KOMISJA
EUROPEJSKA

Bruksela, dnia 25.11.2020 r.
COM(2020) 767 final

2020/0340 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi)

(Tekst mający znaczenie dla EOG)

{SEC(2020) 405 final} - {SWD(2020) 295 final} - {SWD(2020) 296 final}

UZASADNIENIE

1. KONTEKST WNIOSKU

• Przyczyny i cele wniosku

Niniejsze uzasadnienie towarzyszy wnioskowi dotyczącemu rozporządzenia Parlamentu Europejskiego i Rady[1] w sprawie zarządzania danymi. Jest to pierwszy z zestawu środków zapowiedzianych w europejskiej strategii w zakresie danych z 2020 r.[2] Instrument ten ma na celu zwiększenie dostępności danych na potrzeby ich wykorzystywania poprzez zwiększenie zaufania do pośredników w zakresie danych oraz wzmocnienie mechanizmów udostępniania danych w całej UE. Instrument ten będzie odnosić się do następujących sytuacji:

- udostępnianie danych sektora publicznego do ponownego wykorzystywania w sytuacjach, w których dane te są objęte prawami innych osób[3];
- udostępnianie danych między przedsiębiorstwami w zamian za wynagrodzenie w dowolnej postaci;
- umożliwianie wykorzystywania danych osobowych z pomocą „pośrednika w udostępnianiu danych osobowych", który ma pomagać osobom fizycznym w wykonywaniu ich praw wynikających z ogólnego rozporządzenia o ochronie danych (RODO);
- umożliwianie wykorzystywania danych z pobudek altruistycznych.

• Spójność z przepisami obowiązującymi w tej dziedzinie polityki

Niniejsza inicjatywa obejmuje różnego rodzaju pośredników w zakresie danych, którzy zajmują się zarówno danymi osobowymi, jak i nieosobowymi. Szczególnie ważne jest zatem zachowanie wzajemnej zależności z przepisami dotyczącymi danych osobowych. Dzięki ogólnemu rozporządzeniu o ochronie danych (RODO)[4] i dyrektywie o prywatności i łączności elektronicznej[5] UE ustanowiła solidne i godne zaufania ramy prawne w zakresie ochrony danych osobowych, będące standardem dla całego świata.

Niniejszy wniosek uzupełnia dyrektywę Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (dyrektywa w sprawie otwartych danych)[6]. Niniejszy wniosek dotyczy danych będących w posiadaniu organów sektora publicznego, które to dane są objęte prawami innych osób, a zatem wykraczają poza zakres wyżej wspomnianej dyrektywy. Wniosek ten jest logicznie i spójnie powiązany z pozostałymi inicjatywami zapowiedzianymi w europejskiej strategii w zakresie danych. Ma on na celu ułatwienie udostępniania danych, w tym poprzez zwiększenie zaufania do pośredników w udostępnianiu danych, którzy mają świadczyć usługi w poszczególnych przestrzeniach danych. Jego celem nie jest przyznanie,

---

[1] Ostateczna forma aktu prawnego będzie zależała od treści tego instrumentu.

[2] COM(2020) 66 final.

[3] „Dane, których wykorzystanie jest zależne od praw innych osób" lub „dane objęte prawami innych osób" obejmują dane, które mogą podlegać przepisom o ochronie danych i własności intelektualnej lub zawierać tajemnice przedsiębiorstwa bądź inne szczególnie chronione informacje handlowe.

[4] Dz.U. L 119 z 4.5.2016, s. 1.

[5] Dz.U. L 201 z 31.7.2002, s. 37.

[6] Dz.U. L 172 z 26.6.2019, s. 56.

zmiana ani usunięcie istotnych praw w zakresie dostępu do danych i ich wykorzystywania. Przewiduje się, że tego rodzaju środki znajdą się w ewentualnym akcie o danych (2021 r.)[7].

Inspirację dla tego instrumentu stanowią zasady zarządzania danymi i ich ponownego wykorzystywania opracowane w odniesieniu do danych badawczych. Zasady FAIR[8] stanowią, że takie dane powinny być zasadniczo możliwe do znalezienia, dostępne, interoperacyjne oraz możliwe do ponownego wykorzystania.

- **Spójność z innymi politykami Unii**

Istnieją lub są przygotowywane przepisy sektorowe dotyczące dostępu do danych mające na celu zaradzenie zidentyfikowanym niedoskonałościom rynku w takich dziedzinach, jak: przemysł motoryzacyjny[9], dostawcy usług płatniczych[10], informacje pochodzące z inteligentnych systemów pomiarowych[11], dane dotyczące sieci elektroenergetycznej[12], inteligentne systemy transportowe[13], informacje dotyczące środowiska[14], informacje przestrzenne[15] oraz sektor zdrowia[16]. Niniejszy wniosek ma na celu wsparcie wykorzystywania danych udostępnianych na podstawie obowiązujących przepisów, bez zmieniania tych przepisów lub tworzenia nowych obowiązków sektorowych.

Podobnie wniosek nie narusza przepisów prawa konkurencji i jest zaprojektowany zgodnie z art. 101 i 102 TFUE, a także nie narusza przepisów dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego[17].

2. PODSTAWA PRAWNA, POMOCNICZOŚĆ I PROPORCJONALNOŚĆ

- **Podstawa prawna**

Jako odpowiednią podstawę prawną niniejszego rozporządzenia wskazuje się art. 114 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE). Zgodnie z tym artykułem UE musi przyjąć środki dotyczące zbliżenia przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które mają na celu ustanowienie i funkcjonowanie rynku wewnętrznego w UE. Niniejsza inicjatywa stanowi część europejskiej strategii w zakresie danych z 2020 r., której celem jest wzmocnienie jednolitego rynku danych. Istnieje ryzyko, że wraz ze wzrostem cyfryzacji gospodarki i społeczeństwa państwa członkowskie będą w coraz większym stopniu wprowadzać przepisy w zakresie kwestii związanych z danymi w sposób nieskoordynowany, co pogłębi rozdrobnienie jednolitego rynku. Ustanowienie struktur i mechanizmów zarządzania, które pozwolą opracować skoordynowane podejście do wykorzystywania danych we wszystkich sektorach i państwach

---

7 Zob. COM(2020) 66 final.
8 https://www.force11.org/group/fairgroup/fairprinciples
9 Dz.U. L 188 z 18.7.2009, s. 1, zmienione przez Dz.U. L 151 z 14.6.2018, s. 1.
10 Dz.U. L 337 z 23.12.2015, s. 35.
11 Dz.U. L 158 z 14.6.2019, s. 125; Dz.U. L 211 z 14.8.2009, s. 94.
12 Dz.U. L 220 z 25.8.2017, s. 1. Dz.U. L 113 z 1.5.2015, s. 13.
13 Dz.U. L 207 z 6.8.2010, s. 1.
14 Dz.U. L 41 z 14.2.2003, s. 26.
15 Dz.U. L 108 z 25.4.2007, s. 1.
16 Wniosek ustawodawczy w sprawie europejskiej przestrzeni danych dotyczących zdrowia planowany jest na czwarty kwartał 2021 r. https://eur-lex.europa.eu/resource.html?uri=cellar:91ce5c0f-12b6-11eb-9a54-01aa75ed71a1.0020.02/DOC_2&format=PDF
17 Dz.U. L 178 z 17.7.2000, s. 1.

członkowskich, pomoże zainteresowanym stronom w gospodarce opartej na danych w pełni wykorzystać skalę jednolitego rynku. Przyczyni się to do ustanowienia jednolitego rynku danych poprzez zapewnienie powstania i transgranicznego funkcjonowania nowatorskich usług dzięki zbiorowi zharmonizowanych przepisów.

Polityka cyfrowa jest kompetencją dzieloną między UE a jej państwa członkowskie. Art. 4 ust. 2 i 3 TFUE stanowi, że w dziedzinach jednolitego rynku i rozwoju technologicznego UE może prowadzić określone działania bez uszczerbku dla swobody działania państw członkowskich w tych samych dziedzinach.

- **Pomocniczość (w przypadku kompetencji niewyłącznych)**

Do opracowania ogólnounijnych produktów i usług przedsiębiorstwa często potrzebują danych z szeregu państw członkowskich, ponieważ próbki danych dostępne w poszczególnych państwach członkowskich często nie są wystarczająco bogate i zróżnicowane, by umożliwić rozpoznawanie wzorców z użyciem dużych zbiorów danych lub uczenie się maszyn. Ponadto produkty i usługi oparte na danych opracowane w jednym państwie członkowskim mogą wymagać dostosowania do preferencji klientów w innym państwie członkowskim, a do tego potrzebne są dane lokalne na szczeblu państw członkowskich. W związku z tym musi istnieć możliwość łatwego przepływu danych w ogólnounijnych i międzysektorowych łańcuchach wartości, do czego niezbędne jest wysoce zharmonizowane otoczenie prawne. Ponadto – ze względu na transgraniczny charakter udostępniania danych i znaczenie takiego udostępniania – tylko działanie na poziomie Unii może zapewnić przyjęcie się europejskiego modelu udostępniania danych, obejmującego zaufanych pośredników w zakresie danych na potrzeby udostępniania danych między przedsiębiorstwami i na potrzeby przestrzeni danych osobowych.

Jednolity rynek danych powinien zapewniać możliwość dostępu do danych pochodzących z sektora publicznego, od przedsiębiorstw i od obywateli oraz możliwość korzystania z tych danych w sposób jak najbardziej skuteczny i odpowiedzialny, przy jednoczesnym zachowaniu przez przedsiębiorstwa i obywateli kontroli nad generowanymi przez nich danymi i zabezpieczeniu inwestycji poczynionych w gromadzenie danych. W wyniku zwiększonego dostępu do danych przedsiębiorstwa i organizacje badawcze poczyniłyby postępy pod względem reprezentatywnych osiągnięć naukowych i innowacji rynkowych w całej UE, co jest szczególnie ważne w sytuacjach, w których konieczne jest skoordynowane działanie na szczeblu UE, takich jak kryzys związany z COVID-19.

- **Proporcjonalność**

Inicjatywa ta jest proporcjonalna do zamierzonych celów. Proponowane przepisy tworzą ramy wspomagające, które nie wykraczają poza to, co jest konieczne do osiągnięcia tych celów. Harmonizują one szereg praktyk w zakresie udostępniania danych, respektując przy tym prerogatywy państw członkowskich w odniesieniu do organizowania własnej administracji i stanowienia prawa w dziedzinie dostępu do informacji sektora publicznego. Ramy zgłaszania pośredników w zakresie danych, jak również mechanizmy altruistycznego podejścia do danych służą osiągnięciu wyższego poziomu zaufania do tych usług bez niepotrzebnego ograniczania tej działalności oraz przyczyniają się do rozwoju rynku wewnętrznego w odniesieniu do wymiany takich danych. Inicjatywa ta pozostawi również znaczną elastyczność pod względem stosowania na poziomie sektorowym, w tym w odniesieniu do przyszłego rozwoju europejskich przestrzeni danych.

Proponowane rozporządzenie spowoduje powstanie kosztów finansowych i administracyjnych, które będą ponoszone głównie przez organy krajowe, choć w celu zapewnienia zgodności z obowiązkami określonymi w niniejszym rozporządzeniu niektóre koszty obciążą również użytkowników danych i dostawców usług udostępniania danych. Analiza różnych wariantów oraz ich przewidywanych kosztów i korzyści pozwoliła jednak opracować zrównoważony projekt instrumentu. Pozostawi on organom krajowym wystarczającą elastyczność, aby mogły decydować o poziomie inwestycji finansowych i rozważyć możliwości odzyskania takich kosztów poprzez należności lub opłaty administracyjne, jednocześnie zapewniając ogólną koordynację na szczeblu UE. Podobnie koszty dla użytkowników danych i dostawców usług udostępniania danych będą zrównoważone wartością wynikającą z szerszego dostępu do danych i szerszego ich wykorzystywania, jak również z upowszechniania nowych usług na rynku.

- **Wybór instrumentu**

Wybór rozporządzenia jako instrumentu prawnego jest uzasadniony przewagą elementów wymagających jednolitego stosowania, które nie pozostawia państwom członkowskim marginesu swobody pod względem wykonania i które tworzy w pełni horyzontalne ramy. Elementy te obejmują zgłaszanie dostawców usług udostępniania danych, mechanizmy altruistycznego podejścia do danych, podstawowe zasady mające zastosowanie do ponownego wykorzystywania danych sektora publicznego, które nie mogą być dostępne jako otwarte dane lub nie są objęte sektorowymi przepisami Unii, oraz ustanowienie struktur koordynacyjnych na szczeblu europejskim. Bezpośrednie stosowanie rozporządzenia pozwoliłoby uniknąć okresu i procesu wdrażania w państwach członkowskich, umożliwiając jednocześnie ustanowienie w najbliższej przyszłości wspólnych europejskich przestrzeni danych zgodnie z planem odbudowy dla Europy[18].

Jednocześnie przepisy rozporządzenia nie są nadmiernie nakazowe i pozostawiają przestrzeń na różne poziomy działań państw członkowskich w odniesieniu do elementów, które nie podważają celów inicjatywy, w szczególności organizacji właściwych podmiotów wspierających organy sektora publicznego w wykonywaniu zadań związanych z ponownym wykorzystywaniem niektórych kategorii danych sektora publicznego.

3. WYNIKI OCEN EX POST, KONSULTACJI Z ZAINTERESOWANYMI STRONAMI I OCEN SKUTKÓW

- **Konsultacje z zainteresowanymi stronami**

Internetowe konsultacje publiczne rozpoczęto w dniu 19 lutego 2020 r., czyli w dniu przyjęcia europejskiej strategii w zakresie danych[19], a zakończono w dniu 31 maja 2020 r. W konsultacjach wyraźnie określono, że ich celem było przygotowanie niniejszej inicjatywy, a poruszone w niej zagadnienia znalazły odzwierciedlenie w poszczególnych częściach i pytaniach konsultacji. Konsultacje były skierowane do wszystkich rodzajów zainteresowanych stron.

Komisja otrzymała łącznie 806 opinii, z czego 219 pochodziło od przedsiębiorstw, 119 – od stowarzyszeń przedsiębiorców, 201 – od obywateli Unii, 98 – od instytucji akademickich/badawczych, a 57 – od organów publicznych. Siedmiu respondentów reprezentowało głosy konsumentów, a 54 respondentów było organizacjami pozarządowymi (z czego dwie działały na rzecz ochrony środowiska). Z 219 przedsiębiorstw/stowarzyszeń

[18] COM(2020) 456 final.
[19] COM(2020) 66 final.

przedsiębiorców 43,4 % stanowiły MŚP. Ogółem 92,2 % odpowiedzi pochodziło z UE-27. Bardzo niewielu respondentów wskazało, czy ich organizacja ma zasięg lokalny, regionalny, krajowy czy międzynarodowy.

Przedłożono 230 stanowisk – jako załącznik do odpowiedzi na pytania zawarte w kwestionariuszu (210) albo jako samodzielne opinie (20). W stanowiskach tych przedstawiono różne poglądy na tematy uwzględnione w kwestionariuszu internetowym, w szczególności w odniesieniu do zarządzania wspólnymi przestrzeniami danych. Przedstawiono w nich opinie na temat kluczowych zasad dotyczących tych przestrzeni i wyrażono duże poparcie dla potraktowania priorytetowo standardów, jak również koncepcji altruistycznego podejścia do danych. Wskazano również potrzebę wprowadzenia zabezpieczeń przy opracowywaniu środków dotyczących pośredników w zakresie danych.

- **Gromadzenie i wykorzystanie wiedzy eksperckiej**

Aby wraz z odpowiednimi ekspertami zbadać ramowe warunki tworzenia wspólnych europejskich przestrzeni danych w określonych sektorach, w 2019 r. miała miejsce seria 10 warsztatów dotyczących wspólnych europejskich przestrzeni danych, a w maju 2020 r. zorganizowano dodatkowe warsztaty. Warsztaty, w których uczestniczyło łącznie ponad 300 zainteresowanych stron, głównie z sektora prywatnego i publicznego, poświęcone były różnym sektorom (rolnictwa, zdrowia, finansów/bankowości, energetyki, transportu, zrównoważonego rozwoju/środowiska, usług publicznych, inteligentnej produkcji) oraz aspektom bardziej przekrojowym (etyce danych, rynkom danych). W warsztatach uczestniczyły służby Komisji zajmujące się tymi obszarami. Warsztaty sektorowe pomogły określić elementy wspólne dla wszystkich sektorów, którymi to elementami należy zająć się poprzez ustanowienie ram zarządzania horyzontalnego.

- **Ocena skutków**

W odniesieniu do niniejszego wniosku przeprowadzono ocenę skutków. W dniu 9 września 2020 r. Rada ds. Kontroli Regulacyjnej wydała negatywną opinię. W dniu 5 października 2020 r. Rada wydała opinię pozytywną z zastrzeżeniami.

W ocenie skutków przeanalizowano scenariusze odniesienia, warianty strategiczne i ich skutki dla czterech obszarów interwencji, mianowicie: a) mechanizmów mających na celu zwiększone wykorzystywanie danych sektora publicznego, które nie mogą być dostępne jako otwarte dane, b) ram certyfikacji pośredników w zakresie danych lub przyznawania im znaku jakości, c) środków ułatwiających altruistyczne podejście do danych oraz d) mechanizmów koordynacji horyzontalnych aspektów zarządzania i kierowania nimi, mających postać struktury na szczeblu UE.

W odniesieniu do wszystkich obszarów interwencji uznano, że wariant strategiczny 1, polegający na koordynacji na szczeblu UE za pomocą miękkich środków regulacyjnych, jest niewystarczający, ponieważ nie zmieniłby on znacząco sytuacji w porównaniu ze scenariuszem odniesienia. W związku z tym w głównej analizie skoncentrowano się na wariantach strategicznych 2 i 3, które dotyczyły interwencji regulacyjnej odpowiednio o niskiej i wysokiej intensywności. Preferowanym wariantem okazało się połączenie interwencji regulacyjnych o niższej i wyższej intensywności w następujący sposób:

W odniesieniu do mechanizmów mających na celu zwiększone wykorzystywanie niektórych danych sektora publicznego, których wykorzystywanie jest objęte prawami innych osób, zarówno warianty o niskiej, jak i wysokiej intensywności polegałyby na wprowadzeniu ogólnounijnych zasad dotyczących ponownego wykorzystywania takich informacji (w

szczególności braku wyłączności). W przypadku interwencji regulacyjnej o niskiej intensywności poszczególne organy sektora publicznego zezwalające na ten rodzaj ponownego wykorzystywania musiałyby dysponować możliwościami technicznymi zapewniającymi pełne zachowanie ochrony danych, prywatności i poufności. Wariant ten obejmowałby również nałożenie na państwa członkowskie obowiązku przewidzenia co najmniej mechanizmu punktu kompleksowej obsługi wniosków o udzielenie dostępu do takich danych, bez określania dokładnej formy instytucjonalnej i administracyjnej tego mechanizmu. Wariant o wysokiej intensywności nakazywałby ustanowienie w każdym państwie członkowskim jednego organu wydającego zezwolenia dotyczące danych. Ze względu na koszty i kwestie wykonalności związane z tym ostatnim rozwiązaniem preferowanym wariantem jest interwencja regulacyjna o niższej intensywności.

W odniesieniu do certyfikowania zaufanych pośredników w zakresie danych lub przyznawania im znaku jakości przewidziano interwencję regulacyjną o niższej intensywności polegającą na bardziej „miękkim", dobrowolnym mechanizmie przyznawania znaku jakości, w ramach którego właściwe organy wyznaczone przez państwa członkowskie przeprowadzałyby ocenę adekwatności w odniesieniu do zgodności z wymogami dotyczącymi uzyskania znaku jakości, jak również przyznawałyby taki znak jakości (funkcję tę mogłyby także pełnić mechanizmy punktu kompleksowej obsługi ustanowione również na potrzeby zwiększonego ponownego wykorzystywania danych sektora publicznego). Interwencja regulacyjna o wysokiej intensywności polegała na obowiązkowym systemie certyfikacji, zarządzanym przez prywatne jednostki oceniające zgodność. System obowiązkowy generowałby wyższe koszty, mogłoby to zatem mieć potencjalnie zaporowy skutek dla MŚP i przedsiębiorstw typu start-up, a rynek nie dojrzał wystarczająco do obowiązkowego systemu certyfikacji; dlatego za preferowany wariant strategiczny uznano interwencję regulacyjną o niższej intensywności. Interwencję regulacyjną o wyższej intensywności w postaci systemu obowiązkowego również jednak uznano za wykonalną alternatywę, ponieważ znacznie podniosłaby ona zaufanie do funkcjonowania pośredników w zakresie danych i ustanowiłaby jasne zasady dotyczące sposobu, w jaki pośrednicy ci mają działać na europejskim rynku danych. Po dalszych dyskusjach w Komisji utrzymano rozwiązanie pośrednie. Obejmuje ono obowiązek zgłaszania wraz z monitorowaniem *ex post* przez właściwe organy państw członkowskich zgodności z wymogami dotyczącymi prowadzenia działalności. Rozwiązanie to posiada zalety systemu obowiązkowego przy jednoczesnym ograniczeniu obciążenia regulacyjnego dla uczestników rynku.

W przypadku altruistycznego podejścia do danych interwencja regulacyjna o niskiej intensywności polegała na wprowadzeniu dobrowolnych ram certyfikacji dla organizacji chcących oferować takie usługi, interwencja regulacyjna o wysokiej intensywności przewidywała natomiast obowiązkowe ramy udzielania zezwoleń. Ponieważ to drugie rozwiązanie zapewniałoby wyższy poziom zaufania w odniesieniu do udostępniania danych, co mogłoby przyczynić się do udostępniania większej ilości danych przez osoby, których dane dotyczą, oraz przedsiębiorstwa, a także doprowadzić do wyższego poziomu rozwoju i badań, generując jednocześnie podobne koszty, w ocenie skutków wskazano je jako preferowany wariant na potrzeby tego obszaru interwencji. Dalsze dyskusje w Komisji ujawniły jednak dodatkowe obawy odnośnie do potencjalnego obciążenia administracyjnego organizacji o altruistycznym podejściu do danych oraz powiązania obowiązków z przyszłymi inicjatywami sektorowymi w zakresie takiego podejścia. Z tego powodu utrzymano rozwiązanie alternatywne, dające organizacjom o altruistycznym podejściu do danych możliwość rejestrowania się jako „uznana w UE organizacja o altruistycznym podejściu do danych". Ten dobrowolny mechanizm przyczyni się do zwiększenia zaufania, a jednocześnie

wiąże się z mniejszym obciążeniem administracyjnym niż obowiązkowe ramy udzielania zezwolenia i dobrowolne ramy certyfikacji.

Ponadto w odniesieniu do europejskiego mechanizmu zarządzania horyzontalnego interwencja regulacyjna o niskiej intensywności obejmowała utworzenie grupy ekspertów, interwencja regulacyjna o wysokiej intensywności polegała natomiast na utworzeniu niezależnej struktury posiadającej osobowość prawną (podobnej do Europejskiej Rady Ochrony Danych). Ze względu na wysokie koszty i niski poziom wykonalności politycznej związane z realizacją wariantu o wyższej intensywności wybrano wariant strategiczny o niskiej intensywności.

W badaniu przeprowadzonym na potrzeby oceny skutków[20] wskazano, że podczas gdy w scenariuszu odniesienia oczekuje się, iż gospodarka oparta na danych i wartość ekonomiczna udostępniania danych wzrosną do szacunkowego poziomu 510–533 mld EUR (3,87 % PKB), to w preferowanym wariancie pakietowym kwota ta wzrosłaby do 540,7–544,4 mld EUR (3,92–3,95 % PKB). W kwotach tych jedynie w ograniczonym stopniu uwzględnia się dalsze korzyści pod względem lepszych produktów, wyższej wydajności i nowych sposobów stawiania czoła wyzwaniom społecznym (np. zmianie klimatu). W rzeczywistości korzyści te prawdopodobnie będą znacznie większe od korzyści bezpośrednich.

Jednocześnie ten pakietowy wariant strategiczny umożliwiłby utworzenie europejskiego modelu udostępniania danych, który dzięki pojawieniu się neutralnych pośredników w zakresie danych oferowałby podejście alternatywne wobec obecnego modelu biznesowego zintegrowanych platform technologicznych. Inicjatywa ta może mieć znaczny wpływ na gospodarkę opartą na danych, budując zaufanie w zakresie udostępniania danych i sprzyjając tworzeniu wspólnych europejskich przestrzeni danych, w których osoby fizyczne i prawne mają kontrolę nad generowanymi przez siebie danymi.

- **Prawa podstawowe**

Ponieważ dane osobowe wchodzą w zakres stosowania niektórych elementów rozporządzenia, środki są zaprojektowane w sposób w pełni zgodny z przepisami o ochronie danych i w rzeczywistości zwiększają w praktyce kontrolę osób fizycznych nad generowanymi przez nie danymi.

Jeżeli chodzi o zwiększone ponowne wykorzystywanie danych sektora publicznego, przestrzegane będą zarówno prawa podstawowe w zakresie ochrony danych, prywatności i własności (dotyczące praw własności do niektórych danych, które przykładowo stanowią tajemnicę handlową lub są chronione prawami własności intelektualnej). Podobnie dostawcy usług udostępniania danych oferujący usługi osobom, których dane dotyczą, będą musieli przestrzegać obowiązujących przepisów o ochronie danych.

Ramy zgłaszania pośredników w zakresie danych dotyczyłyby wolności prowadzenia działalności gospodarczej, ponieważ nakładałyby pewne ograniczenia w postaci różnych wymogów będących warunkiem wstępnym funkcjonowania takich podmiotów.

4. WPŁYW NA BUDŻET

Niniejszy wniosek nie będzie miał żadnego wpływu na budżet.

[20] Komisja Europejska (2020 r., *w przygotowaniu*). *Badanie uzupełniające niniejszą ocenę skutków [Support Study to this Impact Assessment*], SMART 2019/0024, przygotowane przez Deloitte.

5. ELEMENTY FAKULTATYWNE

- **Plany wdrożenia i monitorowanie, ocena i sprawozdania**

Ze względu na dynamiczny charakter gospodarki opartej na danych monitorowanie kształtowania się skutków stanowi kluczową część interwencji w tej dziedzinie. W celu zapewnienia, aby wybrane środki z zakresu polityki rzeczywiście przyniosły zamierzone wyniki, oraz w celu zgromadzenia informacji na potrzeby ewentualnych przyszłych rewizji konieczne są monitorowanie i ocena wykonania niniejszego rozporządzenia.

Monitorowanie celów szczegółowych i obowiązków regulacyjnych będzie realizowane poprzez reprezentatywne badania zainteresowanych stron, poprzez pracę centrum wsparcia w zakresie wymiany danych, za pośrednictwem rejestrów Europejskiej Rady ds. Innowacji w zakresie Danych dotyczących poszczególnych obszarów interwencji zgłaszanych przez specjalne organy krajowe oraz poprzez badanie oceniające służące wsparciu przeglądu instrumentu.

- **Szczegółowe objaśnienia poszczególnych przepisów wniosku**

W **rozdziale I** zdefiniowano przedmiot rozporządzenia i przedstawiono definicje stosowane w całym instrumencie.

W **rozdziale II** utworzono mechanizm ponownego wykorzystywania niektórych kategorii chronionych danych sektora publicznego, które zależy od poszanowania praw innych osób (szczególnie ze względu na ochronę danych osobowych, lecz także ochronę praw własności intelektualnej i tajemnicy handlowej). Mechanizm ten nie narusza przepisów Unii dotyczących dostępu do tych danych i ich ponownego wykorzystywania. Ponowne wykorzystywanie takich danych wykracza poza zakres stosowania dyrektywy (UE) 2019/1024 (dyrektywa w sprawie otwartych danych). Przepisy zawarte w tym rozdziale nie tworzą prawa do ponownego wykorzystywania takich danych, ale przewidziano w nich zestaw zharmonizowanych podstawowych warunków, na jakich ponowne wykorzystywanie takich danych może być dozwolone (np. wymóg braku wyłączności). Organy sektora publicznego zezwalające na ten rodzaj ponownego wykorzystywania musiałyby dysponować możliwościami technicznymi zapewniającymi pełne zachowanie ochrony danych, prywatności i poufności. Państwa członkowskie będą musiały ustanowić pojedynczy punkt kontaktowy wspierający naukowców i innowacyjne przedsiębiorstwa w identyfikacji odpowiednich danych oraz są zobowiązane do wprowadzenia struktur wspierających organy sektora publicznego za pomocą środków technicznych i pomocy prawnej.

Rozdział III ma na celu zwiększenie zaufania w zakresie udostępniania danych osobowych i nieosobowych oraz obniżenie kosztów transakcji związanych z udostępnianiem danych między przedsiębiorstwami i między konsumentami a przedsiębiorstwami poprzez utworzenie systemu zgłaszania dostawców usług udostępniania danych. Dostawcy ci będą musieli spełnić szereg wymogów, w szczególności wymóg zachowania neutralności w odniesieniu do udostępnianych danych. Nie mogą oni wykorzystywać takich danych do innych celów. W przypadku dostawców usług udostępniania danych oferujących usługi osobom fizycznym konieczne będzie również spełnienie dodatkowego kryterium polegającego na przyjęciu na siebie obowiązków powierniczych wobec osób fizycznych, które korzystają z tych danych.

Podejście to ma na celu zapewnienie, aby usługi udostępniania danych funkcjonowały w sposób otwarty i oparty na współpracy, przy jednoczesnym wzmocnieniu pozycji osób fizycznych i prawnych poprzez umożliwienie im lepszego rozeznania w ich danych i większej

kontroli nad nimi. Za monitorowanie zgodności z wymogami związanymi ze świadczeniem takich usług odpowiedzialny będzie właściwy organ wyznaczony przez państwa członkowskie.

W **rozdziale IV** ułatwiono altruistyczne podejście do danych (dobrowolne udostępnianie danych przez osoby fizyczne lub przedsiębiorstwa dla wspólnego dobra). Przewidziano w nim możliwość rejestrowania się organizacji o altruistycznym podejściu do danych jako „uznana w UE organizacja o altruistycznym podejściu do danych", aby zwiększyć zaufanie do ich działalności. Ponadto opracowany zostanie wspólny europejski formularz zgody na potrzeby altruistycznego podejścia do danych, aby obniżyć koszty uzyskiwania zgody i ułatwić przenoszenie danych (w przypadku gdy dane, które mają zostać udostępnione, nie są w posiadaniu osoby fizycznej).

W **rozdziale V** określono wymogi dotyczące funkcjonowania właściwych organów wyznaczonych do monitorowania i wdrażania ram zgłaszania dostawców usług udostępniania danych oraz podmiotów o altruistycznym podejściu do danych. Zawiera on również przepisy dotyczące prawa do wnoszenia skarg na decyzje takich organów oraz środków zaskarżenia.

W **rozdziale VI** powołano formalną grupę ekspertów („Europejska Rada ds. Innowacji w zakresie Danych"), która będzie ułatwiała opracowywanie najlepszych praktyk przez organy państw członkowskich, w szczególności w zakresie przetwarzania wniosków o ponowne wykorzystywanie danych, które są objęte prawami innych osób (na podstawie rozdziału II), zapewnienia spójnej praktyki odnośnie do ram zgłaszania dostawców usług udostępniania danych (na podstawie rozdziału III) oraz altruistycznego podejścia do danych (rozdział IV). Ponadto formalna grupa ekspertów będzie wspierała Komisję i doradzała jej w zakresie zarządzania normalizacją międzysektorową oraz przygotowywania strategicznych wniosków dotyczących tej normalizacji. W rozdziale tym określono również skład Rady i sposób jej funkcjonowania.

Rozdział VII pozwala Komisji na przyjęcie aktów wykonawczych w sprawie europejskiego formularza zgody na potrzeby altruistycznego podejścia do danych.

Rozdział VIII zawiera przepisy przejściowe dotyczące funkcjonowania systemu ogólnych zezwoleń dla dostawców usług udostępniania danych oraz przepisy końcowe.

2020/0340 (COD)

Wniosek

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY

w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi)

(Tekst mający znaczenie dla EOG)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 114,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[21],

uwzględniając opinię Komitetu Regionów[22],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą,

a także mając na uwadze, co następuje:

(1) Traktat o funkcjonowaniu Unii Europejskiej („TFUE") przewiduje ustanowienie rynku wewnętrznego i wprowadzenie systemu zapewniającego niezakłóconą konkurencję na rynku wewnętrznym. Ustanowienie w państwach członkowskich wspólnych zasad i praktyk odnoszących się do opracowania ram zarządzania danymi powinno przyczynić się do osiągnięcia tych celów.

(2) W ciągu ostatnich kilku lat technologie cyfrowe zmieniły gospodarkę i społeczeństwo, oddziałując na wszystkie sektory działalności i codzienne życie. W centrum tej transformacji znajdują się dane: innowacje oparte na danych przyniosą ogromne korzyści obywatelom, na przykład dzięki udoskonalonej medycynie personalizowanej, nowej mobilności oraz wkładowi w Europejski Zielony Ład[23]. W strategii w zakresie danych[24] Komisja opisała wizję wspólnej europejskiej przestrzeni danych – jednolitego rynku danych, na którym dane mogłyby być wykorzystywane – zgodnie z obowiązującymi przepisami – bez względu na fizyczne miejsce ich przechowywania w Unii. Wezwała również do zapewnienia swobodnego i bezpiecznego przepływu danych z państwami trzecimi, z zastrzeżeniem wyjątków i ograniczeń ze względu na bezpieczeństwo publiczne, porządek publiczny i inne uzasadnione cele polityki publicznej Unii Europejskiej, zgodnie ze zobowiązaniami międzynarodowymi. Aby urzeczywistnić tę wizję, Komisja proponuje ustanowić wspólne europejskie przestrzenie danych w poszczególnych dziedzinach jako konkretne rozwiązania,

---

21 Dz.U. C […] z […], s. […].

22 Dz.U. C […] z […], s. […].

23 Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Europejski Zielony Ład". Bruksela, 11.12.2019 r. (COM(2019) 640 final).

24 COM(2020) 66 final.

w ramach których można będzie udostępniać i łączyć dane. Jak przewidziano w tej strategii, tego rodzaju wspólne europejskie przestrzenie danych mogą obejmować takie obszary, jak: zdrowie, mobilność, produkcja, usługi finansowe, energia lub rolnictwo, lub też obszary tematyczne, takie jak Europejski Zielony Ład lub wspólne europejskie przestrzenie danych dla administracji publicznej lub danych dotyczących umiejętności.

(3) Konieczna jest poprawa warunków udostępniania danych na rynku wewnętrznym poprzez utworzenie zharmonizowanych ram wymiany danych. W przepisach sektorowych można opracować, dostosować i zaproponować nowe i uzupełniające elementy, w zależności od specyfiki sektora, takie jak planowane przepisy dotyczące europejskiej przestrzeni danych dotyczących zdrowia[25] i dostępu do danych z pojazdów. Ponadto niektóre sektory gospodarki są już regulowane sektorowym prawem Unii, które obejmuje przepisy dotyczące transgranicznego lub ogólnounijnego udostępniania danych lub dostępu do nich[26]. Niniejsze rozporządzenie nie narusza zatem przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679([27]), a w szczególności wdrażanie niniejszego rozporządzenia nie może uniemożliwiać transgranicznego przekazywania danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679, przepisów dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 ([28]), dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943 ([29]), rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 ([30]), rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 223/2009 ([31]), dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady ([32]), dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady

---

[25] Zob.: załączniki do komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Program prac Komisji na 2021 r." (COM(2020) 690 final).

[26] Na przykład dyrektywa 2011/24/UE w kontekście europejskiej przestrzeni danych dotyczących zdrowia oraz odpowiednie przepisy dotyczące transportu, takie jak: dyrektywa 2010/40/UE, rozporządzenie (UE) 2019/1239 i rozporządzenie (UE) 2020/1056, w kontekście europejskiej przestrzeni danych dotyczących mobilności.

[27] 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.U. L 119 z 4.5.2016, s. 1).

[28] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.U. L 119 z 4.5.2016, s. 89).

[29] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z dnia 8 czerwca 2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.U. L 157 z 15.6.2016, s. 1).

[30] 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.U. L 303 z 28.11.2018, s. 59).

[31] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich (Dz.U. L 87 z 31.3.2009, s. 164).

[32] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym). (Dz.U. L 178 z 17.7.2000, s. 1)

([33]), dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 ([34]), dyrektywy 2004/48/WE Parlamentu Europejskiego i Rady ([35]), dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 ([36]), jak również rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/858 ([37]), dyrektywy Parlamentu Europejskiego i Rady 2010/40/UE ([38]) oraz przyjętych na jej podstawie rozporządzeń delegowanych, a także wszelkich innych sektorowych przepisów Unii, które dotyczą organizowania dostępu do danych i ich ponownego wykorzystywania. Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla dostępu do danych i ich wykorzystywania do celów współpracy międzynarodowej w kontekście zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar. Należy ustanowić horyzontalny system ponownego wykorzystywania niektórych kategorii chronionych danych będących w posiadaniu organów sektora publicznego oraz świadczenia usług udostępniania danych i usług opartych na altruistycznym podejściu do danych w Unii. Specyfika różnych sektorów może wymagać zaprojektowania sektorowych systemów opartych na danych z uwzględnieniem wymogów niniejszego rozporządzenia. W przypadku gdy sektorowy akt prawny Unii wymaga od organów sektora publicznego, dostawców usług udostępniania danych lub zarejestrowanych podmiotów świadczących usługi z zachowaniem altruistycznego podejścia do danych spełnienia szczególnych dodatkowych wymogów technicznych, administracyjnych lub organizacyjnych, w tym poprzez system zezwoleń lub certyfikacji, zastosowanie powinny mieć również przepisy tego sektorowego aktu prawnego Unii.

(4) Działanie na poziomie Unii jest konieczne w celu usunięcia barier dla dobrze funkcjonującej gospodarki opartej na danych oraz utworzenia ogólnounijnych ram zarządzania w zakresie dostępu do danych i ich wykorzystywania, w szczególności w odniesieniu do ponownego wykorzystywania niektórych rodzajów danych będących w posiadaniu sektora publicznego, świadczenia usług przez dostawców usług udostępniania danych na rzecz użytkowników biznesowych i osób, których dane dotyczą, jak również gromadzenia i przetwarzania danych udostępnianych z pobudek altruistycznych przez osoby fizyczne i prawne.

(5) Koncepcja, że dane wygenerowane na koszt budżetów publicznych powinny przynosić korzyści społeczeństwu, od dawna była częścią polityki Unii. Dyrektywa (UE) 2019/1024 oraz przepisy sektorowe zapewniają, aby sektor publiczny umożliwiał

---

[33] Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z dnia 22 maja 2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.U. L 167 z 22.6.2001, s. 10).

[34] Dyrektywa 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 (Dz.U. L 130 z 17.5.2019, s. 92).

[35] Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.U. L 157 z 30.4.2004).

[36] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z dnia 20 czerwca 2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 172 z 26.6.2019, s. 56).

[37] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 z dnia 30 maja 2018 r. w sprawie homologacji i nadzoru rynku pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, zmieniające rozporządzenie (WE) nr 715/2007 i (WE) nr 595/2009 oraz uchylające dyrektywę 2007/46/WE (Dz.U. L 151 z 14.6.2018).

[38] Dyrektywa Parlamentu Europejskiego i Rady 2010/40/UE z dnia 7 lipca 2010 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu (Dz.U. L 207 z 6.8.2010, s. 1).

łatwy dostęp do większej ilości produkowanych przez siebie danych na potrzeby ich wykorzystywania oraz ponownego wykorzystywania. Niektóre kategorie danych (dane objęte tajemnicą handlową, dane objęte poufnością informacji statystycznych, dane chronione prawami własności intelektualnej osób trzecich, w tym tajemnice przedsiębiorstwa i dane osobowe niedostępne na podstawie szczególnych przepisów krajowych lub unijnych, takich jak rozporządzenie (UE) 2016/679 i dyrektywa (UE) 2016/680) znajdujących się w publicznych bazach danych często jednak nie są udostępniane, nawet na potrzeby działalności badawczej lub innowacyjnej. Ze względu na szczególny charakter tych danych konieczne jest spełnienie przed ich udostępnieniem pewnych wymogów technicznych i prawnych wymogów proceduralnych, aby zapewnić poszanowanie praw innych osób w odniesieniu do takich danych. Spełnienie takich wymogów jest zazwyczaj czasochłonne i wymaga specjalistycznej wiedzy. Okoliczności te spowodowały, że dane takie są wykorzystywane w zbyt małym stopniu. Niektóre państwa członkowskie tworzą wprawdzie struktury, procesy i czasami stanowią prawo ułatwiające tego rodzaju ponowne wykorzystywanie danych, jednak działania te nie są podejmowane w całej Unii.

(6) Istnieją techniki umożliwiające przeprowadzanie analiz baz danych, które zawierają dane osobowe, w sposób przyjazny dla ochrony prywatności, takie jak anonimizacja, pseudonimizacja, prywatność różnicowa, uogólnienie lub ukrywanie i randomizacja. Zastosowanie tych technologii służących wzmocnieniu ochrony prywatności wraz z kompleksowym podejściem do ochrony danych powinno zapewniać bezpieczne ponowne wykorzystywanie danych osobowych i danych biznesowych objętych tajemnicą handlową do celów badań i innowacji oraz do celów statystycznych. W wielu przypadkach oznacza to, że wykorzystywanie i ponowne wykorzystywanie danych w tym kontekście może odbywać się wyłącznie w bezpiecznym środowisku przetwarzania stworzonym i nadzorowanym przez sektor publiczny. Na szczeblu Unii zgromadzono pewne doświadczenie w zakresie takich bezpiecznych środowisk przetwarzania, które są wykorzystywane do badań nad jednostkowymi danymi statystycznymi na podstawie rozporządzenia Komisji (UE) nr 557/2013 ([39]). Ogólnie rzecz biorąc, jeśli chodzi o dane osobowe, przetwarzanie tych danych powinno opierać się na co najmniej jednej podstawie przetwarzania określonej w art. 6 rozporządzenia (UE) 2016/679.

(7) Kategorie danych będących w posiadaniu organów sektora publicznego, które powinny być objęte ponownym wykorzystywaniem na mocy niniejszego rozporządzenia, wykraczają poza zakres stosowania dyrektywy (UE) 2019/1024, z którego wykluczone są dane niedostępne ze względu na tajemnicę handlową i poufność informacji statystycznych oraz dane, do których prawa własności intelektualnej posiadają osoby trzecie. Dane osobowe wykraczają poza zakres dyrektywy (UE) 2019/1024, o ile system dostępu wyklucza lub ogranicza dostęp do takich danych ze względu na ochronę danych, prywatność i integralność osoby fizycznej, w szczególności zgodnie z przepisami o ochronie danych. Ponowne wykorzystywanie danych, które mogą zawierać tajemnice przedsiębiorstwa, nie powinno naruszać przepisów dyrektywy (UE) 2016/943[40], która ustanawia ramy

[39] Rozporządzenie Komisji (UE) nr 557/2013 z dnia 17 czerwca 2013 r. w sprawie wykonania rozporządzenia (WE) nr 223/2009 Parlamentu Europejskiego i Rady w sprawie europejskiej statystyki w zakresie dostępu do poufnych danych do celów naukowych i uchylające rozporządzenie Komisji (WE) nr 831/2002 (Dz.U. L 164 z 18.6.2013, s. 16).

[40] Dz.U. L 157 z 15.6.2016, s. 1

zgodnego z prawem pozyskiwania, wykorzystywania lub ujawniania tajemnic przedsiębiorstwa. Niniejsze rozporządzenie pozostaje bez uszczerbku dla bardziej szczegółowych obowiązków organów sektora publicznego w zakresie zezwalania na ponowne wykorzystywanie danych określonych w sektorowych przepisach prawa unijnego lub krajowego i uzupełnia te obowiązki.

(8) System ponownego wykorzystywania przewidziany w niniejszym rozporządzeniu powinien mieć zastosowanie do danych, których dostarczanie jest jednym z zadań publicznych zainteresowanych organów sektora publicznego, zgodnie z przepisami ustawowymi lub innymi wiążącymi przepisami państw członkowskich. W przypadku braku takich przepisów zadania publiczne należy określić zgodnie z powszechną praktyką administracyjną w państwach członkowskich, z zastrzeżeniem przejrzystości zakresu zadań publicznych i poddawania ich przeglądowi. Zadania publiczne mogą być definiowane ogólnie lub indywidualnie dla poszczególnych organów sektora publicznego. Przedsiębiorstwa publiczne nie są objęte definicją organu sektora publicznego, zatem posiadane przez nie dane nie powinny podlegać niniejszemu rozporządzeniu. Niniejsze rozporządzenie nie obejmuje danych będących w posiadaniu instytucji kulturalnych i edukacyjnych, w przypadku których prawa własności intelektualnej nie mają charakteru dodatkowego, lecz które są zawarte głównie w utworach i innych dokumentach chronionych takimi prawami własności intelektualnej.

(9) Organy sektora publicznego przy ustanawianiu zasad ponownego wykorzystywania posiadanych przez nie danych powinny przestrzegać prawa konkurencji, unikając w miarę możliwości zawierania umów, których celem lub skutkiem mogłoby być tworzenie praw wyłącznych do ponownego wykorzystywania niektórych danych. Takie umowy powinny być możliwe tylko wtedy, gdy jest to uzasadnione i konieczne do celów usługi świadczonej w interesie ogólnym. Może to mieć miejsce w przypadku, gdy wyłączne wykorzystywanie danych jest jedynym sposobem maksymalnego zwiększenia korzyści społecznych z odnośnych danych, na przykład gdy istnieje tylko jeden podmiot (wyspecjalizowany w przetwarzaniu określonego zbioru danych) zdolny do dostarczania usługi lub produktu, które umożliwiają organowi sektora publicznego świadczenie zaawansowanej usługi cyfrowej w interesie ogólnym. Takie uzgodnienia powinny być jednak zawierane zgodnie z przepisami dotyczącymi zamówień publicznych i podlegać regularnym przeglądom opartym na analizie rynkowej, aby ustalić, czy taka wyłączność nadal jest konieczna. Ponadto takie uzgodnienia powinny być w stosownych przypadkach zgodne z odpowiednimi zasadami pomocy państwa i zawierane na czas określony, który nie powinien przekraczać trzech lat. Aby zapewnić przejrzystość, takie umowy o wyłączności należy publikować w internecie, niezależnie od ewentualnej publikacji ogłoszenia o udzieleniu zamówienia publicznego.

(10) Zakazane umowy o wyłączności i inne praktyki lub uzgodnienia między posiadaczami danych a podmiotami ponownie je wykorzystującymi, które wprost nie przyznają praw wyłącznych, lecz w przypadku których można zasadnie oczekiwać, że doprowadzą do ograniczenia dostępności danych do ponownego wykorzystywania i które zostały zawarte lub już istniały przed wejściem w życie niniejszego rozporządzenia, nie powinny być przedłużane po upływie ich okresu obowiązywania. W przypadku umów na czas nieokreślony lub na dłuższy okres należy je rozwiązać w ciągu trzech lat od daty wejścia w życie niniejszego rozporządzenia.

(11) Należy określić warunki ponownego wykorzystywania danych chronionych mające zastosowanie do organów sektora publicznego właściwych na mocy prawa krajowego

do zezwalania na ponowne wykorzystywanie, przy czym warunki te powinny pozostawać bez uszczerbku dla praw lub obowiązków dotyczących dostępu do takich danych. Warunki te powinny być niedyskryminujące, proporcjonalne i obiektywnie uzasadnione, przy czym nie mogą ograniczać konkurencji. W szczególności organy sektora publicznego zezwalające na ponowne wykorzystywanie powinny dysponować środkami technicznymi niezbędnymi do zapewnienia ochrony praw i interesów osób trzecich. Warunki związane z ponownym wykorzystywaniem danych powinny być ograniczone do tego, co jest niezbędne do zachowania praw i interesów innych osób w odniesieniu do danych oraz integralności systemów teleinformatycznych organów sektora publicznego. Organy sektora publicznego powinny stosować warunki, które najlepiej służą interesom podmiotu ponownie wykorzystującego dane, a jednocześnie nie powodują nieproporcjonalnie dużego wysiłku ze strony sektora publicznego. W zależności od przypadku dane osobowe należy przed przekazaniem w pełni zanonimizować, tak aby nieodwołalnie uniemożliwiały identyfikację osób, których dane dotyczą, natomiast dane zawierające poufne informacje handlowe należy zmodyfikować w taki sposób, aby nie ujawniać informacji poufnych. W przypadku gdy dostarczenie danych zanonimizowanych lub zmodyfikowanych nie odpowiadałoby potrzebom podmiotu ponownie wykorzystującego dane, można zezwolić na ponowne wykorzystywanie danych na miejscu lub zdalnie w bezpiecznym środowisku przetwarzania. Organ sektora publicznego powinien nadzorować analizy danych w takich bezpiecznych środowiskach przetwarzania, by chronić prawa i interesy innych osób. W szczególności dane osobowe powinny być przesyłane do ponownego wykorzystywania osobie trzeciej tylko w przypadku, gdy podstawa prawna zezwala na takie przesyłanie. Organ sektora publicznego może uzależnić korzystanie z takiego bezpiecznego środowiska przetwarzania od podpisania przez podmiot ponownie wykorzystujący dane umowy o poufności, zawierającej zakaz ujawniania wszelkich informacji zagrażających prawom i interesom osób trzecich, które podmiot ponownie wykorzystujący dane mógł uzyskać pomimo wprowadzonych zabezpieczeń. Organy sektora publicznego powinny w stosownych przypadkach ułatwiać – za pomocą odpowiednich środków technicznych – ponowne wykorzystywanie danych na podstawie zgody osób, których dane dotyczą, lub zezwoleń osób prawnych na ponowne wykorzystywanie dotyczących ich danych. W tym względzie organ sektora publicznego powinien wspierać potencjalne podmioty ponownie wykorzystujące dane w ubieganiu się o taką zgodę, ustanawiając – jeżeli jest to praktycznie wykonalne – mechanizmy techniczne, które umożliwiają przekazywanie zapytań o zgodę wysłanych przez podmioty ponownie wykorzystujące dane. Nie należy podawać żadnych informacji kontaktowych umożliwiających podmiotom ponownie wykorzystującym dane bezpośredni kontakt z osobami, których dane dotyczą, lub z przedsiębiorstwami.

(12) Niniejsze rozporządzenie nie powinno mieć wpływu na prawa własności intelektualnej osób trzecich. Niniejsze rozporządzenie nie powinno również mieć wpływu na istnienie ani na własność praw własności intelektualnej organów sektora publicznego ani też nie powinno ograniczać wykonywania tych praw w żaden sposób wychodzący poza granice określone w niniejszym rozporządzeniu. Obowiązki nałożone zgodnie z niniejszym rozporządzeniem powinno się stosować tylko w zakresie, w jakim są zgodne z umowami międzynarodowymi o ochronie praw własności intelektualnej, w szczególności z Konwencją berneńską o ochronie dzieł literackich i artystycznych („konwencja berneńska”), Porozumieniem w sprawie handlowych aspektów praw własności intelektualnej („porozumienie TRIPS”) i Traktatem WIPO o prawie

autorskim („WCT”). Organy sektora publicznego powinny jednakże wykonywać swoje prawa autorskie w sposób ułatwiający ponowne wykorzystywanie.

(13) Dane objęte prawami własności intelektualnej, jak również tajemnice przedsiębiorstwa powinny być przekazywane osobie trzeciej wyłącznie w przypadku, gdy przekazanie to jest zgodne z prawem na podstawie prawa unijnego lub krajowego, lub za zgodą uprawnionego. Jeżeli organom sektora publicznego przysługuje prawo przewidziane w art. 7 ust. 1 dyrektywy 96/9/WE Parlamentu Europejskiego i Rady ([41]), nie powinny one wykonywać tego prawa w celu uniemożliwienia lub ograniczenia ponownego wykorzystywania danych w zakresie wykraczającym poza ograniczenia określone w niniejszym rozporządzeniu.

(14) Przedsiębiorstwa i osoby, których dane dotyczą, powinny móc zaufać, że ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu sektora publicznego będzie odbywało się w sposób respektujący ich prawa i interesy. Należy zatem wprowadzić dodatkowe zabezpieczenia na wypadek sytuacji, w których ponowne wykorzystywanie takich danych sektora publicznego odbywa się na podstawie przetwarzania danych poza sektorem publicznym. Takie dodatkowe zabezpieczenia można znaleźć w wymogu, aby organy sektora publicznego w pełni uwzględniały prawa i interesy osób fizycznych i prawnych (w szczególności ochronę danych osobowych i szczególnie chronionych danych handlowych oraz ochronę praw własności intelektualnej) w przypadku przekazywania takich danych do państw trzecich.

(15) Ponadto ważne jest, aby chronić szczególnie chronione dane handlowe o charakterze nieosobowym, zwłaszcza tajemnice przedsiębiorstwa, lecz także dane nieosobowe stanowiące treści chronione prawami własności intelektualnej przed bezprawnym dostępem, który może prowadzić do kradzieży własności intelektualnej lub szpiegostwa przemysłowego. Aby zapewnić ochronę praw podstawowych lub interesów posiadaczy danych, dane nieosobowe, które mają być chronione przed bezprawnym lub nieuprawnionym dostępem na mocy prawa unijnego lub krajowego, a które są w posiadaniu organów sektora publicznego, powinny być przekazywane wyłącznie do państw trzecich, w których zapewnione są odpowiednie zabezpieczenia w zakresie wykorzystywania danych. Należy uznać, że takie odpowiednie zabezpieczenia istnieją, jeżeli w tym państwie trzecim wprowadzono równoważne środki zapewniające, aby dane nieosobowe były objęte poziomem ochrony podobnym do tego, który ma zastosowanie na podstawie prawa unijnego lub krajowego, w szczególności w odniesieniu do ochrony tajemnicy przedsiębiorstwa i ochrony praw własności intelektualnej. W tym celu Komisja może przyjąć akty wykonawcze, w których stwierdza się, że państwo trzecie zapewnia poziom ochrony zasadniczo równoważny poziomowi określonemu w prawie unijnym lub krajowym. W ocenie poziomu ochrony zapewnianej w takim państwie trzecim należy w szczególności uwzględnić odpowiednie przepisy, zarówno ogólne, jak i sektorowe, w tym dotyczące bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego i prawa karnego w zakresie dostępu do danych nieosobowych oraz ich ochrony, wszelki dostęp organów publicznych tego państwa trzeciego do przekazywanych danych, obecność i skuteczne funkcjonowanie w państwie trzecim co najmniej jednego niezależnego organu nadzorczego odpowiedzialnego za zapewnienie i egzekwowanie zgodności z systemem prawnym zapewniającym dostęp do takich danych lub zobowiązania międzynarodowe państw trzecich w zakresie ochrony danych, które

[41] Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z dnia 11 marca 1996 r. w sprawie ochrony prawnej baz danych (Dz.U. L 77 z 27.3.1996, s. 20).

dane państwo trzecie podjęło, lub inne zobowiązania wynikające z prawnie wiążących konwencji lub instrumentów, jak również z uczestnictwa w systemach wielostronnych lub regionalnych. Istnienie skutecznych środków ochrony prawnej dla posiadaczy danych, organów sektora publicznego lub dostawców usług udostępniania danych w danym państwie trzecim ma szczególne znaczenie w kontekście przekazywania danych nieosobowych do tego państwa trzeciego. Takie zabezpieczenia powinny zatem obejmować dostępność egzekwowalnych praw i skutecznych środków ochrony prawnej.

(16) W przypadku braku aktu wykonawczego przyjętego przez Komisję w odniesieniu do państwa trzeciego, w którym to akcie stwierdza się, że zapewnia ono poziom ochrony – w szczególności w odniesieniu do ochrony szczególnie chronionych danych handlowych oraz ochrony praw własności intelektualnej – który zasadniczo jest równoważny poziomowi określonemu w prawie unijnym lub krajowym, organ sektora publicznego powinien przekazać dane chronione podmiotowi ponownie wykorzystującemu dane tylko wtedy, gdy podmiot ten podejmie zobowiązania w interesie ochrony danych. Podmiot ponownie wykorzystujący dane, który zamierza przekazać dane do takiego państwa trzeciego, powinien zobowiązać się do spełniania obowiązków określonych w niniejszym rozporządzeniu nawet po przekazaniu danych do państwa trzeciego. Aby zapewnić właściwe egzekwowanie takich obowiązków, podmiot ponownie wykorzystujący dane powinien również uznać – do celów sądowego rozstrzygania sporów – jurysdykcję państwa członkowskiego organu sektora publicznego, który zezwolił na ponowne wykorzystywanie.

(17) Niektóre państwa trzecie przyjmują ustawy, rozporządzenia i inne akty prawne, których celem jest bezpośrednie przekazywanie danych nieosobowych lub zapewnianie dostępu do nich w Unii pod kontrolą osób fizycznych i prawnych i pod jurysdykcją państw członkowskich. Wyroki sądów lub trybunałów czy decyzje organów administracyjnych państw trzecich nakazujące przekazać dane nieosobowe lub zapewnić dostęp do nich powinny być wykonalne, jeżeli mają za podstawę umowę międzynarodową – np. umowę o wzajemnej pomocy prawnej – obowiązującą między wzywającym państwem trzecim a Unią lub państwem członkowskim. W niektórych przypadkach mogą wystąpić sytuacje, w których obowiązek przekazania danych nieosobowych lub zapewnienia dostępu do nich wynikający z prawa państwa trzeciego pozostaje w sprzeczności z kolidującym obowiązkiem ochrony takich danych wynikającym z prawa unijnego lub krajowego, w szczególności w odniesieniu do ochrony szczególnie chronionych danych handlowych oraz ochrony praw własności intelektualnej, w tym z zobowiązaniami umownymi tego państwa dotyczącymi poufności zgodnie z tym prawem. W przypadku braku umów międzynarodowych regulujących takie kwestie przekazywanie lub dostęp powinny być dozwolone tylko pod pewnymi warunkami, w szczególności pod warunkiem, że system państwa trzeciego wymaga określenia powodów i proporcjonalności decyzji, że orzeczenie sądu lub decyzja mają szczególny charakter oraz że uzasadniony sprzeciw adresata podlega kontroli właściwego sądu w państwie trzecim, który jest upoważniony do należytego uwzględnienia odpowiednich interesów prawnych dostawcy takich danych.

(18) Aby zapobiec bezprawnemu dostępowi do danych nieosobowych, organy sektora publicznego, osoby fizyczne lub prawne, którym przyznano prawo do ponownego wykorzystywania danych, dostawcy usług udostępniania danych i podmioty wpisane do rejestru uznanych organizacji o altruistycznym podejściu do danych powinny wprowadzić wszelkie rozsądne środki w celu zapobieżenia dostępowi do systemów,

w których przechowywane są dane nieosobowe, w tym takie jak szyfrowanie danych lub polityka korporacyjna.

(19) Aby budować zaufanie do mechanizmów ponownego wykorzystywania, konieczne może być obwarowanie niektórych rodzajów danych nieosobowych, które uznano za szczególnie chronione, bardziej rygorystycznymi warunkami w zakresie przekazywania ich do państw trzecich, jeżeli takie przekazywanie mogłoby zagrozić celom polityki publicznej zgodnie ze zobowiązaniami międzynarodowymi. Na przykład w obszarze zdrowia niektóre zbiory danych będące w posiadaniu podmiotów publicznego systemu opieki zdrowotnej takich jak szpitale publiczne można uznać za szczególnie chronione dane dotyczące zdrowia. Aby zapewnić zharmonizowane praktyki w całej Unii, takie rodzaje szczególnie chronionych publicznych danych nieosobowych powinny być określone w prawie Unii, na przykład w kontekście europejskiej przestrzeni danych dotyczących zdrowia lub w innych przepisach sektorowych. Warunki związane z przekazywaniem takich danych do państw trzecich powinny być określone w aktach delegowanych. Warunki powinny być proporcjonalne, niedyskryminujące i niezbędne do ochrony określonych uzasadnionych celów polityki publicznej, takich jak: ochrona zdrowia publicznego, porządku publicznego, bezpieczeństwa, środowiska, moralności publicznej, ochrona konsumentów, ochrona prywatności i danych osobowych. Warunki powinny odpowiadać zidentyfikowanemu ryzyku związanemu ze szczególnym charakterem takich danych, w tym ryzyku deanonimizacji osób fizycznych. Warunki te mogą obejmować warunki mające zastosowanie do przekazywania lub uzgodnień technicznych, takie jak wymóg korzystania z bezpiecznego środowiska przetwarzania, ograniczenia dotyczące ponownego wykorzystywania danych w państwach trzecich lub kategorii osób, które są uprawnione do przekazywania takich danych do państw trzecich lub które mogą uzyskać dostęp do danych w państwie trzecim. W wyjątkowych przypadkach mogą one również obejmować ograniczenia przekazywania danych do państw trzecich ze względu na ochronę interesu publicznego.

(20) Organy sektora publicznego powinny mieć możliwość pobierania opłat za ponowne wykorzystywanie danych, ale powinny również móc podjąć decyzję o udostępnianiu danych po niższych kosztach lub nieodpłatnie, zgodnie z zasadami pomocy państwa, na przykład w przypadku niektórych kategorii ponownego wykorzystywania, takich jak ponowne wykorzystywanie na zasadach niekomercyjnych, lub ponownego wykorzystywania przez małe i średnie przedsiębiorstwa, tak aby zachęcać do takiego ponownego wykorzystywania w celu stymulowania badań naukowych i innowacji oraz wspierania przedsiębiorstw, które są ważnym źródłem innowacji i zazwyczaj mają większe trudności z samodzielnym gromadzeniem odpowiednich danych. Takie opłaty powinny być rozsądne, przejrzyste, opublikowane w internecie i niedyskryminujące.

(21) Aby zachęcać do ponownego wykorzystywania tych kategorii danych, państwa członkowskie powinny ustanowić pojedynczy punkt informacyjny, który będzie pełnił funkcję podstawowego interfejsu dla podmiotów ponownie wykorzystujących dane, które chcą ponownie wykorzystywać takie dane będące w posiadaniu organów sektora publicznego. Powinien on mieć kompetencje międzysektorowe i w razie potrzeby powinien uzupełniać uzgodnienia na poziomie sektorowym. Ponadto państwa członkowskie powinny wyznaczyć właściwe podmioty, ustanowić je lub ułatwić ich ustanowienie, aby wspierać działalność organów sektora publicznego zezwalających na ponowne wykorzystywanie niektórych kategorii chronionych danych. Do zadań

tych organów może należeć udzielanie dostępu do danych, w przypadku gdy jest to przewidziane w przepisach sektorowych Unii lub państw członkowskich. Te właściwe podmioty powinny zapewniać wsparcie organom sektora publicznego za pomocą najnowocześniejszych technik, w tym zabezpieczonych środowisk przetwarzania danych, które umożliwiają analizę danych w sposób chroniący prywatność informacji. Taka struktura wsparcia może być pomocna posiadaczom danych w zarządzaniu zgodą, w tym zgodą na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Przetwarzanie danych powinno odbywać się na odpowiedzialność organu sektora publicznego odpowiedzialnego za rejestr zawierający te dane, który w odniesieniu do danych osobowych pozostaje administratorem danych w rozumieniu rozporządzenia (UE) 2016/679. Państwa członkowskie mogą posiadać jeden właściwy podmiot lub kilka takich podmiotów, które mogą działać w różnych sektorach.

(22) Oczekuje się, że dostawcy usług udostępniania danych (pośrednicy w zakresie danych) będą odgrywali kluczową rolę w gospodarce opartej na danych jako narzędzie ułatwiające agregowanie i wymianę znacznych ilości istotnych danych. Pośrednicy w zakresie danych oferujący usługi, które łączą poszczególne podmioty, mogą przyczynić się do skutecznego łączenia danych, jak również do ułatwienia dwustronnego udostępniania danych. Wyspecjalizowani pośrednicy w zakresie danych, którzy są niezależni zarówno od posiadaczy danych, jak i użytkowników danych, mogą odgrywać rolę polegającą na ułatwianiu powstawania nowych ekosystemów opartych na danych, niezależnych od jakiegokolwiek podmiotu o znaczącej pozycji rynkowej. Niniejsze rozporządzenie powinno obejmować wyłącznie dostawców usług udostępniania danych, których głównym celem jest nawiązanie relacji biznesowych, prawnych i potencjalnie również technicznych między posiadaczami danych, w tym osobami, których dane dotyczą, z jednej strony a potencjalnymi użytkownikami z drugiej strony oraz pomoc obu stronom w przeprowadzaniu transakcji dotyczących zasobów danych. Powinno ono obejmować tylko usługi mające na celu pośredniczenie między nieokreśloną liczbą posiadaczy i użytkowników danych, z wyłączeniem usług udostępniania danych, które mają być wykorzystywane przez zamkniętą grupę posiadaczy i użytkowników danych. Należy wykluczyć dostawców usług w chmurze, jak również dostawców usług, którzy uzyskują dane od posiadaczy danych, agregują, wzbogacają lub przekształcają dane i udzielają licencji na wykorzystywanie powstałych danych użytkownikom danych bez ustanawiania bezpośredniej relacji między posiadaczami danych a użytkownikami danych, na przykład brokerów reklam lub danych, przedsiębiorstwa doradcze w zakresie danych, dostawców produktów uzyskanych z danych, powstałych w wyniku wniesienia wartości dodanej w dane przez dostawcę usług. Jednocześnie należy umożliwić dostawcom usług udostępniania danych dostosowywanie udostępnianych danych – takie jak konwertowanie ich na konkretne formaty – w zakresie, w jakim poprawia to użyteczność danych dla użytkownika danych, w przypadku gdy użytkownik danych sobie tego życzy. Ponadto niniejsze rozporządzenie nie powinno obejmować usług, które koncentrują się na pośrednictwie w udostępnianiu treści, w szczególności treści chronionych prawem autorskim. Niniejsze rozporządzenie nie powinno obejmować platform wymiany danych, które to platformy są użytkowane wyłącznie przez jednego posiadacza danych w celu umożliwienia wykorzystywania posiadanych danych, ani platform opracowanych w kontekście przedmiotów i urządzeń podłączonych do internetu rzeczy, których głównym celem jest zapewnienie funkcji podłączonego przedmiotu lub urządzenia i umożliwienie świadczenia usług o wartości dodanej. Do celów niniejszego

rozporządzenia „dostawców informacji skonsolidowanych” w rozumieniu art. 4 ust. 1 pkt 53 dyrektywy Parlamentu Europejskiego i Rady 2014/65/UE[42], jak również „dostawców świadczących usługę dostępu do informacji o rachunku” w rozumieniu art. 4 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366[43] nie należy uznawać za dostawców usług udostępniania danych. Podmioty, które ograniczają swoją działalność do ułatwiania wykorzystywania danych udostępnianych na podstawie altruistycznego podejścia do danych i które prowadzą działalność o charakterze niekomercyjnym, nie powinny być objęte przepisami rozdziału III niniejszego rozporządzenia, ponieważ działalność ta służy celom leżącym w interesie ogólnym dzięki zwiększaniu ilości danych dostępnych do takich celów.

(23) Szczególna kategoria pośredników w zakresie danych obejmuje dostawców usług udostępniania danych oferujących swoje usługi osobom, których dane dotyczą, w rozumieniu rozporządzenia (UE) 2016/679. Tacy dostawcy usług koncentrują się wyłącznie na danych osobowych i dążą do zwiększenia indywidualnej sprawczości i kontroli osób fizycznych nad dotyczącymi ich danymi. Pomagaliby oni osobom fizycznym w wykonywaniu ich praw wynikających z rozporządzenia (UE) 2016/679, w szczególności w zarządzaniu ich zgodą na przetwarzanie danych, prawem dostępu do własnych danych, prawem do sprostowania nieprawidłowych danych osobowych, prawem do usunięcia danych lub prawem do bycia zapomnianym, prawem do ograniczenia przetwarzania i prawem do przenoszenia danych, które umożliwia osobom, których dane dotyczą, przeniesienie ich danych osobowych od jednego administratora do drugiego. W tym kontekście ważne jest, aby ich model biznesowy zapewniał brak niewłaściwych zachęt dla osób fizycznych do udostępniania do przetwarzania większej ilości danych, niż to leży w ich własnym interesie. Może to obejmować doradzanie osobom fizycznym w zakresie wykorzystywania ich danych, na które mogą one zezwolić, oraz przeprowadzanie kontroli należytej staranności w odniesieniu do użytkowników danych przed umożliwieniem im skontaktowania się z osobami, których dane dotyczą, co ma na celu uniknięcie praktyk stanowiących oszustwo. W określonych sytuacjach, w celu maksymalnego zwiększenia ochrony danych osobowych i prywatności, pożądane może być zestawianie rzeczywistych danych w przestrzeni przechowywania danych osobowych, czyli „przestrzeni danych osobowych”, tak aby przetwarzanie mogło odbywać się w tej przestrzeni bez przekazywania danych osobowych osobom trzecim.

(24) Spółdzielnie danych dążą do wzmocnienia pozycji osób fizycznych przy dokonywaniu świadomych wyborów przed wyrażeniem zgody na wykorzystywanie danych, wywierając wpływ na zasady i warunki organizacji użytkowników danych związane z wykorzystywaniem danych lub potencjalnie rozwiązując spory między członkami grupy dotyczące sposobu wykorzystywania danych, w przypadku gdy dane takie odnoszą się do kilku osób w obrębie grupy, których dane dotyczą. W tym kontekście należy podkreślić, że prawa wynikające z rozporządzenia (UE) 2016/679 mogą być wykonywane tylko przez każdą osobę fizyczną i nie mogą być powierzone ani przekazane spółdzielni danych. Spółdzielnie danych mogą również zapewniać przydatne środki przedsiębiorstwom jednoosobowym, mikroprzedsiębiorstwom oraz

[42] Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, Dz.U. L 173/349.

[43] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE.

małym i średnim przedsiębiorstwom, których wiedza na temat udostępniania danych jest często porównywalna z wiedzą osób fizycznych.

(25) W celu zwiększenia zaufania do takich usług udostępniania danych, w szczególności w odniesieniu do wykorzystywania danych i zgodności z warunkami nałożonymi przez posiadaczy danych, konieczne jest utworzenie ram regulacyjnych na szczeblu Unii, które określałyby wysoce zharmonizowane wymogi związane z godnym zaufania świadczeniem takich usług udostępniania danych. Przyczyni się to do zapewnienia, aby posiadacze danych i użytkownicy danych mieli lepszą kontrolę nad dostępem do ich danych i wykorzystywaniem ich, zgodnie z prawem Unii. Zarówno w sytuacjach, w których udostępnianie danych ma miejsce w kontekście udostępniania między przedsiębiorstwami, jak i w sytuacjach, w których ma to miejsce w kontekście udostępniania między przedsiębiorstwami a konsumentami, dostawcy usług udostępniania danych powinni oferować nowatorski, „europejski" sposób zarządzania danymi, aby zapewnić w gospodarce opartej na danych rozdział pomiędzy udostępnianiem danych, pośrednictwem i wykorzystywaniem. Dostawcy usług udostępniania danych mogą również udostępniać specjalną infrastrukturę techniczną dla wzajemnych połączeń między posiadaczami danych i użytkownikami danych.

(26) Kluczowym elementem zapewniającym zaufanie i lepszą kontrolę posiadaczom danych i użytkownikom danych w odniesieniu do usług udostępniania danych jest neutralność dostawców takich usług względem danych udostępnianych między posiadaczami danych a użytkownikami danych. Dlatego koniecznie jest, aby dostawcy usług udostępniania danych działali jedynie jako pośrednicy w transakcjach i nie wykorzystywali udostępnianych danych do żadnych innych celów. Będzie to również wymagało strukturalnego rozdziału usług udostępniania danych od wszelkich innych świadczonych usług, tak aby uniknąć konfliktu interesów. Oznacza to, że usługi udostępniania danych powinny być świadczone za pośrednictwem podmiotu prawnego, który jest odrębny od pozostałej działalności danego dostawcy usług udostępniania danych. Dostawcy usług udostępniania danych, którzy pośredniczą w wymianie danych między osobami fizycznymi jako posiadaczami danych a osobami prawnymi, powinni ponadto mieć wobec osób fizycznych obowiązek powierniczy, co ma na celu zapewnienie, aby działali w najlepszym interesie posiadaczy danych.

(27) Aby zapewnić zgodność dostawców usług udostępniania danych z warunkami określonymi w niniejszym rozporządzeniu, tacy dostawcy powinni mieć miejsce prowadzenia działalności w Unii. W innym przypadku, jeżeli dostawca usług udostępniania danych nieposiadający miejsca prowadzenia działalności w Unii oferuje usługi w Unii, dostawca taki powinien wyznaczyć przedstawiciela. Wyznaczenie przedstawiciela jest konieczne ze względu na to, że tacy dostawcy usług udostępniania danych zajmują się danymi osobowymi, jak również danymi objętymi tajemnicą handlową, co wymaga dokładnego monitorowania zgodności takich dostawców usług z warunkami określonymi w niniejszym rozporządzeniu. Aby stwierdzić, czy dostawca usług udostępniania danych oferuje usługi w Unii, należy upewnić się, czy jest oczywiste, że ten dostawca usług udostępniania danych zamierza oferować usługi osobom w co najmniej jednym państwie członkowskim. Sama dostępność w Unii strony internetowej lub adresu e-mail i innych danych kontaktowych dostawcy usług udostępniania danych lub posługiwanie się językiem powszechnie używanym w państwie trzecim, w którym dostawca usług udostępniania danych ma siedzibę, należy uznać za niewystarczające do stwierdzenia takiego zamiaru. Czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia usług w tym języku lub

wzmianka o użytkownikach znajdujących się w Unii, mogą jednak potwierdzać oczywistość zamiaru oferowania przez dostawcę usług udostępniania danych określonych usług w Unii. Przedstawiciel powinien występować w imieniu dostawcy usług udostępniania danych, a właściwe organy powinny móc kontaktować się z przedstawicielem. Dostawca usług udostępniania danych powinien wyznaczyć przedstawiciela za pomocą pisemnego upoważnienia do występowania w jego imieniu w zakresie jego obowiązków wynikających z niniejszego rozporządzenia.

(28) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla obowiązku przestrzegania przez dostawców usług udostępniania danych rozporządzenia (UE) 2016/679 oraz odpowiedzialności organów nadzorczych za zapewnienie zgodności z tym rozporządzeniem. W przypadku gdy dostawcami usług udostępniania danych są administratorzy danych lub podmioty przetwarzające dane w rozumieniu rozporządzenia (UE) 2016/679, obowiązują ich przepisy tego rozporządzenia. Niniejsze rozporządzenie powinno również pozostawać bez uszczerbku dla stosowania prawa konkurencji.

(29) Dostawcy usług udostępniania danych powinni również stosować środki mające na celu zapewnienie zgodności z prawem konkurencji. Udostępnianie danych może generować różnego rodzaju korzyści w zakresie efektywności, ale może również prowadzić do ograniczenia konkurencji, w szczególności gdy obejmuje udostępnianie informacji szczególnie chronionych istotnych dla konkurencji. Dotyczy to zwłaszcza sytuacji, w których udostępnianie danych umożliwia przedsiębiorstwom zdobycie wiedzy o strategiach rynkowych ich faktycznych lub potencjalnych konkurentów. Informacje szczególnie chronione istotne dla konkurencji zazwyczaj obejmują informacje o przyszłych cenach, kosztach produkcji, ilościach, obrotach, sprzedaży lub zdolnościach.

(30) Należy ustanowić procedurę zgłaszania usług udostępniania danych, aby zapewnić zarządzanie danymi na terenie Unii oparte na godnej zaufania wymianie danych. Korzyści płynące z godnego zaufania otoczenia najlepiej osiągnąć poprzez nałożenie szeregu wymogów dotyczących świadczenia usług udostępniania danych, ale bez konieczności wydawania przez właściwy organ jakiejkolwiek jednoznacznej decyzji lub aktu administracyjnego na potrzeby świadczenia takich usług.

(31) Aby wesprzeć skuteczne transgraniczne świadczenie usług, należy wymagać od dostawcy usług udostępniania danych przesłania zgłoszenia wyłącznie do wyznaczonego właściwego organu państwa członkowskiego, w którym znajduje się jego główna jednostka organizacyjna lub w którym znajduje się jego przedstawiciel prawny. Takie zgłoszenie nie powinno mieć szerszego zakresu niż zwykłe oświadczenie o zamiarze świadczenia takich usług i powinno zawierać wyłącznie informacje określone w niniejszym rozporządzeniu.

(32) „Główna jednostka organizacyjna” dostawcy usług udostępniania danych w Unii powinna znajdować się w państwie członkowskim, w którym znajduje się jego centralna administracja w Unii. Główną jednostkę organizacyjną dostawcy usług udostępniania danych w Unii należy określać na podstawie obiektywnych kryteriów i powinna ona oznaczać skuteczne i faktycznie zarządzanie.

(33) Właściwe organy wyznaczone do monitorowania zgodności usług udostępniania danych z wymogami niniejszego rozporządzenia powinny być wybierane na podstawie ich możliwości i wiedzy fachowej w zakresie horyzontalnego lub sektorowego udostępniania danych oraz powinny być one niezależne, jak również wykonywać

swoje zadania w sposób przejrzysty i bezstronny. Państwa członkowskie powinny przekazać Komisji dane identyfikacyjne wyznaczonych właściwych organów.

(34) Ramy dotyczące zgłaszania ustanowione w niniejszym rozporządzeniu nie powinny naruszać szczególnych dodatkowych przepisów dotyczących świadczenia usług udostępniania danych, które to przepisy mają zastosowanie na podstawie przepisów sektorowych.

(35) Wykorzystywanie danych udostępnionych dobrowolnie do celów interesu ogólnego przez osoby, których dane dotyczą, na podstawie ich zgody lub – w przypadku danych nieosobowych – udostępnionych przez osoby prawne, ma duży potencjał. Cele takie obejmują opiekę zdrowotną, przeciwdziałanie zmianie klimatu, poprawę mobilności, ułatwianie tworzenia statystyk publicznych lub poprawę świadczenia usług publicznych. Za cele interesu ogólnego należy również uznać wsparcie badań naukowych, obejmujące na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. Niniejsze rozporządzenie ma na celu przyczynienie się do powstania pul danych udostępnianych na podstawie altruistycznego podejścia do danych, mających wielkość wystarczającą do umożliwienia analizy danych i uczenia się maszyn, w tym również w kontekście transgranicznym w Unii.

(36) Podmioty prawne, które starają się wspierać realizację celów interesu ogólnego poprzez udostępnianie na dużą skalę odpowiednich danych w oparciu o altruistyczne podejście do danych i które spełniają określone wymogi, powinny mieć możliwość zarejestrowania się jako „uznana w Unii organizacja o altruistycznym podejściu do danych”. Może to doprowadzić do powstania repozytoriów danych. Rejestracja w państwie członkowskim byłaby ważna w całej Unii, zatem powinno to ułatwić transgraniczne wykorzystywanie danych w Unii oraz tworzenie pul danych obejmujących kilka państw członkowskich. Osoby, których dane dotyczą, wyrażałyby w tym względzie zgodę na konkretne cele przetwarzania danych, ale mogłyby również wyrażać zgodę na przetwarzanie danych w niektórych obszarach badań lub w ramach projektów badawczych, ponieważ w momencie gromadzenia danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. Osoby prawne mogłyby wyrażać zgodę na przetwarzanie ich danych nieosobowych do wielu różnych celów, których nie określono w momencie udzielania zgody. Dobrowolne spełnianie przez takie zarejestrowane podmioty szeregu wymogów powinno budzić zaufanie, że dane udostępniane w celach altruistycznych służą celom interesu ogólnego. Zaufanie takie powinno wynikać w szczególności z miejsca prowadzenia działalności w Unii, a także z wymogu, aby zarejestrowane podmioty prowadziły działalność o charakterze niekomercyjnym, z wymogów dotyczących przejrzystości oraz z istnienia określonych zabezpieczeń służących ochronie praw i interesów osób, których dane dotyczą, oraz przedsiębiorstw. Dalsze zabezpieczenia powinny obejmować umożliwienie przetwarzania odpowiednich danych w bezpiecznym środowisku przetwarzania prowadzonym przez zarejestrowany podmiot, mechanizmy nadzoru, takie jak rady lub zarządy ds. etyki, mające zapewnić utrzymywanie przez administratora danych wysokich standardów etyki naukowej, skuteczne środki techniczne umożliwiające wycofanie lub zmianę zgody w dowolnym momencie, w oparciu o obowiązki informacyjne podmiotów przetwarzających dane na podstawie rozporządzenia (UE) 2016/679, a także środki służące stałemu informowaniu osób, których dane dotyczą, o wykorzystywaniu udostępnionych przez nie danych.

(37) Niniejsze rozporządzenie pozostaje bez uszczerbku dla ustanawiania, organizacji i funkcjonowania podmiotów, które chcą przyjąć altruistyczne podejście do danych zgodnie z prawem krajowym. Opiera się ono na wymogach prawa krajowego dotyczących zgodnego z prawem działania w państwie członkowskim jako organizacja o charakterze niekomercyjnym. Podmioty, które spełniają wymogi niniejszego rozporządzenia, powinny mieć możliwość korzystania z tytułu „uznana w Unii organizacja o altruistycznym podejściu do danych".

(38) Uznane w Unii organizacje o altruistycznym podejściu do danych powinny mieć możliwość gromadzenia odpowiednich danych bezpośrednio od osób fizycznych i prawnych lub przetwarzania danych zgromadzonych przez inne osoby. Zazwyczaj altruistyczne podejście do danych opiera się na zgodzie osób, których dane dotyczą, w rozumieniu art. 6 ust. 1 lit. a) i art. 9 ust. 2 lit. a), wyrażonej zgodnie z wymogami dotyczącymi zgody zgodnej z prawem, określonymi w art. 7 rozporządzenia (UE) 2016/679. Zgodnie z rozporządzeniem (UE) 2016/679 cele badań naukowych można uzasadnić zgodą na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych, lub tylko na niektóre obszary badań lub elementy projektów badawczych. Art. 5 ust. 1 lit. b) rozporządzenia (UE) 2016/679 stanowi, że dalsze przetwarzanie do celów badań naukowych lub historycznych lub do celów statystycznych nie powinno być uznawane w myśl art. 89 ust. 1 rozporządzenia (UE) 2016/679 za niezgodne z pierwotnymi celami.

(39) W celu zapewnienia dodatkowej pewności prawa w odniesieniu do udzielania i wycofywania zgody, w szczególności w kontekście wykorzystywania danych udostępnianych z pobudek altruistycznych do celów badań naukowych i celów statystycznych, należy opracować europejski formularz zgody na potrzeby altruistycznego podejścia do danych i stosować go w kontekście udostępniania danych z pobudek altruistycznych. Formularz taki powinien przyczynić się do zapewnienia osobom, których dane dotyczą, dodatkowej przejrzystości co do tego, że ich dane będą udostępniane i wykorzystywane zgodnie z wyrażoną przez nie zgodą, jak również w pełnej zgodności z przepisami o ochronie danych. Można byłoby go również wykorzystać do usprawnienia altruistycznego podejścia do danych stosowanego przez przedsiębiorstwa i zapewnienia mechanizmu umożliwiającego takim przedsiębiorstwom wycofanie zgody na wykorzystywanie danych. Aby uwzględnić specyfikę poszczególnych sektorów, w tym z punktu widzenia ochrony danych, powinna istnieć możliwość sektorowego dostosowania europejskiego formularza zgody na potrzeby altruistycznego podejścia do danych.

(40) W celu pomyślnego wdrożenia ram zarządzania danymi należy ustanowić Europejską Radę ds. Innowacji w zakresie Danych w formie grupy ekspertów. Rada powinna składać się z przedstawicieli państw członkowskich, Komisji oraz przedstawicieli odpowiednich przestrzeni danych i określonych sektorów (takich jak: opieka zdrowotna, rolnictwo, transport i statystyka). Należy zwrócić się do Europejskiej Rady Ochrony Danych o wyznaczenie przedstawiciela do Europejskiej Rady ds. Innowacji w zakresie Danych.

(41) Rada powinna wspomagać Komisję w koordynowaniu krajowych praktyk i polityk w kwestiach objętych niniejszym rozporządzeniem oraz we wspieraniu międzysektorowego wykorzystywania danych poprzez przestrzeganie zasad europejskich ram interoperacyjności oraz stosowanie norm i specyfikacji (takich jak podstawowe słowniki[44] i moduły instrumentu „Łącząc Europę"[45]), bez uszczerbku dla

[44] https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies

prac normalizacyjnych prowadzonych w konkretnych sektorach lub dziedzinach. Prace nad normalizacją techniczną mogą obejmować określenie priorytetów na potrzeby opracowania norm oraz ustanowienie i utrzymywanie zestawu norm technicznych i prawnych dotyczących przekazywania danych między dwoma środowiskami przetwarzania, co umożliwi organizację przestrzeni danych bez korzystania z usług pośrednika. Rada powinna współpracować z organami sektorowymi, sieciami lub grupami ekspertów lub innymi organizacjami międzysektorowymi zajmującymi się ponownym wykorzystywaniem danych. Odnośnie do altruistycznego podejścia do danych Rada, w porozumieniu z Europejską Radą Ochrony Danych, powinna pomóc Komisji w opracowaniu formularza zgody na potrzeby altruistycznego podejścia do danych.

(42) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze do opracowania europejskiego formularza zgody na potrzeby altruistycznego podejścia do danych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011[46].

(43) W celu uwzględnienia szczególnego charakteru niektórych kategorii danych, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu określenia warunków specjalnych mających zastosowanie do przekazywania do państw trzecich niektórych kategorii danych nieosobowych uznawanych za szczególnie chronione w określonych aktach Unii przyjętych w drodze procedury ustawodawczej. Szczególnie ważne jest, aby w czasie prac przygotowawczych Komisja prowadziła stosowne konsultacje, w tym na poziomie ekspertów, oraz aby konsultacje te prowadzone były zgodnie z zasadami określonymi w Porozumieniu międzyinstytucjonalnym z dnia 13 kwietnia 2016 r. w sprawie lepszego stanowienia prawa. W szczególności, aby zapewnić udział na równych zasadach Parlamentu Europejskiego i Rady w przygotowaniu aktów delegowanych, instytucje te otrzymują wszelkie dokumenty w tym samym czasie co eksperci państw członkowskich, a eksperci tych instytucji mogą systematycznie brać udział w posiedzeniach grup eksperckich Komisji zajmujących się przygotowaniem aktów delegowanych.

(44) Niniejsze rozporządzenie nie powinno mieć wpływu na stosowanie reguł konkurencji, a w szczególności art. 101 i 102 Traktatu o funkcjonowaniu Unii Europejskiej. Środków przewidzianych w niniejszym rozporządzeniu nie należy stosować do ograniczania konkurencji w sposób sprzeczny z Traktatem o funkcjonowaniu Unii Europejskiej. Dotyczy to w szczególności przepisów dotyczących wymiany informacji szczególnie chronionych istotnych dla konkurencji między rzeczywistymi lub potencjalnymi konkurentami za pośrednictwem usług udostępniania danych.

(45) Zgodnie z art. 42 rozporządzenia Parlamentu Europejskiego i Rady ([47]) (UE) 2018/1725 przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, które zakończyły się wydaniem opinii w dniu [...].

---

45 https://joinup.ec.europa.eu/collection/connecting-europe-facility-cef

46 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

47 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 (Dz.U. L 295 z 21.11.2018, s. 39).

(46) Niniejsze rozporządzenie nie narusza praw podstawowych ani zasad uznanych w szczególności w Karcie praw podstawowych, w tym prawa do prywatności, ochrony danych osobowych, wolności działalności gospodarczej, prawa własności oraz integracji osób z niepełnosprawnościami,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I
PRZEPISY OGÓLNE

Artykuł 1
Przedmiot i zakres

1) W niniejszym rozporządzeniu ustanawia się:

   a) warunki ponownego wykorzystywania w Unii niektórych kategorii danych będących w posiadaniu organów sektora publicznego;

   b) ramy dotyczące zgłaszania i nadzoru w odniesieniu do świadczenia usług udostępniania danych;

   c) ramy dotyczące dobrowolnej rejestracji podmiotów, które gromadzą i przetwarzają dane udostępniane z pobudek altruistycznych.

2) Niniejsze rozporządzenie nie narusza przepisów szczegółowych zawartych w innych aktach prawnych Unii dotyczących dostępu do niektórych kategorii danych lub ich ponownego wykorzystywania ani wymogów związanych z przetwarzaniem danych osobowych i nieosobowych. Jeżeli sektorowy akt prawny Unii wymaga od organów sektora publicznego, dostawców usług udostępniania danych lub zarejestrowanych podmiotów świadczących usługi z zachowaniem altruistycznego podejścia do danych, spełnienia szczególnych dodatkowych wymogów technicznych, administracyjnych lub organizacyjnych, w tym poprzez system zezwoleń lub certyfikacji, stosuje się również te przepisy danego sektorowego aktu prawnego Unii.

Artykuł 2
Definicje

Na potrzeby niniejszego rozporządzenia stosuje się następujące definicje:

1) „dane” oznaczają wszelkie cyfrowe odwzorowania działań, faktów lub informacji oraz wszelkie kompilacje takich działań, faktów lub informacji, w tym w formie zapisu dźwiękowego, wizualnego lub audiowizualnego;

2) „ponowne wykorzystywanie” oznacza wykorzystywanie przez osoby fizyczne lub prawne danych będących w posiadaniu organów sektora publicznego, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla którego to celu dane te zostały wyprodukowane, z wyjątkiem wymiany danych między organami sektora publicznego służącej wyłącznie wykonywaniu ich zadań publicznych;

3) „dane nieosobowe” oznaczają dane inne niż dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

4) „metadane” oznaczają dane gromadzone na temat wszelkiej działalności osoby fizycznej lub prawnej w celu świadczenia usługi udostępniania danych, w tym dane

dotyczące daty, godziny i geolokalizacji, czasu trwania działalności, połączeń z innymi osobami prawnymi lub fizycznymi ustanowionymi przez osobę korzystającą z usługi;

5) „posiadacz danych” oznacza osobę prawną lub osobę, której dane dotyczą, która zgodnie z mającym zastosowanie prawem unijnym lub krajowym ma prawo do udzielania dostępu do niektórych danych osobowych lub nieosobowych będących pod jej kontrolą lub do udostępnienia tych danych;

6) „użytkownik danych” oznacza osobę fizyczną lub prawną, która ma zgodny z prawem dostęp do niektórych danych osobowych lub nieosobowych i jest upoważniona do wykorzystywania tych danych w celach komercyjnych lub niekomercyjnych;

7) „udostępnianie danych” oznacza udostępnianie danych przez posiadacza danych podmiotowi wykorzystującemu dane, w celu wspólnego lub indywidualnego wykorzystania udostępnianych danych, na podstawie dobrowolnych porozumień, bezpośrednio lub przez pośrednika;

8) „dostęp” oznacza przetwarzanie danych, które zostały dostarczone przez posiadacza danych, przez użytkownika danych zgodnie ze szczegółowymi wymogami technicznymi, prawnymi lub organizacyjnymi, co niekoniecznie musi się wiązać z przesyłaniem lub pobieraniem takich danych;

9) „główna jednostka organizacyjna” podmiotu prawnego oznacza miejsce, w którym znajduje się jego centralna administracja w Unii;

10) „altruistyczne podejście do danych” oznacza zgodę udzielaną przez osoby, których dane dotyczą, na przetwarzanie dotyczących ich danych osobowych lub zezwolenia innych posiadaczy danych na wykorzystywanie ich danych nieosobowych bez żądania wynagrodzenia, do celów realizowanych w interesie ogólnym, takich jak cele badań naukowych lub poprawa jakości usług publicznych;

11) „organ sektora publicznego” oznacza państwo, władze regionalne lub lokalne, podmioty prawa publicznego lub związki złożone z co najmniej jednej takiej instytucji lub z co najmniej jednego takiego podmiotu prawa publicznego;

12) „podmiot prawa publicznego” oznacza podmiot, który posiada poniższe cechy:

   a) został utworzony w konkretnym celu zaspokajania potrzeb w interesie ogólnym i nie ma charakteru przemysłowego ani handlowego;

   b) posiada osobowość prawną;

   c) jest finansowany w przeważającej części przez państwo, władze regionalne lub lokalne lub inne podmioty prawa publicznego; bądź jego zarząd podlega nadzorowi ze strony tych władz lub podmiotów; bądź ponad połowa członków jego organu administrującego, zarządzającego lub nadzorczego została wyznaczona przez państwo, instytucje regionalne lub lokalne, lub przez inne podmioty prawa publicznego;

13) „przedsiębiorstwo publiczne” oznacza 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; do celów niniejszej definicji zakłada się istnienie dominującego wpływu ze strony organów

sektora publicznego w dowolnym z poniższych przypadków, gdy organy te bezpośrednio lub pośrednio:

a) posiadają większość subskrybowanego kapitału przedsiębiorstwa;

b) kontrolują większość głosów przypadających na akcje wyemitowane przez przedsiębiorstwo;

c) mogą powoływać ponad połowę członków organu administrującego, zarządzającego lub nadzorczego przedsiębiorstwa;

14) „bezpieczne środowisko przetwarzania” oznacza fizyczne lub wirtualne środowisko i środki organizacyjne zapewniające możliwość ponownego wykorzystywania danych w sposób, który pozwala operatorowi bezpiecznego środowiska przetwarzania określić i nadzorować wszystkie działania związane z przetwarzaniem danych, w tym wyświetlanie, przechowywanie, pobieranie, eksport danych i obliczanie danych pochodnych za pomocą algorytmów obliczeniowych;

15) „przedstawiciel” oznacza każdą osobę fizyczną lub prawną mającą siedzibę w Unii, w wyraźny sposób wyznaczoną do podejmowania działań w imieniu dostawcy usług udostępniania danych lub podmiotu gromadzącego dane do celów realizowanych w interesie ogólnym udostępniane przez osoby fizyczne lub prawne na podstawie altruistycznego podejścia do danych, niemających siedziby w Unii, do której właściwy organ krajowy może się zwrócić zamiast dostawcy usług udostępniania danych lub podmiotu w związku z obowiązkami tego dostawcy usług udostępniania danych lub podmiotu ustanowionymi na mocy niniejszego rozporządzenia.

ROZDZIAŁ II
PONOWNE WYKORZYSTYWANIE NIEKTÓRYCH KATEGORII CHRONIONYCH DANYCH BĘDĄCYCH W POSIADANIU ORGANÓW SEKTORA PUBLICZNEGO

Artykuł 3
Kategorie danych

1) Niniejszy rozdział ma zastosowanie do danych będących w posiadaniu organów sektora publicznego, które są chronione ze względu na:

a) tajemnicę handlową;

b) poufność informacji statystycznych;

c) ochronę praw własności intelektualnej osób trzecich;

d) ochronę danych osobowych.

2) Niniejszy rozdział nie ma zastosowania do:

a) danych będących w posiadaniu przedsiębiorstw publicznych;

b) danych będących w posiadaniu publicznych nadawców radiowych i telewizyjnych oraz ich jednostek zależnych, a także innych organów lub ich jednostek zależnych realizujących misję nadawców publicznych;

c) danych będących w posiadaniu instytucji kulturalnych i edukacyjnych;

d) danych chronionych ze względu na bezpieczeństwo narodowe, obronność lub bezpieczeństwo publiczne;

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

3) Przepisy niniejszego rozdziału nie nakładają na organy sektora publicznego obowiązku zezwalania na ponowne wykorzystywanie danych ani nie zwalniają organów sektora publicznego z obowiązku zachowania poufności. Niniejszy rozdział nie narusza przepisów prawa unijnego i krajowego ani postanowień umów międzynarodowych, których Unia lub państwa członkowskie są stronami, dotyczących ochrony kategorii danych przewidzianych w ust. 1. Niniejszy rozdział nie narusza przepisów prawa unijnego i krajowego dotyczących dostępu do dokumentów oraz pozostaje bez uszczerbku dla obowiązków organów sektora publicznego wynikających z prawa unijnego i krajowego w zakresie zezwalania na ponowne wykorzystywanie danych.

Artykuł 4
Zakaz stosowania uzgodnień dotyczących wyłączności

1) Zakazuje się zawierania umów lub stosowania innych praktyk odnoszących się do ponownego wykorzystywania danych będących w posiadaniu organów sektora publicznego, zawierających kategorie danych określone w art. 3 ust. 1, w ramach których przyznaje się prawa wyłączne lub których celem lub skutkiem jest przyznanie takich praw wyłącznych lub ograniczenie dostępności danych do ponownego wykorzystywania przez podmioty niebędące stronami takich umów lub innych praktyk.

2) Na zasadzie odstępstwa od ust. 1, prawo wyłączne do ponownego wykorzystywania danych, o którym mowa w tym ustępie, może zostać przyznane w zakresie niezbędnym do świadczenia usługi lub dostarczania produktu w interesie ogólnym.

3) Prawo wyłączne przyznaje się w kontekście odpowiedniego zamówienia na usługi lub odpowiedniej umowy koncesji zgodnie z mającymi zastosowanie unijnymi i krajowymi przepisami dotyczącymi zamówień publicznych i udzielania koncesji lub, w przypadku umowy o wartości, do której nie mają zastosowania ani unijne, ani krajowe przepisy dotyczące zamówień publicznych i udzielania koncesji, zgodnie z zasadami przejrzystości, równego traktowania i niedyskryminacji ze względu na przynależność państwową.

4) We wszystkich przypadkach nieujętych w ust. 3, a także gdy cel interesu ogólnego nie może być osiągnięty bez przyznania prawa wyłącznego, stosuje się zasady przejrzystości, równego traktowania i niedyskryminacji ze względu na przynależność państwową.

5) Okres obowiązywania prawa wyłącznego do ponownego wykorzystywania danych nie może przekraczać trzech lat. W przypadku udzielenia zamówienia lub zawarcia umowy okres obowiązywania udzielonego zamówienia lub zawartej umowy musi być zgodny z okresem wyłączności.

6) Przyznanie prawa wyłącznego zgodnie z ust. 2–5, w tym powody, dla których konieczne jest przyznanie takiego prawa, muszą być przejrzyste i podane do

wiadomości publicznej w internecie, niezależnie od ewentualnej publikacji ogłoszenia o udzieleniu zamówienia publicznego i zawarciu umowy koncesji.

7) Umowy lub inne praktyki objęte zakresem zakazu, o którym mowa w ust. 1, które nie spełniają warunków określonych w ust. 2, zawarte lub stosowane przed datą wejścia w życie niniejszego rozporządzenia wygasają wraz z końcem obowiązywania stosownej umowy, a w każdym razie najpóźniej w ciągu trzech lat od daty wejścia w życie niniejszego rozporządzenia.

Artykuł 5
Warunki ponownego wykorzystywania

1) Organy sektora publicznego, które na mocy prawa krajowego są właściwe do udzielania lub nieudzielania dostępu do celów ponownego wykorzystywania co najmniej jednej kategorii danych, o których mowa w art. 3 ust. 1, udostępniają publicznie warunki, jakie muszą zostać spełnione w celu zezwolenia na takie ponowne wykorzystywanie. W wykonywaniu tego zadania organy sektora publicznego mogą być wspomagane przez właściwe podmioty określone w art. 7 ust. 1.

2) W odniesieniu do kategorii danych i celów ponownego wykorzystywania oraz charakteru danych, których ponowne wykorzystywanie jest dozwolone, warunki ponownego wykorzystywania muszą być niedyskryminujące, proporcjonalne i obiektywnie uzasadnione. Warunki te nie mogą być stosowane do ograniczania konkurencji.

3) Organy sektora publicznego mogą nałożyć obowiązek ponownego wykorzystywania wyłącznie danych po przetworzeniu wstępnym, jeżeli takie przetwarzanie wstępne ma na celu anonimizację lub pseudonimizację danych osobowych lub usunięcie poufnych informacji handlowych, w tym tajemnic przedsiębiorstwa.

4) Organy sektora publicznego mogą nakładać obowiązki w zakresie:

   a) dostępu do danych i ich ponownego wykorzystywania w bezpiecznym środowisku przetwarzania zapewnianym i kontrolowanym przez sektor publiczny;

   b) dostępu do danych i ich ponownego wykorzystywania w obrębie obiektów fizycznych, w których znajduje się bezpieczne środowisko przetwarzania, jeżeli nie ma możliwości zezwolenia na dostęp zdalny bez stwarzania zagrożenia dla praw i interesów osób trzecich.

5) Organy sektora publicznego wprowadzają warunki, które pozwalają zachować integralność funkcjonowania systemów technicznych wykorzystywanego bezpiecznego środowiska przetwarzania. Organ sektora publicznego musi mieć możliwość weryfikacji wszelkich wyników przetwarzania danych przez podmiot ponownie wykorzystujący dane i zastrzega sobie prawo do zakazania wykorzystywania takich wyników, które zawierają informacje zagrażające prawom i interesom osób trzecich.

6) W przypadku gdy ponowne wykorzystywanie danych nie może być przyznane zgodnie z obowiązkami określonymi w ust. 3–5 i nie ma innej podstawy prawnej do przesłania danych na mocy rozporządzenia (UE) 2016/679, organ sektora publicznego wspiera podmioty ponownie wykorzystujące dane w dążeniu do uzyskania zgody osób, których dane dotyczą, lub zgody podmiotów prawnych,

których prawa i interesy mogą zostać naruszone w wyniku takiego ponownego wykorzystywania, o ile jest to możliwe bez ponoszenia nieproporcjonalnych kosztów przez sektor publiczny. W wykonywaniu tego zadania organy sektora publicznego mogą być wspomagane przez właściwe podmioty określone w art. 7 ust. 1.

7) Ponowne wykorzystywanie danych jest dozwolone wyłącznie z poszanowaniem praw własności intelektualnej. Prawo producenta bazy danych przewidziane w art. 7 ust. 1 dyrektywy 96/9/WE nie może być wykonywane przez organy sektora publicznego w celu uniemożliwienia ponownego wykorzystywania danych lub ograniczenia ponownego wykorzystywania w zakresie wykraczającym poza ograniczenia określone w niniejszym rozporządzeniu.

8) W przypadku gdy wymagane dane są uznawane za poufne zgodnie z prawem unijnym lub krajowym dotyczącym tajemnicy handlowej, organy sektora publicznego zapewniają, aby informacje poufne nie były ujawnione w wyniku ponownego wykorzystywania.

9) Komisja może przyjąć akty wykonawcze, stwierdzając, że stosowane przez państwa trzecie rozwiązania prawne, nadzorcze i wykonawcze:

   a) zapewniają ochronę własności intelektualnej i tajemnic przedsiębiorstwa w sposób zasadniczo równoważny z ochroną zapewnianą na mocy prawa Unii;

   b) są skutecznie stosowane i egzekwowane; oraz

   c) zapewniają skuteczne środki zaskarżenia.

Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 29 ust. 2.

10) Organy sektora publicznego przekazują dane poufne lub dane chronione prawami własności intelektualnej do podmiotu ponownie wykorzystującego dane, który zamierza przekazać te dane do państwa trzeciego innego niż państwo wyznaczone zgodnie z ust. 9, jeżeli podmiot ponownie wykorzystujący dane zobowiązuje się do:

   a) wypełniania obowiązków nałożonych zgodnie z ust. 7–8 nawet po przekazaniu danych do państwa trzeciego; oraz

   b) uznania jurysdykcji sądów państwa członkowskiego organu sektora publicznego w odniesieniu do wszelkich sporów związanych z wypełnieniem obowiązku określonego w lit. a).

11) Jeżeli szczególne akty Unii przyjęte zgodnie z procedurą ustawodawczą stanowią, że niektóre kategorie danych nieosobowych będące w posiadaniu organów sektora publicznego uznaje się za szczególnie chronione do celów niniejszego artykułu, Komisja jest uprawniona do przyjęcia aktów delegowanych zgodnie z art. 28 uzupełniających niniejsze rozporządzenie poprzez ustanowienie warunków szczegółowych mających zastosowanie do przekazywania danych do państw trzecich. Warunki przekazywania danych do państw trzecich określa się w oparciu o charakter kategorii danych określonych w akcie Unii oraz powody uznania ich za szczególnie chronione, niedyskryminujące i ograniczone do tego, co jest niezbędne do osiągnięcia celów polityki publicznej określonych w akcie prawa Unii, takich jak bezpieczeństwo i zdrowie publiczne, a także w oparciu o ryzyko deanonimizacji danych zanonimizowanych w odniesieniu do osób, których dane dotyczą, zgodnie z międzynarodowymi zobowiązaniami Unii. Mogą one obejmować warunki mające zastosowanie do przekazywania lub uzgodnień technicznych w tym zakresie, ograniczenia dotyczące ponownego wykorzystywania danych w państwach trzecich

lub kategorii osób, które są uprawnione do przekazywania takich danych do państw trzecich, lub, w wyjątkowych przypadkach, ograniczenia dotyczące przekazywania danych do państw trzecich.

12) Osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych nieosobowych, może przekazywać dane tylko do tych państw trzecich, w przypadku których spełnione są wymogi określone w ust. 9–11.

13) W przypadku gdy podmiot ponownie wykorzystujący dane zamierza przekazać dane nieosobowe do państwa trzeciego, organ sektora publicznego informuje posiadacza danych o przekazaniu danych do danego państwa trzeciego.

Artykuł 6
Opłaty

1) Organy sektora publicznego, które zezwalają na ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, mogą pobierać opłaty za zezwolenie na ponowne wykorzystywanie takich danych.

2) Wszelkie opłaty muszą być niedyskryminujące, proporcjonalne i obiektywnie uzasadnione oraz nie mogą ograniczać konkurencji.

3) Organy sektora publicznego zapewniają możliwość uiszczania wszelkich opłat przez internet za pośrednictwem powszechnie dostępnej transgranicznej usługi płatniczej, bez dyskryminacji ze względu na miejsce prowadzenia działalności przez dostawcę usług płatniczych, miejsce wydania instrumentu płatniczego lub lokalizację rachunku płatniczego w Unii.

4) W przypadku stosowania opłat organy sektora publicznego wprowadzają środki zachęcające do ponownego wykorzystywania kategorii danych, o których mowa w art. 3 ust. 1, do celów niekomercyjnych oraz przez małe i średnie przedsiębiorstwa, zgodnie z zasadami pomocy państwa.

5) Opłaty wynikają z kosztów związanych z przetwarzaniem wniosków o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1. Metodykę obliczania opłat należy opublikować z wyprzedzeniem.

6) Organ sektora publicznego publikuje opis głównych kategorii kosztów oraz reguł stosowanych przy ich podziale.

Artykuł 7
Właściwe podmioty

1) Państwa członkowskie wyznaczają co najmniej jeden właściwy podmiot, przy czym może to być podmiot sektorowy, którego celem jest wspieranie organów sektora publicznego udzielających dostępu do ponownego wykorzystywania kategorii danych, o których mowa w art. 3 ust. 1, w wykonywaniu tego zadania.

2) Wsparcie, o którym mowa w ust. 1, obejmuje, w stosownych przypadkach:

   a) zapewnienie wsparcia technicznego poprzez udostępnienie bezpiecznego środowiska przetwarzania w celu zapewnienia dostępu do ponownego wykorzystywania danych;

   b) zapewnienie wsparcia technicznego w zakresie stosowania sprawdzonych technik zapewniających przetwarzanie danych w sposób chroniący prywatność informacji zawartych w danych, których ponowne wykorzystywanie jest

dozwolone, w tym technik pseudonimizacji, anonimizacji, uogólnienia, ukrywania i randomizacji danych osobowych;

c) pomoc organom sektora publicznego, w razie potrzeby, w uzyskaniu zgody lub zezwolenia od podmiotów ponownie wykorzystujących dane na ponowne wykorzystywanie do celów związanych z altruistycznym podejściem do danych i innych, zgodnie z określonymi decyzjami posiadaczy danych, w tym dotyczącymi jurysdykcji, w których ma nastąpić przetwarzanie danych;

d) zapewnienie organom sektora publicznego pomocy w zakresie adekwatności zobowiązań podjętych przez podmiot ponownie wykorzystujący dane, zgodnie z art. 5 ust. 10.

3) Właściwym podmiotom można również powierzyć zadanie udzielania dostępu do ponownego wykorzystywania kategorii danych, o których mowa w art. 3 ust. 1, na mocy prawa unijnego lub krajowego, w którym przewidziano udzielenie takiego dostępu. W przypadku gdy takie właściwe podmioty wykonują swoją funkcję polegającą na udzielaniu lub nieudzielaniu dostępu do ponownego wykorzystywania, mają do nich zastosowanie art. 4, 5, 6 i art. 8 ust. 3.

4) Właściwemu podmiotowi lub właściwym podmiotom należy zapewnić odpowiednie możliwości prawne i techniczne oraz wiedzę fachową, aby były w stanie przestrzegać odpowiednich przepisów prawa unijnego lub krajowego dotyczących systemów dostępu do kategorii danych, o których mowa w art. 3 ust. 1.

5) Państwa członkowskie przekazują Komisji dane identyfikacyjne właściwych podmiotów wyznaczonych na podstawie ust. 1 do dnia [data rozpoczęcia stosowania niniejszego rozporządzenia]. Informują również Komisję o wszelkich późniejszych zmianach danych identyfikacyjnych tych organów.

Artykuł 8
Pojedynczy punkt informacyjny

1) Państwa członkowskie zapewniają, aby wszystkie istotne informacje dotyczące stosowania art. 5 i 6 były dostępne za pośrednictwem pojedynczego punktu informacyjnego.

2) Pojedynczy punkt informacyjny otrzymuje wnioski o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, i przekazuje je właściwym organom sektora publicznego lub, w stosownych przypadkach, właściwym podmiotom, o których mowa w art. 7 ust. 1. Pojedynczy punkt informacyjny udostępnia drogą elektroniczną rejestr dostępnych zasobów danych zawierający odpowiednie informacje opisujące charakter dostępnych danych.

3) Wnioski o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, są przyjmowane lub odrzucane przez właściwe organy sektora publicznego lub właściwe podmioty, o których mowa w art. 7 ust. 1, w rozsądnym terminie, a w każdym razie w ciągu dwóch miesięcy od daty złożenia wniosku.

4) Każda osoba fizyczna lub prawna, której dotyczy decyzja organu sektora publicznego lub właściwego podmiotu, w zależności od przypadku, ma prawo do skutecznego środka zaskarżenia takiej decyzji przed sądami państwa członkowskiego, w którym znajduje się właściwy organ.

ROZDZIAŁ III
WYMOGI MAJĄCE ZASTOSOWANIE DO USŁUG UDOSTĘPNIANIA DANYCH

Artykuł 9
Dostawcy usług udostępniania danych

1) Świadczenie następujących usług udostępniania danych podlega procedurze zgłaszania:

   a) usługi pośrednictwa między posiadaczami danych będącymi osobami prawnymi a potencjalnymi użytkownikami danych, w tym udostępnianie środków technicznych lub innych środków umożliwiających świadczenie takich usług; usługi te mogą obejmować dwustronną lub wielostronną wymianę danych lub tworzenie platform lub baz danych umożliwiających wymianę lub wspólne wykorzystywanie danych, jak również tworzenie specjalnej infrastruktury do wzajemnych połączeń między posiadaczami danych i użytkownikami danych;

   b) usługi pośrednictwa między osobami, których dane dotyczą, zamierzającymi udostępnić swoje dane osobowe a potencjalnymi użytkownikami danych, w tym udostępnianie technicznych lub innych środków umożliwiających świadczenie takich usług, w ramach wykonywania praw przewidzianych w rozporządzeniu (UE) 2016/679;

   c) usługi świadczone przez spółdzielnie danych, tj. usługi wspierające osoby, których dane dotyczą, lub jednoosobowe firmy, lub mikroprzedsiębiorstwa oraz małe i średnie przedsiębiorstwa, które są członkami spółdzielni lub które przyznają spółdzielni uprawnienia do negocjowania warunków przetwarzania danych przed wyrażeniem przez nie zgody, w dokonywaniu świadomych wyborów przed wyrażeniem zgody na przetwarzanie danych oraz umożliwiające ustanowienie mechanizmów wymiany poglądów na temat celów i warunków przetwarzania danych, które najlepiej będą odzwierciedlały interesy osób, których dane dotyczą, lub osób prawnych.

2) Niniejszy rozdział pozostaje bez uszczerbku dla stosowania innych przepisów prawa unijnego i krajowego wobec dostawców usług udostępniania danych, w tym uprawnień organów nadzorczych do zapewnienia zgodności z przepisami mającymi zastosowanie, w szczególności w odniesieniu do ochrony danych osobowych i prawa konkurencji.

Artykuł 10
Zgłaszanie dostawców usług udostępniania danych

1) Każdy dostawca usług udostępniania danych, który zamierza świadczyć usługi, o których mowa w art. 9 ust. 1, dokonuje zgłoszenia do właściwego organu, o którym mowa w art. 12.

2) Do celów niniejszego rozporządzenia uznaje się, że dostawca usług udostępniania danych posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim podlega jurysdykcji państwa członkowskiego, w którym ma swoją główną jednostkę organizacyjną.

3) Dostawca usług udostępniania danych, który nie ma siedziby w Unii, ale oferuje usługi, o których mowa w art. 9 ust. 1, na terytorium Unii, wyznacza przedstawiciela prawnego w jednym z państw członkowskich, w których usługi te są oferowane. Uznaje się, że dostawca usług podlega jurysdykcji państwa członkowskiego, w którym ma siedzibę jego przedstawiciel prawny.

4) Po dokonaniu zgłoszenia dostawca usług udostępniania danych może rozpocząć działalność z zastrzeżeniem warunków określonych w niniejszym rozdziale.

5) Zgłoszenie to uprawnia dostawcę usług do świadczenia usług udostępniania danych we wszystkich państwach członkowskich.

6) Zgłoszenie zawiera następujące informacje:

   a) nazwę dostawcy usług udostępniania danych;

   b) status prawny, formę prawną i numer rejestracyjny dostawcy, jeżeli dany dostawca jest zarejestrowany w rejestrze handlowym lub innym podobnym rejestrze publicznym;

   c) adres głównej jednostki organizacyjnej dostawcy w Unii, jeżeli ma to zastosowanie, oraz drugorzędnego oddziału w innym państwie członkowskim, o ile takowy istnieje, lub adres przedstawiciela prawnego wyznaczonego zgodnie z ust. 3;

   d) stronę internetową, na której można znaleźć informacje o dostawcy usług i jego działalności, jeśli taka istnieje;

   e) wskazanie osoby wyznaczonej do kontaktów przez dostawcę usług i dane kontaktowe;

   f) opis usługi, którą dostawca usług zamierza świadczyć;

   g) planowaną datę rozpoczęcia działalności;

   h) państwa członkowskie, w których dostawca usług zamierza świadczyć usługi.

7) Na wniosek dostawcy usług właściwy organ wydaje w terminie jednego tygodnia standardowe oświadczenie, potwierdzające, że dostawca usług przedłożył zgłoszenie, o którym mowa w ust. 4.

8) Właściwy organ niezwłocznie przekazuje każde zgłoszenie właściwym organom krajowym państw członkowskich drogą elektroniczną.

9) Właściwy organ powiadamia Komisję o każdym nowym zgłoszeniu. Komisja prowadzi rejestr dostawców usług udostępniania danych.

10) Właściwy organ może pobierać opłaty. Opłaty te muszą być proporcjonalne i obiektywne oraz muszą opierać się na kosztach administracyjnych związanych z monitorowaniem zgodności i innymi działaniami związanymi z kontrolą rynku prowadzonymi przez właściwe organy w związku ze zgłoszeniami dotyczącymi usług udostępniania danych.

11) W przypadku gdy dostawca usług udostępniania danych zaprzestaje swojej działalności, zgłasza ten fakt w ciągu 15 dni odpowiedniemu właściwemu organowi określonemu zgodnie z ust. 1, 2 i 3. Właściwy organ niezwłocznie przekazuje każde takie zgłoszenie właściwym organom krajowym w państwach członkowskich oraz Komisji drogą elektroniczną.

Artykuł 11
Warunki świadczenia usług udostępniania danych

Świadczenie usług udostępniania danych, o których mowa w art. 9 ust. 1, podlega następującym warunkom:

1) Dostawca usług nie może wykorzystywać danych, w odniesieniu do których świadczy usługi, do celów innych niż oddanie ich do dyspozycji użytkownikom danych, a usługi udostępniania danych powierza się odrębnemu podmiotowi prawnemu.

2) Metadane zebrane w ramach świadczenia usługi udostępniania danych mogą być wykorzystane wyłącznie do celów rozwoju tej usługi.

3) Dostawca usług zapewnia, aby procedura dostępu do usługi była sprawiedliwa, przejrzysta i niedyskryminująca zarówno dla posiadaczy danych, jak i użytkowników danych, w tym w odniesieniu do cen.

4) Dostawca usług ułatwia wymianę danych w formacie, w jakim otrzymuje je od posiadacza danych, i konwertuje te dane do określonych formatów wyłącznie w celu zwiększenia interoperacyjności w ramach sektorów i między sektorami lub na wniosek użytkownika danych bądź w przypadku, gdy jest to wymagane przez prawo Unii, lub w celu zapewnienia harmonizacji z międzynarodowymi lub europejskimi normami dotyczącymi danych.

5) Dostawca usług wprowadza procedury mające na celu zapobieganie praktykom stanowiącym oszustwo lub nadużycie w odniesieniu do dostępu do danych ze strony podmiotów ubiegających się o dostęp za pośrednictwem usług tego dostawcy.

6) Dostawca usług zapewnia odpowiednią ciągłość świadczenia swoich usług oraz, w przypadku usług, które zapewniają przechowywanie danych, wprowadza odpowiednie gwarancje umożliwiające posiadaczom danych i użytkownikom danych uzyskanie dostępu do ich danych w przypadku niewypłacalności dostawcy.

7) Dostawca usług wprowadza odpowiednie środki techniczne, prawne i organizacyjne w celu zapobiegania niezgodnemu z prawem Unii przekazywaniu danych nieosobowych lub dostępowi do tych danych.

8) Dostawca usług podejmuje środki w celu zapewnienia wysokiego poziomu bezpieczeństwa w zakresie przechowywania i przekazywania danych nieosobowych.

9) Dostawca usług wprowadza procedury zapewniające zgodność z unijnymi i krajowymi przepisami dotyczącymi konkurencji.

10) Dostawca usług oferujący usługi osobom, których dane dotyczą, działa w najlepszym interesie osób, których dane dotyczą, ułatwiając im wykonywanie ich praw, w szczególności doradzając im w zakresie potencjalnego wykorzystania danych i standardowych warunków związanych z takim wykorzystaniem.

11) W przypadku gdy dostawca danych zapewnia narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub zezwoleń na przetwarzanie danych udostępnionych przez osoby prawne, określa on jurysdykcję lub jurysdykcje, w których ma nastąpić wykorzystanie danych.

Artykuł 12
Właściwe organy

1) Każde państwo członkowskie wyznacza na swoim terytorium co najmniej jeden organ właściwy do wykonywania zadań związanych z ramami dotyczącymi zgłaszania i przekazuje Komisji dane identyfikacyjne tych wyznaczonych organów do dnia [data rozpoczęcia stosowania niniejszego rozporządzenia]. Powiadamia również Komisję o wszelkich późniejszych zmianach.

2) Wyznaczone właściwe organy spełniają wymogi art. 23.

3) Wyznaczone właściwe organy, organy ochrony danych, krajowe organy ochrony konkurencji, organy odpowiedzialne za cyberbezpieczeństwo oraz inne odpowiednie organy sektorowe wymieniają się informacjami, które są niezbędne do wykonywania ich zadań w odniesieniu do dostawców usług udostępniania danych.

Artykuł 13
Monitorowanie przestrzegania przepisów

1) Właściwy organ monitoruje i nadzoruje przestrzeganie przepisów niniejszego rozdziału.

2) Właściwy organ jest uprawniony do żądania od dostawców usług udostępniania danych wszelkich informacji, które są niezbędne do zweryfikowania zgodności z wymogami określonymi w art. 10 i 11. Każdy wniosek o informacje musi być proporcjonalny do wykonywanego zadania i musi być uzasadniony.

3) W przypadku ustalenia przez właściwy organ, że dostawca usług udostępniania danych nie spełnia co najmniej jednego wymogu określonego w art. 10 lub 11, właściwy organ powiadamia tego dostawcę o swoich ustaleniach i daje mu możliwość przedstawienia jego opinii w rozsądnym terminie.

4) Właściwy organ uprawniony jest do żądania zaprzestania naruszeń, o których mowa w ust. 3, niezwłocznie albo w rozsądnym terminie, a także przyjmuje odpowiednie i proporcjonalne środki służące zapewnieniu przestrzegania przepisów. W związku z tym właściwe organy mogą, w stosownych przypadkach:

   a) nakładać odstraszające kary pieniężne, które mogą obejmować kary okresowe z mocą wsteczną;

   b) zażądać zaprzestania lub odroczenia świadczenia usługi udostępniania danych.

5) Właściwe organy niezwłocznie informują zainteresowany podmiot o środkach nałożonych zgodnie z ust. 4 oraz o powodach ich nałożenia i wyznaczają mu rozsądny termin na ich zastosowanie.

6) Jeżeli dostawca usług udostępniania danych ma swoją główną jednostkę organizacyjną lub swojego przedstawiciela prawnego w państwie członkowskim, ale świadczy usługi w innych państwach członkowskich, właściwe organy państwa członkowskiego, w którym znajdują się główna jednostka organizacyjna lub przedstawiciel prawny, oraz właściwe organy innych państw członkowskich, w których dostawca świadczy usługi, współpracują i udzielają sobie wzajemnej pomocy. Taka pomoc i współpraca mogą obejmować wymianę informacji między zainteresowanymi właściwymi organami oraz wnioski o wprowadzenie środków, o których mowa w niniejszym artykule.

Artykuł 14
Wyjątki

Niniejszy rozdział nie ma zastosowania do podmiotów o charakterze niekomercyjnym, których działalność polega wyłącznie na gromadzeniu danych do celów leżących w interesie ogólnym, udostępnianych przez osoby fizyczne lub prawne na podstawie altruistycznego podejścia do danych.

ROZDZIAŁ IV
ALTRUISTYCZNE PODEJŚCIE DO DANYCH

Artykuł 15
Rejestr uznanych organizacji o altruistycznym podejściu do danych

1) Każdy właściwy organ wyznaczony zgodnie z art. 20 prowadzi rejestr uznanych organizacji o altruistycznym podejściu do danych.

2) Komisja prowadzi unijny rejestr uznanych organizacji o altruistycznym podejściu do danych.

3) Podmiot zarejestrowany w rejestrze zgodnie z art. 16 może w swoich pisemnych i ustnych komunikatach określać się mianem „uznanej w Unii organizacji o altruistycznym podejściu do danych”.

Artykuł 16
Wymogi ogólne dotyczące rejestracji

Aby kwalifikować się do rejestracji, organizacja o altruistycznym podejściu do danych musi:

a) być podmiotem prawnym utworzonym z zamiarem realizacji celów interesu ogólnego;

b) prowadzić działalność o charakterze niekomercyjnym i być niezależna od jakiegokolwiek podmiotu nastawionego na zysk;

c) wykonywać czynności związane z altruistycznym podejściem do danych poprzez prawnie niezależną strukturę, odrębną od innych czynności, które podejmuje.

Artykuł 17
Rejestracja

1) Każdy podmiot, który spełnia wymagania art. 16, może wystąpić z wnioskiem o wpis do rejestru uznanych organizacji o altruistycznym podejściu do danych, o którym mowa w art. 15 ust. 1.

2) Do celów niniejszego rozporządzenia podmiot prowadzący działalność w oparciu o altruistyczne podejście do danych posiadający jednostki organizacyjne w co najmniej dwóch państwach członkowskich dokonuje rejestracji w państwie członkowskim, w którym ma swoją główną jednostkę organizacyjną.

3) Podmiot, który nie ma jednostki organizacyjnej w Unii, ale spełnia wymogi określone w art. 16, wyznacza przedstawiciela prawnego w jednym z państw członkowskich, w których zamierza gromadzić dane w oparciu o altruistyczne podejście do danych. W celu spełnienia wymogów niniejszego rozporządzenia podmiot ten uważa się za podlegający jurysdykcji państwa członkowskiego, w którym znajduje się jego przedstawiciel prawny.

4) Wnioski o rejestrację zawierają następujące informacje:

a) nazwę podmiotu;

b) status prawny, formę prawną i numer rejestracyjny podmiotu, jeżeli dany podmiot jest zarejestrowany w rejestrze publicznym;

c) statut podmiotu, stosownie do przypadku;

d) główne źródła dochodu podmiotu;

e) adres głównej jednostki organizacyjnej podmiotu w Unii, jeżeli ma to zastosowanie, oraz drugorzędnego oddziału w innym państwie członkowskim, o ile takowy istnieje, lub adres przedstawiciela prawnego wyznaczonego zgodnie z ust. 3;

f) stronę internetową, na której można znaleźć informacje o podmiocie i jego działalności;

g) wskazanie osób wyznaczonych do kontaktu przez podmiot i dane kontaktowe;

h) cele interesu ogólnego, które podmiot zamierza wspierać przy gromadzeniu danych;

i) wszelkie inne dokumenty, które wykazują, że wymagania art. 16 są spełnione.

5) W przypadku przedłożenia przez podmiot wszystkich niezbędnych informacji zgodnie z ust. 4, jeśli właściwy organ uzna, że podmiot ten spełnia wymogi art. 16, rejestruje podmiot w rejestrze uznanych organizacji o altruistycznym podejściu do danych w ciągu dwunastu tygodni od daty złożenia wniosku. Rejestracja jest ważna we wszystkich państwach członkowskich. Informacje o każdej rejestracji przekazuje się Komisji w celu włączenia danego podmiotu do unijnego rejestru uznanych organizacji o altruistycznym podejściu do danych.

6) Informacje, o których mowa w ust. 4 lit. a), b), f), g) i h), są publikowane w krajowym rejestrze uznanych organizacji o altruistycznym podejściu do danych.

7) Każdy podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych zgłasza właściwym organom wszelkie zmiany informacji przekazanych zgodnie z ust. 4 w ciągu 14 dni kalendarzowych od dnia, w którym nastąpiła zmiana.

Artykuł 18
Wymagania dotyczące przejrzystości

1) Każdy podmiot wpisany do krajowego rejestru uznanych organizacji o altruistycznym podejściu do danych prowadzi pełną i dokładną dokumentację dotyczącą:

a) wszystkich osób fizycznych lub prawnych, które otrzymały możliwość przetwarzania danych będących w posiadaniu tego podmiotu;

b) daty lub czasu trwania takiego przetwarzania;

c) celu takiego przetwarzania zadeklarowanego przez osobę fizyczną lub prawną, która otrzymała możliwość przetwarzania;

d) ewentualnych opłat wniesionych przez osoby fizyczne lub prawne przetwarzające dane.

2) Każdy podmiot wpisany do krajowego rejestru uznanych organizacji o altruistycznym podejściu do danych sporządza i przekazuje właściwym organom krajowym roczne sprawozdanie z działalności, które zawiera co najmniej następujące informacje:

a) informacje o działalności podmiotu;

b) opis sposobu, w jaki w ciągu danego roku obrotowego wspierano cele interesu ogólnego, do których dane były gromadzone;

c) wykaz wszystkich osób fizycznych i prawnych, którym zezwolono na korzystanie z posiadanych danych, w tym skrócony opis celów interesu ogólnego, którym służy takie korzystanie z danych, oraz opis zastosowanych do tego celu środków technicznych, wraz z opisem technik stosowanych w celu zachowania prywatności i ochrony danych;

d) w stosownych przypadkach podsumowanie wyników wykorzystywania danych dozwolonego przez dany podmiot;

e) informacje o źródłach dochodów podmiotu, w szczególności o wszystkich dochodach wynikających z udzielania dostępu do danych, oraz o wydatkach.

Artykuł 19

Szczególne wymogi dotyczące ochrony praw i interesów osób, których dane dotyczą, oraz podmiotów prawnych w odniesieniu do ich danych

1) Każdy podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych informuje posiadaczy danych:

a) o celach interesu ogólnego, do których zezwala na przetwarzanie ich danych przez użytkowników danych, w sposób łatwy do zrozumienia;

b) o każdym przetwarzaniu poza Unią.

2) Podmiot zapewnia również, aby dane nie były wykorzystywane do celów innych niż cele leżące w interesie ogólnym, w odniesieniu do których zezwala na przetwarzanie.

3) W przypadku gdy podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych zapewnia narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub zezwoleń na przetwarzanie danych udostępnionych przez osoby prawne, określa jurysdykcję lub jurysdykcje, w których ma nastąpić wykorzystanie danych.

Artykuł 20

Właściwe organy odpowiedzialne za rejestrację

1) Każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za prowadzenie rejestru uznanych organizacji o altruistycznym podejściu do danych oraz za monitorowanie zgodności z wymogami niniejszego rozdziału. Wyznaczone właściwe organy spełniają wymogi określone w art. 23.

2) Każde państwo członkowskie przekazuje Komisji dane identyfikacyjne wyznaczonych organów.

3) Właściwy organ wykonuje swoje zadania we współpracy z organem ochrony danych, jeżeli zadania te związane są z przetwarzaniem danych osobowych, oraz z odpowiednimi organami sektorowymi tego samego państwa członkowskiego.

W przypadku wszelkich kwestii wymagających oceny zgodności z rozporządzeniem (UE) 2016/679 właściwy organ w pierwszej kolejności zwraca się o opinię lub decyzję do właściwego organu nadzoru ustanowionego na mocy tego rozporządzenia i stosuje się do tej opinii lub decyzji.

Artykuł 21
Monitorowanie przestrzegania przepisów

1) Właściwy organ monitoruje i nadzoruje spełnianie przez podmioty wpisane do rejestru uznanych organizacji o altruistycznym podejściu do danych warunków określonych w niniejszym rozdziale.

2) Właściwy organ jest uprawniony do żądania od podmiotów wpisanych do rejestru uznanych organizacji o altruistycznym podejściu do danych informacji niezbędnych do zweryfikowania zgodności z przepisami zawartymi w niniejszym rozdziale. Każdy wniosek o informacje musi być proporcjonalny do wykonywanego zadania i musi być uzasadniony.

3) W przypadku ustalenia przez właściwy organ, że dany podmiot nie spełnia co najmniej jednego wymogu określonego w niniejszym rozdziale, właściwy organ powiadamia ten podmiot o swoich ustaleniach i daje mu możliwość przedstawienia jego opinii w rozsądnym terminie.

4) Właściwy organ uprawniony jest do żądania zaprzestania naruszeń, o których mowa w ust. 3, niezwłocznie albo w rozsądnym terminie, a także przyjmuje odpowiednie i proporcjonalne środki służące zapewnieniu przestrzegania przepisów.

5) Jeżeli podmiot nie spełnia co najmniej jednego wymogu niniejszego rozdziału, nawet po otrzymaniu od właściwego organu powiadomienia zgodnie z ust. 3, podmiot ten:

   a) traci prawo do określania się w swoich pisemnych i ustnych komunikatach mianem „uznanej w Unii organizacji o altruistycznym podejściu do danych”;

   b) zostaje usunięty z rejestru uznanych organizacji o altruistycznym podejściu do danych.

6) Jeżeli podmiot wpisany w rejestrze uznanych organizacji o altruistycznym podejściu do danych ma swoją główną jednostkę organizacyjną lub swojego przedstawiciela prawnego w państwie członkowskim, ale prowadzi działalność w innych państwach członkowskich, właściwe organy państwa członkowskiego, w którym znajdują się główna jednostka organizacyjna lub przedstawiciel prawny, oraz właściwe organy innych państw członkowskich, w których podmiot prowadzi działalność, współpracują i udzielają sobie wzajemnej pomocy w razie konieczności. Taka pomoc i współpraca mogą obejmować wymianę informacji między zainteresowanymi właściwymi organami oraz wnioski o wprowadzenie środków nadzorczych, o których mowa w niniejszym artykule.

Artykuł 22
Europejski formularz zgody na potrzeby altruistycznego podejścia do danych

1) Aby ułatwić gromadzenie danych w oparciu o altruistyczne podejście do danych, Komisja może przyjąć akty wykonawcze w celu opracowania europejskiego formularza zgody na potrzeby altruistycznego podejścia do danych. Formularz umożliwia uzyskiwanie zgody we wszystkich państwach członkowskich

w jednolitym formacie. Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 29 ust. 2.

2) W europejskim formularzu zgody na potrzeby altruistycznego podejścia do danych stosuje się podejście modułowe umożliwiające dostosowanie do potrzeb konkretnych sektorów i poszczególnych celów.

3) W przypadku dostarczania danych osobowych europejski formularz zgody na potrzeby altruistycznego podejścia do danych zapewnia osobom, których dane dotyczą, możliwość udzielenia i wycofania zgody na konkretną operację przetwarzania danych zgodnie z wymogami rozporządzenia (UE) 2016/679.

4) Formularz musi być udostępniony w sposób umożliwiający jego wydrukowanie na papierze i odczytanie przez człowieka, jak również w formie elektronicznej, nadającej się do odczytu maszynowego.

ROZDZIAŁ V
WŁAŚCIWE ORGANY I PRZEPISY PROCEDURALNE

Artykuł 23
Wymogi odnoszące się do właściwych organów

1) Właściwe organy wyznaczone zgodnie z art. 12 i 20 muszą być prawnie odrębne i funkcjonalnie niezależne od jakiegokolwiek dostawcy usług udostępniania danych lub podmiotu wpisanego do rejestru uznanych organizacji o altruistycznym podejściu do danych.

2) Właściwe organy wykonują swoje zadania w sposób bezstronny, przejrzysty, spójny, wiarygodny i terminowy.

3) Członkowie kadry kierowniczej wyższego szczebla i personelu odpowiedzialnego za wykonywanie odpowiednich zadań właściwego organu przewidzianych w niniejszym rozporządzeniu nie mogą być projektantami, producentami, dostawcami, instalatorami, nabywcami, właścicielami, użytkownikami ani osobami odpowiedzialnymi za utrzymanie usług, które oceniają, nie mogą też być upoważnionymi przedstawicielami żadnej z tych osób ani ich reprezentować. Nie wyklucza to korzystania z ocenianych usług, które są niezbędne do wykonywania działań właściwego organu, lub korzystania z takich usług do celów osobistych.

4) Członkowie kadry kierowniczej wyższego szczebla i personelu nie angażują się w żadną działalność, która mogłaby zagrozić niezależności ich osądów lub uczciwości w odniesieniu do powierzonych im działań związanych z oceną.

5) Właściwe organy mają do dyspozycji odpowiednie zasoby finansowe i ludzkie, w tym wiedzę techniczną i środki finansowe niezbędne do realizacji powierzonych im zadań.

6) Właściwe organy państwa członkowskiego dostarczają Komisji i właściwym organom innych państw członkowskich, na uzasadniony wniosek, informacje niezbędne do wykonywania ich zadań na mocy niniejszego rozporządzenia. W przypadku gdy właściwy organ krajowy uzna informacje, o które złożono wniosek, za poufne zgodnie z przepisami unijnymi i krajowymi dotyczącymi tajemnicy handlowej i zawodowej, Komisja i wszelkie inne zainteresowane właściwe organy zapewniają poufność takich informacji.

Artykuł 24
Prawo do wniesienia skargi

1) Osoby fizyczne i prawne mają prawo do wniesienia skargi do odpowiedniego właściwego organu krajowego przeciwko dostawcy usług udostępniania danych lub podmiotowi wpisanemu do rejestru uznanych organizacji o altruistycznym podejściu do danych.

2) Organ, do którego wniesiono skargę, informuje skarżącego o przebiegu postępowania i podjętej decyzji, a także informuje skarżącego o prawie do skutecznego środka zaskarżenia przewidzianego w art. 25.

Artykuł 25
Prawo do skutecznego środka zaskarżenia

1) Niezależnie od wszelkich administracyjnych lub innych pozasądowych środków odwoławczych wszystkie pokrzywdzone osoby fizyczne i prawne mają prawo do skutecznego środka zaskarżenia w odniesieniu do:

   a) niepodjęcia działań w sprawie skargi złożonej do właściwego organu, o którym mowa w art. 12 i 20;

   b) decyzji właściwych organów, o których mowa w art. 13, 17 i 21, podjętych w ramach zarządzania systemem zgłaszania dostawców usług udostępniania danych, kontrolowania tego systemu i egzekwowania go, a także w ramach monitorowania podmiotów wpisanych do rejestru uznanych organizacji o altruistycznym podejściu do danych.

2) Postępowania na podstawie niniejszego artykułu toczą się przed sądami państwa członkowskiego, w którym znajduje się organ, przeciwko któremu zastosowano środek zaskarżenia.

ROZDZIAŁ VI
EUROPEJSKA RADA DS. INNOWACJI W ZAKRESIE DANYCH

Artykuł 26
Europejska Rada ds. Innowacji w zakresie Danych

1) Komisja ustanawia Europejską Radę ds. Innowacji w zakresie Danych („Rada”) w formie grupy ekspertów, w skład której wchodzą przedstawiciele właściwych organów wszystkich państw członkowskich, Europejskiej Rady Ochrony Danych, Komisji, odpowiednich przestrzeni danych oraz inni przedstawiciele właściwych organów w poszczególnych sektorach.

2) Zainteresowane strony i odpowiednie osoby trzecie mogą być zapraszane do udziału w posiedzeniach i pracach Rady.

3) Zebraniom Rady przewodniczy Komisja.

4) Rada jest wspierana przez sekretariat zapewniony przez Komisję.

Artykuł 27
Zadania Rady

Rada ma następujące zadania:

a) doradzanie i wspieranie Komisji w rozwijaniu spójnej praktyki organów sektora publicznego i właściwych podmiotów, o których mowa w art. 7 ust. 1, rozpatrujących wnioski o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1;

b) doradzanie i wspieranie Komisji w rozwijaniu spójnej praktyki właściwych organów w zakresie stosowania wymogów mających zastosowanie do dostawców usług udostępniania danych;

c) doradzanie Komisji w zakresie ustalania priorytetów dotyczących norm międzysektorowych, które mają być stosowane i opracowywane do celów wykorzystywania danych i międzysektorowego udostępniania danych, międzysektorowego porównywania i wymiany najlepszych praktyk w odniesieniu do wymogów sektorowych w zakresie bezpieczeństwa i procedur dostępu, przy jednoczesnym uwzględnieniu specyficznych dla danego sektora działań normalizacyjnych;

d) wspieranie Komisji w zwiększaniu interoperacyjności danych, jak również usług udostępniania danych między różnymi sektorami i w różnych dziedzinach, w oparciu o istniejące normy europejskie, międzynarodowe lub krajowe;

e) ułatwianie współpracy między właściwymi organami krajowymi na podstawie niniejszego rozporządzenia poprzez budowanie zdolności i wymianę informacji, w szczególności poprzez ustanowienie metod skutecznej wymiany informacji dotyczących procedury zgłaszania dostawców usług udostępniania danych oraz rejestracji i monitorowania uznanych organizacji o altruistycznym podejściu do danych.

ROZDZIAŁ VII
KOMITET I PRZEKAZANIE UPRAWNIEŃ

Artykuł 28
Wykonywanie przekazanych uprawnień

1) Powierzenie Komisji uprawnień do przyjęcia aktów delegowanych podlega warunkom określonym w niniejszym artykule.

2) Uprawnienia do przyjęcia aktów delegowanych, o których mowa w art. 5 ust. 11, powierza się Komisji na czas nieokreślony od dnia […].

3) Przekazanie uprawnień, o którym mowa w art. 5 ust. 11, może zostać w dowolnym momencie odwołane przez Parlament Europejski lub przez Radę. Decyzja o odwołaniu kończy przekazanie określonych w niej uprawnień. Decyzja o odwołaniu staje się skuteczna od następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej* lub w określonym w tej decyzji późniejszym terminie. Nie wpływa ona na ważność jakichkolwiek już obowiązujących aktów delegowanych.

4) Przed przyjęciem aktu delegowanego Komisja konsultuje się z ekspertami wyznaczonymi przez każde państwo członkowskie zgodnie z zasadami określonymi

w Porozumieniu międzyinstytucjonalnym w sprawie lepszego stanowienia prawa z dnia 13 kwietnia 2016 r.

5) Niezwłocznie po przyjęciu aktu delegowanego Komisja przekazuje go równocześnie Parlamentowi Europejskiemu i Radzie.

6) Akt delegowany przyjęty na podstawie art. 5 ust. 11 wchodzi w życie tylko wówczas, gdy ani Parlament Europejski, ani Rada nie wyraziły sprzeciwu w terminie trzech miesięcy od przekazania tego aktu Parlamentowi Europejskiemu i Radzie, lub gdy, przed upływem tego terminu, zarówno Parlament Europejski, jak i Rada poinformowały Komisję, że nie wniosą sprzeciwu. Termin ten przedłuża się o trzy miesiące z inicjatywy Parlamentu Europejskiego lub Rady.

Artykuł 29
Procedura komitetowa

1) Komisję wspomaga komitet w rozumieniu rozporządzenia (UE) nr 182/2011.

2) W przypadku odesłania do niniejszego ustępu stosuje się art. 4 rozporządzenia (UE) nr 182/2011.

3) W przypadku gdy opinia komitetu ma zostać uzyskana w drodze procedury pisemnej, procedura ta kończy się bez osiągnięcia rezultatu, gdy – przed upływem terminu na wydanie opinii – zdecyduje o tym przewodniczący komitetu lub wniesie o to członek komitetu. W takim przypadku przewodniczący w rozsądnym terminie zwołuje posiedzenie komitetu.

ROZDZIAŁ VIII
POSTANOWIENIA KOŃCOWE

Artykuł 30
Dostęp międzynarodowy

1) Organ sektora publicznego, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału 2, dostawca usług udostępniania danych lub podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych, w zależności od przypadku, wprowadzają wszelkie uzasadnione środki techniczne, prawne i organizacyjne w celu zapobiegania przekazywaniu danych nieosobowych przechowywanych w Unii lub dostępowi do takich danych, w przypadku gdy takie przekazywanie lub dostęp są sprzeczne z prawem Unii lub prawem odpowiedniego państwa członkowskiego, chyba że takie przekazywanie lub dostęp są zgodne z ust. 2 lub 3.

2) Wyrok sądu lub trybunału oraz decyzja organu administracyjnego państwa trzeciego wymagające od organu sektora publicznego, osoby fizycznej lub prawnej, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału 2, dostawcy usług udostępniania danych lub podmiotu wpisanego do rejestru uznanych organizacji o altruistycznym podejściu do danych przekazania danych nieosobowych podlegających niniejszemu rozporządzeniu lub udzielenia dostępu do tych danych w Unii mogą zostać uznane lub być egzekwowalne wyłącznie, gdy opierają się na umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, obowiązującej między wzywającym państwem trzecim a Unią lub na wszelkiej takiej umowie między wzywającym państwem trzecim a państwem członkowskim zawartej przed dniem [data wejścia w życie niniejszego rozporządzenia].

3) W przypadku gdy organ sektora publicznego, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału 2, dostawca usług udostępniania danych lub podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych jest adresatem decyzji sądu lub organu administracyjnego państwa trzeciego wymagającej przekazania danych nieosobowych przechowywanych w Unii lub udzielenia dostępu do takich danych, a zastosowanie się do takiej decyzji wiązałoby się z ryzykiem narażenia adresata na konflikt z prawem Unii lub z prawem danego państwa członkowskiego, przekazanie takich danych lub udzielenie dostępu do takich danych przez ten organ państwa trzeciego odbywa się wyłącznie w przypadku gdy:

   a) system państwa trzeciego wymaga określenia powodów i proporcjonalności decyzji oraz wymaga, aby orzeczenie sądu lub decyzja, w zależności od przypadku, miały szczególny charakter, na przykład poprzez ustanowienie odpowiedniego powiązania z niektórymi podejrzanymi lub naruszeniami;

   b) uzasadniony sprzeciw adresata podlega kontroli właściwego sądu w państwie trzecim; oraz

   c) w tym kontekście właściwy sąd wydający orzeczenie lub dokonujący kontroli decyzji organu administracyjnego jest upoważniony na mocy prawa tego państwa do należytego uwzględnienia odpowiednich interesów prawnych dostawcy danych chronionych prawem Unii lub mającym zastosowanie prawem państwa członkowskiego.

Adresat decyzji zwraca się o opinię do odpowiednich właściwych podmiotów lub organów, zgodnie z niniejszym rozporządzeniem, w celu ustalenia, czy warunki te zostały spełnione.

4) Jeżeli spełnione są warunki określone w ust. 2 lub 3, organ sektora publicznego, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału 2, dostawca usług udostępniania danych lub podmiot wpisany do rejestru uznanych organizacji o altruistycznym podejściu do danych, w zależności od przypadku, dostarcza minimalną ilość danych dozwoloną w odpowiedzi na wniosek, w oparciu o właściwą interpretację wniosku.

5) Organ sektora publicznego, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału 2, dostawca usług udostępniania danych oraz podmiot o altruistycznym podejściu do danych informują posiadacza danych o istnieniu wniosku organu administracyjnego w państwie trzecim o dostęp do jego danych, z wyjątkiem przypadków, w których wniosek służy celom egzekwowania prawa i tak długo, jak jest to konieczne do zachowania skuteczności działań w zakresie egzekwowania prawa.

Artykuł 31
Kary

Państwa członkowskie przyjmują przepisy dotyczące kar mających zastosowanie w przypadku naruszeń niniejszego rozporządzenia i podejmują wszelkie działania niezbędne do zapewnienia ich wdrożenia. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia [data rozpoczęcia stosowania rozporządzenia] oraz niezwłocznie informują Komisję o wszelkich późniejszych zmianach ich dotyczących.

Artykuł 32
Ocena i przegląd

Do dnia [*cztery lata od daty rozpoczęcia stosowania niniejszego rozporządzenia*] Komisja przeprowadza ocenę niniejszego rozporządzenia i przedkłada Parlamentowi Europejskiemu i Radzie, a także Europejskiemu Komitetowi Ekonomiczno-Społecznemu sprawozdanie na temat głównych ustaleń. Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania tego sprawozdania.

Artykuł 33
Zmiana rozporządzenia (UE) 2018/1724

W załączniku II do rozporządzenia (UE) 2018/1724 dodaje się następujący wiersz w pozycji „Rozpoczęcie, prowadzenie i zakończenie działalności gospodarczej”:

Rozpoczęcie, prowadzenie i zakończenie działalności gospodarczej	Zgłoszenie jako dostawca usług udostępniania danych	Potwierdzenie przyjęcia zgłoszenia
	Rejestracja jako europejska organizacja o altruistycznym podejściu do danych	Potwierdzenie rejestracji

Artykuł 34
Przepisy przejściowe

Podmioty świadczące usługi udostępniania danych przewidziane w art. 9 ust. 1 w dniu wejścia w życie niniejszego rozporządzenia spełniają obowiązki określone w rozdziale III najpóźniej do dnia [data – 2 lata od daty rozpoczęcia stosowania rozporządzenia].

Artykuł 35
Wejście w życie i stosowanie

Niniejsze rozporządzenie wchodzi w życie dwudziestego dnia po jego opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Rozporządzenie stosuje się od dnia [12 miesięcy po wejściu w życie niniejszego rozporządzenia].

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Brukseli dnia […] r.

W imieniu Parlamentu Europejskiego
Przewodniczący

W imieniu Rady
Przewodniczący