

8.3.3. Dopuszczalne cele ponownego wykorzystywania danych osobowych

Kolejnym dylematem, jaki należy rozstrzygnąć, jest weryfikacja celów ponownego wykorzystywania pod kątem ich zgodności z celem pierwotnym, w którym dane zostały zebrane. Inaczej ujmując, należy odpowiedzieć na pytanie jakie potencjalne następcze cele użycia danych osobowych można uznać za zgodne z zasadą celowości. Pytanie to w istocie dotyka fundamentalnego zagadnienia, czy w ogóle możliwe jest ponowne wykorzystywanie danych osobowych, które spełniałaby wymogi określone w art. 6 ust. 4 RODO?

Sformułowany w art. 6 ust. 4 RODO test dla weryfikacji zgodności pierwotnego celu przetwarzania danych osobowych z potencjalnym zamierzonym innym celem ich przetwarzania w kontekście ponownego wykorzystywania może okazać się w praktyce stosowania przepisów trudny do zrealizowania. Istota ponownego wykorzystywania, czy

szerzej polityki otwartych danych polega na dowolności celów dalszego korzystania z danych[857].

Doktryna dotychczas skupiała się przede wszystkim na kontekście jawności czy przejrzystości dla których dane osobowe mogą być ujawniane do ponownego wykorzystywania[858]. Podnosi się, że jeżeli dane osobowe zostały pierwotnie zebrane w celu wspierania przejrzystości, mogą być następne publikowane w tym samym celu. Należy wówczas wziąć pod uwagę wpływ na prawa i wolności jednostek, co w konsekwencji może skutkować ograniczeniami (np. zakresu) publikacji danych osobowych przez organy publiczne[859]. Autorzy sami przyznają, że przeprowadzenie testu zgodności celów nie stanowi całkowicie odpowiedniego instrumentu dla zbadania podstawy prawnej dla przetwarzania danych osobowych w związku z ponownym wykorzystywaniem. Jako przykład podają działalność organizacji pozarządowych występujących w roli *watchdoga* wobec administracji publicznej, które przetwarzają publicznie dostępne dane osobowe[860].

Nawet tak wąsko sformułowany cel ponownego wykorzystywania danych osobowych związany z jawnością życia publiczne może nie być uznany za jednoznacznie zgodny z zasadą celowości. Zdanie Grupy Roboczej Art. 29 przykładowo wydatki urzędników państwowych wyższego szczebla są udostępniane w Internecie w celu zapewnienia przejrzystości, ale umożliwienie ponownego wykorzystania takich danych przez któregokolwiek członka społeczeństwa do innych celów może być niezgodne z zasadą celowości[861]"

W mojej opinii jest to zawężające podejście, redukujące instytucję ponownego wykorzystywania do instrumentu służącemu przede wszystkim zapewnianiu transparentności życia publicznego, a jego istota jest zgoła inna. Jak wskazano na wstępie rozprawy, ma ona wymiar przede wszystkim gospodarczy i jej podstawowym celem jest stymulacja rynku europejskiego opartego o dane. Szczególności obecnie w dobie rozwoju Internetu rzeczy i sztucznej inteligencji, instytucja ponownego wykorzystywania pełni rolę ważnego ogniwa w łańcuchu budowy usług społeczeństwa informacyjnego.

Również na gruncie problematyki *big data* w literaturze przedmiotu zwraca się uwagę na problem pogodzenia zasady ograniczonego celu z przetwarzaniem danych osobowych zgromadzonych w wielkich zestawach danych. Z jednej strony dostrzegając rolę przetwarzania

[857] Zob. *LAPSI 2.0 Thematic Network*, Position paper access to data, 2014, s. 11.
[858] Por. J. *Andraško, M. Mesarčík*, Quo Vadis Open Data?, s. 199: „Głównym celem otwartych danych jest zapewnienie i promocja przejrzystość w administracji publicznej i zwiększenie partycypacji obywateli w kontekście spraw publicznych."
[859] *Ibidem*,s. 197.
[860] *Ibidem*, s. 203.
[861] *Grupa Robocza Art. 29*, Opinia 06/2013, s. 20.

tego rodzaju danych dla współczesnej gospodarki przewiduje się koniec zasady celowości czy zapowiada się jej erozję, z drugiej podkreśla fundamentalną rolę zasady w procesie przetwarzania danych[862].

Dorobek doktryny nie pomaga zatem w udzieleniu odpowiedzi na pytanie, jakie inne ponowne (wtórne) cele wykorzystywania danych osobowych mogłyby zostać uznane za zgodne z pierwotnym celem, dla którego zostały zebrane.

Zasada ograniczenia celu była przedmiotem - przywoływanej już - opinii Grupy Roboczej art. 29[863]. Przyjmując za punkt wyjścia treść zasady wyrażonej w art. 6 ust. 1 lit. b dyrektywy 95/46/WE (a w obecnym stanie prawnym ar. 5 ust. 1 lit. b RODO) kluczowym pozostaje odpowiedzenie na pytanie, jakie potencjalne cele ponownego wykorzystywania mogą zostać uznane za przetwarzane w konkretnych, wyraźnych i prawnie uzasadnionych celach.

Jak wskazano wcześniej określenie celów i sposobu przetwarzania danych osobowych należy do zadań administratora (art. 4 pkt 7 RODO). Zatem na gruncie przepisów o ponownym wykorzystywaniu cele ponownego wykorzystywania informacji sektora publicznego stanowiących lub zawierających dane osobowe powinny zostać sformułowane przez organ sektora publicznego udostępniający lub przekazujący informacje (podmiot zobowiązany). Nie jest to zadanie proste. Z pewnością posłużenie się ogólną informacją podawaną podmiotowi danych o tym, że dane osobowe mogą zostać wykorzystane w interesie publicznym nie czyni zadość wymogom, o których mowa w zasadzie ograniczenia celu. Samo pojęcie interesu publicznego pozostaje na gruncie omawianych przepisów niezdefiniowane, należałoby zatem posługiwać się wypracowaną na gruncie prawa administracyjnego definicją doktrynalną.

Przedmiotem wstępnej analizy powinien być zatem cel pierwotnej operacji przetwarzania, w wyniku której doszło do udostępniania informacji. Analiza aktów prawnych przewidujących obowiązki publikacji danych osobowych nie dostarcza w tym zakresie wyczerpującej odpowiedzi. Przykładowo ustawy określające zasady wykonywania zawodów lub działalności regulowanej co do zasady zakładają pierwotny cel zebrania danych osobowych na potrzeby weryfikacji, czy dana osoba spełnia kryteria wynikające z przepisów ustawowych, niezbędne do wykonywania tego zawodu lub działalności. Przepisy szczególne często przesądzają o jawności określonych danych nie wskazując jednocześnie żadnego celu, który można wyinterpretować z całości przepisów regulacji lub jej ogólnych celów. Na przykład

[862] Zob. J. *C Cersosimo*, The purpose limitation principle in the General Data Protection Regulation, Tilburg University 2018, http://arno.uvt.nl/show.cgi?fid=145704 (dostęp: 21.11.2020 r.), s. 8 i nast. oraz powołana tam literatura.
[863] *Grupa Robocza Art. 29*, Opinia 03/2013.

w ustawie z dnia 26 maja 1982 r. o adwokaturze[864] art. 49 stanowi, że okręgowa rada adwokacka prowadzi listy adwokatów i aplikantów adwokackich. Okręgowa rada adwokacka udostępnia na swojej stronie internetowej informacje o wpisanych na prowadzone przez nią listy adwokatach i aplikantach adwokackich, obejmujące imię i nazwisko oraz numer wpisu na listę. Uogólniając można przyjąć, że pierwotnym celem zebrania danych jest wpis na listę potwierdzający prawo do wykonywania zawodu z czym następczo związane jest z ujawnienie danych osobowych (niezależnie jednak od ujawnienia ich w trybie UPW).

Innym przykładem może być art. 43 ustawy z dnia 6 marca 2018 r. prawo przedsiębiorców[865], zgodnie z którym jeżeli odrębne przepisy stanowią, że dany rodzaj działalności jest działalnością regulowaną, przedsiębiorca może wykonywać tę działalność, jeśli spełnia warunki określone tymi przepisami i po uzyskaniu wpisu do właściwego rejestru działalności regulowanej. 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 ochronie danych osobowych (ust. 4).

Po drugie, przedmiotem badania powinna być „wyraźność" celu. Innymi słowy cel powinien być sformułowany w sposób jasny i zrozumiały, a jego treść powinna być dostępna jakimikolwiek środkami[866]. Takie określenie celów może być dokonane na wiele sposobów, również wzajemnie się uzupełniających, np. przez publiczne oświadczenia, informacje przekazywane bezpośrednio podmiotom danych, w przepisach prawa czy licencje[867]. Kontynuując przykład zawodów i działalności regulowanej sytuacja komplikuje się, gdy dane osobowe, które zgodnie z przepisami szczególnymi pozostają jawne, podlegają jednocześnie publikacji w BIP (np. dany rejestr jest prowadzony w BIP) i CRIP (np. z rejestru są automatycznie zbierane przez portal dane.gov.pl poprzez odpowiednie metadane). W świetle zasady domniemanej dopuszczalności ponownego wykorzystywania informacji udostępnionych w BIP i CRIP bez konieczności spełniania jakichkolwiek warunków, jeśli nie zostały określone, dochodzi w istocie do zmiany pierwotnego celu pozyskania danych, na cel związany z ponownym wykorzystaniem już na poziomie pierwotnego rejestru. W przypadku

[864] Dz. U. z 2020 r. poz. 1651.
[865] t.j. Dz. U. z 2021 r. poz. 162.
[866] *J. Andraško, M. Mesarčík*, Quo Vadis Open Data?, s. 201.
[867] Zob. OECD Explanatory Memorandum dla Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, pkt 54. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (dostęp 18.07.2020).

braku określenia z góry warunków ponownego wykorzystywania danych osobowych (co jest dominującą praktyką), nie sposób zatem mówić o wyraźności celu.

Po trzecie cel musi być prawnie uzasadniony, zatem przetwarzanie musi opierać się na przynajmniej jednej przesłance wymienionej w art. 6 ust. RODO. Zdaniem Grupy Roboczej Art. 29 należy tu jednak przyjąć szersze podejście. Cel przetwarzania musi być zgodny z prawem w ogóle, co wynika konieczności spełnienia wymogu legalności. Cele muszą być zatem „zgodne z prawem" w najszerszym znaczeniu. Obejmuje to wszelkie formy prawa pisanego i precedensowego, prawa pierwotnego i wtórnego, samorządowego, orzecznictwa sądowego, zasad konstytucyjnych, prawa podstawowych innych zasad prawnych[868].

Rozdział 9. Ujawnienie danych osobowych do ponownego wykorzystywania

9.1. Udostępnienie a przekazanie danych osobowych do ponownego wykorzystywania

Wszelkie informacje odnoszące się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, niezależnie od tego, czy są dostępne publicznie, stanowią dane osobowe. Zgodnie z definicją przytoczoną wcześniej ponowne wykorzystywanie danych osobowych będzie stanowić ich przetwarzanie w rozumieniu RODO, np. przez gromadzenie danych, łączenie z innymi informacjami, dokonywanie na nich dalszych operacji w celu stworzenia produktu, usługi, aplikacji etc. W związku z tym ponowne wykorzystywanie tych danych nadal podlega właściwym przepisom o ochronie danych osobowych i może następować wyłącznie z poszanowaniem zasad wynikających z tych przepisów, w tym zasady proporcjonalności, minimalizacji danych oraz zasady celowości[869] (Zob. Rozdział 5.1 oraz Rozdział 7), a osoby których dane dotyczą korzystają z pełni uprawnień gwarantowanych przepisami ogólnego rozporządzenia (zob. Rozdział 5.2).

W opinii Grupy Roboczej Art. 29 wskazano, że przy stosowaniu dyrektywy 2003/98/WE i przepisów o ochronie danych w przypadku ponownego wykorzystywania danych osobowych podmiot zobowiązany może podjąć jedną z trzech różnych decyzji. Po pierwsze, może zdecydować o nieudostępnieniu danych osobowych do ponownego wykorzystania. Po drugie, może zdecydować o przekształceniu danych osobowych do formy zanonimizowanej (najczęściej w formie zbiorczych danych statystycznych) i udostępnieniu do ponownego wykorzystania tylko zdepersonalizowanych danych. Po trzecie, może podjąć

[868] *Grupa Robocza Art. 29,* Opinia 03/2013, s. 20.
[869] *Ibidem,* s. 31.

decyzję o udostępnieniu danych osobowych do ponownego wykorzystania (w razie potrzeby podlegającą szczególnym warunkom i odpowiednim zabezpieczeniom).

W przepisach RODO udostępnianie danych, podobnie jak to miało miejsce na gruncie poprzednio obowiązujących przepisów, uznane zostało za jedną z postaci przetwarzania danych osobowych. Brak jest szczególnej regulacji dla czynności udostępniania danych osobowych w ramach realizacji prawa do ponownego wykorzystywania informacji sektora publicznego.

Jak wykazano, dystrybucja informacji sektora publicznego może mieć miejsce w trybie wnioskowym, wówczas dochodzi do przekazania informacji lub w trybie bezwnioskowym, kiedy informacja pozostaje udostępniona. Tym samym ujawnianie danych osobowych ramach informacji sektora publicznego może mieć miejsce w przypadku przekazania informacji do ponownego wykorzystywania lub udostępnienia (w systemie teleinformatycznym) informacji do ponownego wykorzystywania.

Bez względu na tryb w pierwszej kolejności podmiot zobowiązany powinien ustalić podstawę dla udostępniania lub przekazania danych osobowych, czyli oprzeć ujawnienie danych osobowych w celu ich ponownego wykorzystywania o jedną z przesłanek legalizujących przetwarzanie wymienionych w art. 6 ust.1 (lub względnie w art. 9 ust.2) RODO w związku z przepisami o ponownym wykorzystywaniu informacji sektora publicznego (zob. Rozdział 7). Jak wykazano w Rozdziale 6, zarówno w przypadku podjęcia decyzji o nieujawnieniu danych osobowych, jak i ich przekazaniu lub udostepnieniu w celu ponownego wykorzystywania konieczne będzie równoległe stosowanie przepisów RODO i UPW.

Należy podkreślić, że zarówno dyrektywa 2003/98/WE, jak i najnowsza dyrektywa 2019/1024 oraz przepisy prawa krajowego nie wyodrębniają proceduralnie tej szczególnej sytuacji upublicznienia informacji sektora publicznego, jeśli zawiera ona dane osobowe. O ile będzie to prawnie dopuszczalne, udostępnia się lub przekazuje informacje sektora publicznego zawierające dane osobowe w oparciu o przepisy UPW regulujące odpowiednio dany tryb, tj. bezwnioskowy lub wnioskowy (zob. Rozdział 4.3 i 4.4).

Przypomnijmy, że w pierwszym wypadku mamy do czynienia z ujawnieniem danych osobowych z inicjatywy podmiotu zobowiązanego dla nieoznaczonego i co do zasady nieograniczonego kręgu odbiorców, lecz w oparciu o podstawę prawną, w drugim zaś przypadku dochodzi do ujawnienia z inicjatywy konkretnego użytkownika w wyniku złożonego wniosku, w tej sytuacji dane są przekazywane wyłącznie temu oznaczonemu użytkownikowi. Co istotne, tylko przekazując informacje sektora publicznego na wniosek, podmiot zobowiązany ma wiedzę co do celów i sposobu ponownego wykorzystywania, ma to

istotne znaczenie dla prawidłowego określenia warunków (przetwarzania) ponownego wykorzystywania danych osobowych.

W przypadku udostępnienia informacji sektora publicznego może dojść do ujawnienia danych osobowych w BIP, CRIP lub innym systemie teleinformatycznym podmiotu zobowiązanego w wyniku realizacji obowiązku prawnego określonego przepisami prawa. W pierwszym wypadku podstawą udostępnienia informacji danych osobowych są przepisy UDIP wymieniające obowiązki publikacyjne w BIP, jak również inne przepisy szczegółowe przewidujący taki sposób ujawnienia danych osobowych (np. zawartych w oświadczeniach majątkowych). W przypadku udostępnienia informacji w CRIP określone w rozporządzeniu Ministra Cyfryzacji wydanym na podstawie art. 9 ust. 3 UDIP zasoby informacyjne mogą potencjalnie zawierać dane osobowe (np. lista rzeczoznawców majątkowych). Wreszcie w trzecim wypadku, na stronach internetowych podmiotów publicznych również publikowane są dane osobowe na podstawie przepisów, np. na podstawie ustawy o petycjach publikowane są odwzorowania cyfrowe petycji zawierające dane osobowe.

Poza publikacją danych osobowych w przedmiotowych systemach w wyniku realizacji obowiązku wynikającego z przepisu prawa, może dojść do ujawnienia danych osobowych w celu ponownego wykorzystywania z inicjatywy podmiotu zobowiązanego. BIP, CRIP czy strony internetowe urzędów, ze swej natury mają charakter otwarty, a katalogi informacji podlegających publikacji nie mają charakteru wyczerpującego. Jako przykład można wymienić tzw. rejestry umów zawierające dane osobowe kontrahentów podmiotu zobowiązanego, publikowane przez niektóre podmioty zarówno w BIP, jak i w CRIP.

Podmiot zobowiązany rozpatrując wniosek o ponowne wykorzystywanie informacji sektora publicznego (o którym mowa w art. 21 ust 2 UPW), który dotyczy przekazania użytkownikowi informacji zawierającej lub stanowiącej dane osobowe, będzie przetwarzał owe dane w ramach ciążącego na nim obowiązku prawnego. Jak zostało wskazane prawo do ponownego wykorzystywania jest prawem publicznym podmiotowym przysługującym każdemu, którego nieodłącznym uprawnieniem jest możliwość złożenia wniosku do podmiotu zobowiązanego o przekazanie informacji do ponownego wykorzystywania. Podmiot zobowiązany po rozpatrzeniu wniosku o ponowne wykorzystywanie, zgodnie z art. 23 ust. 1 UPW: a) przekazuje informację sektora publicznego w celu ponownego wykorzystywania bez określania warunków ponownego wykorzystywania albo; b) informuje o braku warunków ponownego wykorzystywania w przypadku posiadania informacji sektora publicznego przez wnioskodawcę albo; c) składa ofertę zawierającą warunki ponownego wykorzystywania lub

informację o wysokości opłat za ponowne wykorzystywanie albo d) odmawia, w drodze decyzji, wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego.

Przed rozstrzygnięciem wniosku obejmującego przekazanie danych osobowych, podmiot zobowiązany musi dokonać analizy tych konkretnych danych osobowych w ramach informacji sektora publicznego, zbadać przesłanki ograniczające prawo do ponownego wykorzystywania oraz ustalić podstawę prawną dla ewentualnego przekazania tych danych do ponownego wykorzystywania, w tym konieczne może być przeprowadzenie testu zgodności celów przetwarzania. Nawet w przypadku, gdy dojdzie do ujawnienia wyłącznie danych zanonimizowanych, może dochodzić do przetwarzania danych osobowych na tym wcześniejszym etapie poprzedzającym przekazanie danych anonimowych. Także sama anonimizacja danych jest operacją na danych osobowych. W związku z tym, że anonimizacja w trybie wnioskowym ponownego wykorzystywania w praktyce dotyczyć będzie osób innych niż pełniące funkcje publiczne (w związku z pełnieniem ich funkcji) można przyjąć, że podstawą przetwarzania danych w ramach tej operacji będzie art. 6 ust. 1 lit. e RODO[870].

Po drugie, w ograniczonych przypadkach opisanych w Rozdziale 7, jako podstawę ujawnienia danych osobowych w ramach przekazania informacji sektora publicznego można przyjąć również art. 6 ust. 1 lit. c. Przesłanka ta będzie miała zastosowanie co do zasady w przypadku przekazania danych osobowych osób pełniących funkcje publiczne mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania funkcji (art. 6 ust. 2 UPW).

Rozpatrując możliwość udostępnienia lub przekazania danych osobowych do ponownego wykorzystywania, poza omówionymi wcześniej zagadnieniami materialnymi i proceduralnymi trzeba rozstrzygnąć kilka zasadniczych kwestii. Po pierwsze, trzeba rozważyć dwa zagadnienia poprzedzające samo ujawnienie danych osobowych lub rozpoczęcie ich ponownego wykorzystywania, tj. konieczność przeprowadzenia oceny skutków dla ochrony danych osobowych oraz warunków ponownego wykorzystywania danych osobowych. W mojej opinii oba instrumenty mają kluczowe znaczenie dla ochrony prywatności w związku z dalszą eksploatacją informacji zawierającej dane osobowe. Po drugie, konieczne jest rozstrzygniecie kwestii obowiązku informacyjnego będącego konsekwencją ujawnienia danych osobowych do ponownego wykorzystywania. Na koniec rozważyć trzeba przekazanie lub udostępnienie do ponownego wykorzystywania danych zanonimizowanych. Jeśli w wyniku realizacji prawa do ponownego wykorzystywania dojdzie do przetwarzania danych osobowych może okazać się

[870] Zob. *M. Gumularz*, Ekspertyza s. 40.

zasadne zrealizowanie innych obowiązków przez administratora danych i wykonanie praw przysługujących podmiotowi danych (niż uprawnienia informacyjne), o czym piszę w Rozdziale 10.

9.2. Znaczenie oceny skutków dla ochrony danych osobowych

Ogólne rozporządzenie realizuje koncepcję podejścia do ochrony danych osobowych opartą na ryzyku. Uwzględniając różne potencjalne czynniki ryzyka dla ochrony danych, a w szczególności fakt, że po publicznym udostępnieniu informacji sektora publicznego zawierających dane osobowe sprawowanie skutecznej kontroli nad tymi danymi będzie znacznie utrudnione, istotne jest przestrzeganie zasad dotyczących ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej[871]. Rozwiązania te po raz pierwszy do polskiego porządku prawnego wprowadza art. 25 RODO.

Według Grupy Roboczej Art. 29 podmiot zobowiązany powinien przeprowadzić ocenę skutków w zakresie ochrony danych (*data protection impact assessment*), zanim udostępni informacje sektora publicznego zawierające dane osobowe do ponownego wykorzystania. W ocenie powinno się wskazać m.in. podstawę prawną ujawnienia danych (i ewentualną podstawę prawną ich ponownego wykorzystania), przeanalizować zasady w zakresie celowości, proporcjonalności oraz minimalizacji danych, a także uwzględnić konieczność specjalnej ochrony danych wrażliwych. W trakcie przeprowadzania tej oceny należy starannie uwzględnić możliwy wpływ na osoby, których dane dotyczą[872].

Zdaniem Grupy Roboczej Art. 29 ocena skutków w zakresie ochrony danych powinna również zostać przeprowadzona w sytuacjach, gdy do ponownego wykorzystywania będą udostępniane zanonimizowane zestawy danych uzyskane z danych osobowych. W takim wypadku zasadnicze znaczenie ma ocena ryzyka ponownej identyfikacji oraz dobra praktyka w zakresie przeprowadzania testów na ponowną identyfikację. Wyniki oceny mogłyby pomóc podmiotowi zobowiązanemu w określeniu odpowiednich zabezpieczeń minimalizujących ryzyko, w tym m.in. środków technicznych, prawnych i organizacyjnych, takich jak odpowiednie warunki licencji (warunki ponownego wykorzystywania), środki techniczne uniemożliwiające masowe pobieranie danych czy zastosowanie odpowiedniej techniki anonimizacji[873].

---

[871] *Grupa Robocza Art. 29*, Opinia 06/2013, s. 32.
[872] *Ibidem*, s. 8.
[873] Przeglądu technik anonimizacji dokonała *Grupa Robocza Art. 29* w Opinii Nr 5/2014 z 10.4.2014 r. w sprawie technik anonimizacji

Ponadto, w dyrektywie 2019/1024 po raz pierwszy prawodawca unijny wskazał na konieczność przeprowadzenia oceny skutków dla ochrony danych przy podejmowaniu decyzji w sprawie zakresu i warunków ponownego wykorzystywania dokumentów (informacji) sektora publicznego zawierających danych osobowe, na przykład w sektorze zdrowia (zob. motyw 53 preambuły dyrektywy).

O ocenie skutków planowanych operacji przetwarzania dla ochrony danych osobowych stanowi art. 35 RODO. Ocena skutków jest procesem pozwalającym opisać przetwarzanie oraz ocenić jego konieczność i proporcjonalność, a także instrumentem mającym wspomóc zarządzanie ryzykiem naruszenia praw i wolności osób fizycznych wynikającym z przetwarzania danych osobowych poprzez ocenę ryzyka i określenie środków pozwalających zaradzić tym czynnikom ryzyka. Oceny skutków dla ochrony danych są ważnym narzędziem rozliczalności (zgodnie z art. 5 ust. 2 RODO), ponieważ ułatwiają administratorom nie tylko przestrzeganie wymogów określonych w ogólnym rozporządzeniu, ale także wykazanie, że podjęto odpowiednie środki w celu zapewnienia przestrzegania jego przepisów. Można zatem uznać ocenę skutków za proces budowania i wykazywania zgodności[874]. Nie chodzi zatem o analizę zgodności przetwarzania z przepisami RODO, ale o zbadania skutków takiego przetwarzania dla prywatności. Stąd bardziej zasadnie jest uznanie tego instrumentu za metodologię oceny wpływu projektu, technologii, produktu, usługi, polityki, programu lub innej inicjatywy na ochronę danych osobowych (prywatność) wraz z oceną, jakie działania powinny zostać podjęte w celu wykluczenia lub zminimalizowania potencjalnego negatywnego wpływu[875]. Tym samym ocena skutków dotyczy nie tyle przetwarzania danych w ogóle, ile konkretnych operacji przetwarzania, związanych np. z wprowadzaniem na rynek nowej usługi, nowej aplikacji, wdrożeniem nowego systemu informatycznego itp., o ile operacja ta zmienia dotychczasowe warunki przetwarzania danych[876].

Artykuł 35 RODO wyznacza standard dla przeprowadzenia oceny skutków, który pozostaje aktualny również dla podjęcia decyzji w przedmiocie przetwarzania danych osobowych w ramach ponownego wykorzystywania informacji sektora publicznego.

[874] Zob. szerzej *Grupa Robocza Art. 29,* Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko" do celów rozporządzenia 2016/679 z 04.04.2017 r. (WP 248 rev.01).

[875] *N. Kalinowska, P. Litwiński*, Ocena skutków dla ochrony danych i uprzednie konsultacje – nowe obowiązki podmiotów przetwarzających dane osobowe, „Monitor Prawniczy" 2017, nr 13, s. 695.

[876] Zob. *A. Mednis*, Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych, „Monitor Prawniczy" 2016, nr 20 (dodatek), s. 29-30.

Po pierwsze, ponowne wykorzystywanie może wiązać się z przetwarzaniem – w szczególności z użyciem nowych technologii – które ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Mamy tu do czynienia z obligatoryjnym przeprowadzeniem oceny, która jest wynikiem wstępnej oceny ryzyka naruszenia praw i wolności osób fizycznych. Jeśli ryzyko naruszenia jest wysokie, to ocena jest obowiązkowa. Taka okoliczność może mieć miejsce w ramach ponownego wykorzystywania danych osobowych w produktach, usługach czy aplikacjach. W związku z tym zostanie spełniona podstawowa przesłanka dla obowiązku przeprowadzania oceny skutków. Administrator przed rozpoczęciem takiego przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych.

Należy również potencjalnie rozstrzygnąć pozostałe przesłanki wymienione w art. 35 po wystąpieniu których ocena skutków dla ochrony danych jest wymagana, przy czym katalog ten ma charakter otwarty:

a) systematyczna, kompleksowa oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzanie na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;

c) systematyczne monitorowania na dużą skalę miejsc dostępnych publicznie.

Ponadto należy wziąć pod uwagę, że krajowy organ nadzorczy ustanawia i podaje do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych. Organ nadzorczy może także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych. W komunikacie Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 czerwca 2019 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony[877] wprost nie wymienia ponownego wykorzystywania jako rodzaju przetwarzania, z którym wiązałaby się konieczność przeprowadzania oceny. Niemniej wśród wymienionych kategorii przetwarzania, np. innowacyjnym wykorzystaniu lub zastosowaniu rozwiązań

[877] M.P. z 2019 r. poz. 666.

technologicznych lub organizacyjnych, można potencjalnie zidentyfikować takie cele ponownego wykorzystywania, które mieściłyby się w tej kategorii (np. wykorzystanie danych osobowych pozyskanych z publicznie dostępnych rejestrów gospodarczych w internetowej usłudze tzw. wywiadowni gospodarczej).

Przepisy RODO nie precyzują, w jaki sposób ma być przeprowadzana ocena skutków, ani w jakiej formie mają zostać przedstawione jej rezultaty. Biorąc pod uwagę dyrektywę rozliczalności oraz prawdopodobieństwo konsultacji wyników oceny z organem nadzorczym trzeba przyjąć, że ocena powinna pozostać udokumentowana. W art. 35 ust 7 wyznaczono minimalny zakres oceny skutków, musi ona zawierać co najmniej:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora (dotyczy to zatem przesłanki legalności z art. 6 ust. 1 lit. f RODO, która jak wykazano nie ma zastosowania do podmiotu zobowiązanego, a do użytkownika, w tym wypadku chodzi o opisanie prawnie uzasadnionego interesu);

b) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów (w przypadku wykonywania obowiązku wynikającego z przepisu prawa, niezbędne będzie wskazanie, dlaczego zadanie to wymaga przetwarzania danych osobowych oraz wykazanie, że danego celu nie da się osiągnąć w inny sposób; wymóg proporcjonalności oznacza, że w ocenie należy udowodnić, że zakres danych użytych w danej operacji przetwarzania będzie adekwatny do celu[878]);

c) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą (trzeba uwzględnić zagrożenia, jakie może nieść dana operacja i ocenić ryzyko ich wystąpienia; jeśli potwierdzi się wysoki poziom ryzyka naruszenia, wówczas konieczne będą konsultacje z organem nadzorczym lub nie podejmować przetwarzania);

d) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Jeżeli wyniki oceny skutków dla ochrony danych wskażą, że przetwarzanie powodowałoby wysokie ryzyko, gdyby administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania administrator konsultuje się z organem nadzorczym. Są to uprzednie konsultacje, o których mowa w art. 36 RODO.

[878] *A. Mednis*, Wymóg oceny skutków, s. 31.

Tak ujęta w przepisach RODO ocena skutków stanowi w istocie pogłębiony mechanizmem oceny ryzyka[879]. Ocena ryzyka ma służyć eliminowaniu negatywnych konsekwencji jakie – dla podmiotów danych – może stanowić przetwarzanie danych, a w szczególności chodzi o ocenę czy zaplanowane lub wdrożone środki realizacji wymogów są odpowiednie. Jeżeli ryzyko jest wysokie pomimo zaplanowania określonych środków (np. pseudonimizacji) w celu zapewnienia zgodności tzn., że nie są one odpowiednie i należy rozważyć inne mechanizmy redukcji ryzyka[880]. Ogólny wymóg monitorowania ryzyka przez administratora wynika z art. 24 RODO. W szczególności ocena ryzyka jest zaś elementem ochrony danych w fazie projektowania oraz domyślna ochrona danych, o której mowa w art. 25 RODO.

Przepisy ogólnego rozporządzenia nie definiują pojęcia ryzyka naruszenia praw lub wolności, a także nie zawierają wyraźnych wytycznych jak to ryzyko oceniać. Niemniej, na podstawie wielu postanowień RODO, można stwierdzić, że chodzi o ryzyko rozumiane jako prawdopodobieństwo naruszenia praw i wolności osób, których dane dotyczą[881]. Zgodnie z motywem 76 RODO, prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. W motywie 75 preambuły RODO wymieniono z kolei przykładowe ryzyka mogące prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych[882].

Analiza art. 35 RODO oraz przepisów dyrektywy 2019/1024 prowadzi do wniosku, że po pierwsze, ocena skutków powinna być dokonywania przez podmiot zobowiązany przed udostępnieniem lub przekazaniem informacji sektora publicznego zawierającej lub stanowiącej dane osobowe. Wyniki oceny mogą prowadzić do podjęcia decyzji o rezygnacji udostępniania

[879] Zob. szerzej: *M. Gumularz*, Ochrona danych osobowych w sektorze publicznym, s. 185-226.
[880] *M. Gumularz*, Ekspertyza, s. 14.
[881] Zob. *A. Mednis*, Wymóg oceny, s. 29.
[882] W szczególności: jeżeli przetwarzanie może poskutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną; jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i naruszeń prawa lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

informacji sektora publicznego zawierających dane osobowe do ponownego wykorzystania. Po drugie, ocena skutków powinna być przeprowadzana przez administratora przed rozpoczęciem przetwarzania, co oznacza, że obowiązek jej przeprowadzenia może dotyczyć również tego użytkownika, który spełnia przesłanki art. 4 pkt 7 RODO. Kluczowym elementem oceny skutków jest ocena ryzyka naruszenia praw lub wolności. Analizę ryzyka należy przeprowadzić nawet, jeżeli wstępna ocena operacji realizowanych w ramach ponownego wykorzystania nie wskazuje, że dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Wynika to z ogólnego podejścia RODO do kwestii bezpieczeństwa danych opartego na ocenie ryzyka.

Należałoby również postulować, aby w procesie tworzenia prawa przeprowadzano ocenę skutków planowanej regulacji dla prywatności i ochrony danych osobowych, która uwzględniałaby wpływ przewidywanych w projektach rozwiązań technologicznych na gwarancje autonomii informacyjnej jednostki, np. w ramach przeprowadzanej przez projektodawcę ocenie skutków regulacji[883]. Wniosek ten znajduje podstawę w treści art. 35 ust. 10 RODO zwalniającym z obowiązku przeprowadzania oceny skutków dla ochrony danych, jeśli dokonano już ją w ramach oceny skutków regulacji w związku z przyjęciem podstawy prawnej przetwarzania na mocy art. 6 ust. 1 lit. c) lub e) RODO.

9.3. Ochrona danych osobowych jako warunek ponownego wykorzystywania informacji sektora publicznego

Zarówno dla informacji sektora publicznego udostępnionej, jak i przekazanej do ponownego wykorzystywania podmiot zobowiązany powinien określić warunki korzystania z niej przez użytkownika. Brak określenia warunków ponownego wykorzystywania informacji udostępnionej w systemie teleinformatycznym rodzi – jak udowodniono wcześniej – określone konsekwencje prawne. Problematyka ta nabiera szczególnego znaczenia w sytuacji, w której informacja sektora publicznego stanowi albo zawiera dane osobowe.

Na wstępie, należy podkreślić, prawodawca UE nadaje licencjom[884] ponownego wykorzystywania, które na gruncie przepisów krajowych nabrały kształtu warunków

[883] *P. Drobek*, Ryzyka, s. 240.

[884] Polski ustawodawca w kontekście informacji sektora publicznego nie posługuje się terminem „licencja", a warunkami ponownego wykorzystywania. Oba pojęcia pozostają tożsame znaczeniowo i realizują ten sam cel, określają na jakich warunkach jest możliwa eksploatacja informacji sektora publicznego bez względu na sposób jej dystrybucji przez podmiot publiczny (zobowiązany).

ponownego wykorzystywania, szczególnego znaczenia praktycznego. Dał temu wyraz w motywie 44 preambuły dyrektywy 2019/1024 stwierdzając, że w niektórych przypadkach uzasadnionych celem interesu publicznego może być wydawana licencja określająca warunki ponownego wykorzystywania przez licencjobiorcę, dotycząca spraw takich jak odpowiedzialność, ochrona danych osobowych, prawidłowe wykorzystywanie dokumentów, gwarancja niewprowadzania zmian oraz obowiązek podania źródła. Jeżeli organy sektora publicznego licencjonują dokumenty do ponownego wykorzystywania, warunki licencji powinny być obiektywne, proporcjonalne i niedyskryminacyjne. W tym względzie ważną rolę mogą odgrywać dostępne w Internecie licencje standardowe. Państwa członkowskie powinny więc zapewnić dostępność licencji standardowych. Licencje na ponowne wykorzystywanie informacji sektora publicznego powinny w każdym przypadku jak najmniej limitować ponowne wykorzystywanie, na przykład poprzez ograniczenie się do wymogu wskazania źródła. Istotną rolę w tym zakresie powinny odgrywać otwarte licencje w formie standardowych licencji publicznych dostępnych w Internecie, które umożliwiają swobodny dostęp do danych i treści oraz ich swobodne wykorzystywanie, zmienianie i udostępnianie przez wszystkich do dowolnego celu i które opierają się na otwartych formatach danych.

Kwestią zasadniczą wprost wyrażoną w przytoczonym fragmencie dyrektywy jest rekomendacja dla obejmowania licencją również ochrony danych osobowych, która jednocześnie potwierdza możliwość ponownego wykorzystywania danych osobowych.

Ostatnia zmiana zasad ponownego wykorzystywania dokonana przepisami ustawy z dnia 21 lutego 2019 r. to dodanie – w wymienionym w art. 14 ust. 4 UPW – katalogu warunków ponownego wykorzystywania pkt 4 dotyczącego „informacji sektora publicznego zawierającej dane osobowe." Oznacza to, że podmiot zobowiązany określając warunki ponownego wykorzystywania informacji sektora publicznego, może uwzględnić kwestie ochrony danych osobowych, przez co ochrona danych osobowych stanie się zobowiązaniem umownym[885].

Artykuł 14 ust. 1 UPW w jego pierwotnym brzmieniu upoważniał podmioty zobowiązane do określania warunków ponownego wykorzystywania, które mogły dotyczyć:

1) obowiązku poinformowania o źródle, czasie wytworzenia i pozyskania informacji od podmiotu zobowiązanego;

2) obowiązku poinformowania o przetworzeniu informacji ponownie wykorzystywanej;

[885] Zob. szerzej *D. Sybilski*, Nowelizacja ustawy o ponownym wykorzystywaniu informacji sektora publicznego dostosowująca do przepisów ogólnego rozporządzenia o ochronie danych, „Monitor Prawniczy" 2019, Nr 22 (dodatek), s. 74-79.

3) zakresu odpowiedzialności podmiotu zobowiązanego za udostępniane lub przekazywane informacje.

Jedynie w przypadku informacji sektora publicznego będącej przedmiotem praw własności intelektualnej dotychczasowe przepisy o ponownym wykorzystywaniu przewidywały możliwość określenia innych warunków dalszego użycia informacji niż te wymienione enumeratywnie w art. 14 ust. 1 UPW. Zgodnie z art. 14 ust. 2 w przypadku ponownego wykorzystywania informacji sektora publicznego mających cechy utworu lub przedmiotu praw pokrewnych w rozumieniu przepisów ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych lub stanowiących bazę danych w rozumieniu przepisów ustawy z dnia 27 lipca 2001 r. o ochronie baz danych, podmiot zobowiązany mógł określić warunki korzystania z informacji, w szczególności określić warunek dotyczący obowiązku poinformowania o nazwisku, imieniu lub pseudonimie twórcy lub artysty wykonawcy, jeżeli jest znany[886].

Przepisy UPW w brzmieniu sprzed nowelizacji nie przewidywały możliwości uwzględnienia w warunkach kwestii ochrony danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego. Przedmiotowa nowelizacja stanowi zatem próbę wypełniania istotnej luki prawnej[887]. W mojej opinii ustawodawca uznał dane osobowe – podobnie jak własność intelektualną – za szczególną kategorię informacji sektora publicznego i upoważnił podmiot zobowiązany do ustalania warunków *a casum ad casum*. Zaznaczyć trzeba, że ustawodawca nie wskazał czego warunki ponownego wykorzystywania danych osobowych mogą w istocie dotyczyć, tym samym pozostawiając swobodę ich określenia podmiotowi zobowiązanemu.

Warto odnotować, że kwestia uwzględniania ochrony danych osobowych w katalogu warunków ponownego wykorzystania podnoszona była przez Grupę Roboczą Art. 29. We wspomnianej opinii nr 06/2013 Grupa stwierdziła, że w przypadku gdy informacje, które mogą zostać ponownie wykorzystane, zawierają dane osobowe, ponowni użytkownicy powinni znać zasady przetwarzania takich danych od początku. Można tego dokonać poprzez zawarcie odpowiedniego postanowienia w licencji, przez co ochrona danych osobowych staje się zobowiązaniem umownym.

[886] Na temat warunków ponownego wykorzystywania zob. *D. Sybilski*, Warunki ponownego wykorzystywania informacji sektora publicznego, „Informacja w Administracji Publicznej" 2017, Nr 4.
[887] Na temat licencji dot. ochrony danych osobowych w ramach ponownego wykorzystywania zob. *P. Drobek*, Ryzyka dla ochrony danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego, [w:] *A. Piskorz-Ryń* (red.), Jawność i jej ograniczenia. T. V, Dostęp i wykorzystywanie, Warszawa 2015.

Licencje mogą wpływać na sposób przetwarzania danych osobowych i powinny znaleźć się – zdaniem Grupy Roboczej art. 29 – wśród zabezpieczeń, które mają być stosowane przy udostępnianiu danych osobowych (lub zanonimizowanych danych, które pochodzą z danych osobowych) do ponownego wykorzystania. Licencje nie eliminują konieczności zachowania zgodności z przepisami o ochronie danych, jednak klauzula o ochronie danych przewidziana w warunkach licencji pomogłaby w zapewnieniu zgodności z przepisami o ochronie danych poprzez dodanie elementu „wykonalności". Taka klauzula mogłaby również pomóc w podnoszeniu świadomości poprzez przypomnienie ponownym użytkownikom o ich obowiązkach jako administratorów[888].

Należy rozważyć dwa typy licencji (czyli na gruncie krajowym warunków ponownego wykorzystywania) ze względu na przedmiot ochrony, tj. dane osobowe i dane zanonimizowane. Dane zanonimizowane, a więc dane zdepersonalizowane nie podlegają ochronie danych osobowych (wykraczają poza zakres stosowania ogólnego rozporządzenia), w przeciwieństwie do danych spseudonimizowanych, które wciąż reżimowi ochrony danych osobowych podlegają. Pseudonimizacja jest bowiem procesem odwracalnym, utrudnia identyfikację, natomiast umożliwia przypisanie różnych czynności tej samej osobie (bez znajomości jej danych osobowych) oraz łączenie rożnych zbiorów danych między sobą, podczas gdy anonimizacja jest to proces, w którym dane osobowe są trwale i nieodwracalnie przekształcone[889].

W pierwszym wypadku warunki licencji – w opinii Grupy Roboczej art. 29 – muszą przynajmniej wyraźnie określać, dla jakich celów dane osobowe zostały pierwotnie opublikowane, i wskazywać, co byłoby uznane za wykorzystanie danych osobowych zgodne z pierwotny celem, a co nie. Z powyższego wynika zatem konieczność każdorazowego dokonywania przez podmiot zobowiązany przed udostępnieniem danych do ponownego wykorzystywania testu zgodności celów, tj. zgodności celu pierwotnego dla którego dane zostały zebrane z celem udostępnienia danych do ponownego wykorzystywania (dalszego przetwarzania danych) zgodnie z 6 ust. 4 RODO. Czynność ta mogłaby być elementem oceny skutków dla ochrony danych, która poprzedzałaby decyzję o ujawnieniu danych, o której mowa w art. 35 RODO. Tak określone warunki ponownego wykorzystania danych osobowych mogłyby jednocześnie stanowić środek organizacyjny w rozumieniu art. 25 ust. 1 RODO

[888] *Grupa Robocza Art. 29,* Opinia 06/2013, s. 29.
[889] Zob. Standard bezpieczeństwa. Standardy otwartości danych, Ministerstwo Cyfryzacji, https://dane.gov.pl/media/ckeditor/2018/10/04/standard-bezpieczenstwa_Gopookz.pdf (dostęp: 30.08.2019)

służący redukcji ryzyka[890]. Dotyczyć to będzie zarówno trybu wnioskowego jak i bezwnioskowego.

W drugim wypadku warunki licencji mogą być również określone dla zanonimizowanych zestawów danych i mogą:

- zawierać informację, że zestawy danych zostały zanonimizowane;
- zakazywać licencjobiorcom (użytkownikom) ponownej identyfikacji osób fizycznych;
- zakazywać licencjobiorcom wykorzystywania danych do podejmowania środków lub decyzji wobec zainteresowanych osób fizycznych;
- zawierać zobowiązanie licencjobiorcy (użytkownika) do powiadomienia licencjodawcy (podmiotu zobowiązanego) w przypadku wykrycia, że osoby fizyczne mogą zostać lub zostały ponownie zidentyfikowane.

Ciekawym zagadnieniem podniesionym przez Grupę Roboczą Art. 29 w opinii 06/2013 jest kwestia wycofania zestawów danych, których bezpieczeństwo zostało naruszone. Na wypadek wykrycia przez licencjodawcę zwiększonego ryzyka ponownej identyfikacji należy w licencji przewidzieć procedurę, w ramach której licencjodawca może „wycofać" zestaw danych, „których bezpieczeństwo zostało naruszone". Klauzula o ochronie danych powinna dawać licencjodawcy prawo do zawieszenia lub zakończenia dostępności danych (na przykład prawo do wyłączenia interfejsu API lub usunięcia pliku z platformy)[891].

Na marginesie warto zauważyć, że obecnie standardowe otwarte licencje, takie jak brytyjska otwarta licencja rządowa, w ogóle nie mają zastosowania do informacji zawierających danych osobowych[892].

Kwesta ustalenia warunków ponownego wykorzystywania nie jest zagadnieniem jedynie teoretycznym, ma istotne znaczenie z punktu widzenia praktyki ponownego wykorzystywania informacji sektora publicznego i może rodzić określone konsekwencje prawne zarówno po stronie podmiotu zobowiązanego, użytkownika danych, jak i osoby której dane dotyczą. Warunki ponownego wykorzystywania przekazanej na wniosek (art. 23 ust. 1 pkt 3 UPW), jak i udostępnionej w systemie teleinformatycznym, jak wykazano w Rozdziale 4, stanowić będą (art. 12 ust. 1 i 2 UPW) ofertę. Pojęcie oferty należy rozumieć zgodnie z art. 66 i n. kodeksu cywilnego. W przypadku przyjęcia przez wnioskodawcę oferty złożonej przez podmiot zobowiązany w odpowiedzi na wniosek albo rozpoczęcia ponownego

[890] *M. Gumularz*, Ekspertyza, teza 145, s. 61.
[891] *Grupa Robocza Art. 29,* op. cit., s. 30.
[892] "This licence does not cover personal data in the Information"; zob. Open Government Licence for public sector information; http://www.nationalarchives.gov.uk/doc/open-government-licence/version/3/ (dostęp: 20.11.2020).

wykorzystywania opatrzonej warunkami informacji udostępnionej w systemie teleinformatycznym, dochodzi do zawarcia umowy cywilnoprawnej, której stronami są podmiot zobowiązany (oferent) i użytkownik (oblat). W konsekwencji w przypadku naruszenia warunków określonych w umowie zastosowanie znajdą ogólne zasady odpowiedzialności cywilnej[893]. Co istotne, w przypadku informacji sektora publicznego udostępnionych w BIP lub centralnym repozytorium informacji publicznej brak określenia warunków (bez względu czy w wyniku świadomej oceny organu czy przez zaniechanie) oznacza domniemaną zgodę na bezwarunkowe ponowne wykorzystywanie (art. 11 ust. 4 UPW).

Co to oznacza dla podmiotu danych osobowych? Określenie warunków ponownego wykorzystywania wzmacnia ochronę prawną osób, których dane dotyczą. Wymóg ochrony danych osobowych stał się bowiem zobowiązaniem umownym. Rezygnacja lub zaniechanie z określenia warunków korzystania (przetwarzania) z informacji sektora publicznego zawierających dane osobowe nie oznacza oczywiście pozbawiania ochrony prawnej podmiotów danych. Zastosowanie będą miały ogólne zasady wynikające z przepisów o ochronie danych osobowych, a w szczególności ogólnego rozporządzenia. Trzeba jednak pamiętać, że katalog możliwych warunków ponownego wykorzystywania danych osobowych jest otwarty i może obejmować środki ochrony, które wprost nie są przewidziane przepisami o ochronie danych (np. zakaz łączenia danych pochodzących z różnych źródeł). Warunki mogą również dotyczyć kwestii ochrony osób, których dane uległy anonimizacji (jak np. ogólny zakaz dla użytkowników ponownej identyfikacji osób fizycznych).

Przynajmniej częściową odpowiedzią na dylematy zidentyfikowane w niniejszej rozprawie mógłby być postulat *de lege ferenda* obligujący do każdorazowego określania warunków ponownego wykorzystywania informacji sektora publicznego zawierających dane osobowe lub dane zanonimizowane, podobnie jak to ma miejsce obecnie w przypadku praw własności intelektualnej (art. 13 ust. 2 UPW). Znajomość zasad przetwarzania danych osobowych w ramach informacji sektora publicznego wzmocniłaby pewność prawną przede wszystkim wśród użytkowników danych i optymalizowałaby ponowne wykorzystywanie informacji. Oczywiście wyzwaniem pozostaje sposób formułowania warunków oraz ich zakres w kontekście spełniania zasady związania celem. Rozważyć tutaj można dwie opcje, określenia z góry przez podmiot zobowiązany możliwych, ale konkretnych celów ponownego

[893] Zob. *M. Sakowska – Baryła*, Warunki ponownego wykorzystywania ISP [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 134 i *M. Błachucki, G. Sibiga*, Postępowanie w sprawie ponownego wykorzystywania ISP przekazywanych na wniosek [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 249.

wykorzystywania danych osobowych przez użytkownika lub wskazując użytkownikowi pierwotny cel ujawnienia danych oraz jego obowiązki wynikające z ogólnego rozporządzenia, w tym konieczność realizacji zasady celowości obejmującą przeprowadzenie testu zgodności celów samodzielnie przez użytkownika. Nie ulega wątpliwości, że zarówno pierwsze, jak i drugie rozwiązanie może okazać się w praktyce trudne do realizacji.

9.4. Obowiązki informacyjne

W mojej opinii trzecim – po ustaleniu właściwej podstawy legalizującej przetwarzanie danych i spełnieniu zasady związania celem - wyzwaniem prawnym, jak i praktycznym dla realizacji prawa do ponownego wykorzystywania danych osobowych pozostaje problematyka wypełnienia obowiązku informacyjnego.

Do wymogu spełnienia obowiązku informacyjnego może dojść zarówno po stronie podmiotu zobowiązanego, jak i użytkownika. W przypadku podmiotu zobowiązanego mamy do czynienia ze zbieraniem danych od osoby, której dane dotyczą. Niemniej, jak wykazano wcześniej, w ramach realizacji prawa do ponownego wykorzystywania, co do zasady, dane osobowe są przetwarzane w innym celu niż pierwotny cel ich zebrania. Powoduje to powstanie po stronie podmiotu zobowiązanego konieczności spełnienia obowiązku informacyjnego, którego wykonanie powinno mieć miejsce – myśl art. 14 ust. 3 RODO – przez rozpoczęciem dalszego przetwarzania. Ustawodawca krajowy dokonał w tym przedmiocie istotnej modyfikacji przepisów RODO, wyłączając przepisami UPW *en bloc* obowiązek, o którym mowa w art. 14 ust. 3 ogólnego rozporządzenia.

Z kolei, w przypadku konieczności realizacji obowiązku informacyjnego przez użytkownika mamy do czynienia z tzw. wtórnym zbieraniem danych. Dochodzi do niego niezależnie od trybu pozyskania danych osobowych w ramach informacji sektora publicznego. Nie budzi wątpliwości w doktrynie, że pośrednie pozyskanie danych osobowych będzie miało miejsce w przypadku pobrania danych z publicznie dostępnych rejestrów państwowych, jak np. KRS, CEIDG, rejestr ksiąg wieczystych czy ze stron BIP podmiotów publicznych[894] (zob. Rozdział 5.2.2.2.). W doktrynie prezentowany jest również pogląd, że ze wtórnym

[894] Na temat zasady jawności rejestrów państwowych zob. m.in. *T. Stawecki*, Rejestry publiczne. Funkcje instytucji, Warszawa 2005, *A. Gryszczyńska (red.),* Rejestry publiczne. Jawność i interoperacyjność, Warszawa 2016.

pozyskaniem danych osobowych wiąże się otrzymanie danych osobowych w ramach otrzymanej na wniosek informacji publicznej[895].

W kontekście ponownego wykorzystywania danych osobowych przedmiotową problematykę należy rozpatrywać zatem odrębnie w odniesieniu do dwóch kategorii administratorów, tj. podmiotu zobowiązanego oraz użytkownika, a w dodatku na dwóch płaszczyznach regulacyjnych. Po pierwsze, na płaszczyźnie ogólnej wyznaczonej przepisami RODO, w tym kluczowym art. 13 ust. 3 oraz art. 14 ust. 4 i 5, a po drugie na płaszczyźnie szczegółowej zdeterminowanej przepisami UPW, które dokonały w tym obszarze istotnych zmian. W ramach - omówionego w rozdziale 4 – dostosowania przepisów krajowych do wymogów ogólnego rozporządzenia dokonanego ustawą z 21.2.2019 r. zmieniającej sto sześćdziesiąt dwie ustawy zmieniono również przepisy o ponownym wykorzystywaniu informacji sektora publicznego. Nowelizacja objęła zmianę art. 7 ustawy polegającą na ograniczeniu wykonania obowiązków informacyjnych, o których mowa w art. 13, 14 i 19 RODO w związku z realizacją prawa do ponownego wykorzystywania informacji stanowiących lub zawierających dane osobowe.

9.5.1. Obowiązek informacyjny podmiotu zobowiązanego

W przypadku obowiązku informacyjnego po stronie administratora będącego podmiotem zobowiązanym to właśnie przepisy UPW będą miały decydujące znaczenie, zgodnie bowiem z art. 7 ust. 3 UPW do przetwarzania danych osobowych w celu udostępniania lub przekazywania informacji sektora publicznego do ponownego wykorzystywania nie stosuje się przepisu art. 13 ust. 3 RODO. Oznacza to, że podmiot zobowiązany udostępniając informacje sektora publicznego zawierające dane osobowe z własnej inicjatywy np. na stronie BIP urzędu lub przekazując na wniosek zainteresowanego użytkownika, nie będzie zobligowany do spełnienia obowiązku informacyjnego wymienionego w art. 13 ust. 3 RODO. Przepis ten obliguje administratora (w tym przypadku podmiot zobowiązany), który planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, aby przed takim dalszym przetwarzaniem poinformował on osobę, której dane dotyczą, o tym innym celu oraz udzielił jej wszelkich innych stosownych informacji, o których mowa art. 13 ust. 2 RODO (zob. Rozdział 5.2.2.1). Omawiana norma przewiduje przypadek, w którym konieczne jest ponowienie obowiązku informacyjnego. Faktycznie nie mamy tu jednak do

[895] *J. Łuczak*, Komentarz do art. 14 [w:] *E. Bielak-Jomaa, D. Lubasz*, RODO, s. 495.

czynienia z informowaniem „podczas pozyskiwania danych osobowych", obowiązek ten spełniany jest bowiem po czynności zbierania danych, a w praktyce może być znacząco oddalony w czasie[896]. Zmieniając lub rozszerzając cel przetwarzania danych osobowych, administrator musi liczyć się z koniecznością ponowienia obowiązku informacyjnego tyle tylko, że w zakresie ograniczonym do „stosownych" informacji z art. 13 ust. 2 RODO[897]. Wyłączenie stosowania art. 13 ust. 3 RODO ma istotne znaczenie praktyczne, bowiem udostępnienie lub przekazanie danych osobowych na potrzeby ponownego wykorzystywania co do zasady związane jest ze zmianą pierwotnego celu dla którego dane zostały zebrane. Trudno wyobrazić sobie sytuację, w której podmiot zobowiązany zbierając pierwotnie dane bezpośrednio od osoby, której dane dotyczą, antycypował, że w przyszłości dane te potencjalnie będą mogły być udostępnione lub przekazane w ramach informacji sektora publicznego do ponownego wykorzystywania, dodajmy, w oparciu o którąś z podstaw legalizujących przetwarzanie danych wymienionych w art. 6 RODO.

Kolejna zmiana UPW polegała na dodaniu w art. 7 ust. 5, zgodnie z którym obowiązek wymieniony w art. 19 RODO podmiot zobowiązany wykonuje przez zaktualizowanie danych odpowiednio na swojej stronie podmiotowej BIP, w CRIP lub w inny sposób. Artykuł 19 RODO obciąża administratora wtórnymi obowiązkami informacyjnymi, polegającymi na tym, że administrator (tutaj podmiot zobowiązany) powinien poinformować o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Podejmując próbę wykładni językowej art. 7 ust. 5 UPW nie jest jednoznaczne, czy sposób spełnienia wtórnego obowiązku informacyjnego obejmuje oba tryby udzielenia informacji, tj. przekazania informacji sektora publicznego na wniosek (odbiorca jest podmiotowi zobowiązanemu znany) i udostępnienia informacji sektora publicznego w systemie teleinformatycznym, takim jak BIP czy portal otwartych danych (nieograniczony krąg odbiorców danych nieznanych podmiotowi zobowiązanemu). Moim zdaniem należy przepis ten interpretować funkcjonalnie, tj. przyjąć że obejmuje on wyłącznie przypadek udostępnienia danych w systemie teleinformatycznym. Podmiot zobowiązany informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał, w tym systemie w którym dane udostępnił. *A contrario,* w przypadku ujawnienia danych osobowych w ramach informacji sektora publicznego na wniosek

[896] *M. Sakowska-Baryła*, Komentarz do art. 14, pkt 13 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie.
[897] *Ibidem*.

przedmiotowy sposób spełnienia obowiązku informacyjnego (czyli poprzez BIP lub centralne repozytorium informacji publicznej) nie będzie miał zastosowania.

Jak wskazano wyżej adresatem art. 7 ust. 5 UPW jest podmiot zobowiązany, nowelizacja przepisów UPW z 21.2.2019 r. nie eliminuje problemu realizacji obowiązku informacyjnego przez administratora niebędącego podmiotem zobowiązanym (czyli, co do zasady, podmiotem publicznym), dla którego obowiązek ten może stanowić znaczne obciążenie. Użytkownik (administrator) mógł pozyskać dane osobowe zarówno od podmiotu zobowiązanego na wniosek, jak i ze źródeł publicznie dostępnych, np. jawnych rejestrów publicznych (o czym piszę dalej). W art. 19 RODO nie chodzi o ogólną informację o kategoriach odbiorców, ale o wskazanie przez administratora konkretnych podmiotów, którym dane osobowe zostały ujawnione, a informacja udzielona przez administratora powinna umożliwiać podmiotowi danych identyfikację każdego z odbiorców[898].

9.5.2. Obowiązek informacyjny użytkownika

Użytkownik, pozyskawszy dane osobowe z innych źródeł niż od podmiotu danych, ponownie je wykorzystując w swoich celach mających charakter zarobkowy czy też niekomercyjny, spełnia przesłankę wymienioną w art. 14 ust. 4 RODO. Przepis ten określa zasady realizacji tzw. wtórnego obowiązku informacyjnego, związanego z wtórnym gromadzeniem danych osobowych, a więc gdy mamy do czynienia z przypadkiem pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą[899].Dochodzi bowiem do przetwarzania danych osobowych w innym celu niż cel, w którym dane te zostały pozyskane. Oznacza to, konieczność podania – co do zasady – przez użytkownika przetwarzającego dane osobowe w sposób wtórny informacji wymienionych w art. 14 ust. 1 i 2 ogólnego rozporządzenia (zob. Rozdział 5.2.2.2). W tym przypadku w pierwszej kolejności należy rozważyć, czy spełnienie przedmiotowego obowiązku nie podlega wyłączeniu w oparciu, o którąś z przesłanek wymienionych w art. 14 ust. 5 lub też modyfikacji w ograniczonym tylko zakresie w oparciu o art. 7 ust. 4 UPW.

Artykuł 14 ust. 5 przewiduje kilka przypadków, w których pomimo pozyskania danych osobowych z innego źródła niż osoba, której dane dotyczą, administrator zwolniony jest z realizacji wtórnego obowiązku informacyjnego. To przypadki, w których informowanie podmiotu danych można odpowiednio uznawać za zbędne, nieracjonalne, nieefektywne lub

[898] Zob. *M. Czerniawski,* Komentarz do art. 19 [w:] *E. Bielak-Jomaa, D. Lubasz,* RODO, s. 539.
[899] *M. Sakowska-Baryła,* op. cit., pkt 1.

powodujące naruszenie innych praw i wartości[900]. Zgodnie z tym przepisem ust. 1–4 nie mają zastosowania, gdy – i w zakresie, w jakim:

1) osoba, której dane dotyczą, dysponuje już tymi informacjami;

2) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku; w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1, lub o ile obowiązek, o którym mowa w ust. 1 niniejszego artykułu, może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach administrator podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie;

3) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą; lub

4) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej, przewidzianym w prawie Unii lub w prawie państwa członkowskiego, w tym ustawowym obowiązkiem zachowania tajemnicy.

Z wymienionych przesłanek w przypadku ponownego wykorzystywania danych osobowych przez użytkownika w pierwszej kolejności należy rozważyć okoliczność wymienioną w pkt 2 w zakresie, w jakim udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. W mojej opinii właśnie z tą okolicznością będzie miał do czynienia użytkownik, który pozyskał dane osobowe w ramach realizacji prawa do ponownego wykorzystywania co do zasady w większości przypadków w trybie bezwnioskowym, jak również na wniosek. Przynajmniej teoretycznie nie można bowiem wykluczyć sytuacji, w której przekazanie informacji będzie obiektywnie możliwe, w odniesieniu do konkretnego administratora danych, tj. ponownego użytkownika.

"Niemożliwość" i "nadmiernie duży wysiłek" to przesłanki zwolnienia z informowania, aktualizujące się w przypadkach, w których informowanie podmiotu danych oznaczałoby szczególne, ponadnormatywne, nieuzasadnione w konkretnych okolicznościach zaangażowanie administratora[901]. Okoliczność niewspółmiernie dużego wysiłku będzie miała miejsce wtedy, gdy wysiłek włożony w przekazanie informacji jest nieproporcjonalny

[900] *Ibidem*, pkt 9.
[901] *Ibidem*, pkt 11.

w stosunku do niedogodności spowodowanych brakiem tych informacji u osoby, której dane dotyczą[902]. „Niemożliwość" przekazania odpowiednich informacji osobie fizycznej to z kolei sytuacja, w której administrator z jakichś obiektywnie ocenianych powodów nie może zakomunikować podmiotowi danych, że przetwarza jego dane osobowe i na jakich zasadach to czyni[903]. W myśl motywu 62 preambuły RODO uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia.

W przypadkach, w których administrator danych – ze względu na niemożliwość lub niewspółmierność wysiłku – jest zwolniony z obowiązku informacyjnego, powinien podjąć odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy osoby, której dane dotyczą, w tym udostępnia informacje publicznie. Za spełnienie obowiązku informacyjnego w takim przypadku może zostać uznane zamieszczenie informacji np. stronie internetowej administratora danych[904].

Zgodnie z wytycznymi Grupy Roboczej Art. 29 okoliczności, w których udzielenie informacji okazuje się niemożliwe, nie mogą być stopniowalne, dane działanie jest możliwe lub nie jest możliwe, nie ma tutaj sytuacji pośrednich. W myśl zasady rozliczalności administrator jest zobowiązany wykazać, na czym rzeczywiście owa niemożliwość polega. Jeżeli na skutek zmian tego stanu, w szczególności modyfikacji czynników, które przyczyniły się do „niemożliwości" udzielenia informacji, poinformowanie stałoby się możliwe, wówczas administrator powinien to niezwłocznie uczynić.

Przykład takiej niemożliwości podania informacji podał sam prawodawca unijny w motywie 61 preambuły RODO *in fine.* Nie można podać pochodzenia danych osobowych, jeżeli korzystano z rożnych źródeł, ale jedynie wtedy, gdy rożnych elementów danych osobowych dotyczących tego samego podmiotu danych nie można przypisać do określonego źródła. W takiej sytuacji jednak informacje z art. 14 RODO należy przedstawić w sposób ogólny.

Warunkiem skutecznego powołania się przez administratora na zwolnienia zawarte w art. 14 ust. 5 lit. b RODO jest uprzednie przeprowadzenie testu bilansującego, w ramach którego należy z jednej strony ocenić wysiłek administratora wymagany do udzielenia informacji osobie, której dane dotyczą, a z drugiej – skutki i konsekwencje niepodania

[902] *P. Litwiński (red.)*, op. cit., Komentarz do art. 14, pkt 17.
[903] *M. Sakowska-Baryła*, op. cit., pkt 11.
[904] Por. prawomocna decyzja GIODO z 12.7.2016 r., DIS/DEC 587/16/62309, niepubl. za *P. Litwiński* (red.), op. cit.

informacji podmiotowi danych. Wyniki tego testu podlegają ogólnej zasadzie rozliczalności, a zatem jego przeprowadzenie winno zostać stosowanie udokumentowane[905].

Uregulowanie wyłączenia wtórnego obowiązku informacyjnego stanowi istotną nowość w polskim prawie ochrony danych osobowych, bowiem w UODO1997 nie został wdrożony art. 11 ust. 2 dyrektywy 95/46/WE, przewidujący analogiczne rozwiązanie. W konsekwencji – jak słusznie zauważył *P. Litwiński* – w przypadku pozyskiwania danych osobowych w trybie dostępu do informacji publicznej oraz ponownego wykorzystania informacji sektora publicznego, należało wykonywać obowiązek informacyjny na zasadach ogólnych, co częstokroć istotnie utrudniało lub uniemożliwiało korzystanie z tych uprawnień[906]. W mojej opinii w przypadku ponownego wykorzystywania, którego istota polega na przetwarzaniu danych nieosobowych i osobowych pochodzących z publicznie dostępnych źródeł, w tym przede wszystkim rejestrów państwowych, BIP oraz stron internetowych podmiotów zobowiązanych w celu budowania wartości dodanej do tych informacji, spełnienie wtórnego obowiązku informacyjnego nie tylko znacząco utrudnia, co wręcz niweczy instytucję ponownego wykorzystywania jako instrumentu rozwoju gospodarki krajowej i wspólnotowej opartej o dane.

Trzeba jednocześnie przyznać, że przedmiotowe wyłączenie budzi kontrowersje. Towarzyszyły one pierwszej decyzji wydana przez Prezesa Urzędu Ochrony Danych Osobowych (nr decyzji ZSPR.421.3.2018 z dnia 15 marca 2019 r.)[907]. Decyzja ta – która została następnie uchylona wyrokiem WSA w Warszawie z 11.12.2019, II SA/Wa 1030/19 (wyrok nieprawomocny) – nakładająca karę pieniężną w wysokości 943 470,00 zł, dotyczyła właśnie braku pełnego wykonania wtórnego obowiązku informacyjnego w oparciu o wyłączenie z art. 14 ust. 5 lit. b RODO przez jedną ze spółek świadczącą usługi w zakresie udostępniania i uzupełniania baz danych swoich klientów np. marketingowych, baz danych dłużników czy kontrahentów. Spółka w szczególności oferuje raporty handlowe obejmujące m.in. dane finansowe i rejestrowe firm, opis działalności przedsiębiorstwa, jego kondycji finansowej, powiązania kapitałowe i osobowe, co istotne dane osobowe, które przetwarza (osób fizycznych prowadzących działalność gospodarczą oraz osób będących wspólnikami lub członkami organów spółek, fundacji i stowarzyszeń), które zostały pozyskane ze źródeł ogólnie

[905] *D. Lubasz,* Prawa informacyjne [w:] *D. Lubasz (red.),* Meritum, s. 155.
[906] *P. Litwiński*, Prawo do prywatności hamuje dostęp do danych z urzędów, „Rzeczpospolita" 10.07.2014 r., http://www.allerhand.pl/images/20140710_Rzeczpospolita_dr_P_Litwinski_Prawo_do_prywatnosci_hamuje_dostep.jpg (dostęp: 03.10.2020). Autor wymienia w tym względzie ze koszty związane z ustaleniem adresu podmiotu danych oraz potrzeby czas.
[907] Zob. https://uodo.gov.pl/decyzje/ZSPR.421.3.2018.

dostępnych, w tym z rejestrów publicznych, m.in. z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, z Bazy REGON Głównego Urzędu Statystycznego, z Monitora Sądowego i Gospodarczego[908].

Rozstrzygając sprawę Prezes UODO stwierdził, że Spółka nie spełniła obowiązku określonego w art. 14 RODO wobec tych osób fizycznych prowadzących jednoosobową działalność gospodarczą, co do których nie posiadała adresu e-mail w swojej bazie danych, przy czym zarówno chodzi o przedsiębiorców, którzy prowadzą aktualnie działalność gospodarczą, jak i o tych, którzy zaprzestali prowadzenia działalności gospodarczej. Organ stwierdził, że samo umieszczenie informacji, wymaganych w art. 14 ust. 1 i ust. 2 RODO, na stronie internetowej Spółki, w sytuacji posiadania przez Spółkę danych adresowych (a niekiedy również numerów telefonów) osób fizycznych prowadzących jednoosobową działalność gospodarczą, umożliwiających przesłanie pocztą tradycyjną korespondencji zawierającej wymagane tym przepisem informacje (lub przekazanie ich drogą kontaktu telefonicznego), nie może być uznane za wystarczające spełnienie przez Spółkę obowiązku, o którym mowa w art. 14 ust. 1-3 RODO. Prezes UODO stwierdził też, że przesłanka wyłączająca spełnienie obowiązku informacyjnego, przewidziana w art. 14 ust. 5 lit. b RODO nie znajdzie zastosowania w odniesieniu do osób fizycznych prowadzących jednoosobową działalność gospodarczą, których dane osobowe Spółka przetwarza, ponieważ przekazanie informacji pocztą tradycyjną, na adres osoby fizycznej prowadzącej działalność gospodarczą, lub w drodze kontaktu telefonicznego, nie jest czynnością "niemożliwą" oraz nie wymaga "niewspółmiernie dużego wysiłku", w sytuacji posiadania przez Spółkę w bazie systemu informatycznego danych adresowych. Organ wskazał przy tym, że w odróżnieniu do ww. osób fizycznych, odmienna jest sytuacja osób będących udziałowcami lub członkami organów spółek i innych osób prawnych, których dane Spółka przetwarza. W rejestrach publicznych (w szczególności w KRS) brak jest bowiem danych teleadresowych tych osób, w związku z czym Spółka musiałaby poszukiwać tych danych w innych źródłach, co już mogłoby stanowić dla Spółki "niewspółmiernie duży wysiłek".

WSA w Warszawie wprawdzie uchylił decyzję PUODO, ale jedynie w zakresie w jakim dotyczyła nakazu spełnienia obowiązku informacyjnego wobec osób fizycznych w przeszłości prowadzących działalność gospodarczą i co istotne, uchylenie to były wynikiem uchybień

[908] Na temat problemu wykorzystywania danych osobowych z jawnych rejestrów państwowych zob. *J. Ciesielski*, Rejestry przedsiębiorców a ochrona danych osobowych, „Przegląd Prawa i Administracji" 2018, nr 112 oraz *P. Fajgielski*, Jawność obrotu gospodarczego a prywatność przedsiębiorcy będącego osobą fizyczną – aspekty prawne [w:] *A. Mednis (red.)*, Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość.

proceduralnych (PUODO będzie musiał ponownie przeprowadzić postępowanie zgodnie z wytycznymi Sądu). WSA w Warszawie jednak stwierdził, że obowiązek informacyjny należy spełnić wobec osób aktualnie prowadzących działalność gospodarczą lub tych, które ją zawiesiły (listownie bądź telefonicznie). Ponadto sąd uznał, że obowiązek ten nie musi być spełniony wobec osób, które nie prowadzą już działalności gospodarczej, bo dotarcie do nich może być trudne.

Jednocześnie sąd wskazał, że pojęcie niewspółmiernie dużego wysiłku nie może być utożsamiane z wysokością kosztów, jakie administrator zmuszony będzie ponieść w związku z koniecznością dopełnienia obowiązku, który jest w pełni możliwy do realizacji. Zarówno kwestie organizacyjne w zakresie realizacji obowiązku z art. 14 ust. 1 i 2 rozporządzenia, jak i kwestie finansowe nie przeważają nad prawami osób fizycznych, których dane osobowe przetwarzane są przez administratora, w tym także w przypadku, gdy pozyskane zostały ze źródeł powszechnie dostępnych, a przetwarzane są następnie przez administratora w celach komercyjnych. W ocenie Sądu niewspółmiernie duży wysiłek ma miejsce wtedy, gdy udzielenie informacji jest obiektywnie możliwe, ale niebywale utrudnione (graniczące z brakiem możliwości udzielenia informacji). Administrator, aby udzielić tych informacji zmuszony byłby do podjęcia szeregu działań, które zmierzałyby dopiero do tego, aby udzielenie informacji stało się możliwe. Zakres tych działań (czynności) musiałby mieć przy tym olbrzymią skalę. Zdaniem Sądu w art. 14 ust. 5 lit. b) RODO chodzi o ustalenie, czy wysiłek, jaki musiałby zostać poniesiony, aby w ogóle wypełnić obowiązek z art. 14 ust. 1 i 2 RODO, jest tak znaczny, że przeważa nad prawem do bycia poinformowanym. Zdaniem WSA w Warszawie nie chodzi tu o znaczne obciążenie finansowe wiążące się z koniecznością dopełnienia – w pełni możliwego do realizacji, jak w tej sprawie - obowiązku. Przez niewspółmiernie duży wysiłek nie można na gruncie rozporządzenia rozumieć kosztu (tak organizacyjnego, który stanowi w istocie o sposobie zorganizowania przez administratora w ramach prowadzonej działalności, wykonania tego zadania, jak i finansowego) dopełnienia w pełni możliwego do realizacji obowiązku z art. 14 ust. 1 i 2 RODO. Interes finansowy administratora nie jest i nie może być wartością przeważającą nad prawem do uzyskania przez osobę fizyczną, której dane są przetwarzane, informacji m.in. o tym, jakie są prawnie usprawiedliwione interesy realizowane przez administratora, jak też o prawie do żądania od administratora dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania.

Istotnym dla omawianego zagadnienia jest okoliczność, że dane i informacje udostępniane przez CEIDG są jawne i każdy ma prawo dostępu do tych danych i informacji

ujawnionych w rejestrze (art. 45 ust. 1 ustawy o CEIDG) nie jest równoznaczna – zdaniem WSA w Warszawie – z możliwością dowolnego ich przetwarzania przez inne podmioty w celach innych niż te dane zostały w CEIDG zgromadzone. Ogólne rozporządzenie nie wyłącza w odniesieniu do administratora takich danych osobowych, przetwarzanych dla osiągnięcia określonych celów komercyjnych, stosowania zasad i obowiązków wynikających z tego rozporządzenia, w tym właśnie obowiązku podania informacji określonych w art. 14 ust. 1 i 2 RODO, co prawidłowo stwierdził Prezes UODO. Warto również zauważyć, że sprawa nie dotyczyła przetwarzania danych osób będących członkami organów spółek, fundacji lub stowarzyszeń. Za nietrafne Sąd uznał także odwołanie się do przepisów UPW, jako aktu prawnego, który w ocenie Spółki miałby ograniczać prawo podmiotu danych do informacji. Prawo do ponownego wykorzystywania informacji sektora publicznego nie oznacza, że dane osób fizycznych prowadzących aktualnie jednoosobową działalność gospodarczą oraz osób fizycznych, które zawiesiły wykonywanie tej działalności, wyłączone są z zakresu stosowania RODO.

Na kanwie przedmiotowego postępowania można zatem dojść do konkluzji, że przypadku ponownego wykorzystywania danych osobowych możliwość powołania się na zwolnienie z obowiązku informacyjnego w oparciu o art. 14 ust. 5 RODO będzie miała miejsce w szczególności, gdy użytkownik nie dysponuje danymi kontaktowymi umożliwiającymi podanie podmiotowi danych niezbędnych informacji wymienionych w art. 14 ust. 1 i 2. Taka sytuacja ma miejsce np. w ramach przetwarzania danych osobowych ujawnionych w KRS, w którym brak jest danych teleadresowych osób będących udziałowcami lub członkami organów spółek i innych osób prawnych, w związku z czym administrator danych osobowych musiałby poszukiwać tych danych w innych źródłach, co w ocenie organu już mogłoby stanowić „niewspółmiernie duży wysiłek”.

Drugą płaszczyzną regulacyjną, którą należy wziąć pod uwagę w kontekście obowiązku informacyjnego użytkownika – jak sygnalizowano wcześniej – są przepisy UPW.

Kolejna zmiana – dokonana nowelizacją z 21.2.2019 r. – wprowadziła w art. 7 ust. 4 UPW ograniczenie obowiązku informacyjnego wymienionego w art. 14 RODO. W tym wypadku adresatem zwolnienia z obowiązku informacyjnego będzie użytkownik, który pozyskując dane od podmiotu zobowiązanego staje się ich administratorem. Użytkownik przetwarzając dane osobowe w celu ponownego wykorzystywania nie będzie musiał podawać osobie, której dane dotyczą wszystkich informacji wymienionych w art. 14 ust. 1–4 RODO. Chodzi tu o pozyskiwanie danych osobowych z innego źródła niż podmiot danych; w omawianym przypadku od podmiotu zobowiązanego (w trybie bezwnioskowym, jak i na

wniosek). Przepis określa katalog informacji podawanych osobie, której dane dotyczą, termin spełnienia obowiązku informacyjnego, wymóg ponowienia informowania przy zmianie celu przetwarzania.

Należy podkreślić, że zwolnienie użytkowania z obowiązku informacyjnego dotyczy jedynie trzech kategorii danych wymienionych w art. 7 ust. 4 UPW, tj. danych:

1) osób pełniących funkcje publiczne mających związek z pełnieniem tych funkcji, w tym o warunkach powierzenia i wykonywania tych funkcji,
2) osób fizycznych reprezentujących osoby prawne, w tym ich dane kontaktowe,
3) obejmujących nazwę (firmę), numer identyfikacji podatkowej (NIP) albo imię i nazwisko kontrahenta podmiotu zobowiązanego.

Pierwsza sytuacja stanowi konsekwencję możliwości wykorzystywania danych osobowych osób pełniących funkcje publiczne, mających związek z pełnieniem tych funkcji o której mowa art. 5 ust. 2 UPW i art. 6 ust. 2 UPW. Zgodnie z ugruntowanym orzecznictwem sądowoadministracyjnym osobą pełniącą funkcję publiczną jest każdy, kto pełni funkcję w organach władzy publicznej lub też w strukturach osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej, jeżeli tylko funkcja ta ma związek z dysponowaniem majątkiem państwowym lub samorządowym albo zarządzaniem sprawami związanymi z wykonywaniem swych zadań przez władze publiczne, a także inne podmioty, które tę władzę realizują lub gospodarują mieniem komunalnym lub majątkiem Skarbu Państwa[909]. Najprostszym wyjaśnieniem pojęcia osoby pełniącej funkcję publiczną jest przyjęcie, że osoba, aby mogła być za taką uznana, musi w ramach instytucji publicznej realizować w pewnym zakresie nałożone na tę instytucję zadania publiczne, z wyłączeniem stanowisk usługowych i technicznych (zob. Rozdział 6.3.1).

Druga sytuacja – jak się wydaje – jest wynikiem treści motywu 14 preambuły RODO, w myśl którego rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej. Pojawia się w tym kontekście istotny dylemat interpretacyjny. Po pierwsze, motyw 14 nie znajduje odzwierciedlenia w części normatywnej rozporządzenia. Po drugie, treść motywu 14 nie odwołuje się do kategorii osoby fizycznej, tylko osoby prawnej (wprawdzie „danych osobowych osoby prawnej", które zgodnie z definicją danych osobowych wyrażonej w art. 4

[909] Zob. *I. Kamińska, M. Rozbicka-Ostrowska*, Ustawa o dostępie do informacji publicznej, 2012, s. 87; *M. Bidziński*, [w] *M. Bidziński, M. Chmaj, P. Szustakiewicz*, Ustawa o dostępie do informacji publicznej, 2010, s. 73–74.

pkt 1 RODO przynależeć mogą jedynie osobie fizycznej). Po trzecie, jeśli uznamy, że dane te nie podlegają ochronie w świetle RODO, to ograniczenie obowiązku spełnienia obowiązku informacyjnego należałoby uznać za bezprzedmiotowe. W opinii *P. Litwińskiego* motyw 14 preambuły RODO stanowi klucz do wykładni jego art. 1, który wyłącza zastosowanie rozporządzenia wobec danych osobowych przetwarzanych w związku z funkcjonowaniem osoby prawnej na rynku. Zdaniem autora zakresem wyłączenia objęte powinny być wszystkie dane osobowe gromadzone w Krajowym Rejestrze Sądowym, a służące do oznaczenia takiego podmiotu. Autor ten stwierdza: „Tym samym przetwarzanie informacji o osobach fizycznych sprawujących funkcję organów osób prawnych nie może być uznane za działanie bezprawne dopóki, dopóty przetwarzanie takie odbywa się wyłącznie w celu i zakresie niezbędnym do prawidłowej identyfikacji tych osób jako pełniących funkcję organów osób prawnych”[910]. Argumentując to stanowisko autor powołuje się na pogląd wyrażony na gruncie UODO1997, zgodnie z którym charakteru danych osobowych nie można przypisać chociażby nazwie spółki cywilnej z tego tylko względu, że występują w niej nazwiska wspólników[911], nie dlatego jednak, że nazwa spółki cywilnej nie jest informacją o osobie fizycznej, bo pozwala na zidentyfikowanie takiej osoby, ale z uwagi na ogólne wyłączenie przewidziane we wskazanym motywie 14 RODO[912].

Z kolei trzecia sytuacja, wynika z utrwalonego orzecznictwa sądowego uznającego dane osób, z którymi podmioty publiczne zawierają umowy cywilnoprawne za informacje publiczne[913]. Dla omawianego wyłączenia obowiązku informacyjnego nie będzie miało znaczenia czy kontrahentem podmiotu publicznego jest osoba fizyczna czy osoba prawa, zatem wspominane wątpliwości dotyczące interpretacji motywu 14 RODO nie będą miały znaczenia. Na marginesie należy wspomnieć, że w obowiązującym stanie prawnym dane osobowe osób fizycznych prowadzących działalność gospodarczą na gruncie RODO powinny być traktowane na równi z innymi danymi osobowymi[914]. Zgodnie z art. 43 ust. 4 ustawy - ustawy z dnia 6 marca 2018 r. Prawo przedsiębiorców[915] rejestry działalności regulowanej są jawne. Dane

[910] *P. Litwiński (red.)*, op. cit., Komentarz do art. 4, pkt 1 pkt.
[911] Zob. wyrok SN z 13.11.1997 r., I CKN 710/97.
[912] *P. Litwiński (red.)*, op. cit.
[913] Zob. wyrok SN z 8.11.2012 r., I CSK 190/12, w sprawie ujawnienia przez urząd miasta st. Warszawy nazwiska i imiona osób, z którymi miasto zawarło umowy o dzieło lub zlecenia. Prywatność nie obejmuje imion i nazwisk osób zawierających umowy cywilnoprawne z jednostkami samorządu terytorialnego.
[914] Na przestrzeni lat przed wejściem w życie ustawy z dnia 6 marca 2018 r. - Prawo przedsiębiorców stan ten ulegał zmianie na gruncie przepisów kolejnych regulacji, tj. ustaw – Prawo działalności gospodarczej i – Swobody działalności gospodarczej. Zob szerzej: *P. Fajgielski*, Jawność obrotu gospodarczego a prywatność przedsiębiorcy będącego osobą fizyczną – aspekty prawne [w:] *Arwid Mednis (red.),* Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość.
[915] Dz. U. 2018 poz. 646 z późn. zm.

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. Konsekwencją powyższego powinno być uznanie, że RODO znajduje w całości zastosowanie do przetwarzania danych osobowych dotyczących osób fizycznych prowadzących działalność gospodarczą. Na gruncie RODO nie istnieją więc żadne podstawy do wyodrębniania danych osobowych osób fizycznych prowadzących działalność gospodarczą spośród uniwersum danych osobowych objętych jego zastosowaniem[916].

Ustawodawca nie wyłączył z reżimu ochrony przedmiotowych danych osobowych, które na gruncie orzecznictwa uznaje się za jawne, a jedynie ograniczył wykonanie wobec tych osób obowiązki informacyjne przez użytkownika. Brak konieczności poinformowania podmiotu danych będzie miał istotne znaczenie dla możliwości przetwarzania danych ujawnionych w tzw. rejestrach umów. Już obecnie wiele podmiotów publicznych udostępnia na swoich stronach BIP czy na portalu dane.gov.pl rejestry zwartych umów związanych z wydatkowaniem środków publicznych. Co istotne, przedmiotowe wyłączenie obowiązku informacyjnego obejmować będzie nie tylko dane kontrahentów ujawnione na stronach internetowych, ale również te pozyskane przez użytkowników w trybie wnioskowym.

Nie można oczywiście traktować art. 7 ust. 4 jako odrębnej przesłanki legalizującej przetwarzanie danych osobowych. Podjęcie decyzji o przetwarzaniu danych osobowych w ramach informacji sektora publicznego, polegające na ujawnieniu danych do ponownego wykorzystywania przez podmiot zobowiązany, jak i wykorzystywaniu pozyskanych danych przez użytkownika, w każdym przypadku musi zostać poprzedzone oceną podstawy prawnej dla przetwarzania danych osobowych wymienionej w art. 6 ust. 1 RODO w związku z przepisami UPW.

9.5.2. Ocena modyfikacji sposobu realizacji obowiązku informacyjnego w ustawie o ponownym wykorzystywaniu informacji sektora publicznego

Reasumując wprowadzone zmiany w art. 7 UPW, należy zauważyć, że celem nowelizacji było zoptymalizowanie możliwości ponownego wykorzystywania informacji zawierających lub stanowiących dane osobowe polegające na zwolnieniu z konieczności

[916] *P. Litwiński (red.)*, op. cit., pkt 12.

spełnienia – odpowiednio przez podmiot zobowiązany lub użytkownika – obowiązków informacyjnych wymienionych w art. 13, 14 i 19 RODO. Nowe przepisy mają jednak ograniczone zastosowanie. O ile podmiot zobowiązany został generalnie zwolniony ze spełnienia obowiązku informacyjnego, o którym mowa w art. 13 ust. 3 RODO, w przypadku przetwarzania danych osobowych w ramach udostępnienia lub przekazania każdego rodzaju (kategorii) informacji sektora publicznego do ponownego wykorzystywania, o tyle zwolnienie użytkownika z wypełnienia obowiązku informacyjnego wg art. 14 RODO, dotyczy wyłącznie trzech – wymienionych w art. 7 ust. 4 UPW – kategorii informacji sektora publicznego. Oznacza to, że w odniesieniu do przetwarzania danych osobowych w ramach ponownego wykorzystywania każdego innego rodzaju (kategorii) informacji sektora publicznego niż informacje o osobach pełniących funkcje publiczne, kontrahentach podmiotu zobowiązanego i osobach fizycznych reprezentujących osoby prawne, konieczne będzie spełnienie przez użytkownika obowiązków wymienianych w art. 14 RODO. Nowa regulacja nie eliminuje zatem wątpliwości, które pojawiły się na gruncie decyzji Prezesa Urzędu Ochrony Danych Osobowych z 30.1.2019 r. (ZSPU.440.574.2018)[917] czy wspominanej już decyzji z 15.3.2019 r., w zakresie realizacji wtórnego obowiązku informacyjnego wobec osób fizycznych prowadzących działalność gospodarczą, których dane pochodzą z jawnych, publicznych rejestrów[918].

Należy jednocześnie zadać pytanie o to, czy wprowadzone w UPW ograniczenia obowiązku informacyjnego znajdują podstawy w przepisach ogólnego rozporządzenia. Wyłączenia spod obowiązków informacyjnych mogą zostać sformułowane przez prawodawcę krajowego na podstawie kompetencyjnej zawartej w art. 23 ust. 1 RODO, zgodnie z którym w prawie krajowym możliwe jest ograniczenie zakresu obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym m.in. bezpieczeństwu narodowemu lub publicznemu, zapobieganiu przestępczości, innym celom leżącym w interesie publicznym, zapobieganiu naruszeniom zasad etyki, ochronie podmiotu danych czy też egzekucji roszczeń.

Z uprawnienia tego skorzystał polski ustawodawca m.in. w przepisach art. 3–4 UODO2018 zawierających wyłączenia niektórych obowiązków z art. 13 lub 14 w przypadku

[917] Zob. https://uodo.gov.pl/decyzje/ZSPU.440.574.2018
[918] Zob. szer. *J. Byrski, H. Hoser*, Nałożenie administracyjnej kary pieniężnej, s. 76–90.

zmiany celu przetwarzania danych osobowych w ramach realizacji zadania publicznego oraz pośredniego pozyskiwania danych osobowych przez administratora wykonującego zadanie publiczne, o ile jest niezbędne dla realizacji celów, o których mowa w art. 23 ust. 1. Pojawia się zatem pytanie czy realizacja prawa do ponownego wykorzystywania informacji sektora publicznego mieści się w którymkolwiek z celów wymienionych w art. 23 RODO. Na to pytanie trzeba udzielić jednak odpowiedzi negatywnej.

W mojej opinii można przyjąć, że ustawodawca krajowy formułując ograniczenie obowiązków informacyjnych w UPW pozostał zgodny co do celów, jakie chciał osiągnąć, z prawodawcą unijnym, który wprowadził przesłanki wyłączające obowiązek informacyjny ze względu na niemożliwość lub niewspółmierny wysiłek przekazania informacji, lecz pozostał niezgodny z przepisami RODO wybierając taki instrument prawny. Adresatem bowiem art. 14 ust. 5 jest administrator wtórnie przetwarzający dane, norma w nim zawarta nie stanowi podstawy kompetencyjnej dla krajowego ustawodawcy do fakultatywnej zmiany praw lub obowiązków wynikających z RODO. Ta została sformułowana w art. 23 RODO, dla interwencji legislacyjnej muszą być spełnione przesłanki i standardy określone w tym przepisie. Ograniczenia te będą w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym służącym realizacji wartości wymienionych w tym przepisie – katalog wartości ma charakter zamknięty – oraz nie naruszą istoty podstawowych praw i wolności, a przepisy krajowe muszą zawierać określone elementy mające funkcje gwarancyjne dla procesu przetwarzania danych osobowych[919]. Po drugie, wyłączenie z art. 14 ust. 5 nie będzie miało zastosowania dla podmiotu zobowiązanego, który przetwarza dane osobowe w ramach ponownego wykorzystywania, a więc wypełniając obowiązek prawny na nim ciążący lub wykonując zadanie w interesie publicznym. Literalnie interpretując przepisy RODO podmiot zobowiązany, jeśli pozyskał dane od podmiotu danych (zakładając, że zbierając dane nie informował osoby, której dane dotyczą o celu przetwarzania jakim jest ponowne wykorzystywanie jej danych osobowych w ramach informacji sektora publicznego, co samo w sobie jest wątpliwe), będzie musiał wyklonować dyspozycję zawartą w art. 13 ust. 4 RODO.

Dostrzegam tutaj istotną lukę i niekonsekwencję w przepisach ogólnego rozporządzenia. Skoro bowiem dostęp do dokumentów urzędowych oraz prawo do ponownego wykorzystywania na mocy art. 86 RODO zostało uznane za interes publiczny, a prawodawcy krajowemu pozostawiono swobodę dookreślenia w ustawodawstwie wewnętrznym sposobu pogodzenia prawa do ochrony danych osobowych z prawem dostępu do dokumentów

[919] Por. *G. Sibiga*, Dopuszczalny, s. 20.

urzędowych oraz ponownym wykorzystywaniem informacji sektora publicznego, to niezrozumiałym jest pozbawienie go możliwości modyfikacji, ograniczenia czy wręcz wyłączenia niektórych obowiązków informacyjnych w związku z realizacją obu praw „dostępowych", o ile oczywiście w prawie krajowym zostałyby spełnione wszystkie wymogi gwarancyjne wymienione w art. 23 RODO. W mojej opinii uzupełnienie katalogu wartości wymienionych w art. 23 ust. 1 o realizację prawa dostępu do dokumentów urzędowych, a w konsekwencji prawa do ponownego wykorzystywania jest zasadne celowościowo. Wyeliminowałoby to istotną niepewność prawną, której nie usuwa możliwość powołania się przez administratora na wyłączenie, o którym mowa w art. 14 ust. 5 RODO, te bowiem zawsze może zostać poddane ocenie przez niezależny organ nadzorczy, a jak pokazuje krajowa praktyka decyzje Prezesa UODO mogą w tym zakresie budzić kontrowersje. Po drugie, jest zasadne również z punktu widzenia systemowego, realizację uprawnień „dostępowych" sam ustawodawca UE uznał za interes publiczny. Przepis art. 23 ust. 1 RODO wymienia cele (wartości) ze względu na które możliwe jest ograniczenie praw i obowiązków. Można stwierdzić, że ich obszarem wspólnym będzie dość pojemne kryterium interesu publicznego[920].

9.5. Udostępnienie lub przekazanie danych zanonimizowanych

Instrumentem ochrony danych osobowych zarówno w trybie wnioskowym, jak i bezwnioskowym, jakie podmiot zobowiązany może wziąć pod uwagę jest przekazanie lub udostępnienie do ponownego wykorzystywania zanonimizowanej informacji sektora publicznego.

Wskazuje się, że proces anonimizacji informacji jest sposobem pogodzenia względów przemawiających za umożliwieniem ponownego wykorzystywania informacji sektora publicznego w jak najszerszym zakresie z obowiązkami wynikającymi z przepisów o ochronie danych[921]. Informacje anonimowe oznaczają informacje, które nie odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, lub dane osobowe zanonimizowane w taki sposób, że podmiot, którego dane dotyczą, nie jest zidentyfikowany lub jego identyfikacja nie jest już możliwa. Co ważne, definicję legalną anonimizacji wprowadziła dopiero dyrektywa 2019/1024, choć w obrocie pojęcie to od lat pozostawało

[920] *A. Nerka*, Komentarz do art. 23, pkt 10 [w:] *M. Sakowska-Baryła (red.)*, Ogólne rozporządzenie, podobnie *P. Litwiński* (red.), op. cit., Komentarz do art. 23 pkt 3.
[921] Zob. motyw 52 preambuły dyrektywy 2019/1024.

zdefiniowane[922]. W motywie 26 dyrektywy 95/46/WE wskazano, że w celu zanonimizowania jakichkolwiek danych, dane te muszą być pozbawione wystarczającej liczby elementów tak, aby nie było już możliwości zidentyfikowania osoby, której dane dotyczą. Dane należy przetwarzać w taki sposób, aby nie istniała już możliwość wykorzystania ich do zidentyfikowania osoby fizycznej za pomocą wszystkich sposobów, jakimi może posłużyć się administrator danych lub osoba trzecia. Istotnym czynnikiem jest fakt, że przetwarzanie musi być nieodwracalne[923].

Anonimizacja powinna być brana pod uwagę jako ta forma ograniczenia, która ma pierwszeństwo przed odmową wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego zawierającej dane osobowe. Jeżeli bowiem dla ochrony prywatności jednostki wystarczające będzie zanonimizowanie jej danych w obrębie informacji przekazywanej do ponownego wykorzystywania, nie jest uzasadnione wydawanie decyzji, o której mowa w art. 23 ust. 4 UPW. Konieczność dokonania anonimizacji nie może być utożsamiana z odmową wyrażenia zgody na ponowne wykorzystywanie. Odmowa ta powinna mieć miejsce wtedy, gdyby anonimizacja danych nie zapewniła ochrony prywatności jednostki, bądź w przypadku, gdyby charakter lub zakres informacji, która miałaby być przedmiotem ponownego wykorzystywania, przez wzgląd na prywatność nie pozwalał na wyrażenie takiej zgody"[924].

Jak wskazuje *M. Sakowska-Baryła*, odmowa zgody na ponowne wykorzystywanie z uwagi na prywatność osoby fizycznej wchodzi w rachubę tylko w przypadku ubiegania się o ponowne wykorzystywanie informacji w trybie wnioskowym (art. 23 ust. 4 UPW). Oznacza to, że w przypadku udostępniania ISP w systemie teleinformatycznym, a w szczególności na stronie podmiotowej BIP podmiotu zobowiązanego lub w CRIP bądź w inny sposób, ograniczenie, o którym tu mowa, będzie sprowadzać się w głównej mierze do odpowiedniej anonimizacji danych, ewentualnie do nieudostępniania treści dotyczących prywatności jednostki.

W przypadku braku podstawy dla przekazania lub udostępnienia danych osobowych w ramach informacji sektora publicznego, należy rozważyć dwa scenariusze. W pierwszym przypadku ochrona danych osobowych (przesłanka ograniczenia ponownego wykorzystywania w oparciu o prywatność osoby fizycznej) może stanowić podstawę dla odmowy przekazania

[922] Zob. *Grupa Robocza Art. 29*, Opinia 05/2014 w sprawie technik anonimizacji, 10.04.2014 (WP 216), s. 2.
[923] Ibidem, s. 5-6.
[924] *M. Sakowska-Baryła*, Ograniczenia prawa do ponownego wykorzystywania ISP [w:] *E. Badura, M. Błachucki, X. Konarski, M. Maciejewski, H. Niestrój, A. Piskorz-Ryń, M. Sakowska-Baryła, G. Sibiga, K. Ślaska*, op. cit., s. 75-76.

w trybie wnioskowym informacji sektora publicznego (art. 23 ust. 1 pkt 4 w zw. z art. 6 ust. 2 UPW). Sytuacja ta będzie miała miejsce przede wszystkim w odniesieniu do informacji sektora publicznego stanowiących dane osobowe, kiedy nie jest możliwe częściowe przekazanie informacji niezawierającej danych osobowych (stanowiących przesłankę ograniczającą ponowne wykorzystywanie) po ich anonimizacji, np. przedmiotem wniosku o przekazanie do ponownego wykorzystywania będą informacje o stanie zdrowia osoby fizycznej. W drugim wypadku należy rozważyć czy możliwe jest przekazanie lub udostępnienie danych zanonimizowanych. Sytuacja ta będzie miała miejsce przede wszystkim w odniesieniu do informacji sektora publicznego zawierającej dane osobowe, które można trwale usunąć, np. w dokumencie urzędowym zawarte są dane identyfikujące osobę fizyczną, która nie jest osobą pełniącą funkcje publiczne. Informacja sektora publicznego, co prawda nie jest już nośnikiem danych osobowych, ale wciąż posiada walor informacyjny dla użytkownika. W tym wypadku należy zadbać przede wszystkim o to, aby dane osobowe zostały odpowiednio zanonimizowane, a więc przekształcone w taki sposób, aby nie było możliwe przyporządkowanie wchodzących w ich skład informacji zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Właśnie anonimizacja informacji udostępnianych i przekazywanych do ponownego wykorzystywania służy bowiem poszanowaniu prywatności jednostki i jej prawa do ochrony danych osobowych. Takie informacje nie stanowią danych osobowych w rozumieniu RODO, choć trzeba zadbać o to, by proces anonimizacji nie okazał się odwracalny[925].

W ramach wykorzystywaniu informacji sektora publicznego przedmiotem zainteresowania użytkowników mogą pozostawać różne informacje, w tym niekoniecznie dane osobowe. Poszczególne informacje oddane do dyspozycji zainteresowanym potencjalnie mogą okazać się danymi osobowymi, gdy bez nadmiernych kosztów, czasu czy działań da się ustalić, kogo dotyczą. Niewykluczone jest, że dane powszechnie dostępne, nawet rozbite na "kwanty informacyjne" pochodzące z różnych zasobów w procesie ponownego wykorzystywania połączone ze sobą lub z innymi informacjami mogą pozwolić na uzyskanie (wtórne) informacji dotyczącej konkretnej osoby. Mówić tu możemy o synergii informacji, czyli efekcie zwielokrotnienia siły informacji przez zwiększenie jej zasobu, bo łączne rozpatrywanie kilku komunikatów wywołuje większy efekt, gdy wzajemnie się one wzmacniają i uzupełniają[926]. Przy niemal nieograniczonych możliwościach technicznych informacje mogą być pozyskiwane

[925] *M. Sakowska – Baryła*, Komentarz do art. 86 RODO, pkt 6 [w:] *M. Sakowska – Baryła (red.)*, Ogólne rozporządzenie.
[926] *Ibidem.*

z różnych źródeł, w tym z rejestrów publicznych, i w różnym zakresie łączone lub przekształcane, także w taki sposób, który finalnie pozwala ustalać tożsamość osoby i dowolnie z niej skorzystać[927].

Należy zwrócić uwagę, że nawet w przypadku, gdy zostaną przekazane lub udostępnione wyłącznie dane anonimowe, może dochodzić do przetwarzania danych osobowych przez podmiot zobowiązany (administratora) na etapie wcześniejszym poprzedzającym udzielnie danych, bowiem sam proces anonimizacji danych jest operacją na danych osobowych. Anonimizacja stanowi przetwarzanie danych osobowych, w związku z tym musi spełniać wymóg zgodności poprzez uwzględnienie podstaw prawnych i okoliczności dalszego przetwarzania[928]. Przetworzenie danych musi mieć swoją podstawę prawną, za którą w tym przypadku należy uznać, art. 6 ust. 1 lir. c RODO (przetwarzanie jest niezbędne do wykonania obowiązku prawnego ciążącego na administratorze) w zw. art. 5 pkt 2 UPW (w przypadku przekazania danych zanonimizowanych na wniosek użytkownika) lub w zw. z art. 5 pkt 1 UPW (w przypadku udostępnienia danych z własnej inicjatywy na BIP, portalu otwartych danych czy innej stronie internetowej urzędu).

Anonimizacja może być środkiem zachowania korzyści i ograniczenia ryzyka. Gdy zbiór danych jest prawidłowo zanonimizowany, nie ma już możliwości zidentyfikowania poszczególnych osób fizycznych, wówczas prawo o ochronie danych nie ma dalej zastosowania. Utworzenie prawdziwie anonimowego zbioru danych na podstawie bogatego zbioru danych osobowych przy jednoczesnym zachowaniu odpowiedniej ilości informacji podstawowych niezbędnych na potrzeby wykonania procesu nie jest jednak łatwe do zrealizowania. Na przykład zbiór danych uważany za anonimowy może być połączony z innym zbiorem danych w taki sposób, że istnieje możliwość zidentyfikowania co najmniej jednej osoby fizyczne[929].

[927] *W.R. Wiewiórowski*, Ponowne wykorzystywanie informacji, s. 392 i 394; *P. Drobek, A. Piskorz-Ryń*, Prawne problemy ponownego wykorzystania, s. 220–222.
[928] *Grupa Robocza Art. 29*, Opinia 5/2014, s. 2.
[929] *Ibidem*, s. 5.

Rozdział 10. Realizacja innych obowiązków i uprawnień wynikających z ogólnego rozporządzenia w ramach ponownego wykorzystywania informacji sektora publicznego

10. 1. Obowiązki wynikające z podstawowych zasad przetwarzania danych

Ponowne wykorzystywanie informacji sektora publicznego stanowiących lub zawierających dane osobowe pociąga za sobą konieczność przestrzegania wszystkich podstawowych zasad dotyczących przetwarzania danych osobowych wymienionych w art. 5 RODO. Do ich przestrzegania i wdrażania zobowiązany jest administrator danych osobowych, którym może być zarówno podmiot zobowiązany, jak i użytkownik. Zasady te stanowią źródło, z jednej strony określonych obowiązków po stronie administratora, z drugiej wynikają z nich uprawnienia osób, których dane dotyczą. Omówione wcześniej zasady legalności i ograniczenia celu warunkują w ogóle dopuszczalność ponownego wykorzystywania danych osobowych. Wynikający z zasady przejrzystości obowiązek informacyjny nie jest jedynym obowiązkiem, którego wykonanie wiąże się z ujawnieniem danych osobowych w ramach informacji sektora publicznego. Niemniej w omawianym kontekście uważam go za kluczowy. Tylko skutecznie poinformowana osoba, której dane są przetwarzane w ramach ponownego wykorzystywania może zdecydować o skorzystaniu z uprawnień przysługujących jej na gruncie przepisów o ochronie danych osobowych. Ponadto skorzystanie z niektórych uprawnień przez podmiot danych (sprostowanie, usunięcie i ograniczenie przetwarzania) powoduje konieczność po stronie administratora do spełnienia wtórnego obowiązku informacyjnego. W praktyce – jak wykazano – realizacja zasady przejrzystości w ramach ponownego wykorzystywania może stanowić istotne wyzwanie.

Inne wymogi wynikające z konieczności przestrzegania pozostałych zasad przetwarzania danych nie mają tak istotnego znaczenia dla samej realizacji prawa do ponownego wykorzystywania informacji sektora publicznego, niemniej muszą być respektowane, jeżeli do przetwarzania danych osobowych w ramach ponownego wykorzystywania dojdzie. Administrator danych (zarówno podmiot zobowiązany, jak i użytkownik) jest zatem zobligowany wykonywania również zasady minimalizacji danych, prawidłowości, ograniczenia przechowywania oraz integralności i poufności.

Podmiot zobowiązany i użytkownik będący administratorem danych osobowych obowiązany jest do wdrożenia odpowiednich środków organizacyjno-technicznych, które zapewnią, że dane osobowe będą przetwarzane zgodnie z prawem, merytorycznie poprawne, adekwatne do celów pozyskania oraz odpowiednio zabezpieczone, by ich przetwarzanie nie

naruszało praw i wolności osób fizycznych. Istotne jest także, aby administrator przetwarzał dane osobowe wyłącznie przez czas niezbędny dla realizacji celów pozyskania danych lub czas wynikający z przepisów prawa powszechnie obowiązującego.

Kluczowe jest to, by administrator był w stanie wykazać przestrzeganie zasad przetwarzania danych osobowych, w myśl z nakazem rozliczalności (art. 5 ust. 2 RODO). Biorąc pod uwagę całość norm ogólnego rozporządzenia podkreślić należy, że administrator ma znaczną swobodę w zakresie stosowanych zabezpieczeń, jednocześnie jednak ponosi odpowiedzialność za naruszenie przepisów o ochronie danych osobowych. Z zasady rozliczalności wprost wynika, że to administrator danych powinien wykazać, a zatem udowodnić, że przestrzega przepisów określonych w art. 5 ust. 1 RODO.

10.1.1. Prawidłowość danych osobowych

W kontekście ponownego wykorzystywania informacji sektora publicznego istotna niewątpliwe będzie zasada prawidłowości (zob. Rozdział 5.1.6). Zasada ta bywa również określana mianem prawdziwości danych, merytorycznej poprawności bądź zgodności danych z prawdą[930].

Wymóg prawidłowości danych ma oczywiście istotne znaczenie zarówno z perspektywy podmiotu danych, jak i użytkownika ponownie wykorzystującego dane osobowe. Obowiązkiem administratora jest niezwłoczne usunięcie lub sprostowanie danych, które są nieprawidłowe w świetle celów ich przetwarzania. Pojawia się pytanie czy realizacja zasady prawidłowości pociąga za sobą obowiązek systematycznego poszukiwania danych osobowych nieprawidłowych. Należy podzielić zdane komentatorów, że w praktyce tego rodzaju podejście byłoby niezwykle trudne do realizacji, nie tylko ze względu na ilość przetwarzania danych, ale także na problemy dotyczące weryfikacji ich poprawności[931]. Na gruncie RODO obowiązek ten należałoby interpretować jako obowiązek uaktualniania danych „w razie potrzeby", w wyniku otrzymanych informacji dotyczących nieprawidłowości. Niemniej na gruncie realizacji obowiązków wynikających z UPW należałoby postulować, żeby administrator danych oceniał wiarygodność źródeł ich pozyskania, a przed udostępnieniem lub przekazaniem do ponownego wykorzystywania zweryfikował ich prawdziwość i prawidłowość[932].

[930] *P. Fajgielski*, Komentarz, 2018, s. 152.
[931] *Ibidem.*
[932] Zob. *M. Sakowska-Baryła*, Dostęp do informacji publicznej a ochrona danych osobowych, s. 397.

Z zasady prawidłowości danych wynikają uprawnienia osób, których dane są przetwarzane. W szczególności należy wymienić prawo do żądania niezwłocznego sprostowania nieprawidłowych danych oraz uzupełnienia danych niekompletnych, a także prawo do usunięcia danych.

Dla ponownego użytkownika, który wykorzystuje w ramach swojej aktywności informacje sektora publicznego (np. opiera modele działalności gospodarczej na przetwarzaniu danych) fundamentalne jest, aby dane, które pozyskuje z publicznych źródeł gwarantowały ich prawidłowość, rzetelność, aktualność i zgodność z prawdą. Wymogi te powinny zostać spełnione przez podmiot zobowiązany niezależnie od trybu dystrybucji informacji. Na tym tle szczególną rolę odgrywają warunki ponownego wykorzystywania, w ramach których podmiot zobowiązany może nałożyć na użytkownika obowiązek poinformowania o źródle, czasie wytworzenia i pozyskania informacji. Co istotne, warunki te chronią użytkownika końcowego produktu, usługi czy aplikacji, w której wykorzystywane są dane (zob. Rozdział 4.4.2), dzięki którym ma wiedzę o źródle pochodzenia danych i ich aktualności.

Istotnym zagadnieniem z perspektywy użytkownika danych jest kwestia odpowiedzialności podmiotu zobowiązanego za przekazanie lub udostępnienie nieprawidłowych danych osobowych w ramach informacji sektora publicznego. Problematykę tę należy w mojej opinii rozpatrywać w szerszym kontekście, tj. prawidłowości, czyli merytorycznej poprawności, aktualności oraz zgodności z prawem samej informacji sektora publicznego dystrybuowanej do ponownego wykorzystywania. Z jednej strony udzielenie informacji niespełniającej kryterium prawidłowości (np. przekazanie informacji nieprawdziwych czy niepełnych) może stanowić przyczynę wniesienia skargi na bezczynność w przedmiocie nieudostępnienia informacji sektora publicznego na wniosek[933]. Z drugiej strony, należy rozpatrzeć potencjalną odpowiedzialność cywilnoprawną z uwagi na ponowne wykorzystywanie informacji w drodze przyjętej oferty zawierającej warunki lub opłaty (zob. Rozdział 4.3.2). W tym zakresie wątpliwości jakie mogą się pojawić, dotyczą możliwości uwzględnienia w warunkach ponownego wykorzystywania kwestii odpowiedzialności podmiotu zobowiązanego za aktualność czy kompletność przekazywanych informacji sektora publicznego. *De lege lata* art. 14 ust. 1 pkt 3 UPW stanowi o możliwości określenia „zakresu odpowiedzialności podmiotu zobowiązanego za udostępniane lub przekazywane informacje", które często w praktyce stosowania przepisów sprowadzają się do informowania o wyłączeniu

[933] Tak na gruncie UDIP *M. Sakowska-Baryła*, op. cit., s. 307.

odpowiedzialności podmiotu zobowiązanego[934]. Dostrzegam tutaj przestrzeń, która powinna zostać doregulowana wprost w przepisach UPW. Postulowanym *de lege ferenda* rozwiązaniem byłoby uzupełnienie katalogu fakultatywnych warunków ponownego wykorzystywania o określenie zakresu odpowiedzialności podmiotu zobowiązanego za prawidłowość informacji sektora publicznego. Wówczas w przypadku zawarcia umowy o ponowne wykorzystywanie w trybie ofertowym nieprzestrzeganie warunków dotyczących prawidłowości przez podmiot zobowiązany powinno być kwalifikowane jako niewykonanie lub nienależyte wykonanie zobowiązania w rozumieniu przepisów KC. Problematyka ta ma istotny wymiar dla tworzenia produktów i usług wykorzystujących dane. Ze względu na nakłady inwestycyjne, ciągłość biznesową tego typu przedsięwzięć oraz bezpieczeństwo obrotu ponowni użytkownicy powinni mieć pewność co do prawidłowości danych, służących jako materiał wyjściowy dla innowacyjnych zastosowań i podstawy prawne dla jej wyegzekwowania.

10.1.2. Czasowe ograniczenie przetwarzania danych osobowych

Zasada czasowego ograniczenia przetwarzania danych oznacza, że dane osobowe powinny być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane są przechowywane (zob. Rozdział 5.1.7.). Zasada odnosi się zarówno do podmiotu zobowiązanego, jak i użytkownika, ale odmiennie będzie postrzegana realizacja tej zasady dla tych dwóch różnych kategorii administratorów.

Niewątpliwie ponowne wykorzystywanie, co do zasady, nie wiąże się z żadnym z celów wymienionych w art. 5 ust. 1 lit. e RODO, które uzasadniałoby możliwość dłuższego przechowywania danych (cele statystyczne, archiwalne w interesie publicznym, badań naukowych lub historycznych). Oznacza to, że również w ramach ponownego wykorzystywania danych osobowych, po osiągnięciu celów przetwarzania dane powinny zostać usunięte albo zanonimizowane.

[934] Np. „Naczelny Sąd Administracyjny nie ponosi odpowiedzialności za dalsze udostępnienie informacji (przez podmioty powtórnie je wykorzystujące) z naruszeniem przepisów regulujących ich ochronę (dot. ochrony danych osobowych lub tajemnic ustawowo chronionych, ochrony prawa do prywatności), a także za informacje pozyskane w sposób inny niż określony w pkt 1 lub z pominięciem procedury wnioskowej”. http://www.nsa.gov.pl/ponowne-wykorzystywanie-informacji-sektora-publicznego/warunki-ponownego-wykorzystywania-informacji-sektora-publicznego,news,95,94.php (dostęp: 15.03.2021)

W odniesieniu do niektórych procesów przetwarzania danych przepisy prawa wyraźnie wskazują okresy przechowywania danych (jako przykład można wskazać przepisy dotyczące przechowywania dokumentacji osobowej pracowników[935]).

Jednakże w wielu przypadkach brak normatywnego rozstrzygnięcia tej kwestii powoduje, że to na administratorze spoczywa obowiązek dokonania oceny, czy cele zostały osiągnięte, czy też nie, i czy dane są mu nadal potrzebne. W praktyce dokonanie tego rodzaju oceny może stanowić pewne wyzwanie[936]. Taka sytuacja będzie miała miejsce w ramach realizacji prawa do ponownego wykorzystywania informacji sektora publicznego zawierających dane osobowe. Przepisy UPW nie zawierają w przedmiocie retencji danych osobowych żadnych, nawet szczątkowych regulacji, które wskazywałyby w jakim okresie możliwe jest przetwarzanie danych osobowych ujawnionych w celu ponownego wykorzystywania.

Z tego powodu administrator, który pozyskał dane osobowe w ramach informacji sektora publicznego, samodzielnie będzie musiał w danym stanie faktycznie rozstrzygać, czy osiągnął własne cele przetwarzania danych osobowych. Może się to okazać niezwykle problematyczne, bowiem w przeciwieństwie do realizacji dostępu do informacji publicznej, użytkownik na gruncie UPW nie ma na celu zapoznania się z informacją, co zakłada pewną „jednorazowość" czynności po jego stronie. Upraszczając można przyjąć, że celem użytkownika może być „wielokrotne" wykorzystywanie informacji, które zakłada określoną ciągłość tego procesu przetwarzania danych (np. wykorzystywanie danych w aplikacjach czy serwisach internetowych). Dane osobowe mogą zatem być potrzebne użytkownikowi tak długo, jak uzasadniają to cele gospodarcze produktu czy usługi, w ramach których dochodzi do przetwarzania danych osobowych.

Adresatem zasady czasowego ograniczenia przetwarzania danych jest również podmiot zobowiązany ujawniający dane osobowe w ramach informacji sektora publicznego. Udostępnienie lub przekazanie danych osobowych w trybie UPW nie stanowi – jak wykazano – pierwotnego celu przetwarzania danych osobowych, dla którego zostały one przez podmiot zobowiązany zebrane. Realizacja celu polegająca na przekazaniu lub udostępnieniu danych osobowych w ramach ponownego wykorzystywania informacji sektora publicznego nie

[935] Zgodnie z art. 94 pkt 1b ustawy z dnia 26 czerwca 1974 r. - Kodeks pracy (t.j. Dz. U. z 2020 r. poz. 1320) pracodawca jest obowiązany w przechowywać dokumentację pracowniczą w sposób gwarantujący zachowanie jej poufności, integralności, kompletności oraz dostępności, w warunkach niegrożących uszkodzeniem lub zniszczeniem przez okres zatrudnienia, a także przez okres 10 lat, licząc od końca roku kalendarzowego, w którym stosunek pracy uległ rozwiązaniu lub wygasł, chyba że odrębne przepisy przewidują dłuższy okres przechowywania dokumentacji pracowniczej.
[936] *P. Fajgielski*, Komentarz, 2018, s. 154.

wpływa na – co do zasady – na pierwotny cel przetwarzania danych, „który zwykle pozostaje realizowany i występuje niezależnie od owego wtórnego celu przetwarzania”[937]. Na podstawie przepisów UPW kreujących po jednej stronie uprawnienie do otrzymania informacji w celu ponownego jej wykorzystywania, z drugiej zaś obowiązek przekazania lub udostępnienia informacji, trudno ustalić czas przetwarzania danych niezbędny do osiągnięcia celu przetwarzania zwłaszcza, gdy w trybie bezwnioskowego ponownego wykorzystywania nie jest on podmiotowi zobowiązanemu w ogóle znany.

W mojej opinii w przypadku informacji sektora publicznego, które są udostępnione na wniosek, czas przechowywania po stronie podmiotu zobowiązanego jest zdeterminowany podstawowym celem, dla którego dane osobowe są pierwotnie zbierane. Celem zebrania danych przez podmiot zobowiązany nie było ich przekazanie do ponownego wykorzystywania. Innymi słowy realizacja przez podmiot zobowiązany zasady ograniczenia przechowywania następuje w oderwaniu od przepisów o ponownym wykorzystywaniu.

W przypadku zaś bezwnioskowego trybu ponownego wykorzystywania konieczne jest odwołanie się do przepisów „dostępowych” kreujących obowiązek publikacji pewnych danych osobowych w systemach teleinformatycznych, w szczególności w BIP i centralnym repozytorium. Jest to szczególnie istotne w związku dopuszczalnością bezwarunkowego ponownego wykorzystywania tak udostępnionych informacji. Niestety zarówno przepisy UDIP i rozporządzenia w sprawie w sprawie Biuletynu Informacji Publicznej, jak i rozporządzenia w sprawie w sprawie centralnego repozytorium informacji publicznej oraz rozporządzenia w sprawie zasobu informacyjnego przeznaczonego do udostępniania w centralnym repozytorium informacji publicznej w ogóle nie wskazują czasowego zakresu udostępniania informacji, a przepisy ustaw szczególnych czynią to niezwykle rzadko.

Jako przykład (dość niefortunny z uwagi na brak jednoznacznego wskazania maksymalnego terminu) można podać ustawę z dnia 21 listopada 2008 r. o pracownikach samorządowych[938], która w art. 15 stanowi, że niezwłocznie po przeprowadzonym naborze informacja o wyniku naboru jest upowszechniana przez umieszczenie na tablicy informacyjnej w jednostce, w której był przeprowadzony nabór, oraz opublikowanie w Biuletynie przez okres co najmniej 3 miesięcy. Z kolei maksymalny czas przechowywania danych przewidują przepisy nakładające obowiązek składania oświadczeń majątkowych przez niektórych funkcjonariuszy publicznych. Przykładowo w ustawie o samorządzie gminnym, która w art. 24h ust. 6 wskazuje

[937] Należy podzielić pogląd *M. Sakowskiej – Baryły* prezentowany na gruncie UDIP. Zob. tej autorki: Dostęp do informacji publicznej a ochrona danych osobowych, s. 311.
[938] t.j. Dz. U. z 2019 r. poz. 1282.

sześcioletni termin przechowywania oświadczenia majątkowego. Należy zatem ten okres przyjąć jako maksymalny również dla publikacji oświadczenia w BIP, którego obowiązek przewidują przepisy (zob. Rozdział 7.2.1). Po jego upływie przetwarzanie danych trzeba uznać za niedopuszczalne. Termin ten dotyczy zarówno oświadczeń złożonych przez osoby, które przestały już pełnić swoją funkcję, jak i przez te, które ją nadal sprawują, a których oświadczenie, z uwagi na konieczność złożenia kolejnego, aktualnego oświadczenia o stanie majątkowym, stało się nieaktualne.

W mojej opinii terminy te nie obowiązują użytkownika, które pozyskał dane z BIP w celu ponownego wykorzystywania. Wobec braku sprecyzowania w przepisach prawa dopuszczalnych ram czasowych, w jakich może on ponownie wykorzystywać dane osobowe, należy stosować regułę ogólną wynikającą z art. 5 ust. 1 lit. e, a więc sprawdzenie czy przechowywanie uzasadnione jest celem, w jakim dane są przetwarzane (ponownie wykorzystywane).

Jeśli przepisy nie precyzują okresu udostępniania – ani minimalnego, ani maksymalnego – nie oznacza to, że dane osobowe mają być udostępniane bezterminowo. Skoro w BIP (jak i w centralnym repozytorium) udostępniane są informacje, co do których przepisy nie wskazują okresu udostępnienia, to administrator (podmiot zobowiązany), po przeprowadzeniu analiz, powinien określić ten okres tak, aby przetwarzanie danych było zgodne z celami, z którymi je pozyskano. Zasada ograniczenia czasowego udostępnienia danych osobowych w BIP (lub CRIP) oznacza, że nawet jeśli określone dane odpowiadają celowi, dla którego są zbierane, to – zdaniem PUODO – nie powinny być przetwarzane, w tym udostępniane innym podmiotom bez żadnego czasowego ograniczenia. Czasowym wyznacznikiem powinno być osiągnięcie celu przetwarzania[939]. Naruszeniem ochrony danych osobowych jest brak określenia w procedurach wewnętrznych terminu usuwania danych opublikowanych w BIP, jak również brak procedur dotyczących przeglądu danych pod kątem zapewnienia przetwarzania danych zgodnie z zasadą ograniczenia przechowywania[940]. Przedmiotowa procedura regulować ma istotne dla procesu przetwarzania danych osobowych czynności na tych danych w celu zapewnienia realizacji zasady ograniczenia przechowywania, dlatego należy ją traktować jako politykę ochrony danych, o której mowa w art. 24 ust. 2 RODO. W konsekwencji, podmiot zobowiązany musi być w stanie wykazać istnienie tego rodzaju dokumentu oraz jego przestrzeganie, w kontekście zasady rozliczalności wyrażonej

[939] Zob. Decyzja Prezesa Urzędu Ochrony Danych Osobowych z 18.10.2019 r., nr ZSPU.421.3.2019.
[940] *Ibidem.*

w art. 5 ust. 2 RODO. Zgodnie ze stanowiskiem UODO zawartym w decyzji z 18 października 2019 r., powinny zostać uregulowane kwestie usuwania informacji z BIP, ich archiwizacji, cyklicznych sprawdzań i przeglądu zawartości, z tym zastrzeżeniem, że czas przechowywania (publikowania) określonych informacji w BIP uzależniony jest od: przepisów, które wprost wskazują, przez jaki okres czasu określone informacje muszą zostać podane do publicznej wiadomości; ustania celu publikowania informacji, o ile przepis szczególny nie stanowi inaczej; aktualności zamieszczonych informacji.

Problematyka okresu w jakim udostępniania się informację w BIP było przedmiotem wypowiedzi sądów administracyjnych już na gruncie UODO1997. WSA w Lublinie wyrokiem z 1.3.2016 r., II SA/Lu 876/15 stwierdził, że z art. 26 ust. 1 pkt 4 UODO1997 „wynika zasada ograniczenia czasowego udostępnienia danych osobowych w Biuletynie Informacji Publicznej. Zasada ta oznacza, że nawet jeśli określone dane odpowiadają celowi, dla którego są zbierane, to nie powinny być przetwarzane, w tym udostępniane innym podmiotom *ad finitum*. Czasowym wyznacznikiem powinno być natomiast osiągnięcie celu przetwarzania".

10.1.3. Integralność i poufność przetwarzania

Administrator odpowiada za integralność i poufność przetwarzania danych osobowych (zob. Rozdział 5.1.8). Oznacza to, że zarówno podmiot zobowiązany do przekazania lub udostępnienia danych osobowych w ramach informacji sektora publicznego, jak i użytkownik ponownie je wykorzystujący, są zobligowani jest do przetwarzania ich w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (art. 5 ust. 1 lit. f RODO).

Z obowiązkiem tym wiąże się wdrożenie odpowiednich środków technicznych i organizacyjnych, mających na celu zabezpieczenie danych, o których mowa w art. 32 ogólnego rozporządzenia. Przepis ten nie wymaga od administratora danych wdrożenia jakichkolwiek środków technicznych i organizacyjnych, które mają stanowić środki ochrony danych osobowych, ale wymaga wdrożenia środków adekwatnych. Taką adekwatność oceniać należy pod kątem sposobu i celu, w jakim dane osobowe są przetwarzane, ale też należy brać pod uwagę ryzyko związane z przetwarzaniem tych danych osobowych, które to ryzyko charakteryzować się może różną wysokością. W mojej opinii taka analiza ryzyka powinna być elementem oceny skutków dla ochrony danych osobowych, którą podmiot zobowiązany powinien każdorazowo przeprowadzać przed przekazaniem danych osobowych do ponownego

wykorzystywania na wniosek, jak i udostępnieniem ich w systemie teleinformatycznym (zob. Rozdział 9.2). Przyjęte środki mają mieć charakter skuteczny, w konkretnych przypadkach niektóre środki będą musiały być środkami o charakterze niwelującym niskie ryzyko, inne – muszą niwelować ryzyko wysokie, ważne jednak jest – zdaniem WSA w Warszawie - aby wszystkie środki (a także każdy z osobna) były adekwatne i proporcjonalne do stopnia ryzyka[941].

W tym aspekcie kluczowego znaczenia nabierają standardy techniczne systemów teleinformatyczne, które służą do dystrybucji informacji sektora publicznego do ponownego wykorzystywania. Muszą one zapewniać, że ewentualna awaria techniczna, nie spowoduje utraty danych i nie uniemożliwi administratorowi danych osobowych przywrócenia ich dostępności. Podmiot zobowiązany udostępniający dane musi zapewnić integralność, dostępność i odporność systemów i usług przetwarzania. Ma to szczególne znaczenie dla udostępniania danych w czasie rzeczywistym poprzez interfejsy programowania aplikacji, które umożliwiają profesjonalnym użytkownikom stały i bezpośredni dostęp do danych z publicznych baz czy państwowych rejestrów[942].

10.1.4. Minimalizacja danych osobowych

Zasada minimalizacji danych osobowych oznacza, żeby dane (rodzajem, treścią czy zakresem) nie wykraczały poza potrzeby wynikające z celu ich przetwarzania, a więc były dla osiągniecia tych celów niezbędne (art. 5 ust. 1 lit. c; zob. Rozdział 5.1.5.). Realizacja tej zasady na gruncie UPW wymaga zatem, aby ujawnianie dane do ponownego wykorzystywania nie były w zakresie szerszym niż wymaga do tego realizacja prawa do ponownego wykorzystywania informacji sektora publicznego. Kwestię tę należy rozpatrywać oddzielnie dla dwóch trybów dystrybucji informacji sektora publicznego.

Po pierwsze, podmiot zobowiązany nie powinien przekazywać danych osobowych w zakresie przekraczającym żądanie użytkownika przedstawione we wniosku. Oznacza to, że maksymalny zakres danych osobowych, które potencjalnie mogą zostać przekazane to ponownego wykorzystywania określa wstępnie sam użytkownik (który podlega weryfikacji przez podmiot zobowiązany). Oczywiście w wyniku zbadania podstaw prawnych przetwarzania danych osobowych czy przesłanek ograniczających ponowne wykorzystywanie

[941] Wyrok z 26.08.2020, II SA/Wa 2826/19.
[942] Przykładem takiego rejestru jest REGON, do którego dostęp jest możliwy za pośrednictwem API. https://api.stat.gov.pl/Home/RegonApi

może w ogóle nie dojść do przekazania danych osobowych, przekazane zostaną dane zanonimizowanie lub jedynie część żądanych danych w zakresie w jakim to będzie prawnie dopuszczalne.

Po drugie, podmiot zobowiązany nie powinien udostępniać do ponownego wykorzystywania danych osobowych w zakresie nadmiarowym niż to wynika z przepisów prawa. W tym wypadku należy wziąć pod uwagę przepisy przewidujące obowiązek publikacji danych osobowych w systemach teleinformatycznych, w tym przede wszystkim w BIP i centralnym repozytorium. Zakres danych osobowych ujawnionych w ten sposób jest zdeterminowany właściwym przepisom przewidującym obowiązek publikacji danych informacji. W tym wypadku respektowanie zasady minimalizacji (adekwatności) polega na tym, aby ujawniane były wyłącznie te dane osobowe, które nie należą do zbędnych z punktu widzenia udostępnianej informacji, w tym nie należały do nieistotnych, nadmiernie szczegółowych, szerszych niż wymaga tego dostęp do informacji[943].

Z zasadą minimalizacji wiąże się nowy rozwiązanie w systemie ochrony danych osobowych, wprowadzone przepisami ogólnego rozporządzenia, a więc uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych (art. 25 RODO). Nowe podejście jest wyrazem proaktywnego i prewencyjnego zabezpieczenia praw przysługujących podmiotowi danych. Jego celem jest rezygnacja z wszelkich aspektów przetwarzania danych prowadzących lub mogących prowadzić do ich naruszania czy ograniczania nawet w przypadku, gdy samo przetwarzanie uzna się za konieczne i prawnie dopuszczalne. Już od samego początku przetwarzania, a nawet fazie projektowania danego procesu, aż do jego zakończenia, przetwarzaniu danych towarzyszyć będzie dążenie do minimalizacji przetwarzanych danych, obejmujące maksymalne ograniczenie zakresu i czasu przetwarzania, nieprowadzące jednak do uniemożliwienia realizacji praw jednostki oraz dostępu do przetwarzanych informacji (również wewnątrz struktury administratora)[944].

10.2. Realizacja uprawnień osób, których dane dotyczą

Osobie, której dane dotyczą w związku ponownym wykorzystywaniem jej danych osobowych zawartych w informacji sektora publicznego przysługiwać będę wszystkie uprawnienia wymienione w rozdziale III RODO (zob. Rozdział 5.2). Wynika to wprost

[943] *M. Sakowska-Baryła*, op. cit., s. 308.
[944] *K. Wygoda*, Komentarz do art. 25, pkt 1 [w:] *M. Sakowska-Baryła (red.),* Ogólne rozporządzenie.

z wyrażonej w motywie 154 preambuły RODO i art. 2 ust. 4 dyrektywy 2019/1024 normy, zgodnie z którą przepisy o ponownym wykorzystywaniu nie wpływają na stopień ochrony osób fizycznych w związku z przetwarzaniem danych osobowych wynikający z przepisów prawa Unii i prawa państwa członkowskiego, a w szczególności nie zmieniają obowiązków i praw przewidzianych w ogólnym rozporządzeniu. W związku z ponownym wykorzystywaniem danych osobowych kluczowego znaczenia – w mojej opinii – nabierają uprawnienia informacyjne, z którymi wiążą się obowiązki administratora będącego podmiotem zobowiązanym (zob. Rozdział 9.51.1), jak i użytkownikiem (zob. Rozdział 9.5.2). Nie oznacza to deprecjacji pozostałych uprawnień, żadnego z nich w świetle przepisów nie można z góry wykluczyć, choć wydaje się, że w praktyce nie wszystkie uprawnienia podmiotu danych wymienione w art. 12-22 RODO będą mogły być wykonywane w związku z ponownym wykorzystywaniem.

W ramach współstosowania przepisów UPW oraz RODO marginalne znaczenie będzie miało prawo do przenoszenia danych, o którym mowa w art. 20 RODO (zob. Rozdział 5.2.7). Uprawnienie to przysługuje jedynie w przypadku, gdy podstawą po przetwarzania danych była zgoda lub niezbędność dla wykonania umowy. Jak wykazano przesłanki zgody na ponowne wykorzystywanie danych osobowych nie można wykluczyć, lecz w praktyce będzie miała ona znikome znaczenie. Przesłanka niezbędności dla wykonania umowy w ramach ponownego wykorzystywania w ogóle nie będzie miała miejsca.

Również realizacja prawa do niepodlegania zautomatyzowanym decyzjom będzie miała niewielkie znaczenie (art. 22 RODO). Podmiot danych może skorzystać z prawa do niepodlegania zautomatyzowanym decyzjom), jeśli ta decyzja nie jest dozwolona prawem lub nie opiera się na wyraźnej zgodzie (zob. Rozdział 5.2.9).

10.2.1. Sprzeciw

W mojej opinii w kontekście ponownego wykorzystywania danych osobowych zasadniczym uprawnieniem osoby, której dane dotyczą, a z drugiej strony relewantnym w skutkach jakie wywołuje po stronie użytkownika, jest prawo do sprzeciwu (zob. Rozdział 5.2.8). Jego celem jest wyeliminowanie możliwości przetwarzania danych osobowych przez administratora w ogóle albo wyłączenia możliwości przetwarzania danych osobowych w celu marketingu bezpośredniego, co zwykle prowadzi do całkowitego zaprzestania przetwarzania danych. Odstępstwo od tej reguły będzie możliwe, jeśli dalsze przetwarzanie jest dopuszczalne pod warunkiem, że administrator wykaże istnienie ważnych, prawnie uzasadnionych podstaw

do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Sprzeciw jest wolny od opłat, a forma jego wniesienia jest dowolna.

Prawo wniesienia sprzeciwu – zgodnie z art. 21 RODO – podmiot danych może realizować wyłącznie wtedy, gdy przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. e lub f. Oznacza to, że adresatem sprzeciwu może być zarówno podmiot zobowiązany, który przekazuje lub udostępniana dane osobowe do ponownego wykorzystywania w oparciu o przesłankę wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, jak i użytkownik przetwarzający dane osobowe w oparciu o przesłankę prawnie uzasadnionych interesów (zob. Rozdział 7.2 i 7.3).

Należy jednocześnie przez to rozumieć, że osoba której dane dotyczą nie będzie mogła wnieść sprzeciwu, jeśli ponowne wykorzystywanie ma miejsce w oparciu o jej zgodę na tego rodzaju przetwarzanie (względnie w przypadku „rezygnacji prawa do prywatności", o której mowa w art. 6 ust. 2 UPW), jak i wtedy, kiedy istnieje obowiązek prawny, do którego wykonania niezbędne jest przetwarzanie danych. W praktyce skutkować to będzie brakiem możliwości skierowania sprzeciwu wobec podmiotu zobowiązanego przez osoby pełniące funkcje publicznie, których dane osobowe związane z pełnieniem tych funkcji są ujawniane w celu ponownego wykorzystywania (w oparciu o art. 6 ust. 1 lit. c RODO w związku z art. 6 ust. 2 UPW), jaki i osoby, których dane osobowe są z mocy przepisów publikowane w BIP (np. oświadczenia majątkowe) lub CRIP. Zarazem osoby te, których dane osobowe są udostępniane na podstawie art. 6 lit. c RODO mają prawo do wniesienia sprzeciwu do użytkownika (jako administratora) wobec ponownego wykorzystywania danych osobowych (przez użytkownika, który pozyskał dane z BIP lub CRIP), ponieważ opiera on przetwarzanie o art. 6 ust. 1 lit. f RODO.

Podmiotowi danych będzie przysługiwało zatem prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych adresowane do każdego użytkownika (chyba, że ponowienie wykorzystuje on dane osobowe w oparciu o zgodę, co jak wykazano wcześniej, jest mało prawdopodobne). Konsekwencją wniesienia sprzeciwu jest niedopuszczalność dalszego przetwarzania danych w celach objętych sprzeciwem, a zatem wyeliminowanie przetwarzania danych osobowych w konkretnym przypadku. Rezultatem więc wniesienia sprzeciwu wobec przetwarzania danych osobowych przez użytkownika będzie brak możliwości dalszego ich wykorzystywania w produktach, usługach czy aplikacjach i konieczność usunięcia ich ze swoich zasobów (w związku z art. 17 ust. 1 lit. c RODO).

W odniesieniu do podmiotu zobowiązanego istotnym zagadnieniem jest możliwość wniesienia sprzeciwu wobec udostępniania lub przekazywania danych osobowych w ramach informacji sektora publicznego, w sytuacji w której do takiego ujawnienia nie dochodzi na podstawie wykonywania obowiązku prawnego na nim ciążącego, ale w związku wykonywaniem zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Wydaje się, że w odniesieniu do podmiotu zobowiązanego przedmiotem sprzeciwu będzie zaprzestanie przetwarzania danych bez związku z realizacją prawa do ponownego wykorzystywania. Podmiot zobowiązany, co do zasady, przetwarza dane w pierwotnym innym celu niż przekazanie lub udostępnienie danych do ponownego wykorzystywania, zatem należy założyć, że przedmiotem sprzeciwu będzie ta podstawowa czynność przetwarzania (np. dane zostały przez podmiot zebrane w ramach realizacji zadania publicznego), której dopiero konsekwencją może być ujawnienie danych w ramach ponownego wykorzystywania. Skutkiem wniesienia sprzeciwu będzie zatem zaprzestanie przetwarzania, a zatem również brak możliwości ujawnienia tych danych osobowych do ponownego wykorzystywania przez podmiot zobowiązany.

W świetle art. 21 ust. 1 RODO nie można jednak wykluczyć, że sprzeciw *explicite* będzie dotyczył udostępniania lub przekazywania danych osobowych przez podmiot zobowiązany w ramach wykonywania przez niego prawa do ponownego wykorzystywania.

Bez względu na to czy adresatem sprzeciwu jest podmiot zobowiązany czy użytkownik, osoba, której dane dotyczą musi wykazać przyczyny związane z jej szczególną sytuacją, która uzasadnia wniesienie sprzeciwu.

Pytanie, jakie się nasuwa, dotyczy tego czy za sytuację szczególną można uznać fakt ponownego wykorzystywania danych osobowych. Szczególna sytuacja uzasadniająca zaprzestanie przetwarzania danych osobowych może wiązać się z groźbą ujawnienia poprzez przetwarzanie danych związanych ze sferą prywatności lub życia rodzinnego, w przypadku gdy wykorzystywanie tych danych w konkretnej sytuacji nie jest bezwzględnie konieczne[945]. Przyjmując za sytuację szczególną stan faktyczny, który nie istniał w chwili zbierania danych osobowych, jeżeli dane były zbierane bezpośrednio od osoby, której dotyczą lub który co prawda istniał w chwili zbierania danych, lecz nie był wiadomy administratorowi danych, jeżeli dane osobowe były zbierane nie bezpośrednio od osoby, której dane dotyczą[946], należałoby udzielić odpowiedzi pozytywnej. Podmiot zobowiązany zbiera dane osobowe w innych celach niż realizacja prawa do ponownego wykorzystywania. Osoba, której dane

[945] *J. Barta, P. Fajgielski, R. Markiewicz*, Komentarz, 2015, s. 531
[946] Zob. *P. Litwiński* (red.), op. cit., Komentarz do art. 21, pkt.

dotyczą, jeśli nie zostanie o tym skutecznie poinformowana, nie zakłada, że jej dane osobowe mogą być ponownie wykorzystywane. Ponowne wykorzystywanie danych osobowych nie powinno powodować zachwiania równowagi interesów osoby, której dane dotyczą oraz administratora danych – w wyniku tego interes osoby, której dane dotyczą, powinien przeważyć nad interesem administratora danych. Innymi słowy, potrzeba ochrony prywatności podmiotu danych powinna przeważyć nad potrzebą przetwarzania tych danych przez administratora[947]. W konsekwencji oznacza to konieczność przeprowadzenia testu ważenia interesów podmiotu danych („szczególnej sytuacji" wykazanej w sprzeciwie) z jednej strony, z drugiej zaś ważnych, prawnie uzasadnionych podstaw przetwarzania lub niezbędności do wykonania zadania realizowanego w interesie publicznym. Gdyby administrator miał dać im pierwszeństwo, musi wykazać, z jakich przyczyn pozostają one nadrzędne wobec praw i wolności osoby, której dane dotyczą, lub pozostają niezbędne do wykonania zadania, o jakim tu mowa[948].

Przykładowo, w sprawie dotyczącej przetwarzania przez fundację jawnych danych osobowych pochodzących KRS w udostępnianym przez nią serwisie internetowym za szczególną sytuacją uzasadniającą skorzystanie z prawa do sprzeciwu, Prezes UODO nie uznał poczucia dyskomfortu osoby, której dane dotyczą, związanego z możliwością zapoznania się z danymi przez dowolną osobę. Skoro przetwarzane przez fundację dane są danymi powszechnie dostępnymi w związku z uczestniczeniem podmiotu danych w szeroko rozumianym obrocie gospodarczym, nie można przyjąć, że ich przetwarzanie dla potrzeb związanych z prowadzeniem serwisu, wiąże się – choćby potencjalnie – z ingerencją w sferę jego prywatności[949].

W kontekście ponownego wykorzystywania istotnym jest, że jednym z działań wobec którego przysługuje sprzeciw jest profilowanie.

Obecnie tworzenie profili osobowych osób fizycznych jest powszechną praktyką. Może ono polegać na zestawianiu danych z różnych źródeł – tak wewnętrznych, jak zewnętrznych – dostępnych dla administratora, jak i na uzupełnianiu posiadanych danych o profile predykcyjne, dzięki którym można przewidzieć, jakie cechy może wykazywać osoba fizyczna[950]. Tworzenie profili jest możliwe dzięki połączeniu danych ze źródeł własnych przetwarzającego (użytkownika) i ze źródeł ogólnie dostępnych, w tym danych uzyskanych właśnie w ramach ponownego wykorzystywania informacji sektora publicznego (np. danych pochodzących

[947] *Ibidem.*
[948] *M. Sakowska-Baryła*, Komentarz do art. 21, pkt 9 [w:] *M. Sakowska-Baryła (red.),* Ogólne rozporządzenie.
[949] Decyzja PUODO z 30.01.2019 r., ZSPU.440.574.2018.
[950] Zob. szerzej: *W. R. Wiewiórowski*, Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach *big data*, s. 51.

z rejestrów publicznych), jak i danych z Internetu (włączając w to dane z serwisów społecznościowych)[951]. Ponadto, dzięki łączeniu dużej liczby danych zindywidualizowanych oraz danych pozornie anonimowych, powstają dane, które można przypisać do osoby możliwej do zidentyfikowania.

Profile przypisane podmiotom danych, umożliwiają tworzenie nowych danych osobowych, innych niż te, które sama osoba, której dane dotyczą, podała administratorowi lub których znajomości przez administratora może w uzasadniony sposób się spodziewać. Jednocześnie osoba, której dane dotyczą, najczęściej nie jest świadoma, że takie operacje na jej danych są wykonywane, zaś brak dokładności w tworzeniu profili, wynikający z automatycznego zastosowania przyjętych z góry reguł wnioskowania, może powodować poważne zagrożenia dla praw i wolności obywateli. W szczególności może to prowadzić do różnych form dyskryminacji ze względu na płeć, pochodzenie etniczne i rasowe, wyznanie i przekonania, stan zdrowia, niepełnosprawność, wiek czy orientację seksualną[952].

Wykorzystywane techniki, złożoność zastosowanych algorytmów oraz źródła pozyskiwania danych mogą różnić się znaczący sposób. Niemniej profilowanie charakteryzuje się dwiema cechami. Przy ich zastosowaniu dochodzi do powstania nowych danych osobowych lub nowych powiązań pomiędzy istniejącymi danymi. Zmienia się również cel przetwarzania danych osobowych[953]. Przyjmując, że dane zostały pozyskane w zgodny z prawem sposób, a administrator ma prawo do ich przetwarzania, w tym realizując prawo do ponownego wykorzystywania informacji sektora publicznego, towarzyszące uprawnieniom informacyjnym inne prawa, takie jak prawo do sprzeciwu, mogą stanowić instrument zapobiegający niebezpieczeństwom związanym z profilowaniem osób fizycznych[954].

10.2.2. Prawo do bycia zapomnianym

Kolejnym uprawnieniem, które może mieć zastosowanie w wyniku ponownego wykorzystywania danych osobowych jest prawo żądania do usunięcia danych (zwane „prawem

[951] *Ibidem*, s. 37-38.
[952] *Ibidem.*
[953] *Ibidem*, s. 51.
[954] Z problematyką profilowania wiąże się możliwość skorzystania przez osobę, której daną dotyczą z innego uprawnienia przewidzianego w art. 22 RODO. Osoba, której dane dotyczą ma prawo do tego, aby nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Nie każdy więc przykład profilowania będzie objęty przedmiotowym uprawnieniem, a wyłącznie taki, który prowadzi do podejmowania automatycznych decyzji i wywołuje wobec tej osoby skutki prawne lub w podobny sposób na nią wpływa (zob. Rozdział 5.2.9).

do bycia zapomnianym", zob. Rozdział 5.2.5). Co istotne, ze względu na ograniczenie przedmiotowego uprawnienia, o których mowa w art. 17 ust. 3 RODO, osoba, której dane dotyczą, nie będzie miała prawa skierowania żądania niezwłocznego usunięcia dotyczących jej danych osobowych do podmiotu zobowiązanego, który przekazuje lub udostępnia jej dane osobowe do ponownego wykorzystywania w oparciu o art. 6 ust. 1 lit. c lub e (wyłączenie to wprawdzie nie obejmuje przesłanki zgody, ale ma ona w tym kontekście znikome zastosowanie).

Wyłączenie uprawnienia do żądania usunięcia danych ma bowiem miejsce wtedy, kiedy przetwarzanie danych osobowych jest niezbędne dla realizacji obowiązków wynikających z przepisów prawa oraz wykonywania zadań publicznych. W tych przypadkach osoba, której dane dotyczą, nie może skutecznie domagać się usunięcia danych na swój temat, gdyż usunięcie danych mogłoby uniemożliwić realizację zadań publicznych lub stałoby w sprzeczności z przepisami nakazującymi przetwarzanie danych. Dotyczy to w szczególności administracji publicznej, która prowadzi rozmaite ewidencje, rejestry lub w innych formach przetwarza dane osobowe. Wyłączenie to sprawia, że w większości przypadków, w których organy administracji przetwarzają dane osobowe, uprawnienie do bycia zapomnianym nie będzie miało zastosowania[955].

Jednocześnie osoba, której dane dotyczą będzie mogła wystąpić żądania usunięcia danych do użytkownika, który przetwarza je w ramach realizacji ponownego wykorzystywania informacji sektora publicznego w następujących okolicznościach:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane (a więc ich przetwarzanie nie służy już danym celom ponownego wykorzystywania przez użytkownika);

- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania (nie można takiej przesłanki wykluczyć, jednak jak wykazałem podstawową przesłanką dla ponownego wykorzystywania danych osobowych przez użytkownika będzie stanowił art. 6 ust. 1 lit. f RODO);

- osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania danych przez użytkownika i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania (lub wnosi sprzeciw na mocy art. 21 ust. 2 RODO);

- dane osobowe były przetwarzane niezgodnie z prawem (nie chodzi w tym wypadku o naruszanie przepisów UPW czy wszystkich przepisów RODO tylko brak legitymowania się

[955] *P. Fajgielski*, Komentarz, 2018, s. 276.

stosowną przesłanką legalizującą przetwarzanie danych osobowych[956], w przypadku ponownego wykorzystywania zatem chodzi o brak uzasadnionych interesów realizowanych przez użytkownika, względnie brak zgody na takie przetwarzanie);

- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

Ostania z przesłanek wymieniona w art. 17 ust. 1 w kontekście ponownego wykorzystywania pozostaje irrelewantna, ponieważ obejmuje przypadek, gdy dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Użytkownik, który upublicznił dane osobowe, a następnie wskutek żądania osoby, której dane dotyczą, usunął dane, ma obowiązek podjęcia rozsądnych działań, biorąc pod uwagę dostępną technologię i koszt realizacji (w tym środki techniczne), aby 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. Niezależenie od tego użytkownik powinien poinformować każdego odbiorcę, któremu ujawnił dane o usunięciu danych, chyba że jest to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku (zgodnie z art. 19 RODO).

10.2.3. Dostęp do danych

Osobie, której dane dotyczą przysługuje prawo dostępu do danych. Wynika ono z zasady przejrzystości przetwarzania danych (zob. Rozdział 5.2.3). Źródła realizacji prawa dostępu do danych wobec podmiotu zobowiązanego należy upatrywać w oderwaniu od realizacji przez niego prawa do ponownego wykorzystywania, wszakże podmiot zobowiązany zebrał dane w określonym przepisami prawa pierwotnym celu związanym, co do zasady, z realizacją obowiązku prawnego czy wykonywaniem zadań publicznych. Jako administrator danych podmiot zobowiązany wykonuje uprawnienia podmiotu danych przewidziane w art. 15 ogólnego rozporządzenia.

Z kolei w przypadku użytkownika to przepisy UPW mogą stanowić źródło pozyskania przez niego danych osobowych. W związku z tym osoba, której dane są przetwarzane w ramach ponownego wykorzystywania jest uprawniona do uzyskania dostępu do danych oraz wszystkich informacji, o których mowa w art. 15 ust. 1 i 2 RODO od użytkownika

[956] *Ibidem*, s. 272.

spełniającego przesłanki administratora (zob. Rozdział 3.3.4). Ma również prawo do otrzymania kopii swoich danych osobowych podlegających przetwarzaniu w ramach ponownego wykorzystywania, zgodnie z art. 15 ust. 3 RODO.

10.2.4. Sprostowanie i uzupełnienie danych

Osoba, której dane dotyczą będzie mogła również skorzystać z – wynikającego z zasady poprawności danych – uprawnienia do sprostowania danych (Rozdział 5.2.4). Należy przyjąć, iż realizacja po stronie podmiotu zobowiązanego żądania do skorygowania danych związana będzie przede wszystkim z publikacją w BIP, centralnym repozytorium lub innym systemie teleinformatycznym danych niezgodnych ze stanem faktycznym, nieaktualnych, błędnych czy w inny sposób wadliwych. Prawo wyrażone w art. 16 RODO obejmuje również możliwość zażądania uzupełniania danych niekompletnych. Zatem możliwość skorzystania z przedmiotowego uprawnienia będzie wtórna wobec obowiązków publikowania określonych danych na podstawie przepisów prawa, które powinny spełniać wymóg poprawności.

W kontekście ponownego wykorzystywania problematyczny w realizacji może okazać się obowiązek poinformowania każdego odbiorcy, któremu dane osobowe zostały ujawnione, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Jak zostało omówione w Rozdziale 9.4. sposób realizacji przedmiotowego obowiązku został zmodyfikowany przepisami UPW. Podmiot zobowiązany wykonuje go poprzez zaktualizowanie danych odpowiednio na swojej stronie podmiotowej Biuletynu Informacji Publicznej, w centralnym repozytorium lub w inny sposób. Oznacza to, podmiot zobowiązany przekazujący dane osobowe na wniosek, jak i użytkownik, który dokonał sprostowania danych osobowych, informuje o tym fakcie odbiorców na zasadach ogólnych wyznaczonych przez RODO.

10.2.5. Ograniczenie przetwarzania

Z prawem do sprostowania danych, sprzeciwem wobec przetwarzania oraz usunięciem danych wiąże się uprawnienie do ograniczenia przetwarzania (zob. Rozdział 5.2.6). Osoba, której dane są przetwarzane w ramach ponownego wykorzystywania będzie mogła żądać ograniczenia przetwarzania, w następujących sytuacjach (wymienionych w art. 18 ust. 1 RODO):

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający podmiotowi zobowiązanemu lub użytkownikowi sprawdzić prawidłowość tych danych;

- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian od użytkownika ograniczenia ich wykorzystywania;

- podmiot zobowiązany lub użytkownik nie potrzebują już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;

- osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie podmiotu zobowiązanego lub użytkownika są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

Przedmiotem uprawnienia jest ograniczenie jakiejkolwiek operacji przetwarzania danych na przyszłość, z wyłączeniem czynności przechowywania danych (chyba że osoba, której dane dotyczą wyrazi zgodę na przetwarzanie albo przetwarzanie służy ustaleniu, dochodzeniu lub obrony roszczeń lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego). Realizacja przez podmiot zobowiązany prawa do ograniczenia przetwarzania oznaczać będzie również brak podstawy dla udostępnienia lub przekazania do ponownego wykorzystywania danych osobowych osoby korzystającej z przedmiotowego uprawnienia.

Inne operacje przetwarzania danych są wykluczone, chyba że zachodzą okoliczności z art. 18 ust. 2 RODO. Zgodnie ze wspomnianą zasadą ograniczenia przechowywania dane nie powinny być przechowywane przez czas dłuższy niż to jest konieczne. Treść motywu 39 preambuły wskazuje, że dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do niezbędnego minimum.

Z realizacją przez podmiot zobowiązany lub użytkownika ograniczenia przetwarzania wiążą się dwa obowiązki informacyjne. Po pierwsze, muszą na mocy art. 19 RODO poinformować o ograniczeniu przetwarzania, każdego odbiorcę, któremu ujawniono dane osobowe, po drugie zaś są zobligowani przed uchyleniem przedmiotowego ograniczenia do poinformowania o tym fakcie osoby, której dane dotyczą.

Wnioski

1) Genezę prawa do ponownego wykorzystywania informacji sektora publicznego oraz ochrony danych osobowych należy wiązać z powstaniem i rozwojem sieci Internet, postępującym rozwojem technologii informacyjno-komunikacyjnych oraz automatyzacją procesów przetwarzania danych. O ile źródłem powstania obu porządków regulacyjnych jest rozwój technologiczny, o tyle oba prawa ewoluowały samodzielnie według własnej dynamiki, determinowanej – co do zasady – inicjatywą prawodawcy wspólnotowego. Różne są również prawne umocowania prawa do ochrony danych osobowych oraz prawa do dalszej eksploatacji informacji. Pierwsze silnie zakorzenione w prawie do prywatności znajduje swe podstawy w prawie pierwotnym UE oraz konstytucyjnym. Drugie, pamiętając o jego wtórności względem prawa do informacji, pozostaje przede wszystkim prawem pochodnym UE. Różna jest także hierarchia obu regulacji w systemie źródeł prawa.

Niemniej zarówno ogólne rozporządzenie, jak i dyrektywa 2019/1024 zostały uznane za kluczowe narzędzia służące budowie gospodarki cyfrowej na rynku wewnętrznym UE, czy precyzyjniej, na jednolitym rynku cyfrowym. Obecnie przyjmuje się, że to nie ropa, a dane (wszelkiego rodzaju, w tym osobowe i publiczne) są światowym najbardziej wartościowych zasobem. Współcześnie postrzega się dane jako zasób wielokrotnego użytku o niekonkurencyjnym i praktycznie nieograniczonym charakterze, czy nawet uważa się dane za zasób współdzielony lub dobro wspólne.

Wpływ danych przejawia się w pięciu kluczowych obszarach: technologicznej innowacji, nowatorskich modelach biznesowych, kreowaniu nowych rynków, innowacjach społecznych oraz politykach publicznych bazujących na danych. Są one szczególnie ważne dla podmiotów gospodarczych, które swoje modele biznesowe opierają na ich przetwarzaniu. Przykładem może być projektowanie technologii Internetu rzeczy, analiza wielkich zbiorów danych, uczenie maszynowe czy rozwój sztucznej inteligencji. Jednoczesne zastosowanie danych w nowoczesnych technologiach powoduje przenikanie się regulacji ochrony danych osobowych i ponownego wykorzystywania informacji sektora publicznego.

Dane będące w posiadaniu sektora publicznego stanowią niewyczerpalny rezerwuar dla rozwoju innowacyjnych produktów, usług czy aplikacji. Informacje sektora publicznego, które są dostępne w publicznie dostępnych źródłach, jak BIP, portal dane.gov.pl, strony informacyjne urzędów czy rejestry publiczne mogą zawierać dane osobowe. Już obecnie wiele różnego

rodzaju danych udostępnia się do dalszej eksploatacji w sposób zautomatyzowany (w tym przez interfejsy programowania aplikacji), niewymagający złożenia wniosku czy zgody podmiotu publicznego. Wiele tych źródeł umożliwia również dostęp do danych osobowych. Dane osobowe mogą również być zawarte w informacji sektora publicznego, która jest indywidualnie przekazywana na wniosek. W następstwie może dojść do konfliktu dwóch konkurencyjnych uprawnień, prawa do ochrony danych, osoby, której dane dotyczą z prawem użytkownika do ponownego wykorzystywania informacji sektora publicznego.

2) Przepisy te mają wspólny obszar regulacji, pojęciem w którym krzyżują się oba porządki jest informacja. Informacja sektora publicznego może stanowić lub zawierać dane osobowe, a więc informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Ponowne wykorzystywanie danych osobowych oznaczać będzie jednoczesne ich przetwarzanie. Wówczas podmiot publiczny udostępniający lub przekazujący informację sektora publicznego będzie pełnił także rolę administratora. Z kolei użytkownik przetwarzający dane osobowe w ramach realizacji prawa do ponownego wykorzystywania będzie – w zależności od okoliczności – mógł zostać uznany za administratora danych lub innego odbiorcę danych.

3) Prawo do ponownego wykorzystywania informacji sektora publicznego może zatem wejść w konflikt z prawem do ochrony danych osobowych. Jeśli w ponowne wykorzystywanie danych osobowych znajduje podstawę legalizującą takie przetwarzanie danych, wówczas konieczne jest współstosowanie przepisów pochodzących z dwóch porządków regulacyjnych.

Przeprowadzona analiza art. 86 RODO i motywu 154 preambuły ogólnego rozporządzenia oraz przepisów dotyczących ponownego wykorzystywania informacji sektora publicznego pozwala na wyprowadzenie wniosku, że RODO reguluje relację, w której ponowne wykorzystywanie informacji krzyżuje się z prawem do ochrony danych osobowych.

Artykuł 86 i motyw 154 preambuły RODO przewidują wskazówkę dla krajowego ustawodawcy, który określając w przepisach dopuszczalność przetwarzania danych osobowych w ramach ponownego wykorzystywania, powinien pogodzić prawo do ponownego wykorzystywania informacji z prawem do ochrony danych osobowych.

Ogólne rozporządzenie oddziałuje na system ponownego wykorzystywania informacji sektora publicznego, w którym dochodzi do ujawnienia danych osobowych w ramach informacji sektora publicznego i w konsekwencji umożliwia ponowne wykorzystywanie danych

osobowych. Przetwarzanie danych osobowych w ramach ponownego wykorzystywania informacji sektora publicznego powinno następować w zgodzie z zasadami wynikającymi z RODO. Stanowi o tym bezpośrednio art. 7 ust. 2 UPW, zgodnie z którym ponowne wykorzystywanie nie może naruszać prawa do ochrony danych osobowych. Ponadto wśród warunków ponownego wykorzystywania podmiot zobowiązany może uwzględnić ochronę danych osobowych (art. 14 ust. 1 pkt 4 UPW).

Artykuł 7 ust. 2 jest jedyną normą w UPW, która wprost wyznacza relację pomiędzy prawem do ochrony danych osobowych a prawem do ponownego wykorzystywania. Nie można jednak uznać art. 7 ust. 2 za wystarczający do spełnienia warunku godzenia praw w rozumieniu art. 86 RODO. Ponadto w przepisach UPW zawarto odniesienia do ochrony danych osobowych jako warunku ponownego wykorzystywania oraz sposobu spełnienia obowiązków informacyjnych w związku z ponownym wykorzystywaniem danych osobowych.

Jednocześnie przepisy UPW wskazują na prywatność osoby fizycznej jako jedno z ograniczeń prawa do ponownego wykorzystywania informacji sektora publicznego. Równoległe obowiązywanie w UPW dwóch przepisów wyznaczających relację pomiędzy dwoma prawami, tj. art. 6 ust. 2 oraz 7 ust. 2 powoduje wątpliwość, jaką podstawę prawną należy zastosować dla ograniczenia ponownego wykorzystywania informacji sektora publicznego zawierającej dane osobowe. Jak udowodniono art. 7 ust. 2 nie stanowi samodzielnej podstawy do ograniczenia ponownego wykorzystywania ze względu na ochronę danych osobowych. Ograniczenie to należy rozpatrywać w oparciu o prywatność, o której mowa w art. 6 ust. 2 UPW. Konieczne zatem jest rekonstruowanie ochrony danych osobowych z pojęcia prywatności jako przesłanki ograniczającej ponowne wykorzystywanie informacji sektora publicznego zawierającej dane osobowe.

Ustawodawca krajowy wypełnił jedynie minimalny obowiązek uwzględnienia ochrony danych osobowych w regulacji ponownego wykorzystywania informacji sektora publicznego bez jednoczesnego „pogodzenia" obu praw oraz wyczerpującego wykonania wymogów dotyczących podstaw prawnych przetwarzania wymienionych w art. 6 ust. 2 i 3 RODO.

4) Przepisy ogólnego rozporządzenia nie przewidują szczególnego trybu dla ujawnienia danych osobowych czy innej formy ich udostępnienia. Podobnie w UPW proceduralnie nie wyodrębniono szczególnej sytuacji ujawnienia danych w ramach informacji sektora publicznego do ponownego wykorzystywania. Zastosowanie będą miały ogólne przepisy UPW

dotyczące udostępnienia lub przekazania informacji sektora publicznego. Dychotomiczny podział na dwa rodzaje dystrybucji informacji w celu ponownego wykorzystywania związany jest z trybem ponownego wykorzystywania. Udostępnienie informacji sektora publicznego ma miejsce w ramach trybu bezwnioskowego, a więc sytuacji gdy źródłem pozyskania informacji jest BIP, CRIP lub inny system teleinformatyczny podmiotu zobowiązanego. Z kolei przekazanie informacji sektora publicznego ma miejsce w wyniku realizacji wniosku o ponowne wykorzystywanie. Oba tryby ponownego wykorzystywania łączy przenikanie się cywilnoprawnych i administracyjnoprawnych elementów, czego dobitnym wyrazem są przepisy o ofercie. W wyniku przyjęcia przez wnioskodawcę oferty, w trybie wnioskowym (wprost), a w trybie bezwnioskowym przez użytkownika domyślnie (rozpoczęcie wykorzystywania danych dostępnych w systemie teleinformatycznym), dochodzi do zawarcia umowy cywilnoprawnej, przez co warunki ponownego wykorzystywania (w tym warunki przetwarzania danych osobowych) stają się zobowiązaniem cywilnoprawnym. Ponadto postępowanie w sprawie ponownego wykorzystywania charakteryzuje się w znacznym ograniczeniu znaczenia przepisów KPA dla tego postępowania. UPW samodzielnie reguluje postępowanie wnioskowe, a podmiot zobowiązany będzie stosował KPA w bardzo ograniczonym zakresie, tj. w zakresie wydania decyzji o odmowie wyrażenia zgody na ponowne wykorzystywanie informacji sektora publicznego oraz do decyzji o warunkach ponownego wykorzystywania lub o wysokości opłat za ponowne wykorzystywanie na podstawie zgłoszonego przez wnioskodawcę sprzeciwu od oferty.

5) Ponowne wykorzystywanie danych osobowych musi opierać się na jednej z przesłanek legalizujących przetwarzania danych osobowych. Podmiot zobowiązany do przekazania lub udostępnienia danych osobowych w celu ponownego wykorzystywania będzie mógł oprzeć przetwarzanie – w zależności od istnienia dodatkowej podstawy prawnej w prawie krajowym – o odpowiednio przesłankę obowiązku prawnego ciążącego na administratorze (np. w odniesieniu do danych osobowych osób pełniących funkcje publiczne, art. 6 ust. 1 lit. c RODO w zw. z art. 6 ust. 2 UPW) lub wykonania zadania w interesie publicznym lub w ramach sprawowania władzy publicznej (art. 6 ust. 1 lit. e), która będzie miała zastosowanie w większości przypadków. Podstawa prawna takiego przetwarzania powinna spełniać podstawowe wymogi stawiane krajowym podstawom prawnym przetwarzania danych osobowych, o których mowa w art. 6 ust. 2 i 3 RODO. Z kolei podstawą przetwarzania danych osobowych w ramach ponownego wykorzystywania przez użytkownika stanowić będzie prawnie uzasadniony interes (art. 6 ust. lit. f RODO). Potencjalnie jako podstawę przetwarzania

tak dla podmiotu zobowiązanego, jak i użytkownika rozważyć można zgodę (art. 9 ust. 1 lit. a), w szczególności jeśli uznamy za nią tzw. „rezygnację z prawa do prywatności", o której mowa w art. 6 ust. UPW.

Wybór przesłanki jest kluczowy z punktu widzenia katalogu uprawnień przysługujących osobie, której dane dotyczą. Administrator nie ma obowiązku realizacji prawa do bycia zapomnianym (art. 17 RODO), jeśli przetwarzanie danych jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Prawo do przenoszenia danych, o którym mowa w art. 20 RODO, przysługuje jedynie w przypadku, gdy podstawą do przetwarzania danych była zgoda (lub niezbędność dla wykonania umowy). Z kolei prawo wniesienia sprzeciwu – zgodnie z art. 21 RODO – podmiot danych może realizować wyłącznie wtedy, gdy przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. e lub f.

6) W pracy wykazano wątpliwości w zakresie w jakim przepisy UPW jako podstawa przetwarzania danych osobowych są proporcjonalne do wyznaczonego, prawnie uzasadnionego celu, o czym stanowi art. 6 ust. 3 zd. 4 RODO. UPW służy realizacji celu leżącego w interesie publicznym, którym jest ponowne wykorzystywanie informacji sektora publicznego, nie sposób jednak, opierając ograniczenie ponownego wykorzystywania danych osobowych o ochronę prywatności osoby fizycznej (art. 6 ust. 2 UPW), ze względu nieostrość tego kryterium, przesądzić, że przepis ten jest proporcjonalny do prawnie uzasadnionego celu jakim jest ponowne wykorzystywanie informacji sektora publicznego.

UPW zawiera tylko niektóre elementy podstawy prawnej przetwarzania danych osobowych, o których mowa w art. 6 ust. 3 zd. 3 RODO. Wskazuje kategorie osób, których dane mogą zostać udostępnione i rodzaje danych (*expressis verbis* jedynie osoby pełniące funkcje publiczne i informacje związane pełnieniem tych funkcji, pośrednio podmioty i dane wymienione w art. 7 ust. 4 pkt 2 i 3) oraz podmioty, którym można ujawnić dane osobowe (art. 2 ust. 2 UPW – użytkownik). Można również uznać, że po stronie podmiotu zobowiązanego wskazuje również cel, jest nim realizacja prawa do ponownego wykorzystywania informacji sektora publicznego. Krajowa ustawa nie wyznacza jednak środków zapewniających zgodność z prawem i rzetelność przetwarzania oraz innych elementów, o których mowa w art. 6 ust. 3 zd. 3 RODO, lub określa je w sposób nieprecyzyjny.

7) Ponowne wykorzystywanie informacji sektora publicznego z samej definicji oznacza zmianę pierwotnego celu, dla którego dane zostały zebrane. Skuteczne zastosowanie zasady celowości w przypadku ponownego wykorzystywania stanowi znaczące wyzwanie. Z jednej strony sama koncepcja i siła napędowa innowacyjności stojące za pojęciem otwartych danych i ponownym wykorzystywaniem informacji sprowadzają się do tego, aby dane mogłyby być szeroko dostępne dla ich użycia w nowych, innowacyjnych produktach i usługach, a tym samym w celach, które nie zostały wcześniej określone i nie sposób ich wyraźne przewidzieć.

Postępujące zmiany technologiczne umożliwiające niemal nieograniczone możliwości przetwarzania danych osobowych rodzą głosy o radykalnej konieczności modyfikacji podejścia do ochrony danych osobowych i zakwestionowaniu niektórych zasad ochrony danych osobowych, w tym przede wszystkim zasady celowości, która w połączeniu z koniecznością spełnienia obowiązku informacyjnego i uzyskania zgody podmiotu danych najpóźniej w chwili ich zbierania jest nierealistyczna i wymaga zastąpienia przez właściwe wdrożenie zasady rozliczalności[957].

8) Instrumentem, który przynajmniej częściowo może wyeliminować niepewność prawną co do możliwości przetwarzania danych osobowych w ramach informacji sektora publicznego, stanowią warunki ponownego wykorzystywania danych osobowych (art. 13 ust. 4 pkt 4 UPW), w aktach prawa UE zwane licencjami. Licencje nie eliminują konieczności zachowania zgodności z przepisami o ochronie danych, jednak klauzula o ochronie danych przewidziana w warunkach licencji pomogłaby w zapewnieniu zgodności z przepisami o ochronie danych poprzez dodanie elementu „wykonalności". Taka klauzula mogłaby również pomóc w podnoszeniu świadomości poprzez przypomnienie ponownym użytkownikom o ich obowiązkach jako administratorów.

W mojej opinii *de lege ferenda obecnie* obowiązującą możliwość uwzględnienia kwestii ochrony danych osobowych w warunkach ponownego wykorzystywania, które fakultatywnie może określić podmiot zobowiązany, należałoby zastąpić obowiązkiem prawnym obligujący do każdorazowego określania warunków ponownego wykorzystywania informacji sektora publicznego zawierających dane osobowe lub dane zanonimizowane. Znajomość zasad

[957] Zob. *F.H. Cate, P. Cullen, V. Mayer- Schönenenberger*, Data Protection Principles for the 21st Century. Revising the 1980 OECD Guidelines, December 2013, s. 7–8, za: *P. Drobek*, Zasada celowości w dobie wielkich zbiorów danych (big data), s. 22.

przetwarzania danych osobowych w ramach informacji sektora publicznego wzmocniłaby pewność prawną przede wszystkim wśród użytkowników danych i optymalizowałaby ponowne wykorzystywanie informacji. Wyzwaniem pozostaje sposób formułowania warunków oraz ich zakres w kontekście spełniania zasady związania celem. Rozważyć tutaj można dwie opcje, określenia z góry przez podmiot zobowiązany możliwych, ale konkretnych celów ponownego wykorzystywania danych osobowych przez użytkownika lub wskazując użytkownikowi pierwotny cel ujawnienia danych oraz jego obowiązki wynikające z ogólnego rozporządzenia, w tym konieczność realizacji zasady celowości obejmującą obowiązek przeprowadzenia testu zgodności celów samodzielnie przez użytkownika przed rozpoczęciem przez niego przetwarzania danych.

9) Zidentyfikowaną barierą dla ponownego wykorzystywania informacji sektora publicznego będzie konieczność spełnia obowiązku informacyjnego. Przeszkody tej nie eliminują *de lega lata* przepisy art. 7 ust. 3–5 UPW, a wręcz ze względu na brak jednoznacznego oparcia modyfikacji czy wyłączenia obowiązku informacyjnego o przepisy art. 23 RODO, potęgują niepewność. Dostrzegam tutaj istotną lukę i niekonsekwencję w przepisach ogólnego rozporządzenia. Skoro bowiem prawo do ponownego wykorzystywania na mocy art. 86 RODO zostało uznane za interes publiczny, a prawodawcy krajowemu pozostawiono swobodę dookreślenia w ustawodawstwie wewnętrznym sposobu pogodzenia prawa do ochrony danych osobowych z ponownym wykorzystywaniem informacji sektora publicznego, to niezrozumiałym jest pozbawienie go możliwości modyfikacji, ograniczenia czy wręcz wyłączenia niektórych obowiązków informacyjnych, o ile w prawie krajowym zostałyby spełnione wszystkie wymogi gwarancyjne wymienione w art. 23 ust. 2 RODO.

Według mnie *de lege ferenda* należy rozważyć uzupełnienie katalogu przesłanek umożliwiających ograniczenie obowiązków i praw wymienionych w art. 23 ust. 1 RODO o realizację prawa dostępu do dokumentów urzędowych, a w konsekwencji prawa do ponownego wykorzystywania. Wyeliminowałoby to istotną niepewność prawną, której nie usuwa możliwość powołania się przez administratora na wyłączenie, o którym mowa w art. 14 ust. 5 RODO. Po drugie, jest zasadne również z punktu widzenia systemowego, realizację uprawnień „dostępowych" sam ustawodawca UE uznał za interes publiczny. Przepis art. 23 ust. 1 RODO wymienia cele (wartości) ze względu na które możliwe jest ograniczenie praw i obowiązków. Można stwierdzić, że ich obszarem wspólnym będzie dość pojemne kryterium interesu publicznego.

10) Podmiot zobowiązany przed udostępnieniem lub przekazaniem informacji sektora publicznego zawierającej lub stanowiącej dane osobowe, powinien przeprowadzić ocenę skutków ochrony danych osobowych, o której mowa w art. 35 RODO. Wyniki oceny mogą prowadzić do podjęcia decyzji o rezygnacji przekazania (udostępniania) informacji sektora publicznego zawierających dane osobowe do ponownego wykorzystania lub przekazania (udostępnienia) jedynie danych zanonimizowanych. Po drugie, ocena skutków powinna być przeprowadzana przez administratora przed rozpoczęciem przetwarzania, co oznacza, że obowiązek jej przeprowadzenia można dotyczyć również tego użytkownika, który spełnia przesłanki art. 4 pkt 7 RODO. Kluczowym elementem oceny skutków jest ocena ryzyka naruszenia praw lub wolności. Wynika to z ogólnego podejścia RODO do kwestii bezpieczeństwa danych opartego na ocenie ryzyka.

11) Przekazanie lub udostępnienie informacji sektora publicznego zawierającej danej osobowe powoduje, że podmiotowi danych – poza uprawnieniami informacyjnymi – przysługują również inne uprawnienia, których korelatem są określone obowiązki po stronie administratora. W kontekście ponownego wykorzystywania należy wymienić prawa i obowiązki wynikające z zasady prawidłowości danych, ograniczenia przechowywania, minimalizacji oraz integralności i poufności. Zasady te nie doznają żadnej modyfikacji przepisami o ponownym wykorzystywaniu informacji sektora publicznego; ich realizacja opierać się będzie wprost na przepisach RODO.

Bibliografia

Wykaz literatury

Książki: komentarze, monografie, księgi pamiątkowe, opracowania systemowe oraz podręczniki

Aleksandrowicz T. R., *Komentarz do ustawy o dostępie do informacji publicznej*, Warszawa 2006.

Badura E., Błachucki M., Konarski X, Maciejewski M., Niestrój H., Piskorz-Ryń A., Sakowska-Baryła M., Sibiga G., Ślaska K., *Ponowne wykorzystanie informacji sektora publicznego*, Ministerstwo Cyfryzacji, Warszawa 2016.

Barta P., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Kraków 2004.

Barta P., Fajgielski P., Markiewicz R., *Ochrona danych osobowych. Komentarz*, Warszawa 2015.

Barta P., Litwiński P., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2013.

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

Barta P., Litwiński P., Dörre-Kolasa D., *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 2018.

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

Bernaczyk M., *Obowiązek bezwnioskowego udostępniania informacji publicznej*, Warszawa 2008

Bernaczyk M., *Prawo do informacji publicznej w Polsce i na świecie*, Warszawa 2014.

Bernaczyk M., *Dokument wewnętrzny jako ograniczenie konstytucyjnego prawa do informacji. Rozstrzyganie kolizji w teorii i praktyce prawa*, Warszawa 2017.

Bidziński M., Chmaj M., Szustakiewicz P., *Ustawa o dostępie do informacji publicznej. Komentarz*, Warszawa 2010.

Bielak – Jomaa, Lubasz D. (red.), *Polska i europejska reforma ochrony danych osobowych*, Warszawa 2016.

Bielak – Jomaa, Lubasz D. (red.), *RODO ogólne rozporządzenie o ochronie danych. Komentarz*, Warszawa 2018.

Boć J., *Administracyjnoprawne ograniczenia dostępu do informacji* [w:] Szpor G. (red.), *Wolność informacji i jej granice*, Katowice 1997.

Boć J., *Prawo do prywatności i jego ochrona w prawie konstytucyjnym* [w:] Szpor G. (red.), *Przetwarzanie i ochrona danych*, Katowice 1998.

Braciak J., *Prawo do prywatności*, Warszawa 2004.

Brouwer E., *Legality and data Protection Law: The Forgotten purpose of Purpose Limitation* [w:] Besselink L., Pennings F., Prechel S. (red.) *The Eclipse of the Legality Principle in the European Union*, Alphen aan de Rijn 2011.

Celarek K., *Prawo informacyjne. Problem badawczy teorii prawa administracyjnego*, Warszawa 2013.

Chmielewski J., *Pojęcie nadrzędnego interesu publicznego w prawie administracyjnym*, Warszawa 2005.

Chomiczewski M., *Profilowanie w ogólnym rozporządzeniu o ochronie danych* [w:] Bielak – Jomaa E., Lubasz D. (red.), *Polska i europejska reforma danych osobowych*, Warszawa 2016.

Drobek P., *Ochrona danych osobowych w publicznych bazach danych* [w]: Szpor G. (red.), *Internet. Publiczne bazy danych i Big data*, C.H. Beck, Warszawa 2014.

Drobek P., *Ryzyka dla ochrony danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego* [w:] Piskorz-Ryń A. (red.) *Dostęp i wykorzystywanie* [w:] Szpor G. (red.), J*awność i jej ograniczenia*, *Tom V*, Warszawa 2015.

Drobek P., Piskorz-Ryń A., *Prawne problemy ponownego wykorzystania zasobów rejestrowych. Zagadnienia wybrane* [w:] Gryszczyńska A. (red.), *Rejestry publiczne – jawność i interoperacyjność*, Warszawa 2016.

Drozd A., *Ustawa o ochronie danych osobowych. Komentarz. Wzory pism i przepisy*, Warszawa 2007.

Dye T. R., *Understanding public policy*, Harlow 2014.

Eifert M., *Państwowe struktury informacyjne i ponowne wykorzystywanie informacji w niemieckiej administracji przez podmioty prywatne* [w:] Szpor G. (red.), *Internet. Ochrona wolności, własności i bezpieczeństwo*, Warszawa 2011.

Fajgielski P., *Informacja w administracji publicznej - prawne aspekty gromadzenia, udostępniania i ochrony*, Wrocław 2007.

Fajgielski P., *Zgoda na przetwarzanie danych osobowych*, [w:] Sibiga G., Konarski X. (red.), *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Warszawa 2007.

Fajgielski P., *Zasady ogólne przetwarzania i ochrony danych osobowych* [w:] Goździewicz G., Szabłowska M. (red.), *Prawna ochrona danych osobowych w Polsce na tle europejskich standardów. X-lecie polskiej ustawy o ochronie danych osobowych*, Toruń 2008.

Fajgielski P. (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

Fajgielski P. (red.), *Kontrola przetwarzania i ochrony danych osobowych. Studium teoretyczno - prawne*, Lublin 2008.

Fajgielski P., *Zgoda na przetwarzanie danych osobowych udzielana w Internecie* [w:] G. Szpor (red.) *Internet. Ochrona wolności, własności i bezpieczeństwa,* Warszawa 2011.

Fajgielski P., *Odwoływalność zgody na przetwarzanie danych osobowych – znaczenie dla praktyki gospodarczej* [w:] A. Mednis (red.) *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013.

Fajgielski P., *Ponowne wykorzystanie informacji sektora publicznego w prawie unijnym i w założeniach polskiej ustawy* [w:] P. Fajgielski, P. Potakowski (red.), *Domena publiczna - troska o prawa podstawowe?*, Lublin 2013.

Fajgielski P., *Prawne ograniczenia dostępności informacji* [w:] Sibiga G. (red.), *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej,* Warszawa 2014.

Fajgielski P., *Zasada jawności i prawo do informacji w świetle poglądów profesor Teresy Górzyńskiej,* [w:] Lipowicz I. (red.), *Władza – obywatele – informacja. Ku nowemu porządkowi prawnemu. Księga pamiątkowa ku czci prof. Teresy Górzyńskiej*, Warszawa 2014.

Fajgielski P., *Jawność obrotu gospodarczego a prywatność przedsiębiorcy będącego osobą fizyczną – aspekty prawne* [w:] Arwid Mednis (red.), *Prywatność a jawność. Bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016.

Fajgielski P., *Przetwarzanie danych osobowych w serwisach społecznościowych - wybrane aspekty prawne* [w:] K. Flaga-Gieruszyńska, J. Gołaczyński, D. Szostek (red.), *Media elektroniczne – współczesne problemy prawne,* Warszawa 2016.

Fajgielski P., *Ochrona danych osobowych przedsiębiorcy będącego osobą fizyczną* [w:] E. Kruk, G. Lubeńczuk, M. Zdyb (red.) *Dysfunkcje publicznego prawa gospodarczego,* Warszawa 2018.

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

Feiler L., Forgó N., Weigl M., *The EU General Data Protection Regulation (GDPR): A Commentary,* London 2018.

Fischer B., *Cloud computing – globalny technologiczny paradygmat – zagrożeniem dla ochrony danych osobowych i prywatności*, Kraków 2013.

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

Garlicki L., *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2005.

Goliński M., *Społeczeństwo informacyjne – geneza koncepcji i problematyka pomiaru*, Warszawa 2011.

Góralczyk W. (red.), *Prawo informacji. Prawo do informacji*, Warszawa 2006.

Górzyńska T., *Prawo do informacji i zasada jawności administracyjnej*, Kraków 1999.

Górzyńska T., *Obywatelskie prawo do informacji*, Warszawa 2008.

Górzyńska T., *Prawna regulacja ponownego wykorzystywania* [w:] Sibiga G. (red.), *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej*, Warszawa 2014.

Gryszczyńska A. (red.), *Struktura tajemnic* [w:] Szpor G. (red.), *Jawność i jej ograniczenia, Tom VI,* Warszawa 2014.

Gryszczyńska A. (red.), *Rejestry publiczne. Jawność i interoperacyjność*, Warszawa 2016.

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

Izdebski H., *Samorząd terytorialny: podstawy ustroju i działalności*, Warszawa 2001.

Jabłoński M., Wygoda K., *Dostęp do informacji i jego granice: wolność informacji, prawo dostępu do informacji publicznej, ochrona danych osobowych*, Wrocław 2002.

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

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

Jabłoński M., Sakowska-Baryła M., Wygoda K., *Czy jesteśmy gotowi na stosowanie? Wybrane zagadnienia z zakresu funkcjonowania administracji publicznej*, Wrocław 2018.

Jaśkowska M., *Dostęp do informacji publicznych w świetle orzecznictwa Naczelnego Sądu Administracyjnego*, Toruń 2002.

Jaśkowska M., *Jakość i spójność rozwiązań prawnych w świetle nowelizacji ustawy o dostępie do informacji publicznej* [w:] Kijowski D., Suwaj P. (red.), *Kryzys prawa administracyjnego?*, Kijowski D., Miruć A., Suławko-Karetko A. (red.), t. 1, *Jakość prawa administracyjnego*, Warszawa 2012.

Jaśkowska M., *Ponowne wykorzystywanie informacji publicznej* [w:] Sługocki J. (red.), *Dziesięć lat w Unii Europejskiej. Problemy prawnoadministracyjne, t. 2*, Wrocław 2014.

Jaśkowska M., *Ponowne wykorzystywanie informacji publicznej* [w:] Jagielski J., Wierzbowski M., *Prawo administracyjne dziś i jutro*, Warszawa 2018.

Kamińska I., Rozbicka-Ostrowska M., *Ustawa o dostępie do informacji publicznej. Komentarz*, Warszawa 2012.

Kopff A., *Koncepcja praw do intymności i do prywatności życia osobistego*, „Studia cywilistyczne" t. XX, Kraków 1972

Kulesza M., Izdebski H., *Administracja publiczna. Zagadnienia ogólne*, Warszawa 2004.

Kuner C.,, Bygrave L., Docksey C., *The EU General Data Protection Regulation (GDPR). A Commentary*, Oxford 2019.

Lipowicz I.,, *Konstytucyjne podstawy ochrony danych osobowych* [w:] *Fajgielski P. (red.) Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

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

Lubasz D. (red.), *Meritum. Ochrona danych osobowych*, Warszawa 2020.

Maciejewski M., *Prawna regulacja ponownego wykorzystywania informacji publicznych* [w:] Sibiga G. (red.), *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państwa Unii Europejskiej*, Warszawa 2013.

Młynarski G., Tarkowski A., Jachowicz Ł., *Otwarty rząd w Polsce. Kulisy programu Opengov*, Fundacja Projekt: Polska, Wydanie internetowe – wersja 1.0, Warszawa 2013.

Mednis A., *Prawna ochrona danych osobowych*, Warszawa 1995.

Mednis A., *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016.

Miąsik D., Półtorak N., Wróbel A. (red.), *Traktat o funkcjonowaniu Unii Europejskiej. Komentarz, t. 1*, Warszawa 2012.

Oleński J., *Infrastruktura informacyjna państwa w globalnej gospodarce*, Warszawa 2006.

Piskorz-Ryń A., *Regulacja prawa dostępu do informacji publicznej – uwagi de lege ferenda* [w:] Boć J., Chajbowicz A. (red.), *Nowe problemy badawcze w teorii prawa administracyjnego*, Wrocław 2009.

Piskorz-Ryń A., *Problemy implementacji w polskim porządku prawnym dyrektywy 2013/37/UE zmieniającej dyrektywę w sprawie ponownego wykorzystywania informacji sektora publicznego* [w:] Maciejewski M. (red.), *Prawo do informacji publicznej - efektywność regulacji i perspektywy jej rozwoju*, Warszawa 2014.

Piskorz-Ryń A., *Jawność działania administracji publicznej z perspektywy „otwartego rządu"* [w:] I. Lipowicz (red.), *Władza-Obywatele-Informacja. Ku nowemu porządki prawnemu. Księga pamiątkowa ku czci prof. T. Górzyńskiej*, Warszawa 2014.

Piskorz-Ryń A., *Ponowne wykorzystanie informacji sektora publicznego. Zagadnienia administracyjnoprawne*, Warszawa 2018.

Rosemary J., *Guide to the General Data Protection Regulation, A Companion to Data Protection Law and Practice*, London 2017.

Rydlewski G., Szustakiewicz P., Golat K., *Udzielanie informacji przez administrację publiczną. Teoria i praktyka*, Warszawa 2012.

Safjan M., *Ochrona danych osobowych – granice autonomii informacyjnej*, [w:] Wyrzykowski M., *Ochrona danych osobowych*, Instytut Spraw Publicznych, Warszawa 1999.

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

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

Sakowska-Baryła M., *Problem współstosowania ustawy o dostępie do informacji publicznej i ustawy o ochronie danych osobowych* [w:] Mednis A., *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016.

Sakowska-Baryła M., *Ogólne rozporządzenie o ochronie danych osobowych. Komentarz*, Warszawa 2019.

Sawczuk W., *Określenie warunków ponownego wykorzystywania informacji publicznej w Biuletynie Informacji Publicznej. Możliwość ponownego wykorzystywania baz orzeczeń* [w:] Jaśkowska M. (red.), *Jawność i jej ograniczenia, t. 4: Znaczenie orzecznictwa*, Warszawa 2014.

Sibiga G., *Postępowanie w sprawach ochrony danych osobowych*, Warszawa 2003.

Sibiga G., Konarski X. (red.), *Ochrona danych osobowych. Aktualne problemy i nowe wyzwania*, Warszawa 2007.

Sibiga G., *Komplementarność czy kolizja? Prawna ochrona danych osobowych a dostęp do informacji publicznych oraz informacji o środowisku i jego ochronie* [w:] Fajgielski P. (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008, s. 153-169.

Sibiga G., *Udostępnianie danych z rejestrów publicznych a zastosowanie technologii informacyjno-telekomunikacyjnych* [w:] Szpor G. (red.), *INTERNET. Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011.

Sibiga G., *Zakres stosowania przepisów dostępowych. Sposób ograniczania prawa do informacji, Wybrane rodzaje ograniczeń prawa do informacji* [w:] Sibiga G. (red.), *Główne problemy prawo do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państwa Unii Europejskiej*, Warszawa 2013.

Sibiga G. (red.), *Główne problemy prawa do informacji w świetle prawa i standardów międzynarodowych, europejskich i wybranych państw Unii Europejskiej*, Warszawa 2013.

Sibiga G., *Ochrona danych osobowych a tajemnice prawnie chronione (Personal data protection and legally protected secrets)* [w:] *15-lecie ustawy o ochronie danych osobowych (15th anniversary of personal privacy protection law)*, Kałużyńska M. (red.), Biuro Generalnego Inspektora Ochrony Danych Osobowych, Warszawa 2013.

Sibiga G., *Sposób ustawowego ograniczania dostępu do informacji publicznej w prawie polskim*, [w:] *Władza-obywatele-informacja. Księga pamiątkowa ku czci Profesor Teresy Górzyńskiej*, Lipowicz I. (red.), Warszawa 2014.

Sibiga G., *Ponowne wykorzystanie informacji sektora publicznego – stan obecny i perspektywy rozwoju. Wybrane zagadnienia* [w:] Mednis A. (red.), *Prywatność a jawność – bilans 25-lecia i perspektywy na przyszłość*, Warszawa 2016.

Sitniewski P., *Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz*, Warszawa 2017.

Skrzydło W., *Konstytucja Rzeczypospolitej Polskiej. Komentarz*, Warszawa 2013.

Stawecki T., *Rejestry publiczne. Funkcje instytucji*, Warszawa 2005.

Schoch F., *Zagadnienia równowagi między wolnością informacyjną a ochroną danych w niemieckim profesorskim projekcie Kodeksu Informacyjnego* [w:] Szpor G. (red.) *Internet. Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011.

Szekely I., *Freedom of Information Versus Privacy. Friends Or Foes* [w:] Gutwirth S., Poullet Y., De Hert P., de Terwangne C., Nouwt S. [red.] Reinventing Data Protection?, Springer 2009,.

Szpor G., *Pojęcie informacji a zakres ochrony danych* [w:] Fajgielski P. (red.), *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, Lublin 2008.

Szpor G. (red.), *Wolność informacji i jej granice*, Katowice 1997.

Szpor G. (red.), *Przetwarzanie i ochrona danych*, Katowice 1998.

Szpor G., *Publicznoprawna ochrona danych osobowych*, Przegląd Ustawodawstwa Gospodarczego 1999.

Szpor G. (red.), *Idee i pojęcia,* Szpor G. (red.), *Jawność i jej ograniczenia, Tom I*, Warszawa 2016.

Sybilski D., *Relacja dostępu do informacji publicznej oraz ochrony danych osobowych na gruncie ogólnego rozporządzenia o ochronie danych* [w:] Roman Ł., Krassowski K., Sagan S., Wróblewski J. (red.), *Nowoczesne narzędzia informatyczne w przeciwdziałaniu zagrożeniom bezpieczeństwa*, Józefów 2017.

Sybilski D., *Ewolucja realizacji prawa dostępu do informacji publicznej - od Biuletynów Informacji Publicznej po portale otwartych danych* [w:] Federczyk W. (red), *Stulecie polskiej administracji. Doświadczenia i perspektywy*, Warszawa 2018.

Syryt A., *Konstytucyjne uwarunkowania ponownego wykorzystywania informacji sektora publicznego* [w:] Piskorz-Ryń A. (red.), *Dostęp i wykorzystywanie*, Szpor G. (red.), J*awność i jej ograniczenia. Tom V*, Warszawa 2015.

Wiebe A., Nils D. (red.), *Open data protection. Study on legal barriers to open data sharing – Data protection and PSI*, Göttingen 2017, w: https://www.ouvrirlascience.fr/open-data-protection-study-on-legal-barriers-to-open-data-sharing-data-protection-and-psi/ 09.06.2019).

Wierczyński G., Wiewiórowski W.R., *Informatyka prawnicza*, Gdańsk 2016.

Wiewiórowski W., *Profilowanie osób na podstawie ogólnodostępnych danych* [w:] Mednis A. (red.), *Prywatność a ekonomia. Ochrona danych osobowych w obrocie gospodarczym*, Warszawa 2013.

Wiewiórowski W.R., *Założenia wstępne dla zrównoważonego przetwarzania informacji ze źródeł publicznych w czasach big data* [w:] Bąkowski T. (red.), *Model regulacji* [w:] Szpor G. (red.), *Jawność i jej ograniczenia*, Tom XII, Warszawa 2016.

Wiewiórowski W., Wolska H. (red.), *Rok RODO*, Warszawa 2019.

Wilczyńska A., *Interes publiczny w prawie stanowionym i orzecznictwie Trybunału Konstytucyjnego*, „Przegląd Prawa Handlowego" 2009, Nr 9.

Winczorek P., *Komentarz do Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 r.*, Warszawa 2008.

Wojsyk K [w:] Barczewski M. (red.), Grajewski K., Warylewski J., *Prawne problemy wykorzystywania nowych technologii w administracji publicznej i w wymiarze sprawiedliwości*, Warszawa 2009.

Woźniak M., Pierzchała E., *Dostęp do informacji publicznej w Polsce i Europie - wybrane zagadnienia prawne*, Opole 2011.

Wygoda K., *Ochrona danych osobowych i prawo do informacji o charakterze osobowym* [w:] B. Banaszak, A. Preisner (red.), *Prawa i wolności obywatelskie,* Warszawa 2002.

Wyrzykowski M., *Ochrona danych – zagadnienia konstytucyjne* [w:] M. Wyrzykowski (red.), *Ochrona danych osobowych*, red., Warszawa 1999.

Wyrzykowski M., *Status informacyjnych obywatela* [w:] *Prawo i ład społeczny. Księga jubileuszowa dedykowana Profesor Annie Turskiej*, Warszawa 2000.

Vickery R., *Review of Recent Studies on PSI Re-Use and Related Market Development*, Paryż 2011.

Zybała A., *Polityki publiczne*, Warszawa 2012.

Artykuły i glosy

Andraško J., Mesarčík M., *Quo Vadis Open Data?*, "Masaryk University Journal of Law and Technology", 2018, Vol. 12:2.

Adamski D., Bernaczyk M., *Znaczenie dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego dla ustawy o dostępie do informacji publicznej*, „Elektroniczna Administracja", marzec–kwiecień 2006.

Banaszak B., Bernaczyk M, *Konsultacje społeczne i prawo do informacji w procesie prawotwórczym na tle Konstytucji RP oraz postulatu "otwartego rządu*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2012, Nr 4.

Bass T.*, It's time to think about our data as a common good,* British Council https://www.britishcouncil.org/anyone-anywhere/explore/communities-connections/rethinking-data

Bernaczyk M., Jabłoński M., *Praktyczne problemy wdrażania ustawy o dostępie do informacji publicznej*, „Elektroniczna Administracja" 2006, Nr 6 (7).

Bielak-Jomma E., *Ogólne rozporządzenie o ochronie danych. Rewolucja w ochronie danych?*, „Monitor Prawniczy" 2017, Nr 20 (dodatek).

Bienias M., *Ochrona danych w fazie projektowania oraz domyślna ochrona danych (privacy by design oraz privacy by default) w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 2016, Nr 20 (dodatek).

Błachucki M., Sibiga G., *Przenikanie się cywilnoprawnych i administracyjnoprawnych elementów w nowych procedurach administracyjnych na przykładzie postępowania w sprawie ponownego wykorzystywanie informacji sektora publicznego przekazywanych na wniosek,* „Opolskie Studia Prawno-Administracyjne" 2018, Nr XVI/1[1].

Boni M., *Nowe ramy ochrony danych osobowych w Unii Europejskiej – ważne wyzwanie dla Polski*, „Monitor Prawniczy" 2013, Nr 8.

Borgesius, F.Z., Gray, J., Eechoud, M.V., *Open Data, Privacy, and Fair Information Principles: Towards a Balancing Framework*, "Berkeley Technology Law Journal" 2016, vol. 30, issiue 3.

Cerosismo J.C., *The purpose limitation principle in the General Data Protection Regulation*, Tilburg University 2018, http://arno.uvt.nl/show.cgi?fid=145704

Ciechomska M., *Prawne aspekty profilowania oraz podejmowania zautomatyzowanych decyzji w ogólnym rozporządzeniu o ochronie danych osobowych*, „Europejski Przegląd Sądowy" 2017, nr 5.

Czerniawski M., *Glosa do wyroku TS z 13.5.2014 r., C-131/12*, LEX 2015.

Dziliński B., *Prawo do ponownego wykorzystywania informacji publicznej. Uwagi na tle transpozycji dyrektywy 2003/98/WE z 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego*, „Zeszyty Prawnicze Biura Analiz Sejmowych" 2012, Nr 4.

Fajgielski P., *Obowiązek informacyjny w ogólnym rozporządzeniu o ochronie danych,* „Informacja w administracji publicznej" 2017, Nr 1.

Fajgielski P., *Przetwarzanie szczególnych kategorii danych w świetle RODO*, „Informacja w administracji publicznej" 2017, Nr 2.

Fajgielski P., *Prawo do przenoszenia danych,* „Informacja w administracji publicznej" 2017, Nr 4.

Fajgielski P., *Dostosowanie krajowych przepisów do wymogów ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" 2019, Nr 22 (dodatek).

Gos A., *Serwis danepublicze.gov.pl*, „Informacja w administracji publicznej" 2017, Nr 3.

Janssen K., Dumortier J., *Towards a European Framework for the Re-use of Public Sector Information: a Long and Winding Road*, "International Journal of Law and Information Technology" 2003, vol. 11, Issue 2.

Jaśkowska M., *O pojęciu informacji publicznej raz jeszcze*, „Zeszyty Prawnicze" 2020, Nr 3.

Mednis A., *Cechy zgody na przetwarzanie danych osobowych w opinii Grupy Roboczej Art. 29 dyrektywy 95/46 Nr 15/2011 (WP 187)*, „Monitor Prawniczy" 2012, Nr 7 (dodatek).

Mednis A., *Wymóg oceny skutków przetwarzania w ogólnym rozporządzeniu o ochronie danych*, „Monitor Prawniczy" 2016, Nr 20 (dodatek).

Konarski X., Sibiga G., *Zmiany w ustawie o ochronie danych osobowych w świetle dyrektywy 95/46/WE*, „Monitor Prawniczy" 2004, Nr 12.

Litwiński P., *Pojęcie danych osobowych w ogólnym rozporządzeniu o ochronie danych osobowych – glosa do wyroku Trybunału Sprawiedliwości z 19.10.2016 r. w sprawie C-582/14 Patrik Breyer*, „Europejski Przegląd Sądowy" 2017, Nr 5.

Parkins D., *Regulating the internet giants - The world's most valuable resource is no longer oil, but data*, "The Economist", 06.05.2017.

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

Piskorz-Ryń A., *Prawo dostępu do informacji a ponowne wykorzystywanie informacji sektora publicznego – glosa do wyroku TSUE z 27.10.2011 r. w sprawie C-362/10, Komisja Europejska przeciwko Polsce*, „Europejski Przegląd Sądowy" 2015, Nr 5.

Piskorz-Ryń A., *Zasady ponownego wykorzystywania informacji publicznej będącej utworem w rozumieniu ustawy z dnia 4 lipca 1994 r. o prawie autorskim i prawach pokrewnych*, „Zeszyty Naukowe Sądownictwa Administracyjnego" 2014, Nr 1.

Piskorz-Ryń A., *Opłaty za udostępnianie informacji publicznej do ponownego wykorzystania*, „Kwartalnik Prawa Publicznego" 2012, Nr 3.

Piskorz-Ryń A., *Pojęcie ponownego wykorzystywania informacji sektora publicznego w świetle dyrektywy 2003/98/WE*, „Samorząd Terytorialny" 2015, Nr 4.

Piskorz-Ryń A., *Hybrydowy charakter prawa do ponownego wykorzystywania – wybrane zagadnienia*, „Samorząd Terytorialny" 2017, Nr 1-2.

Polanowski A., *Przepływ danych nieosobowych. Ramy swobodnego przenoszenia informacji w prawie europejskim*, „Biuletyn Euro Info" 2019, Nr 1.

Romanowski M., Weber-Elżanowska A. M., *Prawo członka organu spółki kapitałowej do „bycia zapomnianym" - glosa do wyroku Trybunału Sprawiedliwości z dnia 9 marca 2017 r., C-398/15, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatore Manniemu*, „Europejski Przegląd Sądowy" 2017, Nr 8.

Safjan M., *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, „Państwo i Prawo" 2002, Nr 6.

Safjan M., *Refleksje wokół konstytucyjnych uwarunkowań rozwoju ochrony dóbr osobistych*, „Kwartalnik Prawa Prywatnego" 2002, Z. 1.

Sakowska M., *Pojęcie „zbiór danych" na gruncie ustawy o ochronie danych osobowych*, „Radca Prawny" 2005, Nr 2.

Sakowska-Baryła M., *Konstytucjonalizacja prawa do ochrony danych osobowych w Polsce*, „Przegląd Prawa Konstytucyjnego" 2016, Nr 4 (32).

Sibiga G., *Dostęp do informacji publicznej a prawa do prywatności jednostki i ochrony jej danych osobowych*, „Samorząd Terytorialny" 2003, Nr 11.

Sibiga G., *Opinia prawna o projekcie ustawy o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw (druk 4434) z dnia 26 lipca 2011 r.*, Sejm VII kadencji, druk nr 4555.

Sibiga G, „*Informacja publiczna" oraz „informacja sektora publicznego" – różnice pomiędzy pojęciami wyznaczającymi zakres stosowania ustaw informacyjnych*, „Informacja w Administracji Publicznej" 2016, Nr 4.

Sibiga G., *Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych osobowych – wybrane zagadnienia*, „Monitor Prawniczy" 2016, Nr 20 (dodatek).

Sibiga G., *Skarga do organu nadzorczego oraz jej rozpatrzenie według ogólnego rozporządzenia o ochronie danych. Postępowanie w przedmiocie skargi osoby, której dane dotyczą*, „Prawo Mediów Elektronicznych" 2017, Nr 4 .

Sibiga G., Syska K., *Działania organizacyjne i informacyjne związane z wyznaczeniem i wykonywaniem funkcji inspektora ochrony danych*, „Monitor Prawniczy" 2017 nr 20 (dodatek).

Sibiga G., *Kryterium zadania publicznego w ustawie z 10.5.2018 r. o ochronie danych osobowych oraz jego konsekwencje dla wykonania obowiązków administratora danych oraz realizacji praw osoby, której dane dotyczą*, „Monitor Prawniczy" 2018, Nr 22 (dodatek).

Sibiga G., Małobęcka-Szwast I., *Relacje prawa do informacji publicznej oraz prawa do ochrony danych osobowych w świetle ogólnego rozporządzenia o ochronie danych*, „Monitor Prawniczy" 2019, Nr 22 (dodatek).

Sibiga G., *Jawność – tajność. Dokąd zmierzają relacje obywatela z władzą*, „Monitor Prawniczy" 2019, Nr 2.

Sobczyk P., *Ochrona danych osobowych jako element prawa do prywatności*, „Zeszyty prawnicze UKSW" 2009, Nr 1.

Sybilski D., *Ponowne wykorzystywanie informacji sektora publicznego a ochrona danych osobowych według ogólnego rozporządzenia o ochronie danych oraz dyrektywy 2003/98/WE – wybrane zagadnienia*, „Prawo Mediów Elektronicznych" 2017, Nr 4.

Sybilski D., *Warunki ponownego wykorzystywania informacji sektora publicznego* „Informacja w administracji publicznej" 2017, Nr 4.

Sybilski D., *Centralne Repozytorium Informacji Publicznej jako tryb ponownego wykorzystywania informacji*, „Opolskie studia administracyjno-prawne" 2018, Nr XVI/2.

Sybilski D., *Zagadnienie ponownego wykorzystywania kodu źródłowego programu komputerowego,* „Informacja w administracji publicznej" 2018, Nr 2.

Sybilski D., *Obowiązki informacyjne podmiotu zobowiązanego do udostępnienia informacji w celu ponownego wykorzystywania,* „Informacja w administracji publicznej" 2018, Nr 1.

Sybilski D., *Projekt nowej dyrektywy o ponownym wykorzystywaniu informacji sektora publicznego* „Informacja w administracji publicznej" 2018, nr 3.

Sybilski D., *Jawne dane osobowe ekspertów przygotowujących podstawę programową dla szkół,* „Informacja w administracji publicznej" 2019, Nr 1.

Sybilski D., *Ustawa o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych – kluczowe założenia,* „Informacja w administracji publicznej" 2019, Nr 2.

Sybilski D., *Nowelizacja ustawy o ponownym wykorzystywaniu informacji sektora publicznego dostosowująca do przepisów RODO,* „Informacja w administracji publicznej" 2019, Nr 3.

Sybilski D., *Nowelizacja ustawy o ponownym wykorzystywaniu informacji sektora publicznego dostosowująca do przepisów ogólnego rozporządzenia o ochronie danych osobowych*, "Monitor Prawniczy" 2019, Nr 22 (dodatek).

Syska K., *Administrator bezpieczeństwa informacji a inspektor ochrony danych – porównanie przesłanek powołania, statusu i zadań*, „Monitor Prawniczy" 2016, Nr 20 (dodatek).

Szarfenberg R., Polityka publiczna - zagadnienia i nurty teoretyczne, „Studia z polityki publicznej" 2016, Nr 1.

Szustakiewicz P., *Wzajemny stosunek dwóch ustaw tworzących polski system dostępu do informacji publicznej*, „Informacja w Administracji Publicznej" 2017, Nr 3.

Szymielewicz K., *Reforma europejskiego prawa o ochronie danych osobowych z perspektywy praw obywateli – więcej czy mniej ochrony?*, „Monitor Prawniczy" 2016, Nr 20 (dodatek).

Tene O., Polonetsky J., *Privacy in the Age of Big Data: A Time For Big Decisions*, „Stanford Law Review Online" 2012, Nr 64.

Wiewiórowski W.R., *Nowe ramy ochrony danych osobowych w Unii Europejskiej*, „Monitor Prawniczy" 2012, Nr 7 (dodatek).

Wróbel M., *Prawo do „bycia zapomnianym" – glosa – C-131/12*, „Monitor Prawniczy" 2017, Nr 2.

Zimny W., Przesłanki legalizujące przetwarzanie, „Biuletyn Administratorów Bezpieczeństwa Informacji" 2000, nr 4.

Opinie i Wytyczne Grupy Roboczej Art. 29

Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013.

Opinion 06/2013 on open data and public sector information ('PSI') re-use. Adopted on 5 June 2013.

Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Adopted on 2 April 2013.

Opinion 05/2014 on Anonymisation Techniques. Adopted on 10 April 2014.

Opinion 02/2016 on the publication of Personal Data for Transparency purposes in the Public Sector. Adopted on 8 June 2016.

Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679. Adopted on 4 April 2017.

Guidelines on automated individual decision-making and Profiling for the purpose of Regulation 2016/679. Adopted on 3 October 2017.

Ekspertyzy, raporty, opinie dostępne *on-line*

Abrams M, *The origins of personal data and its implications for governance*, The Information Accountability Foundation, March 2014.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2510927

Arnaut C., Pont M., Scaria E., Berghmans A., Leconte S., *Study on data sharing between companies in Europe. Final report*, European Commission DG Communications Networks, Content & Technology, 2018.
https://op.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en

Information Commissioner, *Big data, artificial intelligence, machine learning and data protection*, 2017.09.04, Version: 2.2.
https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

Gumularz M., Ekspertyza dotycząca czynności niezbędnych do przeprowadzenia oceny skutków ochrony danych osobowych na potrzeby ponownego wykorzystywania informacji sektora publicznego, ekspertyza zlecona przez Ministerstwo Cyfryzacji, 30.08.2019 r. https://mc.bip.gov.pl/rok-2017-2018-2019/ekspertyza-dotyczaca-czynnosci-niezbednych-do-przeprowadzenia-oceny-skutkow-ochrony-danych-osobowych-na-potrzeby-ponownego-wykorzystywania-informacji-sektora-publicznego.html

Fajgielski P., Młynarska-Sobaczewska A., Piskorz-Ryń A., Sibiga G., Ekspertyza Prawna - Rozwiązania mogące stanowić podstawę do zmian przepisów regulujących zasady dostępu do informacji publicznej i jej ponownego wykorzystywania, Instytut Nauk Prawnych Polskiej Akademii Nauk, 19.07.2013 r., ekspertyza zlecona przez Ministerstwo Cyfryzacji. https://mc.bip.gov.pl/fobjects/download/96100/rozwiazania-mogace-stanowic-podstawe-do-zmian-przepisow-regulujacych-zasady-pdf.html

G. Sibiga, Opinia prawna o projekcie ustawy o zmianie ustawy o dostępie do informacji publicznej oraz niektórych innych ustaw (druk 4434), Sejm VI kadencja, 26.07.2011 r. http://orka.sejm.gov.pl/rexdomk6.nsf/Opdodr?OpenPage&nr=4434

G. Vickery, Review of recent studies on psi re-use and related market developments, Paryż 2011 https://ec.europa.eu/digital-single-market/en/news/review-recent-studies-psi-reuse-and-related-market-developments

Open data handbook, http://opendatahandbook.org/guide/en/what-is-open-data/

PRZEMYSŁ +. Gospodarka oparta o dane, Ministerstwo Cyfryzacji 2018 https://www.gov.pl/web/cyfryzacja/gospodarka-oparta-o-dane-przemysl-

Orzecznictwo

Wyrok TSUE z 27.10.2011 r., C-362/10.

Wyrok TSUE z 13.05.2014 r., C-131/12.

Wyrok TSUE z 19.10.2016 r., C-582/14.

Wyrok TSUE z 09.03.2017 r., C-398/15.

Wyrok SN z 08.11.2012 r., I CSK 190/12.

Wyrok TK z 19.5.1998 r., U 5/97.

Wyrok TK z 12.11.2002, SK 40/01.

Wyrok TK z 20.03.2006 r., K 17/05.

Wyrok NSA z 19.11.2001 r., II SA 2702/00.

Wyrok NSA z 30.1.2002 r., II SA 1098/01.

Wyrok NSA z 30.10.2002 r., II SA 1956/02.

Wyrok NSA z 25.03.2002 r., II SA 4059/02.

Wyrok NSA z 25.03.2003 r., II SA 4059/02.

Wyrok NSA z 02.07.2003 r., II SA 837/03.

Wyrok NSA z 14.11.2003 r., II SAB 199/03.

Wyrok NSA z 31.05.2004 r., OSK 205/04.

Wyrok NSA z 13.7.2004 r., OSK 507/04.

Wyrok NSA z 12.12.2006 r., I OSK 123/06.

Wyrok NSA z 09.02.2007 r., I OSK 517/06.

Wyrok NSA z 5.2.2008 r., I OSK 37/07.

Wyrok NSA z 16.06.2009 r., I OSK 89/09.

Wyrok NSA z 15.07.2010 r., I OSK 707/10.

Wyrok NSA z 01.12.2011 r., I OSK 1150/11.

Wyrok NSA z 01.12.2011 r., I OSK 1516/11.

Wyrok NSA z 12.07.2011 r., I OSK 610/11.

Wyrok NSA z 15.7.2011 r., I OSK 667/11.

Wyrok NSA z 01.09.2011 r., I OSK 1002/11.

Wyrok NSA z 20.01.2012 r., I OSK 2118/11.

Wyrok NSA 27.01.2012 r., I OSK 2130/11.

Wyrok NSA z 29.02.2012 r., I OSK 2215/11.

wyrok NSA z 06.09.2012 r., I OSK 1274/12.

Wyrok NSA z 14.09.2012 r., I OSK 1177/12.

Wyrok NSA z 31.01.2013 r., I OSK 2571/12.

Wyrok NSA z 05.04.2013 r., I OSK 175/13.

Wyrok NSA z 31.07.2013 r., I OSK 742/13.

Wyrok NSA z 03.01.2012 r., I OSK 2157/11.

Wyrok NSA z 15.06.2015 r., I OSK 3217/14.

Wyrok NSA z 30.9.2015 r., I OSK 2093/14.

Postanowienie NSA z 13.01.2016 r., I OSK 2932/15.

Wyrok NSA z 05.01.2016 r., I OSK 3184/14.

Wyrok NSA 22.03.2016 r., I OSK 2317/14.

Wyrok NSA z 03.04.2016 r., I OSK 2563/14.

Wyrok NSA z 08.06.2016 r., I OSK 3110/14.

Wyrok NSA z 15.06.2016 r., I OSK 3217/14.

Wyrok NSA z 25.11.2016 r., I OSK 2153/14.

Wyrok NSA z 19.12.2016 r., I OSK 2060/16.

Wyrok NSA z 21.06.2018 r., SA/Wa 735/17.

Wyrok NSA z 01.08.2019 r. I OSK 2270/17.

Wyrok WSA w Warszawie z 11.3.2004 r., II SA 1974/03.

Wyrok WSA w Warszawie 3.06.2004 r., II SA/Wa 328/04.

Wyrok WSA w Kielcach z 26.07.2008 r., II SAB/Ke 7/08.

Wyrok WSA w Warszawie z 29.10.2007 r., II SAB/Wa 85/07.

Wyrok WSA w Krakowie z dnia 30.01.2009 r., II SAB/Kr 109/08.

Wyrok WSA w Krakowie z 16.10.2012 r., II SAB/Kr 138/12.

Wyrok WSA w Gdańsku z 04.09.2013 r., II SA/Gd 447/13.

Wyrok WSA w Szczecinie z 06.02.2014 r., II SAB/Sz 114/13.

Wyrok WSA w Warszawie z 16.03.2017 r., II SA/Wa 1890/16.

Wyrok WSA w Gorzowie Wielkopolskim z 19.05.2016 r., II SAB/Go 33/16.

Wyrok WSA we Wrocławiu z 09.11.2016 r., IV SAB/Wr 183/16.

Wyrok WSA w Łodzi z 20.04.2017 r., II SA/Łd 100/17.

Wyrok WSA w Poznaniu z 06.04.2017 r., IV SA/Po 47/17.

Wyrok WSA w Warszawie z dnia 30.03.2017 r., II SA/Wa 1819/16.

Wyrok WSA w Gdańsku z 13.02.2018 r., II SA/Gd 665/18 (nieprawomocny).

Wyrok WSA w Olsztynie z 19.10.2018 r., II SA/Ol 542/18 (nieprawomocny).

Wyrok WSA w Warszawie z 11.12.2019, II SA/Wa 1030/19 (nieprawomocny).