Ponowne wykorzystywanie informacji sektora publicznego a ochrona danych osobowych według ogólnego rozporządzenia o ochronie danych oraz dyrektywy 2003/98/WE – wybrane zagadnienia

Dominik Sybilski[1]

Informacje sektora publicznego (ISP), które są przekazywane każdemu zainteresowanemu do ponownego wykorzystywania, mogą zawierać dane osobowe. Problem kolizji prawa do wykorzystywania informacji z podstawowym prawem do prywatności i ochroną danych osobowych jest niezwykle aktualny. Ustawa z 25.2.2016 r. o ponownym wykorzystywaniu informacji sektora publicznego[2] weszła w życie 16.6.2016 r. Obecnie trwają prace nad reformą prawa krajowego, która ma na celu wykonanie przepisów 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[3], które zacznie obowiązywać od 25.5.2018 r. W przypadku ponownego wykorzystywania ISP, gdy zagrożona jest ochrona prywatności i ochrona danych osobowych, konieczne jest stosowanie zrównoważonego podejścia. Dotyczy to zarówno prawodawcy na etapie projektowania aktów prawnych, jak i dysponentów danych udostępniających ISP do ponownego wykorzystywania. Pomocne w tym zakresie mogą być wytyczne Grupy Roboczej art. 29 zawarte w opinii 06/2013 w sprawie otwartych danych i ponownego wykorzystywania ISP.

W niniejszym opracowaniu omówiono wybrane zagadnienia dotyczące realizacji prawa do ponownego wykorzystywania informacji sektora publicznego w kontekście konieczności zapewnienia ochrony danych osobowych według dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego[4] oraz rozporządzenia ogólnego. W szczególności analizie poddano zalecenia Grupy Roboczej art. 29 zawarte w Opinii 06/2013 w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego[5] dla nowego porządku prawnego obowiązującego po 25.5.2018 r. Artykuł stanowi wprowadzenie do omawianej problematyki.

Uwagi wstępne

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego wdrożyła do polskiego porządku prawnego dyrektywę 2013/37/UE Parlamentu Europejskiego i Rady z 26.6.2013 r. zmieniającą dyrektywę 2003/98/WE w sprawie ponownego wykorzystywania informacji sektora publicznego[6]. Implementacja dyrektywy zbiegła się z zakończeniem prac nad unijną reformą ochrony danych osobowych, tj. przyjęciem rozporządzenia ogólnego. Od 25.5.2018 r. rozporządzenie będzie obowiązywało we wszystkich państwach UE. Obecnie trwają prace nad reformą prawa krajowego, która ma na celu wykonanie przepisów rozporządzenia.

Informacje sektora publicznego, które są przekazywane każdemu zainteresowanemu do ponownego wykorzystywania, mogą zawierać dane osobowe. Problem kolizji prawa do wykorzystywania informacji, zakotwiczonego w konstytucyjnej zasadzie jawności oraz wolności rozpowszechniania informacji z podstawowym prawem do prywatności i ochroną danych osobowych, jest zatem niezwykle aktualny.

Ponowne wykorzystywanie informacji sektora publicznego

Instytucja ponownego wykorzystywania została po raz pierwszy wprowadzona do polskiego porządku prawnego ustawą z 16.9.2011 r. o zmianie ustawy o dostępie do informacji publicznej i niektórych innych ustaw[7], która stanowiła implementację dyrektywy 2003/98/WE. Nowelizacja ta wprowadziła do ustawy z 6.9.2001 r. o dostępie do informacji publicznej[8] rozdział 2a pt. Ponowne wykorzystywanie informacji publicznej.

W wyniku przeprowadzonego przeglądu wykonania dyrektywy 2003/98/WE podjęto decyzję o jej nowelizacji. Przy-

[1] Asystent w Zakładzie Prawa Administracyjnego Instytutu Nauk Prawnych PAN. Autor specjalizuje się w prawie dostępu do informacji i ponownego jej wykorzystywania.

[2] Dz.U. poz. 352; dalej jako: WykInfPubU.

[3] Dz.Urz. UE L Nr 119, s. 1; dalej jako: ogólne rozporządzenie lub RODO.

[4] Dz.Urz. UE L Nr 345, s. 90; dalej jako: dyrektywa 2003/98/WE.

[5] Grupa robocza art. 29 (Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych ustanowiona na mocy art. 29 dyrektywy 95/46/WE) w związku z wejściem w życia RODO zostanie zastąpiona przez Europejską Radę Ochrony Danych.

[6] Dz.Urz. UE L Nr 175, s. 1; dalej jako: dyrektywa 2013/37/UE.

[7] Dz.U. Nr 204, poz. 1195.

[8] T.j. Dz.U. z 2016 r. poz. 1764 ze zm.; dalej jako: DostInfPubU.

jęta w 2013 r. dyrektywa 2013/37/UE zmieniająca dyrektywę 2003/98/WE stanowiła wykonanie celów, o których mowa w Komunikacie z 12.12.2011 Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów pt. Otwarte dane – siła napędowa innowacji, wzrostu gospodarczego oraz przejrzystego zarządzania[9]. Celem inicjatywy Komisji było zwiększenie wykorzystania potencjału ISP dla wzrostu konkurencyjności i innowacyjności gospodarki europejskiej. Podstawową zmianą dyrektywy 2003/98/WE było rozszerzenie zakresu podmiotowego ponownego wykorzystywania o biblioteki, muzea i archiwa. Treści będące w posiadaniu tych podmiotów na gruncie dyrektywy 2003/98/WE podlegały wyłączeniu z ponownego wykorzystywania. Inną istotną zmianą było wprowadzenie ogólnej zasady, zgodnie z którą wszystkie dokumenty udostępniane przez organy sektora publicznego mogą być ponownie wykorzystane do dowolnych celów komercyjnych lub niekomercyjnych.

Dyrektywa 2013/37/UE została implementowana przepisami ustawy o ponownym wykorzystywaniu informacji sektora publicznego, które obowiązują od 16.6.2016 r. Ustawodawca zaproponował nowy sposób wdrożenia zmienianej dyrektywy w polskim systemie prawnym, który miał zapewnić, że rozwiązania dotyczące ponownego wykorzystywania będą bardziej przejrzyste i łatwiejsze w stosowaniu[10]. Zakładał on wyodrębnienie przepisów o ponownym wykorzystywaniu z ustawy o dostępie do informacji publicznej oraz uregulowanie zasad i procedury ponownego wykorzystywania w nowej ustawie. Takie rozwiązanie miało w sposób precyzyjniejszy i bardziej zrozumiały dla adresatów norm prawnych rozróżnić instytucje dostępu do informacji oraz ponownego wykorzystywania.

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego określa zasady i tryb udostępniania i przekazywania ISP w celu ponownego wykorzystywania, podmioty zobowiązane, które udostępniają lub przekazują te informacje[11], warunki ponownego wykorzystywania oraz zasady ustalania opłat. Co istotne, przepisy o ponownym wykorzystywaniu opierają się na systemach dostępu do informacji obowiązujących w państwach członkowskich[12], dlatego też – zgodnie z art. 7 ust. 1 WykInfPubU – przepisy tej ustawy nie naruszają prawa dostępu do informacji publicznej ani wolności jej rozpowszechniania, ani przepisów innych ustaw określających zasady, warunki i tryb dostępu do informacji będących ISP.

Dla omawianej tematyki kluczowe znaczenie ma wyjaśnienie pojęć ISP oraz ponownego wykorzystywania.

Ustawa o ponownym wykorzystywaniu informacji sektora publicznego wprowadziła do polskiego porządku prawnego nowe pojęcie informacji sektora publicznego (ISP). Przed wejściem w życie tej ustawy zakres przedmiotowy ponownego wykorzystywania wyznaczało pojęcie informacji publicznej. Obecnie zakres ten wyznacza ISP[13]. Zgodnie z art. 2 ust. 1 WykInfPubU jest nią każda treść lub jej część, niezależnie od sposobu utrwalenia, w szczególności w postaci papierowej, elektronicznej, dźwiękowej, wizualnej lub audiowizualnej, będąca w posiadaniu podmiotów zobowiązanych. Zakres pojęcia ISP jest zatem szerszy od pojęcia informacji publicznej (IP) i odpowiada wprost definicji dokumentu, o którym mowa w art. 2 pkt 3 dyrektywy 2003/98/WE. Przyjęcie takiego rozwiązania uzasadnione było przede wszystkim poszerzeniem zakresu podmiotowego dyrektywy 2003/98/WE o biblioteki, archiwa i muzea. Zasoby będące w posiadaniu tych instytucji, mieszczące się w pojęciu dokumentu, o którym mowa w dyrektywie, wykraczają poza zakres pojęcia IP[14]. Oparcie zakresu przedmiotowego ponownego wykorzystywania o ISP – w porównaniu z porządkiem prawnym regulowanym przepisami ustawy o dostępie do informacji publicznej – zwiększa zatem ryzyko udostępnienia w trybie WykInfPubU informacji zawierających dane osobowe[15].

Zawarta w art. 1 ust. 3 WykInfPubU 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 ISP w celach komercyjnych lub niekomercyjnych innych niż pierwotny publiczny cel, dla którego informacja została wytworzona. Przy czym ponownym wykorzystywaniem nie jest udostępnianie lub przekazanie ISP przez podmiot wykonujący zadania publiczne innemu podmiotowi wykonującemu zadania publiczne wyłącznie w celu realizacji takich zadań.

W ocenie skutków wniosku zmiany dyrektywy 2003/98/WE wskazuje się, że ponowne wykorzystywanie ISP oznacza wszelkie twórcze wykorzystywanie danych, np. przez zwiększenie wartości danych, łączenie danych z różnych źródeł w celu wytworzenia pożądanego rezultatu, rozwijanie aplikacji, dokonywane zarówno w celach komercyjnych, jak

[9] KOM(2011) 882.

[10] Uzasadnienie do rządowego projektu ustawy o ponownym wykorzystywaniu informacji sektora publicznego, Druk Nr 141, http://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=141(dostęp z 1.10.2016 r.).

[11] W art. 5 WykInfPubU rozróżniono dwa tryby udzielenia ISP do ponownego wykorzystywania. Udostępnienie ISP odnosi się do bezwnioskowego udzielenia ISP poprzez systemy teleinformatyczne lub inny sposób (w szczególności BIP i centralne repozytorium), z kolei przekazanie ISP obejmuje wyłącznie udzielenie ISP na wniosek. W artykule użyto obydwu sformułowań wymiennie bez rozróżnienia na sposób udzielenia ISP.

[12] Art. 1 ust. 3 dyrektywy 2003/98/WE.

[13] Zob. szerzej: *G. Sibiga*, „Informacja publiczna" oraz „informacja sektora publicznego" – różnice pomiędzy pojęciami wyznaczającymi zakres stosowania ustaw informacyjnych, Informacja w Administracji Publicznej 2016, Nr 4, s. 39–42.

[14] Uzasadnienie do rządowego projektu ustawy o ponownym wykorzystywaniu informacji sektora publicznego, Druk Nr 141.

[15] Por. *A. Piskorz-Ryń* (red.), Ustawa o ponownym wykorzystywaniu informacji sektora publicznego. Komentarz, Wrocław 2017, s. 93.

i niekomercyjnych. Instytucja ponownego wykorzystywania koncentruje się na wykorzystaniu gospodarczej wartości ISP, gdzie służy ona jako materiał wyjściowy 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 ich źródłem (podmiot publiczny) a końcowym użytkownikiem[16].

Dane osobowe w dyrektywie 2003/98/WE i jej zmianie

Prawo do ponownego wykorzystywania podlega licznym ograniczeniom. Jedną z przesłanek ograniczających ponowne wykorzystywanie ISP na gruncie ww. 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[17]. Przepis ten oznacza, 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 ustawy z 29.8.2997 r. o ochronie danych osobowych[18].

Co istotne, dyrektywa 2013/37/UE 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, 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.

Implementując dyrektywę 2003/37/WE zarówno w jej pierwotnym, jak i w zmienionym brzmieniu, krajowy ustawodawca nie zdecydował o wprowadzeniu przesłanki ograniczającej prawo do ponownego wykorzystywania ze względu na ochronę danych osobowych. Za próbę określenia relacji pomiędzy prawem do ponownego wykorzystywania a ochroną danych osobowych nie sposób uznać art. 7 ust. 2 WykInfPubU, zgodnie z którym przepisy tej ustawy nie naruszają przepisów ustawy o ochronie danych osobowych[19].

Wątpliwości w zakresie relacji obu regulacji nie eliminuje również art. 6 ust. 2 WykInfPubU, zgodnie z którym prawo do ponownego wykorzystywania 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. Przepis ten powtarza normę zawartą w art. 5 ust. 2 DostInfPubU ograniczającą dostęp do informacji publicznej.

Ponowne wykorzystywanie w przepisach rozporządzenia

Przepisy RODO określają – w art. 86 – relację prawa ochrony danych osobowych z prawem dostępu do dokumentów. Dane osobowe[20] zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny lub podmiot prywatny w celu wykonania zadania realizowanego w interesie publicznym, mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii lub prawem państwa

[16] Impact Assessment Accompanying The Document Proposal For A Directive Of The European Parliament And The Council amending European Parliament and Council Directive 2003/98/EC on the re-use of public sector information SEC (2011) 1552 final, s. 10.

[17] Dz.Urz. WE L Nr 281, s. 31.

[18] T.j. Dz.U. z 2016 r. poz. 922 ze zm.; dalej jako: OchronaDanychU.

[19] *G. Sibiga*, Dopuszczalny zakres polskich przepisów o ochronie danych osobowych po rozpoczęciu obowiązywania ogólnego rozporządzenia o ochronie danych osobowych – wybrane zagadnienia, Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016, Warszawa 2016, s. 20. Zob. również: *A. Piskorz-Ryń* (red.), Ustawa…, s. 196–215.

[20] W myśl art. 4 RODO dane osobowe oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osobie, której dane dotyczą). Możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora, takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.

członkowskiego, któremu podlegają ten organ lub podmiot, dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych. Przepis ten należy interpretować łącznie z motywem 154 preambuły, który stanowi, że publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny. Organ publiczny (podmiot publiczny) powinien móc publicznie ujawniać dane osobowe z dokumentów przez siebie przechowywanych, jeżeli takie ujawnienie jest przewidziane przepisami prawa Unii lub prawa państwa członkowskiego, któremu organ (lub podmiot) ten podlega.

Artykuł 86 RODO należy zaliczyć do tej kategorii przepisów ogólnego rozporządzenia, które – zdaniem *G. Sibigi* – powinny być obligatoryjnie przyjęte w prawie krajowym[21]. 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[22]. Szersza analiza kwestii wyważania prawa do ochrony danych osobowych i publicznego dostępu do dokumentów, który na gruncie prawa krajowego jest uregulowany przepisami ustawy o dostępie do informacji publicznej, wykracza poza ramy niniejszego opracowania. Niemniej kwestia ta będzie wywoływała konsekwencje dla ponownego wykorzystywania ISP, bo – jak wskazano powyżej – przepisy dyrektywy 2003/37/WE opierają się na systemach dostępu (do dokumentów) istniejących w państwach członkowskich.

Dla omawianej tematyki istotne jest, że – w myśl motywu 154 – przepisy krajowe powinny godzić ponowne wykorzystywanie ISP z prawem do ochrony danych osobowych i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie rozporządzenia. Rozporządzenie nie daje jednak żadnych nowych wytycznych, jak zrealizować ten cel. Motyw 154 powtarza bowiem przywołane wyżej postanowienia dyrektywy 2003/98/WE w brzmieniu nadanym dyrektywą 2013/37/UE (art. 1 ust. 4 lit. cc).

Ponowne wykorzystywanie ISP zawierających dane osobowe

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 ISP stanowiących dane osobowe będzie ich przetwarzaniem w rozumieniu przepisów o ochronie danych osobowych, np. przez gromadzenie danych i dokonywanie na nich dalszych operacji[23]. 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[24].

Zarówno podmioty zobowiązane będące dysponentem danych, jak i „każdy zainteresowany", który pozyska dane jako ISP w trybie ich ponownego wykorzystywania, przetwarzając dane osobowe, od 25.5.2018 r. będą musiały respektować zasady ich przetwarzania określone w przepisach RODO[25]. Ich szczegółowa analiza wykracza poza ramy artykułu, trzeba jednak zaznaczyć, że rozporządzenie poszerzyło uprawnienia osób, których dane są poddane przetwarzaniu, np. w zakresie uprawnień informacyjnych wynikających z zasady przejrzystości.

Wnioski, jakie płyną z analizy przytoczonych aktów prawa UE oraz ustawy o ponownym wykorzystywaniu informacji sektora publicznego, mogą być następujące. Po pierwsze, prawo do ponownego wykorzystywania nie jest stosowane automatycznie i nie ma charakteru nadrzędnego wobec właściwych przepisów o ochronie danych. Po drugie, przepisy te jednocześnie nie wprowadzają bezwzględnego zakazu przekazywania ISP zawierających dane osobowe do ponownego wykorzystywania. Przepisy o ochronie danych osobowych oraz o ponownym wykorzystywaniu pozostają równorzędne. Ich współstosowanie może rodzić dla praktyki pewne trudności[26].

Zasadne będzie odwołanie się do rekomendacji Grupy Roboczej art. 29 zawartych w Opinii 06/2013[27]. Opinia ta została wydana już na gruncie dyrektywy 2013/37/UE, natomiast przed przyjęciem rozporządzenia. Analiza przepisów RODO pozwala wyprowadzić wniosek, że zalecenia zawarte w Opinii 06/2013 co do zasady pozostają aktualne i do czasu wydania nowych w tym obszarze rekomendacji przez Europejską Radę Ochrony Danych mogą być pomocniczo stosowane. Warto w tym miejscu zauważyć, że Wytyczne w sprawie zalecanych licencji standardowych, zbiorów da-

[21] *G. Sibiga*, Dopuszczalny zakres…, s. 19.

[22] *Ibidem*.

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

[24] Opinia 06/2013, s. 31.

[25] Podstawowe zasady przetwarzania danych osobowych zostały enumeratywnie wymienione w art. 5 RODO. Są to: zasada zgodności z prawem, rzetelności i przejrzystości; zasada ograniczenia celu przetwarzania danych; zasada minimalizacji danych; zasada prawidłowości danych; zasada ograniczenia przechowania danych; zasada; integralności i poufności danych; zasada rozliczalności.

[26] O koncepcji współstosowania przepisów ustawy o ponownym wykorzystywaniu informacji sektora publicznego i ustawy o ochronie danych osobowych 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*, Ponowne wykorzystywanie informacji sektora publicznego, Ministerstwo Cyfryzacji 2016.

[27] Grupa Robocza ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, ustanowiona na mocy art. 29 dyrektywy 95/46/WE w związku z wejściem w życia ogólnego rozporządzenia o ochronie danych zostanie zastąpiona przez Europejską Radę Ochrony Danych.

nych i opłat za ponowne wykorzystanie dokumentów[28], wydane przez Komisję Europejską w celu wsparcia państw członkowskich w wykonaniu przepisów dyrektywy 2013/37/UE, zalecają stosowanie Opinii 06/2013 w zakresie ponownego wykorzystania danych osobowych.

W opinii tej wskazano, że przy stosowaniu dyrektywy 2003/98/WE i przepisów o ochronie danych do 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 takich zanonimizowanych danych. Po trzecie, może podjąć decyzję o udostępnieniu danych osobowych do ponownego wykorzystania (w razie potrzeby podlegającą szczególnym warunkom i odpowiednim zabezpieczeniom).

Podejmując decyzję, podmiot zobowiązany musi w szczególności uwzględnić – wymienione wcześniej – wynikające z art. 1 ust. 2 lit. cc dyrektywy 2003/98/WE, jak również z motywu 154 zd. 7 RODO trzy okoliczności, z których wszystkie są wyłączone z zakresu stosowania ponownego wykorzystywania.

Grupa Robocza art. 29 rekomenduje, aby państwa członkowskie na poziomie przepisów krajowych jasno wskazały, które dane 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[29].

W praktyce problematyczna może się okazać realizacja podstawowej dla ochrony danych zasady celowości. Zasada ta wymaga, by dane osobowe, które zgromadzono do konkretnego celu, nie zostały następnie wykorzystane do innego celu niezgodnego z celem pierwotnym[30]. Podmiot, który pozyska ISP zawierające dane osobowe – niezależnie, czy od dysponenta danych, czy ze źródeł publicznie dostępnych – zgodnie z definicją ponownego wykorzystywania będzie je wykorzystywać, czyli przetwarzać, w innych celach niż te, dla których zostały przez podmiot zobowiązany wytworzone. Dyrektywa 2003/98/WE nie wyklucza możliwości, by nałożone w tym względzie warunki dopuszczały przetwarzanie wyłącznie w określonych celach. Dyrektywa ta jednocześnie stanowi, że warunki nie mogą ograniczać niepotrzebnie możliwości ponownego wykorzystywania. Należy wskazać, że postanowienia RODO dotyczące badania zgodności innego celu przetwarzania danych z celem, w którym dane osobowe zostały pierwotnie zebrane (art. 6 ust. 4), co do zasady opierają się na rekomendacjach Grupy Roboczej art. 29 zawartych w Opinii Nr 3/2013 z 2.4.2013 r. w sprawie zasady celowości, a następnie powtórzonych w opinii 06/2013. Analizując, czy dalsze przetwarzanie danych osobowych jest niezgodne z celami, dla których dane te zostały zgromadzone, zdaniem Grupy Roboczej art. 29 należy w szczególności uwzględnić: a) związek między celami, dla których zgromadzono dane osobowe, a celami dalszego przetwarzania; b) kontekst, w jakim gromadzono określone dane osobowe, oraz uzasadnione oczekiwania osób, których dane dotyczą, co do ich dalszego wykorzystania[31]; c) charakter danych osobowych oraz wpływ dalszego przetwarzania tych danych na osoby, których dane dotyczą; d) zabezpieczenia wprowadzone przez administratora w celu zapewnienia uczciwego przetwarzania danych oraz zapobieżenia niepożądanym skutkom dla osób, których dane dotyczą[32].

Aktualne pozostaje przedstawione w Opinii 06/2013 zalecenie, by w przypadku, gdy ISP zawierają dane osobowe i dozwolone jest ich ponowne wykorzystywanie, ponowni użytkownicy znali zasady przetwarzania takich danych od początku. Można tego dokonać poprzez zawarcie odpowiedniego postanowienia w licencji (warunkach ponownego wykorzystywania), przez co ochrona danych osobowych staje się zobowiązaniem umownym[33]. Licencje powinny określać granice wykorzystywania danych, w tym zapewnienie zgodności z celem, dla których zostały pierwotnie zebrane. Oznacza to, że w warunkach licencji należy określić pierwotny cel opublikowania danych oraz operacje, które byłyby z nim zgodne[34].

Grupa Robocza art. 29 zaleca, aby klauzula o ochronie danych była uwzględniania również w sytuacjach, gdy do ponownego wykorzystania udostępnione zostaną zanonimizowane zestawy danych uzyskanych z danych osobowych. Warunki ponownego wykorzystywania danych zanonimizowanych powinny zakazywać ponownej identyfikacji osób fizycznych i ponownego wykorzystania danych osobowych do celów, które mogą mieć wpływ na osoby, których dane dotyczą[35].

Rozporządzenie realizuje koncepcję podejścia do ochrony danych osobowych opartą na ryzyku[36]. Uwzględniając różne potencjalne czynniki ryzyka dla ochrony danych, a w szczególności fakt, że po publicznym udostępnieniu ISP 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[37]. Rozwiązania te po raz pierwszy do polskiego porządku prawnego wprowadza art. 25 RODO.

[28] Dz.Urz. UE C Nr 240, s. 1.

[29] *Ibidem*, s. 10–11.

[30] *Ibidem*, s. 23.

[31] Art. 6 ust. 4 lit. b RODO stanowi o wzięciu pod uwagę kontekstu, w którym zebrano dane osobowe, w szczególności relacji między osobami, których dane dotyczą, a administratorem.

[32] Opinia 06/2013, s. 23.

[33] Na gruncie ustawy o ponownym wykorzystywaniu informacji sektora publicznego postanowienie to mogłoby stanowić element warunków ponownego wykorzystywania przedstawianych w ofercie, o której mowa w art. 23 ust. 1 pkt 3. W ustawie tej wprost nie przewidziano możliwości licencjonowania ISP, natomiast ISP można udostępnić, określając warunki ponownego wykorzystywania.

[34] *P. Drobek*, Ryzyka dla ochrony danych osobowych w związku z ponownym wykorzystywaniem informacji sektora publicznego, [w:] *G. Szpor* (red. nauk.), Jawność i jej ograniczenia, *A. Piskorz-Ryń* (red. tomu), T. V, Dostęp i wykorzystywanie, Warszawa 2015, s. 260.

[35] Opinia 06/2013, s. 32.

[36] *P. Drobek*, Ryzyka…, s. 241 i n.

[37] Opinia 06/2013, s. 32.

Ponadto według Grupy Roboczej art. 29 podmiot zobowiązany powinien przeprowadzić ocenę skutków w zakresie ochrony danych, zanim udostępni ISP 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[38]. O ocenie skutków planowanych operacji przetwarzania dla ochrony danych osobowych stanowi art. 35 RODO.

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[39].

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[40]. Wyniki oceny mogą również prowadzić do podjęcia decyzji o rezygnacji udostępniania ISP zawierających dane osobowe do ponownego wykorzystania[41].

Podsumowanie

W przypadku ponownego wykorzystywania ISP, gdy zagrożona jest ochrona prywatności i ochrona danych osobowych, konieczne jest stosowanie zrównoważonego podejścia. Dotyczy to zarówno prawodawcy na etapie projektowania aktów prawnych, jak i dysponentów danych udostępniających ISP do ponownego wykorzystywania. Z jednej strony przepisy w zakresie ochrony danych osobowych nie powinny stanowić przeszkody w rozwoju rynku ponownego wykorzystywania. Z drugiej strony niezbędne jest poszanowanie prawa do ochrony danych osobowych i prawa do prywatności. Dlatego ważna jest realizacja przez administrację rządową we współpracy z Generalnym Inspektorem Danych Osobowych i interesariuszami postulatu Grupy Roboczej art. 29 dotyczącego ustanowienia i wspierania sieci wiedzy lub centrów doskonałości, a tym samym umożliwienie wymiany dobrych praktyk w zakresie anonimizacji i otwartych danych[42].

[38] *Ibidem*, s. 8.
[39] *P. Drobek*, Ryzyka…, s. 240.
[40] Przeglądu technik anonimizacji dokonała Grupa Robocza art. 29 w Opinii Nr 5/2014 z 10.4.2014 r. w sprawie technik anonimizacji.
[41] *Ibidem*.
[42] Przykładem dobrej praktyk może być sieć anonimizacyjna Zjednoczonego Królestwa (UK Anonymisation Network, UKAN), powołana jako konsorcjum Uniwersytetu w Manchesterze, Uniwersytetu w Southampton, Biura Statystyk Krajowych i Open Data Institute.

Słowa kluczowe: sektor publiczny, dane osobowe, RODO, informacje sektora publicznego, informacja publiczna.

Re-use of public sector information and personal data protection according to the General Data Protection Regulation and the directive 2003/98/EC – selected aspects

Public sector information, which is given to anyone who is interested, may contain personal data. The problem of collision of law to re-use information with right to privacy and data protection is extremely topical. The law of 25.2.2016 on re-use of public sector information took effect on 16.6.2016. Currently, work is conducted in regard to reforming state law which aims to implement provisions of General Data Protection Regulation which will be in force since 25.5.2018. In case of re-use of public sector information, when privacy and personal data protection are in a risk it is necessary to use balanced approach. It regards both the lawmaker on the stage of drafting legal acts, and holders of data who share public sector information in order to re-use it. Guidelines of the Article 29 Working Party might be helpful in this matter, which are included in the Opinion 06/2013. In the present article there is a discussion on selected aspects regarding implementation of the right to re-use of public sector information in the context of necessity to provide personal data protection Special analysis was devoted to recommendation of the Article 29 Working Party for the new legal order effective after 25.5.2018.

Keywords: public sector, personal data, GDPR, information of public sector, public information.