I

(Akty ustawodawcze)

ROZPORZĄDZENIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2022/868

z dnia 30 maja 2022 r.

w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (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 ([1]),

po konsultacji z Komitetem Regionów,

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą ([2]),

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, przy pełnym poszanowaniu praw podstawowych. Powinno ono również gwarantować wzmocnienie otwartej strategicznej autonomii Unii przy jednoczesnym sprzyjaniu międzynarodowemu swobodnemu przepływowi danych.

(2) W ciągu ostatniej dekady technologie cyfrowe zmieniły gospodarkę i społeczeństwo, oddziałując na wszystkie sektory działalności i codzienne życie. W centrum tej transformacji znajdują się dane: innowacje wykorzystujące potencjał danych przyniosą ogromne korzyści zarówno obywatelom Unii, jak i gospodarce, na przykład poprzez udoskonalenie i personalizację medycyny, zapewnienie nowej mobilności oraz wniesienie wkładu w komunikat Komisji z 11 grudnia 2019 r. w sprawie Europejskiego Zielonego Ładu. Aby uczynić gospodarkę opartą o dane inkluzywną dla wszystkich obywateli Unii, szczególną uwagę zwrócić należy na zmniejszanie przepaści cyfrowej, zwiększanie udziału kobiet w gospodarce danych i wspieranie rozwijania najnowocześniejszej europejskiej wiedzy fachowej w sektorze technologii. Gospodarkę danych należy budować w sposób umożliwiający prosperowanie przedsiębiorstwom – w szczególności mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom (MŚP) zgodnie z definicją w załączniku do zalecenia Komisji 2003/361/WE ([3]), a także przedsiębiorstwom typu start-up – zapewniając neutralność dostępu do danych oraz możliwość przenoszenia danych i ich interoperacyjność oraz unikając efektów lock-in. W swoim komunikacie z 19 lutego 2020 r. w sprawie europejskiej strategii w zakresie danych (zwanym dalej „europejską strategią w sprawie danych") Komisja opisała wizję wspólnej europejskiej przestrzeni danych, oznaczającej rynek wewnętrzny danych, na którym dane mogłyby być wykorzystywane, zgodnie z obowiązującymi przepisami, bez względu na fizyczne miejsce ich przechowywania w Unii, która to wizja może mieć kluczowe znaczenie dla między innymi szybkiego rozwoju technologii sztucznej inteligencji.

([1]) Dz.U. C 286 z 16.7.2021, s. 38.

([2]) Stanowisko Parlamentu Europejskiego z dnia 6 kwietnia 2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z dnia 16 maja 2022 r.

([3]) Zalecenie Komisji 2003/361/WE z dnia 6 maja 2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36).

Komisja 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, zgodnie ze zobowiązaniami międzynarodowymi, w tym w zakresie praw podstawowych. Aby urzeczywistnić tę wizję, Komisja zaproponowała ustanowienie wspólnych europejskich przestrzeni danych w poszczególnych dziedzinach do celów dzielenia się danymi i ich konsolidacji. Jak zaproponowano w europejskiej strategii w zakresie danych, tego rodzaju wspólne europejskie przestrzenie danych mogą obejmować takie obszary, jak zdrowie, mobilność, produkcja, usługi finansowe, energia lub rolnictwo lub obejmować te obszary w sposób łączny, na przykład w zakresie energii i klimatu, jak również obszary tematyczne, takie jak Europejski Zielony Ład lub europejskie przestrzenie danych dla administracji publicznej lub umiejętności. Wspólne europejskie przestrzenie danych powinny czynić dane możliwymi do znalezienia, dostępnymi, interoperacyjnymi i nadającymi się do ponownego wykorzystania („zasady FAIR"), zapewniając jednocześnie wysoki poziom cyberbezpieczeństwa. Gdy w gospodarce danych istnieją równe warunki działania, przedsiębiorstwa konkurują ze sobą pod względem jakości usług, a nie ilości kontrolowanych przez siebie danych. Do celów projektowania, tworzenia i utrzymywania równych warunków działania w gospodarce danych potrzebne jest prawidłowe zarządzanie, w którym powinni uczestniczyć i być reprezentowani odpowiedni interesariusze wspólnej europejskiej przestrzeni danych.

(3) Konieczna jest poprawa warunków dzielenia się danymi na rynku wewnętrznym poprzez utworzenie zharmonizowanych ram wymiany danych i ustanowienie pewnych podstawowych wymogów w zakresie zarządzania danymi, przy zwróceniu szczególnej uwagi na ułatwianie współpracy między państwami członkowskimi. Celem niniejszego rozporządzenia powinno być dalsze rozwijanie wewnętrznego rynku cyfrowego wolnego od granic oraz opartego o dane społeczeństwa i opartej o dane gospodarki, ukierunkowanych na człowieka, godnych zaufania i bezpiecznych. W sektorowym prawie Unii można opracować, dostosować i zaproponować nowe i uzupełniające elementy, w zależności od specyfiki sektora, takie jak planowane przepisy prawa Unii dotyczące europejskiej przestrzeni danych dotyczących zdrowia lub dostępu do danych dotyczących pojazdów. Ponadto niektóre sektory gospodarki są już regulowane sektorowym prawem Unii, które obejmuje przepisy dotyczące transgranicznego lub ogólnounijnego dzielenia się danymi lub udzielania do nich dostępu, na przykład dyrektywą Parlamentu Europejskiego i Rady 2011/24/UE ([4]) – w kontekście europejskiej przestrzeni danych dotyczących zdrowia, czy stosownymi aktami ustawodawczymi w dziedzinie transportu, jak rozporządzeniami Parlamentu Europejskiego i Rady (UE) 2019/1239 ([5]) i (UE) 2020/1056 ([6]) oraz dyrektywą Parlamentu Europejskiego i Rady 2010/40/UE ([7]) – w kontekście europejskiej przestrzeni danych dotyczących mobilności.

([4]) Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.U. L 88 z 4.4.2011, s. 45).

([5]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1239 z dnia 20 czerwca 2019 r. ustanawiające europejski system morskich pojedynczych punktów kontaktowych i uchylające dyrektywę 2010/65/UE (Dz.U. L 198 z 25.7.2019, s. 64).

([6]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/1056 z dnia 15 lipca 2020 r. w sprawie elektronicznych informacji dotyczących transportu towarowego (Dz.U. L 249 z 31.7.2020, s. 33).

([7]) 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).

Niniejsze rozporządzenie powinno więc pozostawać bez uszczerbku dla rozporządzeń Parlamentu Europejskiego i Rady (WE) nr 223/2009 ([8]), (UE) 2018/858 ([9]) i (UE) 2018/1807 ([10]) oraz dla dyrektyw Parlamentu Europejskiego i Rady 2000/31/WE ([11]), 2001/29/WE ([12]), 2004/48/WE ([13]), 2007/2/WE ([14]), 2010/40/UE, (UE) 2015/849 ([15]), (UE) 2016/943 ([16]), (UE) 2017/1132 ([17]), (UE) 2019/790 ([18]) i (UE) 2019/1024 ([19]) oraz innego sektorowego prawa Unii regulującego dostęp do danych i ich ponowne wykorzystywanie. Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla prawa Unii i prawa krajowego dotyczącego dostępu do danych i ich wykorzystywania do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar, jak również dla współpracy międzynarodowej w tym zakresie.

Niniejsze rozporządzenie nie powinno naruszać kompetencji państw członkowskich w odniesieniu do ich działań z zakresu bezpieczeństwa publicznego, obrony i bezpieczeństwa narodowego. Niniejsze rozporządzenie nie powinno obejmować ponownego wykorzystywania chronionych z powyższych względów danych będących w posiadaniu podmiotów sektora publicznego, w tym danych pochodzących z procedur udzielania zamówień, które wchodzą w zakres stosowania dyrektywy Parlamentu Europejskiego i Rady 2009/81/WE ([20]). Należy ustanowić w Unii horyzontalny system ponownego wykorzystywania niektórych kategorii chronionych danych będących w posiadaniu podmiotów sektora publicznego oraz świadczenia usług pośrednictwa danych i usług w ramach altruizmu danych. Specyfika różnych sektorów może wymagać zaprojektowania sektorowych systemów opartych o dane z uwzględnieniem wymogów niniejszego rozporządzenia. Dostawcy usług pośrednictwa danych spełniający wymogi określone w niniejszym rozporządzeniu powinni mieć możliwość posługiwania się oznakowaniem „uznany w Unii dostawca usług pośrednictwa danych". Osoby prawne, które starają się wspierać realizację celów leżących w interesie ogólnym poprzez udostępnianie na dużą skalę odpowiednich danych w ramach altruizmu danych i które spełniają wymogi określone w niniejszym rozporządzeniu, powinny mieć możliwość zarejestrowania się jako „uznana w Unii organizacja altruizmu danych" i posługiwania się tym oznakowaniem. W przypadku gdy sektorowe prawo Unii lub sektorowe prawo krajowe wymaga od podmiotów sektora publicznego, takich dostawców usług pośrednictwa danych lub takich osób prawnych (uznanych organizacji altruizmu danych) spełnienia szczególnych dodatkowych wymogów technicznych, administracyjnych lub organizacyjnych, w tym poprzez system zezwoleń lub certyfikacji, należy stosować również przepisy tego sektorowego prawa Unii lub sektorowego prawa krajowego.

([8]) 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).

([9]) 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, s. 1).

([10]) 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).

([11]) 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).

([12]) 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).

([13]) 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, s. 45).

([14]) Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z dnia 14 marca 2007 r. ustanawiająca infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE) (Dz.U. L 108 z 25.4.2007, s. 1).

([15]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 20 maja 2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.U. L 141 z 5.6.2015, s. 73).

([16]) 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).

([17]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1132 z dnia 14 czerwca 2017 r. w sprawie niektórych aspektów prawa spółek (Dz.U. L 169 z 30.6.2017, s. 46).

([18]) 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).

([19]) 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).

([20]) Dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z dnia 13 lipca 2009 r. w sprawie koordynacji procedur udzielania niektórych zamówień na roboty budowlane, dostawy i usługi przez instytucje lub podmioty zamawiające w dziedzinach obronności i bezpieczeństwa i zmieniająca dyrektywy 2004/17/WE i 2004/18/WE (Dz.U. L 216 z 20.8.2009, s. 76).

(4) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla rozporządzeń Parlamentu Europejskiego i Rady (UE) 2016/679 ([21]) i (UE) 2018/1725 ([22]) oraz dyrektyw Parlamentu Europejskiego i Rady 2002/58/WE ([23]) i (UE) 2016/680 ([24]) oraz odpowiednich przepisów prawa krajowego, w tym w przypadku, gdy dane osobowe i nieosobowe w zbiorze danych są ze sobą nierozerwalnie powiązane. W szczególności niniejsze rozporządzenie nie powinno być rozumiane jako tworzące nową podstawę prawną dla przetwarzania danych osobowych w ramach regulowanych działań lub jako zmieniające wymogi informacyjne określone w rozporządzeniu (UE) 2016/679. Wykonanie niniejszego rozporządzenia nie powinno uniemożliwiać transgranicznego przekazywania danych zgodnie z rozdziałem V rozporządzenia (UE) 2016/679. W przypadku kolizji pomiędzy niniejszym rozporządzeniem a prawem Unii w dziedzinie ochrony danych osobowych lub prawem krajowym przyjętym zgodnie z takim prawem Unii pierwszeństwo ma odpowiednie prawo Unii lub prawo krajowe w dziedzinie ochrony danych osobowych. Należy zapewnić możliwość uznawania organów ochrony danych za właściwe organy do celów niniejszego rozporządzenia. W przypadku gdy inne organy działają jako właściwe organy do celów niniejszego rozporządzenia, powinny to robić to bez uszczerbku dla nadzorczych uprawnień i kompetencji organów ochrony danych na podstawie rozporządzenia (UE) 2016/679.

(5) Działanie na poziomie Unii jest konieczne w celu zwiększenia zaufania do dzielenia się danymi poprzez ustanowienie odpowiednich mechanizmów kontroli sprawowanej przez osoby, których dane dotyczą, i posiadaczy danych nad danymi, które ich dotyczą, oraz w celu usunięcia innych barier dla dobrze funkcjonującej i konkurencyjnej gospodarki opartej o dane. Działanie to powinno pozostawać bez uszczerbku dla obowiązków i zobowiązań ustanowionych w międzynarodowych umowach handlowych zawartych przez Unię. Ogólnounijne ramy zarządzania powinny mieć na celu budowanie zaufania osób fizycznych i przedsiębiorstw w zakresie dostępu do danych, ich kontroli, dzielenia się nimi, ich wykorzystywania i ponownego wykorzystywania, w szczególności poprzez ustanowienie odpowiednich mechanizmów umożliwiających osobom, których dane dotyczą, poznanie przysługujących im praw i ich skuteczne wykonywanie, a także w odniesieniu do ponownego wykorzystywania niektórych rodzajów danych będących w posiadaniu podmiotów sektora publicznego, świadczenia usług przez dostawców usług pośrednictwa danych na rzecz osób, których dane dotyczą, posiadaczy danych i użytkowników danych, jak również gromadzenia i przetwarzania danych udostępnianych z pobudek altruistycznych przez osoby fizyczne i prawne. Do zwiększenia zaufania przyczynić może się w szczególności większa przejrzystość w zakresie celu wykorzystywania danych i warunków ich przechowywania przez przedsiębiorstwa.

(6) Koncepcja, że dane wygenerowane lub zgromadzone przed podmioty sektora publicznego lub inne podmioty na koszt budżetów publicznych powinny przynosić korzyści społeczeństwu, od dawna była częścią polityki Unii. Dyrektywa (UE) 2019/1024 oraz sektorowe prawo Unii zapewniają, aby podmioty sektora publicznego umożliwiały łatwy dostęp do większej ilości wytworzonych przez siebie danych na potrzeby ich wykorzystywania oraz ponownego wykorzystywania. Niektóre kategorie danych, takie jak dane poufne ze względów handlowych, dane objęte poufnością informacji statystycznych i dane chronione prawami własności intelektualnej osób trzecich, w tym tajemnice przedsiębiorstwa i dane osobowe, znajdujące się w publicznych bazach danych często jednak nie są udostępniane, nawet na potrzeby działalności badawczej lub innowacyjnej prowadzonej w interesie publicznym, mimo że taka dostępność jest możliwa zgodnie z obowiązującym prawem Unii, w szczególności rozporządzeniem (UE) 2016/679 oraz dyrektywami 2002/58/WE i (UE) 2016/680. Ze względu na fakt, że dane takie są szczególnie chronione, przed ich udostępnieniem muszą zostać spełnione pewne techniczne i prawne wymogi proceduralne, przede wszystkim po to, aby zapewnić poszanowanie praw innych osób w odniesieniu do takich danych lub ograniczyć negatywny wpływ na prawa podstawowe, zasadę niedyskryminacji i ochronę danych. Spełnienie takich wymogów jest zazwyczaj czasochłonne i wymaga specjalistycznej wiedzy. Stąd też dane takie są wykorzystywane w niewystarczającym stopniu. Wprawdzie niektóre państwa członkowskie ustanawiają struktury, procesy lub prawo ułatwiające tego rodzaju ponowne wykorzystywanie danych, działania te nie są jednak podejmowane w całej Unii. Aby ułatwić podmiotom prywatnym i publicznym wykorzystywanie danych na potrzeby europejskich badań naukowych i innowacji, w całej Unii potrzebne są jasne warunki dostępu do takich danych i ich wykorzystywania.

([21]) 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).

([22]) 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).

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

([24]) 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).

(7) Istnieją techniki umożliwiające przeprowadzanie analiz baz danych zawierających dane osobowe, takie jak anonimizacja, prywatność różnicowa, uogólnienie, ukrywanie i randomizacja, wykorzystywanie danych syntetycznych lub podobne metody oraz inne najnowocześniejsze metody zachowania prywatności, które mogą przyczynić się do przetwarzania danych w sposób bardziej przyjazny dla ochrony prywatności. Państwa członkowskie powinny zapewniać wsparcie podmiotom sektora publicznego, aby optymalnie wykorzystywały one takie techniki, a tym samym dzieliły się jak największą ilością danych. Stosowanie takich technik wraz z kompleksowymi ocenami skutków dla ochrony danych i innymi zabezpieczeniami może przyczynić się do większego bezpieczeństwa wykorzystywania i ponownego wykorzystywania danych osobowych i powinno zapewniać bezpieczne ponowne wykorzystywanie poufnych ze względów handlowych danych biznesowych do celów badań naukowych i innowacji oraz do celów statystycznych. W wielu przypadkach stosowanie takich technik, ocen skutków i innych zabezpieczeń oznacza, że wykorzystywanie i ponowne wykorzystywanie danych może odbywać się wyłącznie w bezpiecznym środowisku przetwarzania zapewnionym lub nadzorowanym przez podmiot sektora publicznego. Na poziomie Unii zgromadzono doświadczenie w zakresie takich bezpiecznych środowisk przetwarzania, które są wykorzystywane do badań nad jednostkowymi danymi statystycznymi na podstawie rozporządzenia Komisji (UE) nr 557/2013 ([25]). Ogólnie rzecz biorąc, przetwarzanie danych w przypadku danych osobowych powinno opierać się na co najmniej jednej podstawie prawnej przetwarzania określonej w art. 6 i 9 rozporządzenia (UE) 2016/679.

(8) Zgodnie z rozporządzeniem (UE) 2016/679 zasady ochrony danych nie powinny mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Deanonimizacja osób, których danych dotyczą, na podstawie danych pochodzących ze zanonimizowanych zbiorów danych powinna być zabroniona. Powinno to pozostawać bez uszczerbku dla możliwości prowadzenia badań nad technikami anonimizacji, szczególnie do celów zapewniania bezpieczeństwa informacji, poprawy istniejących technik anonimizacji i przyczyniania się do ogólnej solidności anonimizacji, podejmowanych zgodnie z rozporządzeniem (UE) 2016/679.

(9) Aby ułatwić ochronę danych osobowych i danych poufnych oraz przyspieszyć proces udostępniania takich danych do ponownego wykorzystywania na podstawie niniejszego rozporządzenia, państwa członkowskie powinny zachęcać podmioty sektora publicznego do tworzenia i udostępniania danych zgodnie z zasadą „otwartości w fazie projektowania i otwartości domyślnej", o której mowa w art. 5 ust. 2 dyrektywy (UE) 2019/1024, oraz do promowania tworzenia i pozyskiwania danych w formatach i strukturach ułatwiających anonimizację w tym zakresie.

(10) Kategorie danych będących w posiadaniu podmiotów sektora publicznego, które powinny podlegać ponownemu wykorzystywaniu na podstawie niniejszego rozporządzenia, nie są objęte zakresem stosowania dyrektywy (UE) 2019/1024, z którego to zakresu wykluczone są dane niedostępne ze względu na poufność informacji handlowych i statystycznych oraz dane zawarte w utworach lub w innych treściach, do których prawa własności intelektualnej posiadają osoby trzecie. Dane poufne ze względów handlowych obejmują dane chronione tajemnicą przedsiębiorstwa, chronionym know-how oraz wszelkie inne informacje, których nienależyte ujawnienie miałoby wpływ na pozycję rynkową lub kondycję finansową przedsiębiorstwa. Niniejsze rozporządzenie powinno mieć zastosowanie do tych danych osobowych, które nie są objęte zakresem stosowania 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, powinno odbywać się bez uszczerbku dla dyrektywy (UE) 2016/943, która określa ramy zgodnego z prawem pozyskiwania, wykorzystywania lub ujawniania tajemnic przedsiębiorstwa.

(11) Niniejsze rozporządzenie nie powinno tworzyć obowiązku zezwalania na ponowne wykorzystywanie danych będących w posiadaniu podmiotów sektora publicznego. W szczególności każde państwo członkowskie powinno mieć możliwość decydowania, czy udostępnia dane do ponownego wykorzystywania, a także określania celów i zakresu takiego dostępu. Niniejsze rozporządzenie powinno uzupełniać i pozostawać bez uszczerbku dla bardziej szczególnych obowiązków podmiotów sektora publicznego w zakresie zezwalania na ponowne wykorzystywanie danych określonych w sektorowym prawie Unii lub sektorowym prawie krajowym. Publiczny dostęp do dokumentów urzędowych można uznawać za leżący w interesie publicznym. Uwzględniając rolę publicznego dostępu do dokumentów urzędowych oraz przejrzystości w społeczeństwie demokratycznym, niniejsze rozporządzenie powinno pozostawać również bez uszczerbku dla prawa Unii lub prawa krajowego dotyczącego udzielania dostępu do dokumentów urzędowych i ich ujawniania. Dostęp do dokumentów urzędowych może być w szczególności przyznany zgodnie z prawem krajowym bez nakładania szczególnych warunków lub poprzez nakładanie szczególnych warunków nieprzewidzianych w niniejszym rozporządzeniu.

([25]) 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).

(12) System ponownego wykorzystywania przewidziany w niniejszym rozporządzeniu powinien mieć zastosowanie do danych, których dostarczanie jest jednym z zadań publicznych zainteresowanych podmiotów 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, pod warunkiem że zakres zadań publicznych jest przejrzysty i poddawany przeglądowi. Zadania publiczne mogą być definiowane ogólnie lub indywidualnie dla poszczególnych podmiotów sektora publicznego. Przedsiębiorstwa publiczne nie są objęte definicją podmiotu sektora publicznego, zatem dane będące w posiadaniu przedsiębiorstw publicznych nie powinny być objęte niniejszym rozporządzeniem. Niniejsze rozporządzenie nie powinno obejmować danych będących w posiadaniu instytucji kulturalnych, takich jak biblioteki, archiwa i muzea oraz orkiestry, teatry operowe, zespoły baletowe czy teatry, i placówek edukacyjnych, ponieważ posiadane przez nie utwory i inne dokumenty są przeważnie objęte prawami własności intelektualnej osób trzecich. Organizacje prowadzące badania naukowe i organizacje finansujące badania naukowe także mogą być zorganizowane jako podmioty sektora publicznego lub podmioty prawa publicznego.

Niniejsze rozporządzenie powinno mieć zastosowanie do takich organizacji hybrydowych wyłącznie odnośnie do ich roli jako organizacji prowadzących badania naukowe. Jeśli organizacja prowadząca badania naukowe jest w posiadaniu danych w ramach konkretnego stowarzyszenia publiczno-prywatnego z organizacjami sektora prywatnego lub innymi podmiotami sektora publicznego, podmiotami prawa publicznego lub hybrydowymi organizacjami prowadzącymi badania naukowe, tj. zorganizowanymi jako podmioty prawa publicznego albo przedsiębiorstwa publiczne, którego głównym celem jest prowadzenie badań naukowych, dane te również nie powinny być objęte niniejszym rozporządzeniem. W stosownych przypadkach państwa członkowskie powinny mieć możliwość stosowania niniejszego rozporządzenia do przedsiębiorstw publicznych lub prywatnych, które wykonują obowiązki sektora publicznego lub świadczą usługi w interesie ogólnym. Wymiana danych, wyłącznie w ramach wykonywania zadań publicznych, między podmiotami sektora publicznego w Unii lub między podmiotami sektora publicznego w Unii a podmiotami sektora publicznego w państwach trzecich lub organizacjami międzynarodowymi, jak również wymiana danych między badaczami do niekomercyjnych celów badań naukowych, nie powinna podlegać przepisom niniejszego rozporządzenia dotyczącym ponownego wykorzystywania niektórych kategorii danych chronionych będących w posiadaniu podmiotów sektora publicznego.

(13) Podmioty sektora publicznego przy ustanawianiu zasad ponownego wykorzystywania posiadanych przez nie danych powinny przestrzegać prawa konkurencji, unikając 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 świadczenia usługi lub dostarczania produktu w interesie ogólnym. Może to mieć miejsce w przypadku, gdy wyłączne wykorzystywanie danych jest jedynym sposobem maksymalnego zwiększenia korzyści społecznych z przedmiotowych danych, na przykład gdy istnieje tylko jeden podmiot (wyspecjalizowany w przetwarzaniu określonego zbioru danych) zdolny do świadczenia usługi lub dostarczania produktu, które umożliwiają podmiotowi sektora publicznego świadczenie usługi lub dostarczanie produktu w interesie ogólnym. Takie uzgodnienia powinny być jednak dokonywane zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym oraz podlegać regularnym przeglądom opartym na analizie rynkowej, aby ustalić, czy taka wyłączność pozostaje konieczna. Ponadto takie uzgodnienia powinny być w stosownych przypadkach zgodne z odpowiednimi zasadami pomocy państwa i być dokonywane na czas określony, który nie powinien przekraczać 12 miesięcy. Aby zapewnić przejrzystość, takie umowy o wyłączności należy publikować w internecie w formie zgodnej z właściwym prawem Unii dotyczącym zamówień publicznych. Jeżeli wyłączne prawo do ponownego wykorzystywania danych nie jest zgodne z niniejszym rozporządzeniem, to wyłączne prawo powinno być nieważne.

(14) Zakazane umowy o wyłączności i inne praktyki lub uzgodnienia dotyczące ponownego wykorzystywania danych będących w posiadaniu podmiotów sektora publicznego, 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 były już stosowane przed dniem wejścia 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 30 miesięcy od dnia wejścia w życie niniejszego rozporządzenia.

(15) Niniejsze rozporządzenie powinno ustanawiać warunki ponownego wykorzystywania danych chronionych mające zastosowanie do podmiotów sektora publicznego wyznaczonych jako podmioty właściwe na podstawie prawa krajowego do udzielania lub odmowy udzielania dostępu do celów ponownego wykorzystywania, przy czym warunki te powinny pozostawać bez uszczerbku dla praw lub obowiązków dotyczących dostępu do takich danych. Warunki te powinny być niedyskryminujące, przejrzyste, proporcjonalne i obiektywnie uzasadnione, a jednocześnie nie powinny ograniczać konkurencji, ze szczególnym naciskiem na propagowanie dostępu do takich danych dla MŚP i przedsiębiorstw typu start-up. Warunki ponownego wykorzystywania powinny być opracowywane w sposób promujący badania naukowe, tak aby przykładowo uprzywilejowanie badań naukowych było co do zasady uznawane za niedyskryminujące. Podmioty sektora publicznego zezwalające na ponowne wykorzystywanie powinny dysponować środkami technicznymi niezbędnymi do zapewnienia ochrony praw i interesów osób trzecich oraz być uprawnione do żądania niezbędnych informacji od ponownego użytkownika. Warunki związane z ponownym wykorzystywaniem danych powinny być ograniczone do tego, co jest niezbędne do ochrony praw i interesów osób trzecich

w odniesieniu do danych oraz integralności systemów informacyjno-komunikacyjnych podmiotów sektora publicznego. Podmioty sektora publicznego powinny stosować warunki, które najlepiej służą interesom ponownego użytkownika, a jednocześnie nie powodują nieproporcjonalnie dużego obciążenia dla podmiotów sektora publicznego. Należy określić warunki ponownego wykorzystywania danych, aby zapewnić skuteczne zabezpieczenia w odniesieniu do ochrony danych osobowych. Przed przesłaniem danych osobowych należy je zanonimizować, aby uniemożliwić identyfikację osób, których dane dotyczą, a 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 ponownego użytkownika, można zezwolić na ponowne wykorzystywanie danych na miejscu lub zdalnie w bezpiecznym środowisku przetwarzania, z zastrzeżeniem spełnienia wymogów dotyczących dokonania oceny skutków dla ochrony danych i przeprowadzenia konsultacji z organem nadzorczym zgodnie z art. 35 i art. 36 rozporządzenia (UE) 2016/679, oraz gdy ryzyko dla praw i interesów osób, których dane dotyczą, uznano za minimalne.

Mogłoby to stanowić odpowiednie rozwiązanie w zakresie ponownego wykorzystywania danych spseudonimizowanych. Podmiot sektora publicznego powinien nadzorować analizy danych w takich bezpiecznych środowiskach przetwarzania, by chronić prawa i interesy osób trzecich. W szczególności dane osobowe powinny być przesyłane osobie trzeciej do ponownego wykorzystywania tylko w przypadku, gdy podstawa prawna określona w prawie dotyczącym ochrony danych zezwala na takie przesyłanie. Dane nieosobowe powinny być przesyłane tylko wtedy, gdy nie ma powodów, by sądzić, że połączenie zbiorów danych nieosobowych doprowadziłoby do identyfikacji osób, których dane dotyczą. Powinno to mieć również zastosowanie do danych spseudonimizowanych, które zachowują status danych osobowych. W przypadku deanonimizacji osób, których dane dotyczą, oprócz obowiązku zgłoszenia takiego naruszenia ochrony danych organowi nadzorczemu i osobie, której dane dotyczą, zgodnie z rozporządzeniem (UE) 2016/679, powinien mieć zastosowanie obowiązek zgłoszenia tego naruszenia podmiotowi sektora publicznego. Podmioty sektora publicznego powinny, w stosownych przypadkach, ułatwiać – za pomocą odpowiednich środków technicznych – ponowne wykorzystywanie danych na podstawie zgody osób, których dane dotyczą, lub pozwolenia posiadaczy danych na ponowne wykorzystywanie dotyczących ich danych. W tym względzie podmiot sektora publicznego powinien dołożyć wszelkich starań, by udzielić pomocy w ubieganiu się o taką zgodę lub takie pozwolenie potencjalnym ponownym użytkownikom, ustanawiając – jeżeli jest to praktycznie wykonalne – mechanizmy techniczne, które umożliwiają przekazywanie pochodzących od ponownych użytkowników wniosków o wyrażenie zgody lub udzielenie pozwolenia. Nie należy podawać żadnych informacji kontaktowych umożliwiających ponownym użytkownikom bezpośredni kontakt z osobami, których dane dotyczą, lub z posiadaczami danych. Jeżeli podmiot sektora publicznego przekazuje wniosek o wyrażenie zgody lub udzielnie pozwolenia, powinien zapewnić, by osoba, której dane dotyczą, lub posiadacz danych byli wyraźnie poinformowani o możliwości odmowy wyrażenia zgody lub udzielenia pozwolenia.

(16) By ułatwiać wykorzystywanie danych będących w posiadaniu podmiotów sektora publicznego do celów badań naukowych i zachęcać do takiego ich wykorzystywania, zachęca się podmioty sektora publicznego do opracowywania zharmonizowanego podejścia i zharmonizowanych procesów na rzecz zapewnienia łatwego dostępu do takich danych do celów badań naukowych leżących w interesie publicznym. Mogłoby to obejmować między innymi opracowywanie sprawnych procedur administracyjnych, normalizację formatowania danych, metadane zawierające informacje w zakresie wyboru metodyki i gromadzenia danych oraz normalizację pól danych, które umożliwiają łatwe łączenie zbiorów danych sektora publicznego pochodzących z różnych źródeł, w zakresie w jakim jest to przydatne do celów analizy. Celem tych praktyk powinno być promowanie wykorzystywania do celów badań naukowych danych sfinansowanych i wytworzonych przez sektor publiczny zgodnie z zasadą „otwarte jak to najbardziej możliwe, zamknięte jak to konieczne".

(17) Niniejsze rozporządzenie nie powinno mieć wpływu na prawa własności intelektualnej osób trzecich. Niniejsze rozporządzenie nie powinno mieć wpływu na istnienie praw własności intelektualnej podmiotów sektora publicznego ani na ich własność, ani w żaden sposób ograniczać wykonywania tych praw. 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 (zwaną dalej „konwencją berneńską"), Porozumieniem w sprawie handlowych aspektów praw własności intelektualnej (zwanym dalej „porozumieniem TRIPS") i Traktatem Światowej Organizacji Własności Intelektualnej o prawie autorskim (WCT) oraz z prawem Unii i prawem krajowym dotyczącym własności intelektualnej. Podmioty sektora publicznego powinny jednakże wykonywać swoje prawa autorskie w sposób ułatwiający ponowne wykorzystywanie.

(18) Dane objęte prawami własności intelektualnej, jak również tajemnice przedsiębiorstwa powinny być przesyłane osobie trzeciej wyłącznie w przypadku, gdy takie przesyłanie jest zgodne z prawem na mocy prawa Unii lub prawa krajowego, lub w porozumieniu z posiadaczami praw. Jeżeli podmiotom sektora publicznego przysługuje prawo producenta bazy danych ustanowione w art. 7 ust. 1 dyrektywy 96/9/WE Parlamentu Europejskiego i Rady ([26]), nie powinny one wykonywać tego prawa w celu uniemożliwienia lub ograniczenia ponownego wykorzystywania danych w zakresie wykraczającym poza ograniczenia określone w niniejszym rozporządzeniu.

([26]) 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).

(19) Przedsiębiorstwa i osoby, których dane dotyczą, powinny mieć zaufanie co do faktu, że ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu podmiotów 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 jak wymóg, aby podmioty sektora publicznego zapewniały pełną ochronę praw i interesów osób fizycznych i prawnych, w szczególności w odniesieniu do danych osobowych, szczególnie chronionych danych handlowych oraz praw własności intelektualnej, we wszystkich przypadkach, w tym w przypadku przekazywania takich danych do państw trzecich. Podmioty sektora publicznego nie powinny zezwalać na ponowne wykorzystywanie informacji przechowywanych w zastosowaniach w zakresie e-zdrowia przez zakłady ubezpieczeń lub innych dostawców usług w celu dyskryminacji przy ustalaniu cen, ponieważ byłoby to sprzeczne z podstawowym prawem dostępu do opieki zdrowotnej.

(20) Ponadto w celu zachowania uczciwej konkurencji i otwartej gospodarki rynkowej niezwykle ważne jest, aby zabezpieczyć chronione dane o charakterze nieosobowym, w szczególności tajemnice przedsiębiorstwa, a 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 lub interesów posiadaczy danych, powinno być możliwe przekazywanie danych nieosobowych, które zgodnie z prawem Unii lub prawem krajowym mają być chronione przed niezgodnym z prawem lub niedozwolonym dostępem, a które są w posiadaniu podmiotów sektora publicznego, do państw trzecich, ale wyłącznie wtedy gdy zapewnione są odpowiednie zabezpieczenia w zakresie wykorzystywania danych. Takie odpowiednie zabezpieczenia powinny zawierać wymóg, aby podmiot sektora publicznego przesyłał chronione dane ponownemu użytkownikowi wyłącznie wtedy, gdy ten ponowny użytkownik podejmie zobowiązania umowne służące ochronie tych danych. Ponowny użytkownik, który zamierza przekazać chronione dane do państwa trzeciego, powinien spełniać obowiązki określone w niniejszym rozporządzeniu nawet po przekazaniu danych do państwa trzeciego. Aby zapewnić właściwe egzekwowanie takich obowiązków, ponowny użytkownik powinien również uznać – do celów sądowego rozstrzygania sporów – jurysdykcję państwa członkowskiego podmiotu sektora publicznego, który zezwolił na ponowne wykorzystywanie.

(21) Należy uznać, że wdrożono takie odpowiednie zabezpieczenia, jeżeli w państwie trzecim, do którego przekazano danie nieosobowe, wprowadzono równoważne środki zapewniające, aby te dane były objęte poziomem ochrony podobnym do tego, który ma zastosowanie na podstawie prawa Unii, w szczególności w odniesieniu do ochrony tajemnicy przedsiębiorstwa i praw własności intelektualnej. W tym celu Komisja powinna mieć możliwość stwierdzenia w drodze aktów wykonawczych, gdy jest to uzasadnione ze względu na znaczącą liczbę wniosków składanych w całej Unii dotyczących ponownego wykorzystywania danych nieosobowych w określonych państwach trzecich, że dane państwo trzecie zapewnia poziom ochrony zasadniczo równoważny poziomowi ochrony zapewnianemu przez prawo Unii. Komisja powinna ocenić konieczność takich aktów wykonawczych w oparciu o informacje przekazane przez państwa członkowskie za pośrednictwem Europejskiej Rady ds. Innowacji w zakresie Danych. Takie akty wykonawcze upewniłyby podmioty sektora publicznego, że ponowne wykorzystywanie danych będących w posiadaniu podmiotów sektora publicznego w danym państwie trzecim nie zagroziłoby chronionemu charakterowi tych danych. W ocenie poziomu ochrony zapewnianej w danym państwie trzecim należy w szczególności uwzględnić odpowiednie prawo ogólne i sektorowe, w tym dotyczące bezpieczeństwa publicznego, obronności, bezpieczeństwa narodowego i prawa karnego, w zakresie dostępu do danych nieosobowych oraz ich ochrony, dostęp podmiotów sektora publicznego tego państwa trzeciego do przekazywanych danych, obecność i skuteczne funkcjonowanie w danym państwie trzecim co najmniej jednego niezależnego organu nadzorczego odpowiedzialnego za zapewnienie i egzekwowanie zgodności z systemem prawnym zapewniającym dostęp do takich danych, zobowiązania międzynarodowe państwa trzeciego w zakresie ochrony danych 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, podmiotów sektora publicznego lub dostawców usług pośrednictwa 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. Takie akty wykonawcze powinny pozostawać bez uszczerbku dla obowiązków prawnych lub uzgodnień umownych podjętych już przez ponownego użytkownika, które służą ochronie danych nieosobowych, w szczególności danych przemysłowych, oraz dla prawa podmiotów sektora publicznego do zobowiązania ponownych użytkowników do spełniania warunków ponownego wykorzystywania, zgodnie z niniejszym rozporządzeniem.

(22) Niektóre państwa trzecie przyjmują przepisy ustawowe, wykonawcze i inne akty prawne, których celem jest bezpośrednie przekazywanie lub zapewnianie dostępu administracji rządowej do danych nieosobowych w Unii znajdujących się pod kontrolą osób fizycznych i prawnych, podlegających jurysdykcji państw członkowskich. Orzeczenia i wyroki sądów lub trybunałów państw trzecich lub decyzje organów administracyjnych państw trzecich nakazujące takie przekazanie danych nieosobowych lub zapewnienie dostępu do nich powinny być wykonalne, jeżeli mają one za podstawę umowę międzynarodową, jak na przykład 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 Unii lub prawa krajowego, w szczególności w odniesieniu do ochrony praw podstawowych osób fizycznych lub podstawowych interesów państwa członkowskiego związanych z bezpieczeństwem narodowym lub obronnością, a także w odniesieniu do ochrony szczególnie chronionych danych handlowych oraz ochrony praw własności intelektualnej, w tym z zobowiązaniami umownymi dotyczącymi poufności zgodnie z tym prawem.

W przypadku braku umów międzynarodowych regulujących takie kwestie przekazywanie danych nieosobowych lub dostęp do nich powinny być dozwolone jedynie w przypadku, gdy w szczególności zweryfikowano, że system prawny państwa trzeciego wymaga, aby powody i proporcjonalność orzeczenia, wyroku lub decyzji zostały określone, aby orzeczenie, wyrok lub decyzja miały szczególny charakter oraz aby uzasadniony sprzeciw adresata podlegał kontroli właściwego sądu lub trybunału państwa trzeciego, które są uprawnione do należytego uwzględnienia odpowiednich interesów prawnych dostawcy takich danych. Ponadto podmioty sektora publicznego, osoby fizyczne lub prawne, którym przyznano prawo do ponownego wykorzystywania danych, dostawcy usług pośrednictwa danych oraz uznane organizacje altruizmu danych powinny zapewnić, w przypadku podpisywania przez nie umów z innymi podmiotami prywatnymi, aby dostęp do danych nieosobowych będących w posiadaniu Unii uzyskiwany w państwach trzecich lub przekazywanie tych danych do państw trzecich odbywało się wyłącznie zgodnie z prawem Unii lub prawem krajowym danego państwa członkowskiego.

(23) Aby budować większe zaufanie do unijnej gospodarki danych, konieczne jest wdrożenie zabezpieczeń zapewniających obywatelom Unii, sektorowi publicznemu i przedsiębiorstwom kontrolę nad ich danymi strategicznymi i szczególnie chronionymi oraz przestrzeganie prawa Unii, jej wartości i norm dotyczących między innymi bezpieczeństwa, ochrony danych i ochrony konsumentów. Aby zapobiec niezgodnemu z prawem dostępowi do danych nieosobowych, podmioty sektora publicznego, osoby fizyczne lub prawne, którym przyznano prawo do ponownego wykorzystywania danych, dostawcy usług pośrednictwa danych i uznane organizacje altruizmu danych powinny wprowadzić wszelkie rozsądne środki w celu zapobieżenia dostępowi do systemów, w których przechowywane są dane nieosobowe, w tym środki takie jak szyfrowanie danych lub polityka korporacyjna. W tym celu należy zapewnić, by podmioty sektora publicznego, osoby fizyczne lub prawne, którym przyznano prawo do ponownego wykorzystywania danych, dostawcy usług pośrednictwa danych i organizacje altruizmu danych stosowały wszystkie odpowiednie normy techniczne, kodeksy postępowania i systemy certyfikacji na poziomie Unii.

(24) Aby budować zaufanie do mechanizmów ponownego wykorzystywania, konieczne może być obwarowanie niektórych rodzajów danych nieosobowych, które mogą być uznane za szczególnie chronione w najwyższym stopniu w przyszłych szczególnych aktach ustawodawczych Unii, bardziej rygorystycznymi warunkami w zakresie przekazywania ich do państw trzecich, zgodnie ze zobowiązaniami międzynarodowymi, jeżeli takie przekazywanie mogłoby zagrozić celom polityki publicznej Unii. 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 w najwyższym stopniu dane dotyczące zdrowia. Inne istotne sektory obejmują transport, energię, środowisko i finanse. Aby zapewnić zharmonizowane praktyki w całej Unii, takie rodzaje szczególnie chronionych w najwyższym stopniu publicznych danych nieosobowych powinny być określone w prawie Unii, na przykład w kontekście europejskiej przestrzeni danych dotyczących zdrowia lub w innych przepisach prawa sektorowego. Warunki te 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 Unii, takich jak: ochrona zdrowia publicznego, bezpieczeństwo, środowisko, moralność publiczna, ochrona konsumentów, prywatność i ochrona danych osobowych. Warunki powinny odpowiadać zidentyfikowanemu ryzyku związanemu z faktem, że dane takie są szczególnie chronione, w tym ryzyku deanonimizacji osób fizycznych. Warunki takie mogą obejmować zasady 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 do uzyskania dostępu do danych w państwie trzecim. W wyjątkowych przypadkach warunki takie mogą również obejmować ograniczenia dotyczące przekazywania danych do państw trzecich ze względu na ochronę interesu publicznego.

(25) Podmioty sektora publicznego powinny mieć możliwość pobierania opłat za ponowne wykorzystywanie danych, ale powinny również móc zezwolić na ponowne wykorzystywanie danych za obniżoną opłatą lub nieodpłatnie, zgodnie z zasadami pomocy państwa, na przykład w przypadku niektórych kategorii ponownego wykorzystywania, takich jak ponowne wykorzystywanie na zasadach niekomercyjnych do celów badań naukowych, lub ponownego wykorzystywania przez MŚP, przedsiębiorstwa typu start-up, społeczeństwo obywatelskie i placówki edukacyjne, tak aby stwarzać zachęty 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. W tym szczególnym kontekście cele badań naukowych należy

rozumieć jako obejmujące wszelkiego rodzaju cele związane z badaniami, niezależnie od struktury organizacyjnej lub finansowej danej instytucji badawczej, z wyłączeniem badań prowadzonych przez przedsiębiorstwo w celu rozwijania, ulepszania lub optymalizacji produktów lub usług. Takie opłaty powinny być przejrzyste, niedyskryminujące i ograniczone do niezbędnych poniesionych kosztów i nie powinny one ograniczać konkurencji. Należy upublicznić wykaz kategorii ponownych użytkowników, którym udostępnia się dane do ponownego wykorzystywania za obniżoną opłatą lub nieodpłatnie, a także kryteria zastosowane do sporządzenia takiego wykazu.

(26) Aby stwarzać zachęty do ponownego wykorzystywania szczególnych kategorii danych będących w posiadaniu podmiotów sektora publicznego, państwa członkowskie powinny ustanowić pojedynczy punkt informacyjny, który będzie punktem kontaktowym dla ponownych użytkowników, którzy chcą ponownie wykorzystywać te dane. Punkt taki powinien mieć kompetencje międzysektorowe i w razie potrzeby powinien uzupełniać uzgodnienia na poziomie sektorowym. Pojedynczy punkt informacyjny powinien móc przekazywać zapytania lub wnioski o ponowne wykorzystywanie za pomocą zautomatyzowanych środków. W procesie przekazywania zapewnić należy wystarczający nadzór ze strony człowieka. Do tego celu można wykorzystać istniejące rozwiązania praktyczne, takie jak portale otwartych danych. Pojedynczy punkt informacyjny powinien dysponować wykazem zasobów zawierającym przegląd wszystkich dostępnych zasobów danych, w tym w stosownych przypadkach zasobów danych dostępnych w sektorowych, regionalnych lub lokalnych punktach informacyjnych, wraz z odpowiednim opisem tych dostępnych danych. Ponadto państwa członkowskie powinny wyznaczyć właściwe podmioty, ustanowić je lub ułatwić ich ustanowienie, aby wspierać działalność podmiotów sektora publicznego zezwalających na ponowne wykorzystywanie niektórych kategorii chronionych danych. Do zadań tych właściwych podmiotów może należeć udzielanie dostępu do danych, w przypadku gdy jest to przewidziane w sektorowym prawie Unii lub w sektorowym prawie krajowym. Te właściwe podmioty powinny udzielać pomocy podmiotom sektora publicznego za pomocą najnowocześniejszych technik, w tym w zakresie najlepszego sposobu strukturyzowania i przechowywania danych, tak aby były łatwo dostępne, w szczególności poprzez interfejsy programowania aplikacji, a także interoperacyjne, możliwe do przekazywania i wyszukiwania, z uwzględnieniem najlepszych praktyk w zakresie przetwarzania danych, a także istniejących norm regulacyjnych i technicznych oraz w zakresie bezpiecznych środowisk przetwarzania danych, które umożliwiają analizę danych w sposób chroniący prywatność informacji.

Właściwe podmioty powinny działać zgodnie z instrukcjami otrzymanymi od danego podmiotu sektora publicznego. Taka struktura udzielania pomocy może być pomocna osobom, których dane dotyczą, i posiadaczom danych w zarządzaniu zgodą lub pozwoleniem na ponowne wykorzystanie, w tym zgodą i pozwoleniem na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Właściwe podmioty nie powinny pełnić funkcji nadzorczej, która jest zarezerwowana dla organów nadzorczych wyznaczonych na podstawie rozporządzenia (UE) 2016/679. Bez uszczerbku dla uprawnień nadzorczych organów ochrony danych podmiot sektora publicznego odpowiadający za rejestr zawierający dane ponosi odpowiedzialność za przetwarzanie tych danych; podmiot ten w odniesieniu do danych osobowych pozostaje administratorem danych zgodnie z definicją w rozporządzeniu (UE) 2016/679. Państwa członkowskie powinny mieć możliwość posiadania jednego właściwego podmiotu lub kilku takich właściwych podmiotów, które mogą działać w różnych sektorach. Służby wewnętrzne podmiotów sektora publicznego mogą również działać w charakterze właściwych podmiotów. Właściwy podmiot może być podmiotem sektora publicznego udzielającym pomocy, w stosownych przypadkach, innym podmiotom sektora publicznego w zezwalaniu na ponowne wykorzystywanie danych lub podmiotem sektora publicznego, który sam zezwala na ponowne wykorzystywanie. Udzielanie pomocy innym podmiotom sektora publicznego powinno wiązać się z informowaniem ich, na ich wniosek, o najlepszych praktykach dotyczących sposobu spełnienia wymogów ustanowionych w niniejszym rozporządzeniu, na przykład w zakresie środków technicznych udostępniających bezpieczne środowisko przetwarzania lub środków technicznych zapewniających prywatność i poufność w przypadku udzielania dostępu do celów ponownego wykorzystywania danych objętych zakresem stosowania niniejszego rozporządzenia.

(27) Oczekuje się, że usługi pośrednictwa danych odgrywać będą kluczową rolę w gospodarce danych, w szczególności we wspieraniu i promowaniu praktyk dobrowolnego dzielenia się danymi między przedsiębiorstwami lub w ułatwianiu dzielenia się danymi w związku z obowiązkami ustanowionymi w prawie Unii lub prawie krajowym. Mogą one stać się narzędziem ułatwiającym wymianę znacznych ilości istotnych danych. Dostawcy usług pośrednictwa danych, którymi mogą być podmioty sektora publicznego, oferujący usługi, które łączą poszczególne podmioty, mogą przyczynić się do skutecznej konsolidacji danych, jak również do ułatwienia dwustronnego dzielenia się danymi. Wyspecjalizowane usługi pośrednictwa danych, które są niezależne od osób, których dane dotyczą, posiadaczy danych oraz użytkowników danych, mogą ułatwiać powstawanie nowych ekosystemów opartych o dane, niezależnych od podmiotów o znaczącej pozycji rynkowej, umożliwiając jednocześnie niedyskryminacyjny dostęp do gospodarki danych przedsiębiorstwom o dowolnej wielkości, w szczególności MŚP i przedsiębiorstwom typu start-up o ograniczonych środkach finansowych, prawnych lub administracyjnych. Będzie to miało szczególne znaczenie w kontekście ustanawiania wspólnych europejskich przestrzeni danych, oznaczających interoperacyjne ramy wspólnych norm i praktyk, specyficzne dla danego celu lub sektora bądź międzysektorowe, służące dzieleniu się danymi lub ich wspólnemu przetwarzaniu na potrzeby między innymi opracowywania nowych produktów i usług, badań naukowych lub inicjatyw społeczeństwa obywatelskiego. Usługi pośrednictwa danych mogą obejmować między innymi dwustronne lub wielostronne dzielenie się danymi lub tworzenie platform lub baz danych umożliwiających dzielenie się danymi lub ich wspólne wykorzystywanie, jak również tworzenie specjalnej infrastruktury do stworzenia powiązań między osobami, których dane dotyczą, i posiadaczami danych a użytkownikami danych.

(28) Niniejsze rozporządzenie powinno obejmować usługi, która mają na celu ustanowienie stosunków handlowych do celów dzielenia się danymi między – z jednej strony – nieokreśloną liczbą osób, których dane dotyczą, i posiadaczy danych, oraz – z drugiej strony – użytkownikami danych, za pomocą środków technicznych, prawnych lub innych, w tym w celu wykonywania praw osób, których dane dotyczą, w odniesieniu do danych osobowych. W przypadku gdy przedsiębiorstwa lub inne podmioty oferują liczne usługi związane z danymi, niniejszym rozporządzeniem powinny być objęte jedynie te działania, które bezpośrednio dotyczą świadczenia usług pośrednictwa danych. Świadczenie usług przechowywania w chmurze, usług analitycznych, dostarczanie oprogramowania na potrzeby dzielenia się danymi, przeglądarek internetowych, wtyczek do przeglądarek lub świadczenie usług poczty elektronicznej nie powinno być uznawane za usługę pośrednictwa danych w rozumieniu niniejszego rozporządzenia, pod warunkiem że usługi takie dostarczają jedynie narzędzi technicznych osobom, których dane dotyczą, lub posiadaczom danych, służących do dzielenia się z innymi danymi i o ile celem dostarczania takich narzędzi nie jest nawiązywanie stosunków handlowych między posiadaczami danych a użytkownikami danych, ani umożliwienie dostawcy usług pośrednictwa danych uzyskiwania informacji na temat nawiązywania stosunków handlowych do celów dzielenia się danymi. Do usług pośrednictwa danych zalicza się między innymi rynki danych, na których przedsiębiorstwa mogą udostępniać innym dane, usługi koordynatorów otwartych dla wszystkich zainteresowanych stron ekosystemów dzielenia się danymi, na przykład w kontekście wspólnych europejskich przestrzeni danych, a także pule danych utworzone wspólnie przez grupę osób prawnych lub fizycznych z zamiarem udzielania licencji na korzystanie z takich puli danych wszystkim zainteresowanym stronom, przy założeniu, że wszyscy uczestnicy wnoszący wkład do puli danych otrzymują wynagrodzenie za swój wkład.

Na tej zasadzie nie należą do nich usługi, w ramach których dane są pozyskiwane od posiadaczy danych i agregowane, wzbogacane lub przekształcane w celu istotnego dodania im wartości, a następnie użytkownikom danych udzielana jest licencja na wykorzystywanie uzyskanych w ten sposób danych bez nawiązania stosunku handlowego między posiadaczami danych a użytkownikami danych. Nie należą do nich również usługi, z których korzysta wyłącznie jeden posiadacz danych w celu umożliwienia wykorzystywania danych będących w jego posiadaniu, lub usługi, z których korzysta wiele osób prawnych w zamkniętej grupie, w tym w ramach stosunków z dostawcami lub klientami lub współpracy nawiązanej na podstawie umowy, w szczególności usługi, których głównym celem jest zapewnienie funkcjonalności przedmiotów i urządzeń podłączonych do internetu rzeczy.

(29) Usługi skoncentrowane na pośrednictwie treści chronionych prawem autorskim, takie jak dostawcy usług udostępniania treści online zgodnie z definicją w art. 2 pkt 6 dyrektywy (UE) 2019/790, nie powinny być objęte niniejszym rozporządzeniem. Dostawcy informacji skonsolidowanych zgodnie z definicją w art. 2 ust. 1 pkt 35 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 600/2014 ([27]) oraz dostawcy świadczący usługę dostępu do informacji o rachunku zgodnie z definicją w art. 4 pkt 19 dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/2366 ([28]) nie powinni być uznawani za dostawców usług pośrednictwa danych do celów niniejszego rozporządzenia. Niniejsze rozporządzenie nie powinno mieć zastosowania do usług oferowanych przez podmioty sektora publicznego w celu ułatwienia ponownego wykorzystywania chronionych danych będących w posiadaniu podmiotów sektora publicznego zgodnie z niniejszym rozporządzeniem albo wykorzystywania wszelkich innych danych, o ile usługi te nie mają na celu ustanowienia stosunków handlowych. Organizacje altruizmu danych regulowane niniejszym rozporządzeniem nie powinny być uznawane za pomioty oferujące usługi pośrednictwa danych, pod warunkiem że usługi te nie ustanawiają stosunków handlowych pomiędzy potencjalnymi użytkownikami danych, z jednej strony, a osobami, których dane dotyczą, i posiadaczami danych, którzy udostępniają dane z pobudek altruistycznych, z drugiej strony. Inne usługi, których celem nie jest ustanowienie stosunków handlowych, takie jak repozytoria służące umożliwieniu ponownego wykorzystywania danych pochodzących z badań naukowych zgodnie z zasadami otwartego dostępu nie powinny być uznawane za usługi pośrednictwa danych w rozumieniu niniejszego rozporządzenia.

(30) Szczególna kategoria usług pośrednictwa danych obejmuje dostawców oferujących swoje usługi osobom, których dane dotyczą. Tacy dostawcy usług pośrednictwa danych dążą do zwiększenia sprawczości osób, których dane dotyczą, a w szczególności kontroli osób fizycznych nad dotyczącymi ich danymi. Tacy dostawcy pomagają osobom fizycznym w wykonywaniu ich praw wynikających z rozporządzenia (UE) 2016/679, w szczególności prawa do wyrażania i wycofywania zgody na przetwarzanie danych, prawa dostępu do własnych danych, prawa do sprostowania nieprawidłowych danych osobowych, prawa do usunięcia danych lub prawa do bycia zapomnianym, prawa do ograniczenia przetwarzania i prawa do przenoszenia danych, które umożliwia osobom, których dane dotyczą, przeniesienie ich danych osobowych od jednego administratora danych do drugiego. W tym kontekście ważne jest, aby model biznesowy takich dostawców zapewniał brak niewłaściwych zachęt dla osób fizycznych do korzystania z takich usług w celu udostępniania do przetwarzania większej ilości dotyczących ich danych, niż leży to w ich interesie. Może to obejmować doradzanie osobom fizycznym w zakresie możliwego wykorzystywania ich danych oraz przeprowadzanie kontroli należytej staranności w odniesieniu do użytkowników danych przed umożliwieniem im skontaktowania się z osobami, których dane dotyczą, co ma na celu unikanie oszukańczych praktyk. W określonych

([27]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012 (Dz.U. L 173 z 12.6.2014, s. 84).

([28]) 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 (Dz.U. L 337 z 23.12.2015, s. 35).

sytuacjach, w celu maksymalnego zwiększenia ochrony danych osobowych i prywatności, pożądane może być zestawianie rzeczywistych danych w przestrzeni danych osobowych, tak aby przetwarzanie mogło odbywać się w tej przestrzeni bez przesyłania danych osobowych osobom trzecim. Takie przestrzenie danych osobowych mogą zawierać statyczne dane osobowe, takie jak imię i nazwisko, adres lub data urodzenia oraz dane dynamiczne generowane przez daną osobę fizyczną, na przykład w ramach korzystania z usługi internetowej lub z przedmiotu połączonego z internetem rzeczy. Przestrzenie te mogą być również wykorzystywane do przechowywania zweryfikowanych informacji dotyczących tożsamości, takich jak numer paszportu lub informacje dotyczące zabezpieczenia społecznego, jak również danych uwierzytelniających, takich jak prawo jazdy, dyplomy lub informacje o rachunkach bankowych.

(31) Spółdzielnie danych dążą do osiągnięcia szeregu celów, w szczególności 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 w sposób dający lepsze możliwości wyboru poszczególnym członkom grupy lub potencjalnie godząc sprzeczne stanowiska poszczególnych członków grupy dotyczące sposobu wykorzystywania danych, w przypadku gdy dane takie odnoszą się do kilku należących do tej grupy osób, których dane dotyczą. W tym kontekście ważne jest uznanie, że prawa wynikające z rozporządzenia (UE) 2016/679 są prawami osobistymi osób, których dane dotyczą, i że osoby te nie mogą zrzec się takich praw. Spółdzielnie danych mogą również zapewniać przydatne środki przedsiębiorstwom jednoosobowym oraz MŚP, których wiedza na temat dzielenia się danymi jest często porównywalna z wiedzą osób fizycznych.

(32) W celu zwiększenia zaufania do takich usług pośrednictwa danych, w szczególności w odniesieniu do wykorzystywania danych i spełniania warunków nałożonych przez osoby, których dane dotyczą, oraz posiadaczy danych, konieczne jest utworzenie ram regulacyjnych na poziomie Unii, które ustanowią wysoce zharmonizowane wymogi związane z godnym zaufania świadczeniem takich usług pośrednictwa danych i które wdrożone zostaną przez właściwe organy. Ramy takie przyczynią się do zapewnienia, aby osoby, których dane dotyczą, i posiadacze danych, a także użytkownicy danych mieli lepszą kontrolę nad dostępem do ich danych i wykorzystywaniem ich, zgodnie z prawem Unii. Komisja może również zachęcać do opracowywania kodeksów postępowania na poziomie Unii, przy zaangażowaniu odpowiednich interesariuszy, w szczególności w zakresie interoperacyjności, oraz ułatwiać opracowywanie takich kodeksów postępowania. Zarówno w sytuacjach, w których dzielenie się danymi ma miejsce między przedsiębiorstwami, jak i w sytuacjach, w których ma to miejsce między przedsiębiorstwami a konsumentami, dostawcy usług pośrednictwa danych powinni oferować nowatorski, „europejski" sposób zarządzania danymi, zapewniając w gospodarce danych rozdział pomiędzy dostarczaniem danych, pośrednictwem w ich zakresie i ich wykorzystywaniem. Dostawcy usług pośrednictwa danych mogą również udostępniać specjalną infrastrukturę techniczną do stworzenia powiązań między osobami, których dane dotyczą, i posiadaczami danych a użytkownikami danych. W tym kontekście szczególnie istotne jest zaprojektowanie infrastruktury w taki sposób, aby przeszkody techniczne ani inne nie utrudniały uczestnictwa MŚP i przedsiębiorstw typu start-up w gospodarce danych.

Dostawcy usług pośrednictwa danych powinni móc oferować posiadaczom danych lub osobom, których dane dotyczą, dodatkowe specjalne narzędzia i usługi ułatwiające wymianę danych, takie jak tymczasowe przechowywanie, kuratorstwo, konwersja, anonimizacja i pseudonimizacja. Z tych narzędzi i usług powinno korzystać się wyłącznie na wyraźny wniosek lub za zgodą posiadacza danych lub osoby, której dane dotyczą, a narzędzia osób trzecich oferowane w tym kontekście nie powinny wykorzystywać danych do innych celów. Jednocześnie należy umożliwić dostawcom usług pośrednictwa danych dostosowywanie danych podlegających wymianie w celu poprawy użyteczności danych dla użytkownika danych, w przypadku gdy użytkownik danych sobie tego życzy, lub w celu poprawy interoperacyjności poprzez na przykład konwertowanie danych na konkretne formaty.

(33) Ważne jest stworzenie konkurencyjnego środowiska na potrzeby dzielenia się danymi. Kluczowym elementem służącym zwiększeniu zaufania i lepszej kontroli ze strony posiadaczy danych, osób, których dane dotyczą, i użytkowników danych w odniesieniu do usług pośrednictwa danych jest neutralność dostawców takich usług względem danych wymienianych między posiadaczami danych lub osobami, których dane dotyczą, a użytkownikami danych. Dlatego koniecznie jest, aby dostawcy usług pośrednictwa danych działali jedynie jako pośrednicy w transakcjach i nie wykorzystywali wymienianych danych do żadnych innych celów. Warunki handlowe świadczenia usług pośrednictwa danych, w tym ceny, nie powinny zależeć od tego, czy potencjalny posiadacz danych lub użytkownik danych korzysta z innych usług – w tym usług przechowywania danych, usług analitycznych, sztucznej inteligencji lub innych aplikacji opartych o dane – świadczonych przez tego samego dostawcę usług pośrednictwa danych lub powiązany podmiot ani od tego w jakim zakresie posiadacz danych lub użytkownik danych korzysta z takich innych usług. Będzie to również wymagało strukturalnego rozdziału usług pośrednictwa danych od innych świadczonych usług, tak aby uniknąć konfliktu interesów. Oznacza to, że usługi pośrednictwa danych powinny być świadczone za pośrednictwem osoby prawnej, która jest odrębna od pozostałej działalności danego dostawcy usług pośrednictwa danych. Jednakże dostawcy usług pośrednictwa danych powinni mieć możliwość wykorzystywania danych dostarczonych przez posiadacza danych w celu poprawy swoich usług pośrednictwa.

Dostawcy usług pośrednictwa danych powinni móc udostępniać posiadaczom danych, osobom, których dane dotyczą, lub użytkownikom danych własne narzędzia lub narzędzia osób trzecich ułatwiające wymianę danych, na przykład narzędzia do konwersji lub kuratorstwa danych, wyłącznie na wyraźny wniosek lub za zgodą osoby, której dane dotyczą, lub posiadacza danych. Oferowane w tym kontekście narzędzia osób trzecich nie powinny wykorzystywać danych do celów

innych niż te związane z usługami pośrednictwa danych. Dostawcy usług pośrednictwa danych, którzy pośredniczą w wymianie danych między osobami fizycznymi jako osobami, których dane dotyczą, a osobami prawnymi jako użytkownikami danych, powinni ponadto mieć wobec osób fizycznych obowiązek powierniczy, co ma na celu zapewnienie, by działali w najlepszym interesie osób, których dane dotyczą. Kwestie odpowiedzialności za wszelkie szkody materialne i niematerialne oraz straty wynikające z jakiegokolwiek zachowania dostawców usług pośrednictwa danych mogą być ujęte w odpowiedniej umowie w oparciu o krajowe systemy odpowiedzialności.

(34) Dostawcy usług pośrednictwa danych powinni podejmować rozsądne środki w celu zapewnienia interoperacyjności w obrębie danego sektora i między różnymi sektorami, tak aby zapewnione zostało właściwe funkcjonowanie rynku wewnętrznego. Takie rozsądne środki mogą obejmować przestrzeganie istniejących, powszechnie stosowanych norm w sektorze, w którym działają dostawcy usług pośrednictwa danych. Europejska Rada ds. Innowacji w zakresie Danych powinna w razie potrzeby ułatwiać tworzenie dodatkowych norm sektorowych. Dostawcy usług pośrednictwa danych powinni w odpowiednim terminie wdrażać środki na rzecz interoperacyjności między usługami pośrednictwa danych przyjęte przez Europejską Radę ds. Innowacji w zakresie Danych.

(35) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla obowiązku przestrzegania przez dostawców usług pośrednictwa danych rozporządzenia (UE) 2016/679 oraz odpowiedzialności organów nadzorczych za zapewnienie przestrzegania tego rozporządzenia. W przypadku gdy dostawcy usług pośrednictwa danych przetwarzają dane osobowe, niniejsze rozporządzenie nie powinno mieć wpływu na ochronę danych osobowych. W przypadku gdy dostawcy usług pośrednictwa danych są administratorami danych lub podmiotami przetwarzającymi dane zgodnie z definicją w rozporządzeniu (UE) 2016/679, obowiązują ich przepisy tego rozporządzenia.

(36) Od dostawców usług pośrednictwa danych wymaga się wprowadzenia procedur i środków służących nakładaniu kar za nieuczciwe praktyki lub nadużycia w odniesieniu do podmiotów ubiegających się o dostęp za pośrednictwem ich usług pośrednictwa danych, w tym takich środków jak wykluczenie użytkowników danych, którzy nie przestrzegają warunków korzystania z usług lub naruszają obowiązujące prawo.

(37) Dostawcy usług pośrednictwa danych powinni również stosować środki mające na celu zapewnienie przestrzegania prawa konkurencji i wprowadzić odpowiednie do tego celu procedury. Dotyczy to w szczególności sytuacji, w których dzielenie się danymi umożliwia przedsiębiorstwom zdobycie wiedzy o strategiach rynkowych ich faktycznych lub potencjalnych konkurentów. Istotne dla konkurencji szczególnie chronione informacje zazwyczaj obejmują dane klientów, informacje o przyszłych cenach, o kosztach produkcji, ilościach, obrotach, sprzedaży lub wydajności.

(38) Należy ustanowić procedurę zgłaszania usług pośrednictwa danych, aby zapewnić zarządzanie danymi w Unii oparte na godnej zaufania wymianie danych. Korzyści płynące z godnego zaufania środowiska najlepiej osiągnąć poprzez nałożenie szeregu wymogów dotyczących świadczenia usług pośrednictwa danych, ale bez konieczności wydawania przez organ właściwy do spraw usług pośrednictwa danych konkretnej decyzji lub konkretnego aktu administracyjnego na potrzeby świadczenia takich usług. Procedura zgłaszania nie powinna stwarzać nadmiernych utrudnień dla MSP, przedsiębiorstw typu start-up i organizacji społeczeństwa obywatelskiego i powinna być zgodna z zasadą niedyskryminacji.

(39) Aby wesprzeć skuteczne transgraniczne świadczenie usług, należy wymagać od dostawcy usług pośrednictwa danych przesłania zgłoszenia wyłącznie do organu właściwego do spraw usług pośrednictwa danych w państwie członkowskim, 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. Po dokonaniu odpowiedniego zgłoszenia dostawca usług pośrednictwa danych powinien móc rozpocząć działalność w dowolnym państwie członkowskim, bez dodatkowych obowiązków w zakresie zgłaszania.

(40) Procedura dotycząca zgłaszania ustanowiona w niniejszym rozporządzeniu powinna pozostawać bez uszczerbku dla szczególnych dodatkowych przepisów dotyczących świadczenia usług pośrednictwa danych, które mają zastosowanie na podstawie prawa sektorowego.

(41) Główną jednostką organizacyjną dostawcy usług pośrednictwa danych w Unii powinno być miejsce, w którym znajduje się jego centralna administracja w Unii. Główną jednostkę organizacyjną dostawcy usług pośrednictwa danych w Unii należy określać na podstawie obiektywnych kryteriów i powinna ona wiązać się ze skutecznym i faktycznym wykonywaniem zadań w zakresie zarządzania. Działalność dostawcy usług pośrednictwa danych powinna być zgodna z prawem krajowym państwa członkowskiego, w którym ma główną jednostkę organizacyjną.

(42) Aby zapewnić przestrzeganie przez dostawców usług pośrednictwa danych niniejszego rozporządzenia, ich główna jednostka organizacyjna powinna znajdować się w Unii. Jeżeli dostawca usług pośrednictwa danych niemający jednostki organizacyjnej w Unii oferuje usługi w Unii, powinien on wyznaczyć przedstawiciela prawnego. Wyznaczenie przedstawiciela prawnego jest w takich przypadkach konieczne ze względu na to, że tacy dostawcy usług pośrednictwa danych zajmują się danymi osobowymi, jak również danymi poufnymi ze względów handlowych, co wymaga dokładnego monitorowania przestrzegania przez dostawców usług pośrednictwa danych niniejszego rozporządzenia. Aby ustalić, czy dostawca usług pośrednictwa danych oferuje usługi w Unii, należy stwierdzić, czy jest oczywiste, że ten dostawca usług pośrednictwa 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 pośrednictwa danych lub posługiwanie się językiem powszechnie używanym w państwie trzecim, w którym dany dostawca pośrednictwa danych ma jednostkę organizacyjną, należy uznać za niewystarczające do stwierdzenia takiego zamiaru. Czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim z możliwością zamówienia usług w tym języku lub wzmianka o użytkownikach znajdujących się w Unii, mogą jednak potwierdzać oczywistość zamiaru oferowania przez dostawcę usług pośrednictwa danych usług w Unii.

Wyznaczony przedstawiciel prawny powinien działać w imieniu dostawcy usług pośrednictwa danych, a organy właściwe do spraw usług pośrednictwa danych powinny móc zwracać się jednocześnie do wyznaczonego przedstawiciela prawnego i dostawcy usług pośrednictwa danych albo do takiego przedstawiciela zamiast do dostawcy usług pośrednictwa danych, w tym w przypadku naruszenia, w celu wszczęcia postępowania egzekucyjnego przeciwko dostawcy usług pośrednictwa danych niemającego jednostki organizacyjnej w Unii, który nie przestrzega niniejszego rozporządzenia. Dostawca usług pośrednictwa danych powinien wyznaczyć przedstawiciela prawnego za pomocą pisemnego upoważnienia do działania w jego imieniu w zakresie jego obowiązków wynikających z niniejszego rozporządzenia.

(43) Oprócz oznakowania „uznany w Unii dostawca usług pośrednictwa danych" należy stworzyć wspólne logo rozpoznawalne w całej Unii, aby pomóc osobom, których dane dotyczą, i posiadaczom danych w łatwym rozpoznawaniu uznanych w Unii dostawców usług pośrednictwa danych, a tym samym zwiększyć ich zaufanie do takich dostawców.

(44) Organy właściwe do spraw usług pośrednictwa danych wyznaczone do monitorowania spełniania przez dostawców usług pośrednictwa danych wymogów niniejszego rozporządzenia powinny być wybierane na podstawie ich zdolności i wiedzy fachowej w zakresie horyzontalnego lub sektorowego dzielenia się danymi. Powinny być one niezależne od dostawców usług pośrednictwa danych, jak również wykonywać swoje zadania w sposób przejrzysty i bezstronny. Państwa członkowskie powinny przekazać Komisji dane identyfikacyjne tych organów właściwych do spraw usług pośrednictwa danych. Uprawnienia i kompetencje organów właściwych do spraw usług pośrednictwa danych powinny pozostawać bez uszczerbku dla uprawnień organów ochrony danych. W szczególności w przypadku wszelkich kwestii wymagających oceny przestrzegania rozporządzenia (UE) 2016/679 organ właściwy do spraw usług pośrednictwa danych powinien zwrócić się, w stosownych przypadkach, o opinię lub decyzję do właściwego organu nadzorczego ustanowionego na podstawie tego rozporządzenia.

(45) Wykorzystywanie danych udostępnionych dobrowolnie przez osoby, których dane dotyczą, na podstawie ich świadomej zgody lub – w przypadku danych nieosobowych – udostępnionych przez posiadaczy danych, ma duży potencjał w zakresie celów leżących w interesie ogólnym. Cele takie obejmują opiekę zdrowotną, przeciwdziałanie zmianie klimatu, poprawę mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawę świadczenia usług publicznych lub kształtowania polityki publicznej. Wspieranie badań naukowych należy również uznać za jeden z celów leżących w interesie ogólnym. Niniejsze rozporządzenie powinno mieć na celu przyczynienie się do powstania wystarczająco dużych pul danych udostępnianych na podstawie altruizmu danych w celu umożliwienia analizy danych i uczenia się maszyn, w tym w całej Unii. Aby osiągnąć ten cel, państwa członkowskie powinny mieć możliwość wprowadzania rozwiązań organizacyjnych lub technicznych sprzyjających altruizmowi danych. Rozwiązania takie mogą obejmować dostępność łatwych do wykorzystania narzędzi dla osób, których dane dotyczą, i posiadaczy danych w celu wyrażenia zgody lub udzielenia pozwolenia na wykorzystywanie ich danych na zasadzie altruizmu danych, organizowanie kampanii uświadamiających lub ustrukturyzowany dialog między właściwymi organami na temat tego, jakie korzyści altruizm danych przynosi politykom publicznym, jak na przykład poprawa ruchu w transporcie, zdrowia publicznego oraz przeciwdziałanie zmianie klimatu. W tym celu państwa członkowskie powinny mieć możliwość określenia krajowych polityk w zakresie altruizmu danych. Osoby, których dane dotyczą, powinny mieć możliwość otrzymania zwrotu ograniczonego do wysokości kosztów poniesionych w związku z udostępnieniem ich danych do celów leżących w interesie ogólnym.

(46) Oczekuje się, że rejestrowanie uznanych organizacji altruizmu danych oraz posługiwanie się oznakowaniem „uznana w Unii organizacja altruizmu danych" doprowadzi do powstania repozytoriów danych. Rejestracja w jednym państwie członkowskim byłaby ważna w całej Unii; oczekuje się, że ułatwi ona transgraniczne wykorzystywanie danych w Unii oraz powstawanie pul danych obejmujących kilka państw członkowskich. Posiadacze danych mogliby udzielać pozwolenia na przetwarzanie ich danych nieosobowych do wielu różnych celów, których nie określono w momencie udzielania pozwolenia. Spełnienie przez takie uznane organizacje altruizmu danych szeregu wymogów ustanowionych w niniejszym rozporządzeniu powinno budzić zaufanie, że dane udostępniane z pobudek

altruistycznych służą celom leżącym w interesie ogólnym. Zaufanie takie powinno wynikać w szczególności z posiadania jednostki organizacyjnej lub przedstawiciela prawnego w Unii, a także z wymogu, aby uznane organizacje altruizmu danych były organizacjami o charakterze niekomercyjnym, z wymogów dotyczących przejrzystości oraz z istnienia szczególnych 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 uznane organizacje altruizmu danych, mechanizmy nadzoru, takie jak rady lub komisje ds. etyki, z udziałem przedstawicieli społeczeństwa obywatelskiego, mające zapewnić utrzymywanie przez administratora danych wysokich standardów etyki naukowej oraz ochrony praw podstawowych, skuteczne i jasno komunikowane 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. Rejestracja jako uznana organizacja altruizmu danych nie powinna być warunkiem wstępnym prowadzenia działalności w zakresie altruizmu danych. Komisja powinna przygotować, w ścisłej współpracy z organizacjami altruizmu danych i odpowiednimi interesariuszami, w drodze aktów delegowanych zbiór zasad. Przestrzeganie tego zbioru zasad powinno być warunkiem rejestracji jako uznana organizacja altruizmu danych.

(47) Należy stworzyć wspólne logo rozpoznawalne w całej Unii, aby pomóc osobom, których dane dotyczą, oraz posiadaczom danych w łatwym rozpoznawaniu uznanych organizacji altruizmu danych, a tym samym zwiększyć ich zaufanie do takich organizacji. Wspólnemu logo powinien towarzyszyć kod QR z linkiem do publicznego unijnego rejestru uznanych organizacji altruizmu danych.

(48) Niniejsze rozporządzenie powinno pozostać bez uszczerbku dla ustanawiania, organizacji i funkcjonowania podmiotów, które chcą uczestniczyć w altruizmie danych zgodnie z prawem krajowym i opierać się na wymogach prawa krajowego w celu prowadzenia zgodnie z prawem działalności w państwie członkowskim jako organizacja o charakterze niekomercyjnym.

(49) Niniejsze rozporządzenie powinno pozostawać bez uszczerbku dla ustanawiania, organizacji i funkcjonowania podmiotów innych niż podmioty sektora publicznego, które uczestniczą w dzieleniu się danymi i udostępnianiu treści na podstawie otwartych licencji, przyczyniając się w ten sposób do tworzenia dostępnych dla wszystkich wspólnych zasobów. Powinno to obejmować otwarte i oparte na współpracy platformy dzielenia się wiedzą, otwarte repozytoria naukowe i akademickie, platformy rozwoju otwartego oprogramowania oraz otwarte platformy agregacji treści.

(50) Uznane organizacje altruizmu danych powinny mieć możliwość gromadzenia odpowiednich danych bezpośrednio od osób fizycznych i prawnych lub przetwarzania danych zgromadzonych przez innych. Organizacje altruizmu danych mogą przetwarzać zgromadzone dane do celów, które same określają, lub, w stosownych przypadkach, mogą zezwalać na przetwarzanie danych do tych celów przez osoby trzecie. W przypadku gdy uznane organizacje altruizmu danych są administratorami danych lub podmiotami przetwarzającymi dane zgodnie z definicją w rozporządzeniu (UE) 2016/679, powinny one przestrzegać tego rozporządzenia. Zazwyczaj altruizm danych opiera się na zgodzie osób, których dane dotyczą, w rozumieniu art. 6 ust. 1 lit. a) i art. 9 ust. 2 lit. a) rozporządzenia (UE) 2016/679, która powinna być wyrażona zgodnie z wymogami dotyczącymi zgody zgodnej z prawem, określonymi w art. 7 i 8 tego rozporządzenia. Zgodnie z rozporządzeniem (UE) 2016/679 cele badań naukowych można wspierać zgodą na niektóre obszary badań naukowych, w przypadku gdy 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. W przypadku danych nieosobowych ograniczenia wykorzystania powinny być wskazane w pozwoleniu udzielanym przez posiadacza danych.

(51) Organy właściwe do spraw rejestracji organizacji altruizmu danych wyznaczone do monitorowania spełniania przez uznane organizacje altruizmu danych wymogów niniejszego rozporządzenia powinny być wybierane na podstawie ich zdolności i wiedzy fachowej. Powinny być one niezależne od organizacji altruizmu danych, jak również wykonywać swoje zadania w sposób przejrzysty i bezstronny. Państwa członkowskie powinny przekazać Komisji dane identyfikacyjne tych organów właściwych do spraw rejestracji organizacji altruizmu danych. Uprawnienia i kompetencje organów właściwych do spraw rejestracji organizacji altruizmu danych powinny pozostawać bez uszczerbku dla uprawnień organów ochrony danych. W szczególności w sprawie wszelkich kwestii wymagających oceny przestrzegania rozporządzenia (UE) 2016/679 organ właściwy do spraw rejestracji organizacji altruizmu danych powinien zwrócić się, w stosownych przypadkach, o opinię lub decyzję do właściwego organu nadzorczego ustanowionego na podstawie tego rozporządzenia.

(52) W celu promowania zaufania i zapewnienia dodatkowej pewności prawa oraz przyjazności dla użytkownika w odniesieniu do procesu wyrażania 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 altruizmu danych i stosować go w kontekście dzielenia się danymi 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. Powinien on również ułatwiać wyrażanie i wycofywanie zgody oraz posłużyć do usprawnienia altruizmu danych stosowanego przez przedsiębiorstwa i zapewniać mechanizm umożliwiający takim przedsiębiorstwom wycofanie pozwolenia na wykorzystywanie danych. Aby uwzględnić specyfikę poszczególnych sektorów, w tym z punktu widzenia ochrony danych, w europejskim formularzu zgody na potrzeby altruizmu danych należy stosować podejście modułowe umożliwiające dostosowanie do potrzeb konkretnych sektorów i poszczególnych celów.

(53) W celu pomyślnego wdrożenia ram zarządzania danymi należy ustanowić Europejską Radę ds. Innowacji w zakresie Danych w postaci grupy ekspertów. Europejska Rada ds. Innowacji w zakresie Danych powinna składać się z przedstawicieli organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych wszystkich państw członkowskich, Europejskiej Rady Ochrony Danych, Europejskiego Inspektora Ochrony Danych, Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), Komisji, pełnomocnika UE ds. MŚP lub przedstawiciela wyznaczonego przez sieć pełnomocników ds. MŚP i z innych przedstawicieli odpowiednich podmiotów w poszczególnych sektorach, a także podmiotów dysponujących szczególną wiedzą fachową. Europejska Rada ds. Innowacji w zakresie Danych powinna składać się z kilku podgrup, w tym podgrupy ds. zaangażowania interesariuszy składającej się z odpowiednich przedstawicieli przemysłu, takich jak opieka zdrowotna, środowisko, rolnictwo, transport, energia, produkcja przemysłowa, media, sektor kultury i sektor kreatywny oraz statystyka, a także środowisk naukowych i akademickich, społeczeństwa obywatelskiego, organizacji normalizacyjnych, odpowiednich wspólnych europejskich przestrzeni danych oraz innych odpowiednich interesariuszy i osób trzecich, między innymi podmiotów posiadających szczególną wiedzę fachową, takich jak krajowe urzędy statystyczne.

(54) Europejska Rada ds. Innowacji w zakresie Danych powinna pomagać Komisji 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 europejskich i międzynarodowych norm i specyfikacji, w tym poprzez unijną wielostronną platformę ds. normalizacji ICT, słowniki podstawowe i moduły instrumentu „Łącząc Europę", a także powinna uwzględniać prace normalizacyjne prowadzone 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 przesyłania danych między dwoma środowiskami przetwarzania, co umożliwi organizację przestrzeni danych, w szczególności zaś wyjaśnienie i rozróżnienie, które normy i praktyki są międzysektorowe, a które sektorowe. Europejska Rada ds. Innowacji w zakresie Danych powinna współpracować z sektorowymi podmiotami, sieciami lub grupami ekspertów lub z innymi organizacjami międzysektorowymi zajmującymi się ponownym wykorzystywaniem danych. Odnośnie do altruizmu danych Europejska Rada ds. Innowacji w zakresie Danych, po konsultacji z Europejską Radą Ochrony Danych, powinna pomagać Komisji w opracowaniu formularza zgody na potrzeby altruizmu danych. Proponując wytyczne dotyczące wspólnych europejskich przestrzeni danych, Europejska Rada ds. Innowacji w zakresie Danych powinna wspierać rozwój prawidłowo funkcjonującej europejskiej gospodarki danych, której te przestrzenie danych służą za podstawę, o czym mowa w europejskiej strategii w zakresie danych.

(55) Państwa członkowskie powinny ustanowić przepisy dotyczące kar mających zastosowanie w przypadku naruszenia niniejszego rozporządzenia i powinny podjąć wszelkie niezbędne środki, aby zapewnić ich wdrożenie. Ustanowione kary powinny być skuteczne, proporcjonalne i odstraszające. Duże rozbieżności między przepisami dotyczącymi kar mogą prowadzić do zakłócenia konkurencji na jednolitym rynku cyfrowym. Harmonizacja takich przepisów mogłaby być w tym względzie korzystna.

(56) W celu zapewnienia skutecznego egzekwowania niniejszego rozporządzenia i zapewnienia dostawcom usług pośrednictwa danych oraz podmiotom, które chcą zarejestrować się jako uznane organizacje altruizmu danych, możliwości dostępu do procedur zgłaszania i rejestracji oraz ich ukończenia – w całości przez internet i w kontekście transgranicznym, procedury te powinny być udostępnione za pośrednictwem jednolitego portalu cyfrowego ustanowionego na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1724 ([29]). Procedury te należy dodać do wykazu procedur zawartego w załączniku II do rozporządzenia (UE) 2018/1724.

(57) Należy zatem odpowiednio zmienić rozporządzenie (UE) 2018/1724.

([29]) Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1724 z dnia 2 października 2018 r. w sprawie utworzenia jednolitego portalu cyfrowego w celu zapewnienia dostępu do informacji, procedur oraz usług wsparcia i rozwiązywania problemów, a także zmieniające rozporządzenie (UE) nr 1024/2012 (Dz.U. L 295 z 21.11.2018, s. 1).

(58) W celu zapewnienia skuteczności niniejszego rozporządzenia należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE w celu uzupełnienia niniejszego rozporządzenia poprzez określenie warunków szczególnych mających zastosowanie do przekazywania do państw trzecich pewnych kategorii danych nieosobowych uznawanych za szczególnie chronione w najwyższym stopniu w szczególnych aktach ustawodawczych Unii i poprzez opracowanie zbioru zasad dla uznanych organizacji altruizmu danych, którego organizacje te mają przestrzegać, zawierającego wymogi informacyjne, techniczne i w zakresie bezpieczeństwa, a także plany działania w zakresie komunikacji i normy interoperacyjności. 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 ([30]). W szczególności, aby zapewnić Parlamentowi Europejskiemu i Radzie udział na równych zasadach 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.

(59) W celu zapewnienia jednolitych warunków wykonywania niniejszego rozporządzenia należy powierzyć Komisji uprawnienia wykonawcze do: udzielania pomocy podmiotom sektora publicznego i ponownym użytkownikom w spełnianiu określonych w niniejszym rozporządzeniu warunków ponownego wykorzystywania danych poprzez określenie wzorów klauzul umownych na potrzeby przekazywania przez ponownych użytkowników danych nieosobowych do państwa trzeciego; stwierdzenia, że stosowane przez dane państwo trzecie rozwiązania prawne, w zakresie nadzoru i egzekwowania przepisów są równoważne z ochroną zapewnianą na podstawie prawa Unii; opracowania projektu wspólnego logo dla dostawców usług pośrednictwa danych i wspólnego logo dla uznanych organizacji altruizmu danych; oraz ustanowienia i opracowania europejskiego formularza zgody na potrzeby altruizmu danych. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 182/2011 ([31]).

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

(61) Zgodnie z art. 42 ust. 1 rozporządzenia (UE) 2018/1725 skonsultowano się z Europejskim Inspektorem Ochrony Danych i Europejską Radą Ochrony Danych, które wydały opinię w dniu 10 marca 2021 r.

(62) Niniejsze rozporządzenie ma za przewodnią zasadę poszanowanie praw podstawowych i zasad uznanych w szczególności w Karcie praw podstawowych Unii Europejskiej, w tym prawa do prywatności, ochrony danych osobowych, wolności działalności gospodarczej, prawa własności oraz integracji osób z niepełnosprawnościami. W kontekście integracji osób z niepełnosprawnościami podmioty sektora publicznego oraz usługi objęte zakresem stosowania niniejszego rozporządzenia powinny, w stosownych przypadkach, przestrzegać dyrektyw Parlamentu Europejskiego i Rady (UE) 2016/2102 ([32]) i (UE) 2019/882 ([33]). Ponadto należy wziąć pod uwagę koncepcję „projektowania dla wszystkich" w kontekście technologii informacyjno-komunikacyjnych, polegającą na świadomych i systematycznych działaniach na rzecz proaktywnego stosowania zasad, metod i narzędzi promujących projektowanie uniwersalne w technologiach komputerowych, w tym w technologiach internetowych, co pozwala uniknąć konieczności adaptacji a posteriori lub specjalistycznego projektowania.

(63) Ponieważ cele niniejszego rozporządzenia, a mianowicie ponowne wykorzystywanie w Unii niektórych kategorii danych będących w posiadaniu podmiotów sektora publicznego, a także ustanowienie ram dotyczących zgłaszania i nadzoru w odniesieniu do świadczenia usług pośrednictwa danych, ram dotyczących dobrowolnej rejestracji podmiotów, które udostępniają dane z pobudek altruistycznych oraz ram dotyczących ustanowienia Europejskiej Rady ds. Innowacji w zakresie Danych, nie mogą zostać osiągnięte w sposób wystarczający przez państwa członkowskie, natomiast ze względu na rozmiary i skutki działań możliwe jest ich lepsze osiągnięcie na poziomie Unii, może ona podjąć działania zgodnie z zasadą pomocniczości określoną w art. 5 Traktatu o Unii Europejskiej. Zgodnie z zasadą proporcjonalności określoną w tym artykule niniejsze rozporządzenie nie wykracza poza to, co jest konieczne do osiągnięcia tych celów,

([30]) Dz.U. L 123 z 12.5.2016, s. 1.

([31]) 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).

([32]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z dnia 26 października 2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.U. L 327 z 2.12.2016, s. 1).

([33]) Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z dnia 17 kwietnia 2019 r. w sprawie wymogów dostępności produktów i usług (Dz.U. L 151 z 7.6.2019, s. 70).

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

ROZDZIAŁ I

Przepisy ogólne

Artykuł 1

Przedmiot i zakres stosowania

1. W niniejszym rozporządzeniu ustanawia się:

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

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

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

d) ramy dotyczące ustanowienia Europejskiej Rady ds. Innowacji w zakresie Danych.

2. Niniejsze rozporządzenie nie nakłada na podmioty sektora publicznego obowiązku zezwalania na ponowne wykorzystywanie danych ani nie zwalnia podmiotów sektora publicznego z obowiązków w zakresie zachowania poufności wynikających z prawa Unii lub prawa krajowego.

Niniejsze rozporządzenie pozostaje bez uszczerbku dla:

a) szczególnych przepisów prawa Unii lub prawa krajowego dotyczących dostępu do niektórych kategorii danych lub ich ponownego wykorzystywania, w szczególności w odniesieniu do udzielania dostępu do dokumentów urzędowych i ich ujawniania; oraz

b) wynikających z prawa Unii lub prawa krajowego obowiązków podmiotów sektora publicznego dotyczących zezwolenia na ponowne wykorzystywanie danych, a także dla wymogów związanych z przetwarzaniem danych nieosobowych.

Jeżeli sektorowe prawo Unii lub sektorowe prawo krajowe wymagają od podmiotów sektora publicznego, dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych spełnienia szczególnych dodatkowych wymogów technicznych, administracyjnych lub organizacyjnych, w tym poprzez system zezwoleń lub certyfikacji, stosuje się również te przepisy danego sektorowego prawa Unii lub sektorowego prawa krajowego. Wszelkie takie szczególne dodatkowe wymogi muszą być niedyskryminujące, proporcjonalne i obiektywnie uzasadnione.

3. Do danych osobowych przetwarzanych w związku z niniejszym rozporządzeniem zastosowanie mają prawo Unii i prawo krajowe w dziedzinie ochrony danych osobowych. W szczególności niniejsze rozporządzenie pozostaje bez uszczerbku dla rozporządzeń (UE) 2016/679 i (UE) 2018/1725 oraz dyrektyw 2002/58/WE i (UE) 2016/680, w tym z uwzględnieniem uprawnień i kompetencji organów nadzorczych. W przypadku kolizji pomiędzy niniejszym rozporządzenia a prawem Unii w dziedzinie ochrony danych osobowych lub prawem krajowym przyjętym zgodnie z takim prawem Unii pierwszeństwo ma odpowiednie prawo Unii lub prawo krajowe w dziedzinie ochrony danych osobowych. Niniejsze rozporządzenie nie tworzy podstawy prawnej dla przetwarzania danych osobowych ani nie ma wpływu na obowiązki i prawa określone w rozporządzeniach (UE) 2016/679 lub (UE) 2018/1725 lub w dyrektywach 2002/58/WE lub (UE) 2016/680.

4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania prawa konkurencji.

5. Niniejsze rozporządzenie nie narusza kompetencji państw członkowskich w odniesieniu do ich działań z zakresu bezpieczeństwa publicznego, obronności i bezpieczeństwa narodowego.

Artykuł 2

Definicje

Do celów niniejszego rozporządzenia stosuje się następujące definicje:

1) „dane” oznaczają 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 podmiotów sektora publicznego, do celów komercyjnych lub niekomercyjnych innych niż ich pierwotne przeznaczenie w ramach zadań publicznych, dla którego to celu dane te zostały wytworzone, z wyjątkiem wymiany danych między podmiotami sektora publicznego służącej wyłącznie wykonywaniu zadań publicznych;

3) „dane osobowe” oznaczają dane osobowe zgodnie z definicją w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

4) „dane nieosobowe” oznaczają dane inne niż dane osobowe;

5) „zgoda” oznacza zgodę zgodnie z definicją w art. 4 pkt 11 rozporządzenia (UE) 2016/679;

6) „pozwolenie” oznacza przyznanie użytkownikom danych prawa do przetwarzania danych nieosobowych;

7) „osoba, której dane dotyczą” oznacza osobę, której dane dotyczą, o której mowa w art. 4 pkt 1 rozporządzenia (UE) 2016/679;

8) „posiadacz danych” oznacza osobę prawną, w tym podmiot sektora publicznego lub organizację międzynarodową, lub osobę fizyczną niebędącą w odniesieniu do przedmiotowych konkretnych danych osobą, której dane dotyczą, która ma – zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym – prawo do udzielania dostępu do niektórych danych osobowych lub danych nieosobowych lub do dzielenia się nimi;

9) „użytkownik danych” oznacza osobę fizyczną lub osobę prawną, która ma zgodny z prawem dostęp do niektórych danych osobowych lub nieosobowych i prawo, w tym – w przypadku danych osobowych – na podstawie rozporządzenia (UE) 2016/679, do wykorzystywania tych danych w celach komercyjnych lub niekomercyjnych;

10) „dzielenie się danymi” oznacza dostarczanie danych przez osobę, której dane dotyczą, lub przez posiadacza danych użytkownikowi danych do celów wspólnego lub indywidualnego wykorzystywania takich danych w oparciu o dobrowolne umowy lub na podstawie prawa Unii lub prawa krajowego, bezpośrednio lub z udziałem pośrednika, na przykład w ramach licencji otwartych lub handlowych, bezpłatnie lub za opłatą;

11) „usługa pośrednictwa danych” oznacza usługę, która ma na celu ustanowienie – za pomocą środków technicznych, prawnych lub innych – stosunków handlowych między – z jednej strony – nieokreśloną liczbą osób, których dane dotyczą, i posiadaczy danych oraz – z drugiej strony – użytkownikami danych do celów dzielenia się danymi, w tym do celów wykonywania praw osób, których dane dotyczą, w odniesieniu do danych osobowych, z wyłączeniem co najmniej:

    a) usług, w ramach których dane są pozyskiwane od posiadaczy danych i agregowane, wzbogacane lub przekształcane w celu dodania im znaczącej wartości, a następnie użytkownikom danych udzielana jest licencja na wykorzystanie uzyskanych w ten sposób danych bez ustanawiania stosunku handlowego między nimi a posiadaczami danych;

    b) usług skoncentrowanych na pośrednictwie treści chronionych prawem autorskim;

    c) usług, z których korzysta wyłącznie jeden posiadacz danych w celu umożliwienia wykorzystywania danych będących w jego posiadaniu, lub usługi, z których korzysta wiele osób prawnych w zamkniętej grupie, w tym w ramach stosunków z dostawcami lub klientami lub współpracy nawiązanej na podstawie umowy, w szczególności usług, których głównym celem jest zapewnienie funkcjonalności przedmiotów i urządzeń podłączonych do internetu rzeczy;

    d) usług dzielenia się danymi oferowanych przez podmioty sektora publicznego, które to usługi nie mają na celu ustanowienia stosunków handlowych;

12) „przetwarzanie” oznacza przetwarzanie zgodnie z definicją w art. 4 pkt 2 rozporządzenia (UE) 2016/679 w odniesieniu do danych osobowych lub zgodnie z definicją w art. 3 ust. 2 rozporządzenia (UE) 2018/1807 w odniesieniu do danych nieosobowych;

13) „dostęp” oznacza wykorzystywanie danych zgodnie ze szczegółowymi wymogami technicznymi, prawnymi lub organizacyjnymi, które niekoniecznie musi się wiązać z przesyłaniem lub pobieraniem danych;

14) „główna jednostka organizacyjna” osoby prawnej oznacza miejsce, w którym znajduje się jej centralna administracja w Unii;

15) „usługi świadczone przez spółdzielnie danych" oznaczają usługi pośrednictwa danych oferowane przez strukturę organizacyjną utworzoną przez osoby, których dane dotyczą, przedsiębiorstwa jednoosobowe lub MŚP będące członkami tej struktury, mającą za główne cele wspieranie swoich członków w wykonywaniu ich praw w odniesieniu do niektórych danych, w tym w odniesieniu do dokonywania świadomego wyboru przed wyrażeniem przez nich zgody na przetwarzanie danych, wymienianie poglądów na temat celów przetwarzania danych i warunków, które najlepiej będą odzwierciedlać interesy jej członków w odniesieniu do ich danych, oraz negocjowanie w imieniu jej członków warunków i zasad przetwarzania danych przed udzieleniem pozwolenia na przetwarzanie danych nieosobowych lub przed wyrażeniem zgody na przetwarzanie danych osobowych;

16) „altruizm danych" oznacza dobrowolne dzielenie się danymi na podstawie wyrażonej przez osoby, których dane dotyczą, zgody na przetwarzanie dotyczących ich danych osobowych lub na podstawie udzielonego przez posiadaczy danych pozwolenia na wykorzystywanie ich danych nieosobowych, bez żądania ani otrzymania za to wynagrodzenia wykraczającego poza zwrot kosztów poniesionych przez te osoby lub posiadaczy w związku z udostępnieniem ich danych do celów leżących w interesie ogólnym określonych – w stosownych przypadkach – w prawie krajowym, takich jak opieka zdrowotna, zwalczanie zmiany klimatu, poprawa mobilności, ułatwianie opracowywania, tworzenia i rozpowszechniania statystyk urzędowych, poprawa świadczenia usług publicznych, kształtowanie polityki publicznej lub do celów badań naukowych leżących w interesie ogólnym;

17) „podmiot sektora publicznego" oznacza państwo, organy regionalne lub lokalne, podmioty prawa publicznego lub stowarzyszenia złożone z co najmniej jednego takiego organu lub z co najmniej jednego takiego podmiotu prawa publicznego;

18) „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 komercyjnego;

    b) posiada osobowość prawną;

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

19) „przedsiębiorstwo publiczne" oznacza przedsiębiorstwo, na które podmioty sektora publicznego mogą wywierać, bezpośrednio lub pośrednio, dominujący wpływ z racji bycia jego właścicielem, posiadania w nim udziału finansowego lub na podstawie przepisów, które regulują działalność tego przedsiębiorstwa; do celów niniejszej definicji zakłada się istnienie dominującego wpływu ze strony podmiotów sektora publicznego w dowolnym z poniższych przypadków, gdy podmioty 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;

20) „bezpieczne środowisko przetwarzania" oznacza środowisko fizyczne lub wirtualne oraz środki organizacyjne służące zapewnieniu przestrzegania prawa Unii, takiego jak rozporządzenie (UE) 2016/679, w szczególności pod względem praw osób, których dane dotyczą, praw własności intelektualnej oraz poufności informacji handlowych i statystycznych, integralności i dostępności, jak również mającego zastosowanie prawa krajowego oraz umożliwiające podmiotowi zapewniającemu bezpieczne środowisko przetwarzania określenie i nadzorowanie wszystkich działań związanych z przetwarzaniem danych, w tym wyświetlania, przechowywania, pobierania i eksportowania danych oraz obliczania danych pochodnych za pomocą algorytmów obliczeniowych;

21) „przedstawiciel prawny" oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, wyznaczoną w wyraźny sposób do działania w imieniu niemających jednostki organizacyjnej w Unii dostawcy usług pośrednictwa danych lub podmiotu gromadzącego dane udostępniane do celów leżących w interesie ogólnym i na zasadzie altruizmu danych przez osoby fizyczne lub prawne; organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych mogą się zwracać jednocześnie do tej osoby oraz dostawcy usług pośrednictwa danych lub podmiotu albo do tej osoby zamiast do dostawcy usług pośrednictwa danych lub podmiotu w związku z obowiązkami ustanowionymi na podstawie niniejszego rozporządzenia, w tym w związku ze wszczęciem postępowania egzekucyjnego przeciwko niespełniającym wymogów dostawcy usług pośrednictwa danych lub podmiotowi niemającym jednostki organizacyjnej w Unii.

ROZDZIAŁ II

Ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu podmiotów sektora publicznego

Artykuł 3

Kategorie danych

1. Niniejszy rozdział stosuje się do danych będących w posiadaniu podmiotów sektora publicznego, które są chronione ze względu na:

a) poufność informacji handlowych, w tym tajemnicę handlową, zawodową i tajemnicę przedsiębiorstwa;

b) poufność informacji statystycznych;

c) ochronę praw własności intelektualnej osób trzecich; lub

d) ochronę danych osobowych w zakresie, w jakim dane te wykraczają poza zakres stosowania dyrektywy (UE) 2019/1024.

2. Niniejszego rozdziału nie stosuje się 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 podmiotów lub ich jednostek zależnych realizujących misję nadawców publicznych;

c) danych będących w posiadaniu instytucji kulturalnych i placówek edukacyjnych;

d) danych będących w posiadaniu podmiotów sektora publicznego, które są chronione ze względów bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego; lub

e) danych, których dostarczanie jest działalnością wykraczającą poza zakres zadań publicznych zainteresowanych podmiotów 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. Niniejszy rozdział pozostaje bez uszczerbku dla:

a) przepisów prawa Unii i prawa krajowego oraz postanowień umów międzynarodowych, których Unia lub państwa członkowskie są stronami, dotyczących ochrony kategorii danych, o których mowa w ust. 1; oraz

b) przepisów prawa Unii i prawa krajowego dotyczących dostępu do dokumentów.

Artykuł 4

Zakaz uzgodnień dotyczących wyłączności

1. Nie jest dozwolone zawieranie umów lub stosowanie innych praktyk odnoszących się do ponownego wykorzystywania danych będących w posiadaniu podmiotów 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 na potrzeby ponownego wykorzystywania przez podmioty niebędące stronami takich umów lub niestosujące innych tego typu 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, które w przeciwnym razie nie byłyby możliwe.

3. Prawo wyłączne, o którym mowa w ust. 2, jest przyznawane w drodze aktu administracyjnego lub uzgodnienia umownego zgodnie z mającym zastosowanie prawem Unii lub prawem krajowym oraz zgodnie z zasadami przejrzystości, równego traktowania i niedyskryminacji.

4. Prawo wyłączne do ponownego wykorzystywania danych nie może zostać przyznane na okres dłuższy niż 12 miesięcy. W przypadku zawarcia umowy okres obowiązywania zawartej umowy musi być taki sam jak okres, na który przyznano prawo wyłączne.

5. Przyznanie prawa wyłącznego zgodnie z ust. 2, 3 i 4, w tym uzasadnienie konieczności przyznania takiego prawa, musi być przejrzyste i podane do wiadomości publicznej w internecie, w formie zgodnej z odpowiednim prawem Unii dotyczącym zamówień publicznych.

6. Umowy lub inne praktyki objęte zakresem stosowania zakazu, o którym mowa w ust. 1, niespełniające warunków ustanowionych w ust. 2 i 3, a które zostały zawarte przed dniem 23 czerwca 2022 r. ulegają rozwiązaniu wraz z końcem okresu obowiązywania danej umowy, a w każdym razie do dnia 24 grudnia 2024 r.

Artykuł 5

Warunki ponownego wykorzystywania

1. Podmioty sektora publicznego, które na mocy prawa krajowego są właściwe do udzielania lub odmowy udzielania dostępu do celów ponownego wykorzystywania co najmniej jednej kategorii danych, o których mowa w art. 3 ust. 1, muszą udostępniać publicznie warunki, które muszą zostać spełnione w celu zezwolenia na takie ponowne wykorzystywanie, oraz procedurę występowania z wnioskiem o ponowne wykorzystywanie za pośrednictwem pojedynczego punktu informacyjnego, o którym mowa w art. 8. Podmiotom sektora publicznego mogą pomagać w udzielaniu lub odmowie udzielania dostępu do celów ponownego wykorzystania właściwe podmioty określone w art. 7 ust. 1.

Państwa członkowskie zapewniają, aby podmioty sektora publicznego były wyposażone w niezbędne zasoby w celu przestrzegania niniejszego artykułu.

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

3. Podmioty sektora publicznego zapewniają, zgodnie z prawem Unii i prawem krajowym, aby chroniony charakter danych został zachowany. Mogą one ustanawiać następujące wymagania:

a) dostępu do celów ponownego wykorzystywania danych udziela się wyłącznie pod warunkiem, że podmiot sektora publicznego lub właściwy podmiot po otrzymaniu wniosku o ponowne wykorzystywanie zapewniły, by dane te:

   (i) zostały zanonimizowane – w przypadku danych osobowych; oraz

   (ii) zostały zmodyfikowane, zagregowane lub przekształcone za pomocą innej metody zapobiegającej ujawnieniu – w przypadku poufnych informacji handlowych, w tym tajemnic handlowych lub treści chronionych prawami własności intelektualnej;

b) dostęp do danych i ich ponowne wykorzystywanie odbywa się w sposób zdalny w bezpiecznym środowisku przetwarzania zapewnianym lub kontrolowanym przez podmiot sektora publicznego;

c) jeżeli nie można zezwolić na dostęp zdalny bez stwarzania zagrożenia dla praw i interesów osób trzecich, dostęp do danych i ich ponowne wykorzystywanie odbywa się w obrębie obiektów fizycznych, w których panuje bezpieczne środowisko przetwarzania zgodnie z rygorystycznymi normami bezpieczeństwa.

4. W przypadku ponownego wykorzystywania, na które zezwolono zgodnie z ust. 3 lit. b) i c), podmioty sektora publicznego nakładają warunki, które pozwalają zachować integralność funkcjonowania systemów technicznych wykorzystywanego bezpiecznego środowiska przetwarzania. Podmiot sektora publicznego zastrzega sobie prawo weryfikacji procesu, środków oraz wszelkich wyników przetwarzania danych przez ponownego użytkownika, aby zachować integralność ochrony danych oraz zastrzega sobie prawo do zakazania wykorzystywania takich wyników, które zawierają informacje zagrażające prawom i interesom osób trzecich. Decyzja o zakazie wykorzystywania wyników musi być zrozumiała i przejrzysta dla ponownego użytkownika.

5. O ile w prawie krajowym nie ustanowiono szczególnych zabezpieczeń dotyczących mających zastosowanie obowiązków w zakresie zachowania poufności związanych z ponownym wykorzystywaniem danych, o których mowa w art. 3 ust. 1, podmiot sektora publicznego uzależnia ponowne wykorzystywanie danych przekazanych zgodnie z ust. 3 niniejszego artykułu od przestrzegania przez ponownego użytkownika obowiązku w zakresie zachowania poufności, zgodnie z którym zakazane jest ujawniania informacji, które stwarzają zagrożenie dla praw i interesów osób trzecich, a które pomimo wprowadzonych zabezpieczeń mogłyby się znaleźć w posiadaniu ponownego użytkownika. Ponowni użytkownicy mają zakaz deanonimizacji osób, których dane dotyczą, i podejmują środki techniczne i operacyjne w celu zapobieżenia deanonimizacji oraz zawiadomienia podmiotu sektora publicznego o wszelkich naruszeniach ochrony danych prowadzących do deanonimizacji osób zainteresowanych, których dane dotyczą. W przypadku niedozwolonego ponownego wykorzystywania danych nieosobowych ponowny użytkownik bez zwłoki i – w stosownych przypadkach – z pomocą podmiotu sektora publicznego informuje osoby prawne, na których prawa i interesy może to mieć wpływ.

6. W przypadku gdy nie można zezwolić na ponowne wykorzystywanie danych zgodnie z obowiązkami określonymi w ust. 3 i 4 niniejszego artykułu i nie ma podstawy prawnej do przesłania danych na podstawie rozporządzenia (UE) 2016/679, podmiot sektora publicznego dokłada wszelkich starań zgodnie z prawem Unii i prawem krajowym, by potencjalnym ponownym użytkownikom udzielić pomocy w uzyskiwaniu zgody osób, których dane dotyczą, lub pozwolenia posiadaczy danych – na których prawa i interesy takie ponowne wykorzystywanie może mieć wpływ – oraz – o ile jest to możliwe – bez powodowania nieproporcjonalnie dużego obciążenia dla danego podmiotu sektora publicznego. Podmiotowi sektora publicznego mogą pomagać w udzielaniu takiej pomocy właściwe podmioty, o których mowa w art. 7 ust. 1.

7. Na ponowne wykorzystywanie danych można zezwolić wyłącznie z poszanowaniem praw własności intelektualnej. Prawo producenta bazy danych ustanowione w art. 7 ust. 1 dyrektywy 96/9/WE nie może być wykonywane przez podmioty 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 dane, o które się zwrócono, są uznawane za poufne zgodnie z prawem Unii lub prawem krajowym dotyczącym poufności informacji handlowych lub statystycznych, podmioty sektora publicznego zapewniają, aby w wyniku zezwolenia na ponowne wykorzystywanie nie zostały ujawnione dane poufne, chyba że na takie ponowne wykorzystywanie zezwolono zgodnie z ust. 6.

9. W przypadku gdy ponowny użytkownik zamierza przekazać do państwa trzeciego dane nieosobowe chronione ze względów określonych w art. 3 ust. 1, informuje o swoim zamiarze przekazania takich danych podmiot sektora publicznego, podając w momencie składania wniosku o ponowne wykorzystywanie takich danych również cel tego przekazania. W przypadku ponownego wykorzystywania zgodnie z ust. 6 niniejszego artykułu ponowny użytkownik, w stosownych przypadkach z pomocą podmiotu sektora publicznego, informuje osobę prawną, na której prawa i interesy może to mieć wpływ, o swoim zamiarze, celu oraz o odpowiednich zabezpieczeniach. Podmiot sektora publicznego nie zezwala na ponowne wykorzystywanie, o ile dana osoba prawna nie udzieli pozwolenia na przekazanie.

10. Podmioty sektora publicznego przesyłają poufne dane nieosobowe lub dane chronione prawami własności intelektualnej ponownemu użytkownikowi, który zamierza przekazać te dane do państwa trzeciego innego niż państwo wyznaczone zgodnie z ust. 12 wyłącznie wtedy, gdy ponowny użytkownik zobowiąże się na podstawie umowy do:

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

b) uznania jurysdykcji sądów lub trybunałów państwa członkowskiego podmiotu sektora publicznego przesyłającego dane w odniesieniu do wszelkich sporów związanych z przestrzeganiem ust. 7 i 8.

11. Podmioty sektora publicznego, w stosownych przypadkach i w miarę swoich zdolności, udzielają ponownym użytkownikom wskazówek oraz udzielają pomocy w wypełnianiu obowiązków, o których mowa w ust. 10 niniejszego artykułu.

Aby udzielać pomocy podmiotom sektora publicznego i ponownym użytkownikom, Komisja może przyjmować akty wykonawcze określające wzory klauzul umownych dotyczących wypełniania obowiązków, o których mowa w ust. 10 niniejszego artykułu. Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 33 ust. 3.

12. Jeżeli jest to uzasadnione ze względu na znaczącą liczbę wniosków składanych w całej Unii dotyczących ponownego wykorzystywania danych nieosobowych w określonych państwach trzecich, Komisja może przyjąć akty wykonawcze, w których stwierdza, że stosowane przez dane państwo trzecie rozwiązania prawne, w zakresie nadzoru i egzekwowania przepisów:

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

b) są skutecznie stosowane i egzekwowane; oraz

c) zapewniają skuteczne sądowe środki zaskarżenia.

Te akty wykonawcze przyjmuje się zgodnie z procedurą sprawdzającą, o której mowa w art. 33 ust. 3.

13. Na podstawie szczególnych aktów ustawodawczych Unii można do celów niniejszego artykułu uznać niektóre kategorie danych nieosobowych będące w posiadaniu podmiotów sektora publicznego za szczególnie chronione w najwyższym stopniu, w przypadku gdy ich przekazanie do państw trzecich może zagrozić celom polityki publicznej Unii, takim jak bezpieczeństwo i zdrowie publiczne, lub może prowadzić do ryzyka deanonimizacji zanonimizowanych danych nieosobowych. W przypadku gdy taki akt zostanie przyjęty, Komisja przyjmuje zgodnie z art. 32 akty delegowane uzupełniające niniejsze rozporządzenie poprzez ustanowienie warunków szczególnych mających zastosowanie do przekazywania takich danych do państw trzecich.

Te warunki szczególne są ustalane w oparciu o charakter określonych w szczególnym akcie ustawodawczym Unii kategorii danych nieosobowych oraz w oparciu o powody uznania tych kategorii za szczególnie chronione w najwyższym stopniu, z uwzględnieniem ryzyka deanonimizacji zanonimizowanych danych nieosobowych. Te warunki szczególne muszą być niedyskryminujące i ograniczone do tego, co jest niezbędne do osiągnięcia celów polityki publicznej Unii określonych w tym akcie, zgodnie z międzynarodowymi zobowiązaniami Unii.

Jeżeli wymagają tego szczególne akty ustawodawcze Unii, o których mowa w akapicie pierwszym, takie warunki szczególne mogą 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 do państw trzecich.

14. Osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych nieosobowych, może przekazywać te dane tylko do tych państw trzecich, w przypadku których spełnione są wymogi określone w ust. 10, 12 i 13.

Artykuł 6

Opłaty

1. Podmioty 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. Opłaty pobierane zgodnie z ust. 1 muszą być niedyskryminujące, przejrzyste, proporcjonalne i obiektywnie uzasadnione oraz nie mogą ograniczać konkurencji.

3. Podmioty sektora publicznego zapewniają możliwość uiszczania opłat także 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. Jeżeli podmioty sektora publicznego pobierają opłaty, podejmują one działania mające na celu stwarzanie zachęt do ponownego wykorzystywania kategorii danych, o których mowa w art. 3 ust. 1, do celów niekomercyjnych, takich jak cele badań naukowych, oraz przez MŚP i przedsiębiorstwa typu start-up zgodnie z zasadami pomocy państwa. W związku z tym podmioty sektora publicznego mogą również udostępniać dane za obniżoną opłatą lub nieodpłatnie, w szczególności MŚP i przedsiębiorstwom typu start-up, społeczeństwu obywatelskiemu oraz placówkom edukacyjnym. W tym celu podmioty sektora publicznego mogą sporządzić wykaz kategorii ponownych użytkowników, którym udostępnia się dane do ponownego wykorzystywania za obniżoną opłatą lub nieodpłatnie. Wykaz ten wraz z kryteriami stosowanymi do jego sporządzenia podaje się do wiadomości publicznej.

5. Opłaty muszą wynikać z kosztów związanych z prowadzeniem procedur dotyczących wniosków o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, oraz ograniczać się do niezbędnych kosztów związanych z:

a) powielaniem, dostarczaniem i rozpowszechnianiem danych;

b) weryfikacją praw;

c) anonimizacją lub innymi formami przygotowania danych osobowych i danych poufnych ze względów handlowych, jak przewidziano w art. 5 ust. 3;

d) utrzymaniem bezpiecznego środowiska przetwarzania;

e) nabywaniem przez osoby trzecie spoza sektora publicznego prawa do zezwalania na ponowne wykorzystywanie zgodnie z niniejszym rozdziałem; oraz

f) udzielaniem pomocy ponownym użytkownikom w uzyskiwaniu zgody osób, których dane dotyczą, oraz pozwolenia posiadaczy danych, w przypadku gdy takie ponowne wykorzystywanie może mieć wpływ na prawa i interesy tych osób i posiadaczy.

6. Kryteria i metodyka obliczania opłat są określane przez państwa członkowskie i publikowane. Podmiot sektora publicznego publikuje opis głównych kategorii kosztów oraz zasad stosowanych przy ich rozdziale.

Artykuł 7

Właściwe podmioty

1. Na potrzeby wykonywania zadań, o których mowa w niniejszym artykule, każde państwo członkowskie wyznacza co najmniej jeden właściwy podmiot, którym może być podmiot właściwy w zakresie szczególnych sektorów, w celu udzielania pomocy podmiotom sektora publicznego udzielającym dostępu lub odmawiającym udzielenia dostępu do celów ponownego wykorzystywania kategorii danych, o których mowa w art. 3 ust. 1. Państwa członkowskie mogą ustanowić jeden nowy właściwy podmiot lub większą ich liczbę albo opierać się na istniejących podmiotach sektora publicznego lub na wewnętrznych służbach podmiotów sektora publicznego spełniających warunki określone w niniejszym rozporządzeniu.

2. Właściwe podmioty mogą zostać upoważnione do udzielania dostępu do celów ponownego wykorzystywania kategorii danych, o których mowa w art. 3 ust. 1, zgodnie z prawem Unii lub prawem krajowym, w którym przewidziano udzielenie takiego dostępu. W przypadku gdy takie właściwe podmioty udzielają lub odmawiają udzielenia dostępu do celów ponownego wykorzystywania, stosuje się do nich art. 4, 5, 6 i 9.

3. Właściwym podmiotom należy zapewnić odpowiednie zasoby prawne, finansowe, techniczne i ludzkie do wykonywania powierzonych im zadań, w tym niezbędną wiedzę techniczną, aby były w stanie przestrzegać odpowiednich przepisów prawa Unii lub prawa krajowego dotyczących systemów dostępu do kategorii danych, o których mowa w art. 3 ust. 1.

4. Pomoc, o której mowa w ust. 1, obejmuje, w razie potrzeby:

a) zapewnienie wsparcia technicznego poprzez udostępnienie bezpiecznego środowiska przetwarzania na potrzeby zapewnienia dostępu do celów ponownego wykorzystywania danych;

b) udzielenie wskazówek i zapewnianie wsparcia technicznego w zakresie jak najlepszego ustrukturyzowania danych i ich przechowywania, tak by były one łatwo dostępne;

c) zapewnienie wsparcia technicznego w zakresie pseudonimizacji oraz zapewnienie przetwarzania danych w sposób skutecznie chroniący prywatność, poufność, integralność i dostępność informacji zawartych w danych, na których ponowne wykorzystywanie zezwolono, w tym technik anonimizacji, uogólnienia, ukrywania i randomizacji danych osobowych lub innych najnowocześniejszych metod zachowania prywatności, oraz usuwania poufnych informacji handlowych, w tym tajemnic przedsiębiorstwa lub treści chronionych prawami własności intelektualnej;

d) udzielanie pomocy, w stosownych przypadkach, podmiotom sektora publicznego w zapewnianiu wsparcia ponownym użytkownikom w występowaniu do osób, których dane dotyczą, o zgodę na ponowne wykorzystywanie danych oraz do posiadaczy danych – o pozwolenie, zgodnie z ich konkretnymi decyzjami, w tym odnośnie do jurysdykcji, w której ma się odbywać przetwarzanie danych, oraz – w sytuacji, gdy jest to wykonalne w praktyce – udzielanie pomocy podmiotom sektora publicznego w ustanawianiu mechanizmów technicznych umożliwiających przekazywanie wniosków ponownych użytkowników o wyrażenie zgody lub udzielenie pozwolenia.

e) udzielenie pomocy podmiotom sektora publicznego w zakresie oceny adekwatności zobowiązań umownych zaciągniętych przez ponownego użytkownika zgodnie z art. 5 ust. 10.

5. Każde państwo członkowskie powiadamia Komisję o danych identyfikacyjnych właściwych podmiotów wyznaczonych na podstawie ust. 1 do dnia 24 września 2023 r. Każde państwo członkowskie powiadamia również Komisję o wszelkich późniejszych zmianach danych identyfikacyjnych tych właściwych podmiotów.

Artykuł 8

Pojedyncze punkty informacyjne

1. Państwa członkowskie zapewniają, aby wszystkie istotne informacje dotyczące stosowania art. 5 i 6 były łatwo dostępne za pośrednictwem pojedynczego punktu informacyjnego. Państwa członkowskie ustanawiają podmiot lub wyznaczają istniejący podmiot lub strukturę jako pojedynczy punkt informacyjny. Pojedynczy punkt kontaktowy może być powiązany z sektorowymi, regionalnymi lub lokalnymi punktami informacyjnymi. Funkcje danego pojedynczego punktu informacyjnego mogą być zautomatyzowane, pod warunkiem że podmiot sektora publicznego zapewnienia odpowiednie wsparcie.

2. Pojedynczy punkt informacyjny jest właściwy do przyjmowania zapytań lub wniosków o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, i przekazuje je, jeśli jest to możliwe i odpowiednie za pomocą zautomatyzowanych środków, właściwym podmiotom sektora publicznego lub, w stosownych przypadkach, właściwym podmiotom, o których mowa w art. 7 ust. 1. Pojedynczy punkt informacyjny udostępnia za pomocą środków elektronicznych przeszukiwalny wykaz zasobów zawierający przegląd wszystkich dostępnych zasobów danych, w tym – w stosownych przypadkach – tych zasobów danych, które są dostępne w sektorowych, regionalnych lub lokalnych punktach informacyjnych, wraz z odpowiednimi informacjami opisującymi dostępne dane, w tym przynajmniej format i rozmiar danych oraz warunki ich ponownego wykorzystywania.

3. Pojedynczy punkt informacyjny może utworzyć odrębny, uproszczony i dobrze udokumentowany kanał informacyjny dla MŚP i przedsiębiorstw typu start-up, odpowiadający ich potrzebom i zdolnościom w zakresie składania wniosków o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1.

4. Komisja ustanawia europejski pojedynczy punkt dostępu oferujący elektroniczny przeszukiwalny rejestr danych dostępnych w krajowych pojedynczych punktach informacyjnych oraz dalsze informacje na temat sposobu wnioskowania o dane za pośrednictwem tych krajowych pojedynczych punktów informacyjnych.

Artykuł 9

Procedura składania wniosków o ponowne wykorzystywanie

1. O ile zgodnie z prawem krajowym nie zostały określone krótsze terminy, właściwe podmioty sektora publicznego lub właściwe podmioty, o których mowa w art. 7 ust. 1, podejmują decyzję w sprawie wniosku o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, w terminie dwóch miesięcy od dnia otrzymania wniosku.

W przypadku wyjątkowo obszernych i złożonych wniosków o ponowne wykorzystywanie, termin dwóch tygodni może zostać przedłużony do 30 dni. W takich przypadkach właściwe podmioty sektora publicznego lub właściwe podmioty, o których mowa w art. 7 ust. 1, powiadamiają jak najszybciej wnioskodawcę o tym, że do przeprowadzenia procedury potrzeba więcej czasu, wraz z uzasadnieniem tego opóźnienia.

2. Każda osoba fizyczna lub prawna, której bezpośrednio dotyczy decyzja, o której mowa w ust. 1, ma prawo do skutecznego środka zaskarżenia w państwie członkowskim, w którym znajduje się dany podmiot. Takie prawo do środka zaskarżenia musi zostać ustanowione w prawie krajowym i obejmować możliwość kontroli przez bezstronny podmiot posiadający odpowiednią wiedzę fachową – taki jak krajowy organ ochrony konkurencji, odpowiedni organ regulujący dostęp do dokumentów, organ nadzorczy ustanowiony zgodnie z rozporządzeniem (UE) 2016/679 lub krajowy organ sądowy – którego decyzje są wiążące dla danego podmiotu sektora publicznego lub właściwego podmiotu.

ROZDZIAŁ III

Wymogi dotyczące usług pośrednictwa danych

Artykuł 10

Usługi pośrednictwa danych

Świadczenie następujących usług pośrednictwa danych musi być zgodne z art. 12 i podlega procedurze zgłaszania:

a) usługi pośrednictwa między posiadaczami danych a potencjalnymi użytkownikami danych, w tym udostępnianie środków technicznych lub innych 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 innej specjalnej infrastruktury do stworzenia powiązań między posiadaczami danych a użytkownikami danych;

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

c) usługi świadczone przez spółdzielnie danych.

Artykuł 11

Zgłoszenia dokonywane przez dostawców usług pośrednictwa danych

1. Każdy dostawca usług pośrednictwa danych, który zamierza świadczyć usługi pośrednictwa danych, o których mowa w art. 10, dokonuje zgłoszenia do organu właściwego do spraw usług pośrednictwa danych, o którym mowa w art. 13.

2. Do celów niniejszego rozporządzenia uznaje się, że dostawca usług pośrednictwa danych posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim podlega jurysdykcji państwa członkowskiego, w którym ma swoją główną jednostkę organizacyjną, bez uszczerbku dla przepisów prawa Unii regulujących transgraniczne roszczenia odszkodowawcze i powiązane postępowania.

3. Dostawca usług pośrednictwa danych, który nie ma w Unii jednostki organizacyjnej, ale oferuje w Unii usługi pośrednictwa danych, o których mowa w 10, wyznacza przedstawiciela prawnego w jednym z państw członkowskich, w których usługi te są oferowane.

Do celów zapewnienia przestrzegania niniejszego rozporządzenia przedstawiciel prawny musi być upoważniony przez dostawcę usług pośrednictwa danych, by organy właściwe do spraw usług pośrednictwa danych lub osoby, których dane dotyczą, i posiadacze danych mogli się zwracać jednocześnie do przedstawiciela prawnego i dostawcy usług pośrednictwa danych albo do przedstawiciela prawnego zamiast do dostawcy usług pośrednictwa danych we wszystkich kwestiach dotyczących świadczonych usług pośrednictwa danych. Przedstawiciel prawny współpracuje z organami właściwymi do spraw usług pośrednictwa danych i na żądanie szczegółowo przedstawia im działania i przepisy wprowadzone przez dostawcę usług pośrednictwa danych w celu zapewnienia przestrzegania niniejszego rozporządzenia.

Uznaje się, że dostawca usług pośrednictwa danych podlega jurysdykcji tego państwa członkowskiego, w którym znajduje się jego przedstawiciel prawny. Wyznaczenie przedstawiciela prawnego przez dostawcę usług pośrednictwa danych pozostaje bez uszczerbku dla działań prawnych, które mogą zostać podjęte przeciwko dostawcy usług pośrednictwa danych.

4. Po dokonaniu zgłoszenia zgodnie z ust. 1 dostawca usług pośrednictwa danych może rozpocząć działalność z zastrzeżeniem warunków określonych w niniejszym rozdziale.

5. Zgłoszenie, o którym mowa w ust. 1, uprawnia dostawcę usług pośrednictwa danych do świadczenia usług pośrednictwa danych we wszystkich państwach członkowskich.

6. Zgłoszenie, o którym mowa w ust. 1, musi zawierać następujące informacje:

a) nazwę dostawcy usług pośrednictwa danych;

b) status prawny, formę prawną, strukturę własności oraz odpowiednie jednostki zależne dostawcy usług pośrednictwa danych, a w przypadku gdy dostawca usług pośrednictwa danych jest zarejestrowany w rejestrze handlowym lub innym podobnym rejestrze publicznym – jego numer rejestracyjny;

c) adres głównej jednostki organizacyjnej dostawcy usług pośrednictwa danych w Unii, o ile takowa istnieje, oraz, jeżeli ma to zastosowanie, drugorzędnego oddziału w innym państwie członkowskim lub adres przedstawiciela prawnego;

d) ogólnodostępną stronę internetową, na której można znaleźć kompletne i aktualne informacje na temat dostawcy usług pośrednictwa danych oraz jego działalności, w tym co najmniej informacje, o których mowa w lit. a), b), c) i f);

e) osoby wyznaczone do kontaktów przez dostawcę usług pośrednictwa danych i dane kontaktowe tych osób;

f) opis usługi pośrednictwa danych, którą dostawca usług pośrednictwa danych zamierza świadczyć, oraz wskazanie kategorii wymienionych w art. 10, do których należą takie usługi pośrednictwa danych;

g) planowaną datę rozpoczęcia działalności, jeżeli jest inna od daty zgłoszenia.

7. Organ właściwy do spraw usług pośrednictwa danych zapewnia, by procedura zgłoszenia była niedyskryminująca i nie zakłócała konkurencji.

8. Na wniosek dostawcy usług pośrednictwa danych organ właściwy do spraw usług pośrednictwa danych wydaje w terminie jednego tygodnia od zgłoszenia wypełnionego w sposób należyty i całkowity standardowe oświadczenie, potwierdzające, że dostawca usług pośrednictwa danych dokonał zgłoszenia, o którym mowa w ust. 1, oraz że zgłoszenie zawiera informacje, o których mowa w ust. 6.

9. Na wniosek dostawcy usług pośrednictwa danych, organ właściwy do spraw usług pośrednictwa danych potwierdza, że dostawca usług pośrednictwa danych przestrzega niniejszego artykułu oraz art. 12. Po otrzymaniu takiego potwierdzenia dostawca usług pośrednictwa danych może w swojej komunikacji pisemnej i ustnej posługiwać się oznakowaniem „uznany w Unii dostawca usług pośrednictwa danych" oraz używać wspólnego logo.

Aby zapewnić łatwą rozpoznawalność uznanych w Unii dostawców usług pośrednictwa danych w całej Unii, Komisja ustanawia w drodze aktów wykonawczych projekt wspólnego logo. Uznani w Unii dostawcy usług pośrednictwa danych wyraźnie eksponują wspólne logo na każdej publikacji w internecie i poza nim, odnoszącej się do ich działalności związanej z pośrednictwem danych.

Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 33 ust. 2.

10. Organ właściwy do spraw usług pośrednictwa danych niezwłocznie powiadamia drogą elektroniczną Komisję o każdym nowym zgłoszeniu. Komisja prowadzi i regularnie aktualizuje publiczny rejestr wszystkich dostawców usług pośrednictwa danych świadczących swoje usługi w Unii Informacje, o których mowa w ust. 6 lit. a), b), c), d),f) i g), są publikowane w publicznym rejestrze.

11. Organ właściwy do spraw usług pośrednictwa danych może pobierać opłaty za zgłoszenie zgodnie z prawem krajowym. Opłaty te muszą być proporcjonalne i obiektywne oraz muszą opierać się na kosztach administracyjnych związanych z monitorowaniem spełniania wymogów i innymi działaniami związanymi z kontrolą rynku prowadzonymi przez organy właściwe do spraw usług pośrednictwa danych w związku ze zgłoszeniami dotyczącymi usług pośrednictwa danych. W przypadku MŚP i przedsiębiorstw typu start-up organ właściwy do spraw usług pośrednictwa danych może pobierać obniżoną opłatę lub zrezygnować z pobrania opłaty.

12. Dostawcy usług pośrednictwa danych powiadamiają organy właściwe do spraw usług pośrednictwa danych o wszelkich zmianach informacji przekazanych na podstawie ust. 6 w terminie 14 dni od dnia, w którym nastąpiła zmiana.

13. W przypadku gdy dostawca usług pośrednictwa danych zaprzestaje swojej działalności, zgłasza ten fakt w terminie 15 dni odpowiedniemu organowi właściwemu do spraw pośrednictwa danych określonemu zgodnie z ust. 1, 2 i 3.

14. Organ właściwy do spraw usług pośrednictwa danych niezwłocznie powiadamia Komisję drogą elektroniczną o każdym zgłoszeniu, o którym mowa w ust. 12 i 13. Komisja odpowiednio aktualizuje publiczny rejestr dostawców usług pośrednictwa danych w Unii.

Artykuł 12

Warunki świadczenia usług pośrednictwa danych

Świadczenie usług pośrednictwa danych, o których mowa w art. 10, podlega następującym warunkom:

a) dostawca usług pośrednictwa danych nie może wykorzystywać danych będących przedmiotem świadczonych przez niego usług pośrednictwa danych do celów innych niż oddanie ich do dyspozycji użytkownikom danych, a usługi pośrednictwa danych świadczy poprzez odrębną osobę prawną;

b) warunki handlowe, w tym ceny, świadczenia usług pośrednictwa danych posiadaczowi danych lub użytkownikowi danych nie mogą być uzależnione od tego, czy posiadacz danych lub użytkownik danych korzysta z innych usług świadczonych przez tego samego dostawcę usług pośrednictwa danych powiązany podmiot, ani od tego w jakim zakresie posiadacz danych lub użytkownik danych korzysta z takich innych usług;

c) dane zebrane w odniesieniu do działalności osoby fizycznej lub prawnej w celu świadczenia usługi pośrednictwa danych, w tym dane dotyczące daty, godziny i geolokalizacji, czasu trwania działalności oraz połączeń ustanowionych przez osobę korzystającą z usługi pośrednictwa danych z innymi osobami fizycznymi lub prawnymi, mogą być wykorzystywane wyłącznie do celów rozwoju tej usługi pośrednictwa danych, co może obejmować wykorzystywanie danych do wykrywania oszustw lub na potrzeby cyberbezpieczeństwa; udostępnia się je na żądanie posiadaczom danych;

d) dostawca usług pośrednictwa danych ułatwia wymianę danych w formacie, w jakim otrzymuje je od osoby, której dane dotyczą, lub od posiadacza danych, konwertuje te dane do określonych formatów wyłącznie w celu zwiększenia interoperacyjności w obrębie sektorów i między sektorami lub na wniosek użytkownika danych lub w przypadku, gdy jest to wymagane przez prawo Unii, lub w celu zapewnienia harmonizacji z międzynarodowymi lub europejskimi standardami danych oraz oferuje osobom, których dane dotyczą, lub posiadaczom danych możliwość rezygnacji z tych konwersji, chyba że taka konwersja jest wymagana przez prawo Unii;

e) usługi pośrednictwa danych mogą obejmować oferowanie posiadaczom danych lub osobom, których dane dotyczą, dodatkowych specjalnych narzędzi i usług ułatwiających wymianę danych, takich jak tymczasowe przechowywanie, kuratorstwo, konwersja, anonimizacja i pseudonimizacja; przy czym z tych narzędzi korzysta się wyłącznie na wyraźny wniosek lub za zgodą posiadacza danych lub osoby, której dane dotyczą, a narzędzia osób trzecich oferowane w tym kontekście nie mogą wykorzystywać danych do innych celów;

f) dostawca usług pośrednictwa danych zapewnia, aby procedura dostępu do usługi była sprawiedliwa, przejrzysta i niedyskryminująca zarówno dla osób, których dane dotyczą, jak i posiadaczy danych, a także użytkowników danych, w tym w odniesieniu do cen i warunków świadczenia usługi;

g) dostawca usług pośrednictwa danych wprowadza procedury mające na celu zapobieganie praktykom stanowiącym oszustwo lub nadużycie w odniesieniu do podmiotów ubiegających się o dostęp za pośrednictwem jego usług pośrednictwa danych;

h) dostawca usług pośrednictwa danych zapewnia w przypadku niewypłacalności odpowiednią ciągłość świadczenia swoich usług pośrednictwa danych, a w przypadku gdy takie usługi pośrednictwa danych zapewniają przechowywanie danych, wprowadza mechanizmy umożliwiające posiadaczom danych i użytkownikom danych uzyskanie dostępu do ich danych, ich przekazywanie lub pobieranie, zaś w przypadku świadczenia takich usług pośrednictwa danych między osobami, których dane dotyczą, a użytkownikami danych umożliwiające osobom, których dane dotyczą, wykonywanie przysługujących im praw;

i) dostawca usług pośrednictwa danych podejmuje odpowiednie środki w celu zapewnienia interoperacyjności z innymi usługami pośrednictwa danych, między innymi za pomocą standardów otwartych, które są powszechnie stosowane w sektorze działalności danego dostawcy usług pośrednictwa danych;

j) dostawca usług pośrednictwa danych wprowadza odpowiednie środki techniczne, prawne i organizacyjne w celu zapobiegania niezgodnemu z prawem Unii lub z prawem krajowym danego państwa członkowskiego przekazywaniu danych nieosobowych lub dostępowi do tych danych;

k) dostawca usług pośrednictwa danych informuje niezwłocznie posiadaczy danych w przypadku gdy nastąpiły niedozwolone przekazanie, dostęp lub wykorzystanie danych nieosobowych, którymi się podzielił;

l) dostawca usług pośrednictwa danych podejmuje niezbędne środki w celu zapewnienia odpowiedniego poziomu bezpieczeństwa w zakresie przechowywania, przetwarzania i przesyłania danych nieosobowych; dostawca usług pośrednictwa danych zapewnia również najwyższy poziom bezpieczeństwa przy przechowywaniu i przesyłaniu istotnych dla konkurencji szczególnie chronionych informacji;

m) dostawca usług pośrednictwa danych oferujący usługi osobom, których dane dotyczą, działa w najlepszym interesie tych osób w przypadku gdy ułatwia wykonywanie przysługujących im praw, w szczególności zapewniając – zanim osoby, których dane dotyczą, wyrażą zgodę – informacje oraz, w stosownych przypadkach, doradztwo w zwięzły, przejrzysty, zrozumiały i łatwo dostępny sposób co do zamierzonego wykorzystywania danych przez użytkowników danych oraz co do standardowych warunków związanych z takim wykorzystywaniem;

n) w przypadku gdy dostawca usług pośrednictwa danych zapewnia narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub pozwoleń na przetwarzanie danych udostępnionych przez posiadaczy danych, określa on – w stosownych przypadkach – jurysdykcję państwa trzeciego, w których ma odbywać się wykorzystywanie danych, oraz dostarcza osobom, których dane dotyczą, narzędzia umożliwiające zarówno wyrażenie, jak i wycofanie zgody, a posiadaczom danych – narzędzia umożliwiające zarówno udzielenie, jak i wycofanie pozwolenia na przetwarzanie danych;

o) dostawca usług pośrednictwa danych prowadzi rejestr zdarzeń dotyczących działalności w zakresie pośrednictwa danych.

Artykuł 13

Organy właściwe do spraw usług pośrednictwa danych

1. Każde państwo członkowskie wyznacza co najmniej jeden organ właściwy do wykonywania zadań związanych z procedurą zgłaszania dotyczącą usług pośrednictwa danych i powiadamia Komisję o danych identyfikacyjnych tych właściwych organów do dnia 24 września 2023 r. Każde państwo członkowskie powiadamia również Komisję o wszelkich późniejszych zmianach danych identyfikacyjnych tych właściwych organów.

2. Organy właściwe do spraw usług pośrednictwa danych muszą spełniać wymogi określone art. 26.

3. Uprawnienia organów właściwych do spraw usług pośrednictwa danych nie naruszają uprawnień organów ochrony danych, krajowych organów ochrony konkurencji, organów odpowiedzialnych za cyberbezpieczeństwo oraz innych odpowiednich organów sektorowych. Zgodnie z zakresem właściwości każdego z nich na podstawie prawa Unii i prawa krajowego organy te ustanawiają ścisłą współpracę i wymieniają się informacjami, które są niezbędne do wykonywania ich zadań w odniesieniu do dostawców usług pośrednictwa danych, oraz dbają o spójność w zakresie decyzji podejmowanych w związku ze stosowaniem niniejszego rozporządzenia.

Artykuł 14

Monitorowanie spełniania wymogów

1. Organy właściwe do spraw usług pośrednictwa danych monitorują i nadzorują spełnianie przez dostawców usług pośrednictwa danych wymogów niniejszego rozdziału. Organy właściwe do spraw usług pośrednictwa danych mogą również monitorować i nadzorować spełnianie tych wymogów przez dostawców usług pośrednictwa danych na podstawie wniosków osób fizycznych lub prawnych.

2. Organy właściwe do spraw usług pośrednictwa danych są uprawnione do zwracania się do dostawców usług pośrednictwa danych lub ich przedstawicieli prawnych z wnioskiem o wszelkie informacje niezbędne do zweryfikowania spełniania wymogów określonych w niniejszym rozdziale. Każdy wniosek o informacje musi być proporcjonalny do wykonywanego zadania i musi być uzasadniony.

3. W przypadku ustalenia przez organ właściwy do spraw usług pośrednictwa danych, że dostawca usług pośrednictwa danych nie spełnia co najmniej jednego wymogu określonego w niniejszym rozdziale, organ ten powiadamia dostawcę usług pośrednictwa danych o swoich ustaleniach i daje mu możliwość przedstawienia swojego stanowiska w terminie 30 dni od dnia otrzymania powiadomienia.

4. Organ właściwy do spraw usług pośrednictwa danych jest uprawniony do żądania zaprzestania naruszeń, o których mowa w ust. 3, w rozsądnym terminie lub – w przypadku poważnego naruszenia – niezwłocznie, a także przyjmuje odpowiednie i proporcjonalne środki służące spełnianiu wymogów. W związku z tym organy właściwe do spraw usług pośrednictwa danych są w stosownych przypadkach uprawnione do:

a) nakładania, w drodze procedur administracyjnych, odstraszających kar pieniężnych, które mogą obejmować kary okresowe i kary z mocą wsteczną, lub wszczynania postępowań sądowych w celu nałożenia grzywien;

b) żądania przesunięcia rozpoczęcia lub zawieszenia świadczenia usługi pośrednictwa danych do czasu wprowadzenia zmian w warunkach, zgodnie z żądaniem organu właściwego do spraw usług pośrednictwa danych; lub

c) żądania zaprzestania świadczenia usługi pośrednictwa danych w przypadku gdy poważne lub powtarzające się naruszenia nie zostały usunięte pomimo uprzedniego powiadomienia zgodnie z ust. 3.

Organ właściwy do spraw usług pośrednictwa danych zwraca się do Komisji o usunięcie dostawcy usług pośrednictwa danych z rejestru dostawców usług pośrednictwa danych po nakazaniu zaprzestania świadczenia usługi pośrednictwa danych zgodnie z akapitem pierwszym lit. c).

Jeżeli dostawca usług pośrednictwa danych usunie naruszenia, dokonuje do organu właściwego do spraw usług pośrednictwa danych ponownego zgłoszenia. Organ właściwy do spraw usług pośrednictwa danych powiadamia Komisję o każdym ponownym zgłoszeniu.

5. W przypadku gdy niemający jednostki organizacyjnej w Unii dostawca usług pośrednictwa danych nie wyznaczy przedstawiciela prawnego lub przedstawiciel prawny nie dostarczy na żądanie organu właściwego do spraw usług pośrednictwa danych niezbędnych informacji, które w pełni wykazują przestrzeganie niniejszego rozporządzenia, organ właściwy do spraw usług pośrednictwa danych jest uprawniony do przesunięcia rozpoczęcia lub zawieszenia świadczenia usługi pośrednictwa danych do czasu wyznaczenia przedstawiciela prawnego lub dostarczenia niezbędnych informacji.

6. Organy właściwe do spraw usług pośrednictwa danych niezwłocznie powiadamiają zainteresowanego dostawcę usług pośrednictwa danych o środkach nałożonych zgodnie z ust. 4 i 5 oraz o powodach ich nałożenia, jak również o niezbędnych środkach, jakie należy wprowadzić w celu usunięcia odpowiednich niedociągnięć, i wyznaczają rozsądny – ale nie dłuższy niż 30 dni – termin na zastosowanie tych środków.

7. Jeżeli dostawca usług pośrednictwa danych ma swoją główną jednostkę organizacyjną lub swojego przedstawiciela prawnego w państwie członkowskim, ale świadczy usługi w innych państwach członkowskich, organ właściwy do spraw usług pośrednictwa danych państwa członkowskiego, w którym znajduje się główna jednostka organizacyjna lub przedstawiciel prawny, oraz organy właściwe do spraw usług pośrednictwa danych innych państw członkowskich, w których dostawca świadczy usługi, współpracują i udzielają sobie wzajemnej pomocy. Taka pomoc i współpraca mogą obejmować wymianę między zainteresowanymi organami właściwymi do spraw usług pośrednictwa danych informacji do celów ich zadań na podstawie niniejszego rozporządzenia oraz uzasadnione wnioski o wprowadzenie środków, o których mowa w niniejszym artykule.

W przypadku gdy organ właściwy do spraw usług pośrednictwa danych jednego państwa członkowskiego zwraca się o pomoc do organu właściwego do spraw usług pośrednictwa danych innego państwa członkowskiego, przedkłada przy tym uzasadniony wniosek. Organ właściwy do spraw usług pośrednictwa danych, do którego zwrócono się z takim wnioskiem, udziela odpowiedzi bez zbędnej zwłoki i w terminie proporcjonalnym do pilności wniosku.

Wszelkie informacje wymieniane w ramach pomocy, o którą zwraca się i której udziela się na podstawie niniejszego ustępu, są wykorzystywane jedynie w odniesieniu do kwestii, w której o nie wnioskowano.

Artykuł 15

Wyjątki

Niniejszego rozdziału nie stosuje się do uznanych organizacji altruizmu danych ani do innych podmiotów o charakterze niekomercyjnym w zakresie, w jakim ich działalność polega na gromadzeniu danych do celów leżących w interesie ogólnym, udostępnianych przez osoby fizyczne lub prawne w myśl altruizmu danych, chyba że te organizacje i podmioty mają na celu ustanowienie stosunków handlowych między nieokreśloną liczbą osób, których dane dotyczą, i posiadaczy danych z jednej strony oraz użytkownikami danych z drugiej strony.

ROZDZIAŁ IV

Altruizm danych

Artykuł 16

Krajowe rozwiązania w zakresie altruizmu danych

Państwa członkowskie mogą wprowadzić rozwiązania organizacyjne lub techniczne sprzyjające altruizmowi danych. W tym celu państwa członkowskie mogą określić krajowe polityki w zakresie altruizmu danych. Te krajowe polityki mogą w szczególności udzielać pomocy osobom, których dane dotyczą, w dobrowolnym udostępnianiu – do celów altruizmu danych – dotyczących ich danych osobowych będących w posiadaniu podmiotów sektora publicznego, a także określać niezbędne informacje na temat ponownego wykorzystywania ich danych w interesie ogólnym, które to informacje muszą być przekazywane osobom, których dane dotyczą.

Jeżeli państwo członkowskie opracowuje takie polityki krajowe, powiadamia o tym Komisję.

Artykuł 17

Publiczne rejestry uznanych organizacji altruizmu danych

1. Każdy organ właściwy do spraw rejestracji organizacji altruizmu danych prowadzi i regularnie aktualizuje publiczny krajowy rejestr uznanych organizacji altruizmu danych.

2. Komisja prowadzi do celów informacyjnych publiczny unijny rejestr uznanych organizacji altruizmu danych. Dany podmiot może w swojej komunikacji pisemnej i ustnej posługiwać się oznakowaniem „uznana w Unii organizacja altruizmu danych" oraz używać wspólnego logo, pod warunkiem rejestracji w publicznym krajowym rejestrze uznanych organizacji altruizmu danych zgodnie z art. 18.

Aby zapewnić łatwą rozpoznawalność uznanych organizacji altruizmu danych, Komisja ustanawia w drodze aktów wykonawczych projekt wspólnego logo. Uznane organizacje altruizmu danych wyraźnie eksponują wspólne logo na każdej publikacji w internecie i poza nim, odnoszącej się do ich działalności w zakresie altruizmu danych. Wspólnemu logo towarzyszy kod QR z linkiem do publicznego unijnego rejestru uznanych organizacji altruizmu danych.

Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 33 ust. 2.

Artykuł 18

Ogólne wymogi dotyczące rejestracji

Do zarejestrowania się w publicznym krajowym rejestrze uznanych organizacji altruizmu danych uprawniony jest podmioty, który:

a) prowadzi działalność w zakresie altruizmu danych;

b) jest osobą prawną ustanowioną zgodnie z prawem krajowym do realizacji celów leżących w interesie ogólnym określonych, w stosownych przypadkach, w prawie krajowym;

c) prowadzi działalność o charakterze niekomercyjnym i jest prawnie niezależny od jakiegokolwiek podmiotu nastawionego na zysk;

d) prowadzi działalność w zakresie altruizmu danych, wykorzystując przy tym strukturę funkcjonalnie odrębną od pozostałej działalności tego podmiotu;

e) przestrzega zbioru zasad, o którym mowa w art. 22 ust. 1, najpóźniej 18 miesięcy po dniu wejścia w życie aktów delegowanych, o których mowa w tym ustępie.

Artykuł 19

Rejestracja uznanych organizacji altruizmu danych

1. Podmiot, który spełnia wymogi art. 18, może złożyć wniosek o rejestrację w publicznym krajowym rejestrze uznanych organizacji altruizmu danych w tym państwie członkowskim, w którym ma jednostkę organizacyjną

2. Podmiot, który spełnia wymogi art. 18 i ma swoje jednostki organizacyjne w więcej niż jednym państwie członkowskim, może złożyć wniosek o rejestrację w publicznym krajowym rejestrze uznanych organizacji altruizmu danych w tym państwie członkowskim, w którym znajduje się jego główna jednostka organizacyjna.

3. Podmiot, który spełnia wymogi art. 18, ale nie ma w Unii jednostki organizacyjnej, wyznacza przedstawiciela prawnego w jednym z państw członkowskich, w których oferowane są usługi oparte na altruizmie danych.

Do celów zapewnienia przestrzegania niniejszego rozporządzenia przedstawiciel prawny musi być upoważniony przez podmiot, by organy właściwe do spraw rejestracji organizacji altruizmu danych lub osoby, których dane dotyczą, i posiadacze danych mogli się zwracać jednocześnie do przedstawiciela prawnego i podmiotu albo do przedstawiciela prawnego zamiast do podmiotu we wszystkich kwestiach dotyczących tego podmiotu. Przedstawiciel prawny współpracuje z organami właściwymi do spraw rejestracji organizacji altruizmu danych i na żądanie szczegółowo przedstawia im działania i przepisy wprowadzone przez dany podmiot w celu zapewnienia przestrzegania niniejszego rozporządzenia.

Uznaje się, że podmiot podlega jurysdykcji tego państwa członkowskiego, w którym znajduje się jego przedstawiciel prawny. Taki podmiot może złożyć wniosek o rejestrację w publicznym krajowym rejestrze uznanych organizacji altruizmu danych w tym państwie członkowskim. Wyznaczenie przedstawiciela prawnego przez podmiot pozostaje bez uszczerbku dla działań prawnych, które mogą zostać podjęte przeciwko podmiotowi.

4. Wnioski o rejestrację, o których mowa w ust. 1, 2 i 3, zawierają następujące informacje:

a) nazwę podmiotu;

b) status prawny oraz formę prawną podmiotu, a w przypadku gdy podmiot jest zarejestrowany w publicznym rejestrze krajowym – jego numer rejestracyjny;

c) statut podmiotu, stosownie do przypadku;

d) 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;

f) ogólnodostępną stronę internetową, na której można znaleźć kompletne i aktualne informacje o podmiocie oraz jego działalności, w tym co najmniej informacje, o których mowa w lit. a), b), d), e) i h);

g) osoby wyznaczone do kontaktów przez podmiot i dane kontaktowe tych osób;

h) cele leżące w interesie ogólnym, które podmiot zamierza wspierać przy gromadzeniu danych;

i) charakter danych, które podmiot zamierza kontrolować lub przetwarzać, a w przypadku danych osobowych – wskazanie ich kategorii;

j) wszelkie inne dokumenty, które wykazują, że wymagania art. 18 zostały spełnione.

5. W przypadku gdy podmiot przedłożył wszystkie niezbędne informacje zgodnie z ust. 4, organ właściwy do spraw rejestracji organizacji altruizmu danych – po przeprowadzeniu oceny wniosku o rejestrację i stwierdzeniu, że podmiot ten spełnia wymogi art. 18 – rejestruje ten podmiot w publicznym krajowym rejestrze uznanych organizacji altruizmu danych w terminie 12 tygodni od otrzymania wniosku o rejestrację. Rejestracja jest ważna we wszystkich państwach członkowskich.

Organ właściwy do spraw rejestracji organizacji altruizmu danych powiadamia Komisję o wszelkich rejestracjach. Komisja uwzględnia rejestrację w publicznym unijnym rejestrze uznanych organizacji altruizmu danych.

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

7. Uznana organizacja altruizmu danych powiadamia odpowiedni organ właściwy do spraw rejestracji uznanych organizacji altruizmu danych o wszelkich zmianach informacji przekazanych zgodnie z ust. 4 w terminie 14 dni od dnia, w którym nastąpiła zmiana.

Organ właściwy do spraw rejestracji organizacji altruizmu danych niezwłocznie powiadamia Komisję o każdym takim powiadomieniu drogą elektroniczną. Na podstawie takiego powiadomienia Komisja niezwłocznie aktualizuje publiczny unijny rejestr uznanych organizacji altruizmu danych.

Artykuł 20

Wymogi dotyczące przejrzystości

1. Uznana organizacja altruizmu danych prowadzi pełną i dokładną dokumentację dotyczącą:

a) wszystkich osób fizycznych lub prawnych, które otrzymały możliwość przetwarzania danych będących w posiadaniu tej uznanej organizacji altruizmu danych, oraz ich dane kontaktowe;

b) daty lub czasu trwania przetwarzania danych osobowych lub wykorzystywania danych nieosobowych;

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

d) opłat uiszczonych przez osoby fizyczne lub prawne przetwarzające dane.

2. Uznana organizacja altruizmu danych sporządza i przekazuje odpowiedniemu organowi właściwemu do spraw rejestracji organizacji altruizmu danych roczne sprawozdanie z działalności, które zawiera co najmniej:

a) informację o działalności uznanej organizacji altruizmu danych;

b) opis sposobu, w jaki w ciągu danego roku obrotowego wspierano cele leżące w interesie ogólnym, dla których dane były gromadzone;

c) wykaz wszystkich osób fizycznych i prawnych, którym zezwolono na przetwarzanie posiadanych danych, w tym skrócony opis celów leżących w interesie ogólnym, którym służy takie przetwarzanie 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 przetwarzania danych, na które zezwoliła uznana organizacja altruizmu danych;

e) informacje o źródłach dochodów uznanej organizacji altruizmu danych, w szczególności o wszystkich dochodach z tytułu zezwolenia na dostęp do danych, oraz o wydatkach.

Artykuł 21

Szczególne wymogi dotyczące zabezpieczenia praw i interesów osób, których dane dotyczą, oraz posiadaczy danych w odniesieniu do ich danych

1. Uznana organizacja altruizmu danych informuje w jasny i łatwo zrozumiały sposób osoby, których dane dotyczą, lub posiadaczy danych, przed przetwarzaniem ich danych, o:

a) celach leżących w interesie ogólnym oraz, w stosownych przypadkach, o konkretnym, wyraźnym i zgodnym z prawem celu przetwarzania danych osobowych, dla których uznana organizacja altruizmu danych pozwala na przetwarzanie danych osób, których dane dotyczą, lub posiadaczy danych przez użytkowników danych;

b) miejscu przetwarzania oraz celach leżących w interesie ogólnym, dla których uznana organizacja altruizmu danych pozwala na przetwarzanie w państwie trzecim, jeżeli przetwarzania dokonuje uznana organizacja altruizmu danych.

2. Uznana organizacja altruizmu danych nie może wykorzystywać danych do celów innych niż cele leżące w interesie ogólnym, w odniesieniu do których osoba, której dane dotyczą, lub posiadacz danych zezwolili na przetwarzanie. Uznana organizacja altruizmu danych nie może stosować wprowadzających w błąd praktyk marketingowych, by nakłaniać do przekazywania danych.

3. Uznana organizacja altruizmu danych zapewnia narzędzia umożliwiające uzyskanie zgody od osób, których dane dotyczą, lub pozwoleń na przetwarzanie danych udostępnianych przez posiadaczy danych. Uznana organizacja altruizmu danych zapewnia także narzędzia umożliwiające łatwe wycofanie takiej zgody lub takiego pozwolenia.

4. Uznana organizacja altruizmu danych podejmuje środki w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przechowywania i przetwarzania danych nieosobowych, które zgromadziła w ramach altruizmu danych.

5. Uznana organizacja altruizmu danych niezwłocznie informuje posiadaczy danych w przypadku gdy nastąpiły niedozwolone przekazanie, dostęp lub wykorzystanie danych nieosobowych, którymi się podzieliła.

6. W przypadku gdy uznana organizacja altruizmu danych ułatwia osobom trzecim przetwarzanie danych, w tym poprzez zapewnianie narzędzi umożliwiających uzyskanie zgody od osób, których dane dotyczą, lub pozwoleń na przetwarzanie danych udostępnionych przez posiadaczy danych, określa – w stosownych przypadkach –jurysdykcję państwa trzeciego, w których ma się odbywać wykorzystywanie danych.

Artykuł 22

Zbiór zasad

1. Komisja przyjmuje zgodnie z art. 32 akty delegowane w celu uzupełnienia niniejszego rozporządzenia przez ustanowienie zbioru zasad określającego:

a) odpowiednie wymogi informacyjne w celu zapewnienia, aby osoby, których dane dotyczą, i posiadacze danych otrzymali przed wyrażeniem zgody lub udzieleniem pozwolenia na altruizm danych wystarczająco szczegółowe, jasne i przejrzyste informacje dotyczące wykorzystywania danych, narzędzi wyrażania zgody lub udzielania pozwolenia i ich wycofywania oraz środków podejmowanych w celu uniknięcia nieprawidłowego wykorzystywania danych, którymi podzielono się z organizacją altruizmu danych;

b) odpowiednie wymogi techniczne i wymogi bezpieczeństwa, by zapewnić odpowiedni poziom bezpieczeństwa przy przechowywaniu i przetwarzaniu danych, a także w odniesieniu do narzędzi wyrażania zgody lub udzielania pozwolenia i ich wycofywania;

c) plany działania w zakresie komunikacji zakładające multidyscyplinarne podejście do budowania wśród odpowiednich interesariuszy – w szczególności posiadaczy danych i osób, których dane dotyczą, potencjalnie dzielących się swoimi danymi – świadomości na temat altruizmu danych, określania mianem „uznanej w Unii organizacji altruizmu danych" oraz na temat zbioru zasad;

d) zalecenia dotyczące odpowiednich standardów interoperacyjności.

2. Zbiór zasad, o którym mowa w ust. 1, jest przygotowywany w ścisłej współpracy z organizacjami altruizmu danych i odpowiednimi interesariuszami.

Artykuł 23

Organy właściwe do spraw rejestracji organizacji altruizmu danych

1. Każde państwo członkowskie wyznacza co najmniej jeden właściwy organ odpowiedzialny za prowadzenie jego publicznego krajowego rejestru uznanych organizacji altruizmu danych.

Organy właściwe do spraw rejestracji organizacji altruizmu danych muszą spełniać wymogi określone w art. 26.

2. Każde państwo członkowskie powiadamia Komisję o danych identyfikacyjnych swoich organów właściwych do spraw rejestracji organizacji altruizmu danych do dnia 24 września 2023 r. Każde państwo członkowskie powiadamia również Komisję o wszelkich późniejszych zmianach danych identyfikacyjnych tych właściwych organów.

3. Organ właściwy do spraw rejestracji organizacji altruizmu danych w państwie członkowskim wykonuje swoje zadania we współpracy z odpowiednim organem ochrony danych, jeżeli zadania takie związane są z przetwarzaniem danych osobowych, oraz z odpowiednimi organami sektorowymi tego państwa członkowskiego.

Artykuł 24

Monitorowanie spełniania wymogów

1. Organy właściwe do spraw rejestracji organizacji altruizmu danych monitorują i nadzorują spełnianie przez uznane organizacje altruizmu danych wymogów określonych w niniejszym rozdziale. Organ właściwy do spraw rejestracji organizacji altruizmu danych może również monitorować i nadzorować spełnianie tych wymogów przez takie uznane organizacje altruizmu danych na podstawie wniosków osób fizycznych lub prawnych.

2. Organy właściwe do spraw rejestracji organizacji altruizmu danych są uprawnione do zwracania się do uznanych organizacji altruizmu danych z wnioskiem o informacje niezbędne do zweryfikowania spełniania wymogów określonych w niniejszym rozdziale. Każdy wniosek o informacje musi być proporcjonalny do wykonywanego zadania i musi być uzasadniony.

3. W przypadku ustalenia przez organ właściwy do spraw rejestracji organizacji altruizmu danych, że uznana organizacja altruizmu danych nie spełnia co najmniej jednego wymogu określonego w niniejszym rozdziale, organ ten powiadamia tę uznaną organizację altruizmu danych o swoich ustaleniach i daje jej możliwość przedstawienia swojego stanowiska w terminie 30 dni od dnia otrzymania powiadomienia.

4. Organ właściwy do spraw rejestracji organizacji altruizmu danych jest uprawniony do żądania zaprzestania naruszeń, o których mowa w ust. 3, niezwłocznie albo w rozsądnym terminie, a także przyjmuje odpowiednie i proporcjonalne środki służące zapewnieniu spełnianiu wymogów.

5. Jeżeli uznana organizacja altruizmu danych nie spełnia co najmniej jednego wymogu określonego w niniejszym rozdziale, nawet po otrzymaniu od organu właściwego do spraw rejestracji organizacji altruizmu danych powiadomienia zgodnie z ust. 3, ta uznana organizacja altruizmu danych:

a) traci prawo do posługiwania się w swojej komunikacji pisemnej i ustnej oznakowaniem „uznana w Unii organizacja altruizmu danych";

b) zostaje usunięta z odpowiedniego publicznego krajowego rejestru uznanych organizacji altruizmu danych oraz z publicznego unijnego rejestru uznanych organizacji altruizmu danych.

Decyzja o pozbawieniu prawa do posługiwania się oznakowaniem „uznana w Unii organizacja altruizmu danych" podjęta na podstawie akapitu pierwszego lit. a) jest podawana do wiadomości publicznej przez organ właściwy do spraw rejestracji organizacji altruizmu danych.

6. Jeżeli uznana organizacja altruizmu danych ma swoją główną jednostkę organizacyjną lub swojego przedstawiciela prawnego w państwie członkowskim, ale prowadzi działalność w innych państwach członkowskich, organ właściwy do spraw rejestracji organizacji altruizmu danych państwa członkowskiego, w którym znajdują się główna jednostka organizacyjna lub przedstawiciel prawny, oraz organy właściwe do spraw rejestracji organizacji altruizmu danych innych państw członkowskich, w których podmiot prowadzi działalność, współpracują i udzielają sobie wzajemnej pomocy. Taka pomoc i współpraca mogą obejmować wymianę między zainteresowanymi organami właściwymi do spraw rejestracji organizacji altruizmu danych informacji do celów ich zadań na podstawie niniejszego rozporządzenia oraz uzasadnione wnioski o wprowadzenie środków, o których mowa w niniejszym artykule.

W przypadku gdy organ właściwy do spraw rejestracji organizacji altruizmu danych jednego państwa członkowskiego zwraca się o pomoc do organu właściwego do spraw rejestracji organizacji altruizmu danych innego państwa członkowskiego, przedkłada przy tym uzasadniony wniosek. Organ właściwy do spraw rejestracji organizacji altruizmu danych, do którego zwrócono się z takim wnioskiem, udziela odpowiedzi bez zbędnej zwłoki i w terminie proporcjonalnym do pilności wniosku.

Wszelkie informacje wymieniane w ramach pomocy, o którą zwraca się i której udziela się na podstawie niniejszego ustępu, są wykorzystywane jedynie w odniesieniu do kwestii, w której o nie wnioskowano.

Artykuł 25

Europejski formularz zgody do celów altruizmu danych

1. Aby ułatwić gromadzenie danych w ramach altruizmu danych, Komisja – po konsultacji z Europejską Radą Ochrony Danych, z uwzględnieniem stanowiska Europejskiej Rady ds. Innowacji w zakresie Danych i z należyty udziałem odpowiednich interesariuszy – przyjmuje akty wykonawcze w celu ustanowienia i opracowania europejskiego formularza zgody do celów altruizmu danych. Formularz umożliwia uzyskiwanie we wszystkich państwach członkowskich zgody lub pozwolenia w jednolitym formacie. Te akty wykonawcze przyjmuje się zgodnie z procedurą doradczą, o której mowa w art. 33 ust. 2.

2. W europejskim formularzu zgody do celów altruizmu danych stosuje się podejście modułowe umożliwiające dostosowanie do potrzeb konkretnych sektorów i poszczególnych celów.

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

4. Formularz musi być udostępniony w sposób umożliwiający wydruk na papierze, być łatwo zrozumiały, jak również dostępny w formie elektronicznej, nadającej się do odczytu maszynowego.

ROZDZIAŁ V

Właściwe organy i przepisy proceduralne

Artykuł 26

Wymogi dotyczące właściwych organów

1. Organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych muszą być prawnie odrębne i funkcjonalnie niezależne od dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych. Funkcje organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych może wykonywać ten sam organ. Państwa członkowskie mogą w tym celu ustanowić jeden nowy organ lub większą ich liczbę albo opierać się na istniejących organach.

2. Organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych wykonują swoje zadania w sposób bezstronny, przejrzysty, spójny, wiarygodny i terminowy. Przy wykonywaniu swoich zadań dbają one o ochronę uczciwej konkurencji i niedyskryminację.

3. Członkowie kadry kierowniczej wyższego szczebla i personel odpowiedzialny za wykonywanie odpowiednich zadań organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych nie mogą być projektantami, producentami, dostawcami, instalatorami, nabywcami, właścicielami, użytkownikami ani osobami odpowiedzialnymi za utrzymanie usług, które oceniają, nie mogą też być przedstawicielem upoważnionym przez którąkolwiek z tych osób. Nie wyklucza to korzystania z ocenianych usług, które są niezbędne do wykonywania działań organu właściwego do spraw usług pośrednictwa danych ani organu właściwego do spraw rejestracji organizacji altruizmu danych, lub korzystania z takich usług do celów osobistych.

4. Członkowie kadry kierowniczej wyższego szczebla i personel organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych nie angażują się w żadną działalność, która mogłaby zagrozić niezależności ich osądów lub uczciwości w odniesieniu do powierzonych im działań związanych z oceną.

5. Organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych mają do dyspozycji odpowiednie zasoby finansowe i ludzkie do wykonywania powierzonych im zadań, w tym niezbędną wiedzę techniczną i niezbędne zasoby techniczne.

6. Organy właściwe do spraw usług pośrednictwa danych i organy właściwe do spraw rejestracji organizacji altruizmu danych państwa członkowskiego dostarczają Komisji i organom właściwym do spraw usług pośrednictwa danych i organom właściwym do spraw rejestracji organizacji altruizmu danych innych państw członkowskich, na uzasadniony wniosek i niezwłocznie, informacje niezbędne do wykonywania ich zadań na podstawie niniejszego rozporządzenia. W przypadku gdy organ właściwy do spraw usług pośrednictwa danych lub organ właściwy do spraw rejestracji organizacji altruizmu danych uznają wnioskowane informacje za poufne zgodnie z przepisami prawa Unii i prawa krajowego dotyczącymi tajemnicy handlowej i zawodowej, Komisja i wszelkie inne zainteresowane organy właściwe do spraw usług pośrednictwa danych lub organy właściwe do spraw rejestracji organizacji altruizmu danych zapewniają poufność takich informacji.

Artykuł 27

Prawo do wniesienia skargi

1. Osoby fizyczne i prawne mają prawo, w odniesieniu do każdej sprawy wchodzącej w zakres stosowania niniejszego rozporządzenia, do wniesienia indywidualnej lub – w stosownym przypadkach – zbiorowej skargi do odpowiedniego organu właściwego do spraw usług pośrednictwa danych przeciwko dostawcy usług pośrednictwa danych lub do organu właściwego do spraw rejestracji organizacji altruizmu danych przeciwko uznanej organizacji altruizmu danych.

2. Organ właściwy do spraw usług pośrednictwa danych lub organ właściwy do spraw rejestracji organizacji altruizmu danych, do którego wniesiono skargę, informuje skarżącego o:

a) przebiegu postępowania i podjętej decyzji; oraz

b) środkach ochrony prawnej przed sądem określonych w art. 28.

Artykuł 28

Prawo do skutecznego środka ochrony prawnej przed sądem

1. Niezależnie od administracyjnych lub innych pozasądowych środków ochrony prawnej osoby fizyczne i prawne, których to dotyczy, mają prawo do skutecznego środka ochrony prawnej przed sądem przeciwko prawnie wiążącym decyzjom, o których mowa w art. 14, wydanych przez organy właściwe do spraw usług pośrednictwa danych, w ramach zarządzania systemem zgłaszania dostawców usług pośrednictwa danych, kontrolowania tego systemu i egzekwowania go, oraz przeciwko prawnie wiążącym decyzjom, o których mowa w art. 19 i 24, wydanych przez organy właściwe do spraw rejestracji organizacji altruizmu danych w ramach monitorowania uznanych organizacji altruizmu danych.

2. Postępowanie wszczęte na podstawie niniejszego artykułu toczy się przed sądem lub trybunałem państwa członkowskiego, w którym znajduje się organ właściwy do spraw usług pośrednictwa danych lub organ właściwy do spraw rejestracji organizacji altruizmu danych, przeciwko któremu wniesiony został indywidualnie lub – w stosownych przypadkach – wspólnie przez przedstawicieli osoby fizycznej lub prawnej lub kilku takich osób środek ochrony prawnej przed sądem.

3. W przypadku gdy organ właściwy do spraw usług pośrednictwa danych lub organ właściwy do spraw rejestracji organizacji altruizmu danych pozostanie bezczynny w odniesieniu do skargi, osoba fizyczna i prawna, których to dotyczy, ma zgodnie z prawem krajowym prawo do skutecznego środka ochrony prawnej przed sądem albo możliwość skorzystania z kontroli przez bezstronny podmiot dysponujący odpowiednią wiedzą fachową.

ROZDZIAŁ VI

Europejska Rada ds. Innowacji w zakresie Danych

Artykuł 29

Europejska Rada ds. Innowacji w zakresie Danych

1. Komisja ustanawia Europejską Radę ds. Innowacji w zakresie Danych w postaci grupy ekspertów składającej się z przedstawicieli organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych ze wszystkich państw członkowskich, Europejskiej Rady Ochrony Danych, Europejskiego Inspektora Ochrony Danych, ENISA, Komisji, pełnomocnika UE ds. MŚP lub przedstawiciela wyznaczonego przez sieć pełnomocników ds. MŚP i z innych przedstawicieli odpowiednich podmiotów w poszczególnych sektorach, a także podmiotów dysponujących szczególną wiedzą fachową. Przy powoływaniu poszczególnych ekspertów Komisja dąży do osiągnięcia wśród członków grupy ekspertów równowagi płci i równowagi geograficznej.

2. Europejska Rada ds. Innowacji w zakresie Danych składa się z co najmniej trzech podgrup:

a) podgrupy organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych, z myślą o wykonywaniu zadań zgodnie z art. 30 lit. a, c), j) i k);

b) podgrupy ds. dyskusji technicznych dotyczących normalizacji, przenoszenia i interoperacyjności zgodnie z art. 30 lit. f) i g);

c) podgrupy ds. zaangażowania interesariuszy składającej się z odpowiednich przedstawicieli przemysłu, środowisk naukowych i akademickich, społeczeństwa obywatelskiego, organizacji normalizacyjnych, odpowiednich wspólnych europejskich przestrzeni danych oraz innych odpowiednich interesariuszy i osób trzecich doradzających Europejskiej Radzie ds. Innowacji w zakresie Danych w zakresie zadań zgodnie z art. 30 lit. d), e), f), g) i h).

3. Posiedzeniom Europejskiej Rady ds. Innowacji w zakresie Danych przewodniczy Komisja.

4. Europejską Radę ds. Innowacji w zakresie Danych wspiera sekretariat zapewniony przez Komisję.

Artykuł 30

Zadania Europejskiej Rady ds. Innowacji w zakresie Danych

Europejska Rada ds. Innowacji w zakresie Danych ma następujące zadania:

a) doradzanie Komisji i udzielanie jej pomocy w odniesieniu do rozwijania spójnej praktyki podmiotów sektora publicznego i właściwych podmiotów, o których mowa w art. 7 ust. 1, w zakresie rozpatrywania wniosków o ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1;

b) doradzanie Komisji i udzielanie jej pomocy w odniesieniu do rozwijania spójnej praktyki w zakresie altruizmu danych w całej Unii;

c) doradzanie Komisji i udzielanie jej pomocy w odniesieniu do rozwijania spójnej praktyki organów właściwych do spraw usług pośrednictwa danych i organów właściwych do spraw rejestracji organizacji altruizmu danych w zakresie stosowania wymogów mających zastosowanie do dostawców usług pośrednictwa danych oraz uznanych organizacji altruizmu danych;

d) doradzanie Komisji i udzielanie jej pomocy w odniesieniu do opracowywania spójnych wytycznych dotyczących sposobów zapewniania jak najlepszej ochrony w kontekście niniejszego rozporządzenia szczególnie chronionych danych handlowych o charakterze nieosobowym, w szczególności tajemnic handlowych, a także danych nieosobowych przedstawiających treści chronione prawami własności intelektualnej, przed niezgodnym z prawem dostępem, który może prowadzić do kradzieży własności intelektualnej lub szpiegostwa przemysłowego;

e) doradzanie Komisji i udzielanie jej pomocy w odniesieniu do opracowywania spójnych wytycznych dotyczących wymogów w zakresie cyberbezpieczeństwa w odniesieniu do wymiany i przechowywania danych;

f) doradzanie Komisji, w szczególności z uwzględnieniem wkładu organizacji normalizacyjnych, w zakresie ustalania priorytetów dotyczących norm międzysektorowych, które mają być stosowane i opracowywane do celów wykorzystywania danych i międzysektorowego dzielenia się danymi między powstającymi wspólnymi europejskimi przestrzeniami danych, międzysektorowego porównywania i wymiany najlepszych praktyk w odniesieniu do wymogów sektorowych w zakresie bezpieczeństwa oraz procedur dostępu, z uwzględnieniem specyficznych dla danego sektora działań normalizacyjnych, w szczególności w zakresie wyjaśniania i rozróżniania, które normy i praktyki są międzysektorowe, a które sektorowe;

g) udzielanie pomocy Komisji, w szczególności z uwzględnieniem wkładu organizacji normalizacyjnych, w rozwiązywaniu problemu fragmentacji rynku wewnętrznego i gospodarki danych na rynku wewnętrznym przez zwiększanie transgranicznej międzysektorowej interoperacyjności danych, jak również usług dzielenia się danymi między różnymi sektorami i w różnych dziedzinach, w oparciu o istniejące normy europejskie, międzynarodowe lub krajowe, między innymi w celu pobudzania tworzenia wspólnych europejskich przestrzeni danych;

h) proponowanie wytycznych dotyczących wspólnych europejskich przestrzeni danych, oznaczających interoperacyjne ramy wspólnych norm i praktyk, specyficzne dla danego celu lub sektora bądź międzysektorowe, służących dzieleniu się danymi lub ich wspólnemu przetwarzaniu na potrzeby między innymi opracowywania nowych produktów i usług, badań naukowych lub inicjatyw społeczeństwa obywatelskiego; przy czym takie wspólne normy i praktyki uwzględniają istniejące normy, są zgodne z regułami konkurencji i zapewniają wszystkim uczestnikom niedyskryminacyjny dostęp w celu ułatwiania dzielenia się danymi w Unii i wykorzystania potencjału istniejących i przyszłych przestrzeni danych, obejmując między innymi:

   (i) normy międzysektorowe, które mają być stosowane i opracowywane do celów wykorzystywania danych i międzysektorowego dzielenia się danymi, międzysektorowego porównywania i wymiany najlepszych praktyk w odniesieniu do sektorowych wymogów bezpieczeństwa oraz procedur dostępu, z uwzględnieniem specyficznych dla danego sektora działań normalizacyjnych, w szczególności w zakresie wyjaśniania i rozróżniania, które normy i praktyki są międzysektorowe, a które sektorowe;

   (ii) wymogi związane z usuwaniem barier utrudniających wejście na rynek i z zapobieganiem efektom lock-in, aby zapewnić uczciwą konkurencję i interoperacyjność;

(iii) odpowiedni poziom ochrony zgodnego z prawem przekazywania danych do państw trzecich, w tym zabezpieczenia przed przekazywaniem zabronionym w prawie Unii;

(iv) odpowiednią i niedyskryminacyjną reprezentację odpowiednich interesariuszy w zarządzaniu wspólnymi europejskimi przestrzeniami danych;

(v) obowiązek stosowania się do wymogów w zakresie cyberbezpieczeństwa zgodnie z prawem Unii;

i) ułatwianie współpracy między państwami członkowskimi w zakresie ustalenia zharmonizowanych warunków pozwalających na ponowne wykorzystywanie kategorii danych, o których mowa w art. 3 ust. 1, będących w posiadaniu podmiotów sektora publicznego na całym rynku wewnętrznym;

j) ułatwianie współpracy między organami właściwymi do spraw usług pośrednictwa danych i organami właściwymi do spraw rejestracji organizacji altruizmu danych, poprzez budowanie zdolności i wymianę informacji, w szczególności poprzez ustanowienie metod skutecznej wymiany informacji dotyczących procedury zgłaszania dostawców usług pośrednictwa danych oraz rejestracji i monitorowania uznanych organizacji altruizmu danych, w tym koordynacji w zakresie ustalania opłat lub kar, a także ułatwianie współpracy między organami właściwymi do spraw usług pośrednictwa danych i organami właściwymi do spraw rejestracji organizacji altruizmu danych w zakresie międzynarodowego dostępu do danych i ich przekazywania;

k) doradzanie Komisji i udzielanie jej pomocy w odniesieniu do dokonywania oceny odnośnie do przyjmowania aktów wykonawczych, o których mowa w art. 5 ust. 11 i 12;

l) doradzanie Komisji i udzielanie jej pomocy w odniesieniu do opracowywania europejskiego formularza zgody do celów altruizmu danych zgodnie z art. 25 ust. 1;

m) doradzanie Komisji w zakresie poprawy międzynarodowego otoczenia regulacyjnego w zakresie danych nieosobowych, z uwzględnieniem normalizacji.

ROZDZIAŁ VII

Dostęp międzynarodowy i przekazywanie międzynarodowe

Artykuł 31

Dostęp międzynarodowy i przekazywanie międzynarodowe

1. Podmiot sektora publicznego, osoba fizyczna lub prawna, którym przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału II, dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych wprowadzają wszelkie uzasadnione środki techniczne, prawne i organizacyjne, w tym uzgodnienia umowne, w celu zapobiegania międzynarodowemu przekazywaniu danych nieosobowych będących w posiadaniu Unii lub międzynarodowemu dostępowi administracji rządowej do takich danych, w przypadku gdy takie przekazywanie lub dostęp pozostawały w sprzeczności z prawem Unii lub prawem krajowym danego państwa członkowskiego, bez uszczerbku dla ust. 2 lub 3.

2. Orzeczenia lub wyroki sądu lub trybunału państwa trzeciego oraz decyzje organu administracyjnego państwa trzeciego nakazujące podmiotowi sektora publicznego, osobie fizycznej lub prawnej, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału II, dostawcy usług pośrednictwa danych lub uznanej organizacji altruizmu danych przekazanie objętych zakresem stosowania niniejszego rozporządzenia danych nieosobowych będących w posiadaniu Unii lub udzielenie do nich dostępu uznaje się lub podlegać wykonuje wyłącznie wtedy, gdy są oparte na obowiązującej między wzywającym państwem trzecim a Unią umowie międzynarodowej, takiej jak umowa o wzajemnej pomocy prawnej, lub na umowie tego rodzaju między wzywającym państwem trzecim a państwem członkowskim.

3. Przy braku umowy międzynarodowej, o której mowa w ust. 2 niniejszego artykułu, w przypadku gdy podmiot sektora publicznego, osoba fizyczna lub prawna, której przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału II, dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych jest adresatem orzeczenia lub wyroku sądu lub trybunału państwa trzeciego lub decyzji organu administracyjnego państwa trzeciego nakazującej przekazanie objętych zakresem stosowania niniejszego rozporządzenia danych nieosobowych będących w posiadaniu Unii lub udzielenia do nich dostępu, a zastosowanie się do takiej decyzji wiązałoby się dla adresata z ryzykiem pozostawania w sprzeczności z prawem Unii lub z prawem krajowym danego państwa członkowskiego, przekazanie takich danych organowi państwa trzeciego lub udzielenie mu dostępu do takich danych może mieć miejsce wyłącznie gdy:

a) system państwa trzeciego wymaga, aby powody i proporcjonalność takiego orzeczenia, wyroku lub decyzji zostały określone oraz aby takie orzeczenie, wyrok lub decyzja miały szczególny charakter, na przykład poprzez ustanowienie wystarczającego związku z niektórymi osobami podejrzanymi lub naruszeniami;

b) uzasadniony sprzeciw adresata podlega kontroli właściwego sądu lub trybunału państwa trzeciego; oraz

c) właściwy sąd lub trybunał państwa trzeciego wydający orzeczenie lub wyrok lub dokonujący kontroli decyzji organu administracyjnego jest upoważniony na podstawie prawa tego państwa trzeciego do należytego uwzględnienia odpowiednich interesów prawnych dostawcy danych chronionych na podstawie prawa Unii lub prawa krajowego danego państwa członkowskiego.

4. Jeżeli warunki określone w ust. 2 lub 3 są spełnione, podmiot sektora publicznego, osoba fizyczna lub prawna, którym przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału II, dostawca usług pośrednictwa danych lub uznana organizacja altruizmu danych dostarczają minimalną ilość danych dozwoloną w odpowiedzi na wniosek, na podstawie racjonalnej interpretacji wniosku.

5. Podmiot sektora publicznego, osoba fizyczna lub prawna, którym przyznano prawo do ponownego wykorzystywania danych na podstawie rozdziału II, dostawca usług pośrednictwa danych oraz uznana organizacja altruizmu danych informują – przed zastosowaniem się do tego wniosku – posiadacza danych o istnieniu wniosku organu administracyjnego państwa trzeciego o dostęp do jego danych, z wyjątkiem gdy wniosek służy celom ścigania przestępstw, i tak długo, jak jest to konieczne do zachowania skuteczności działań w zakresie ścigania przestępstw.

ROZDZIAŁ VIII

Przekazanie uprawnień i procedura komitetowa

Artykuł 32

Wykonywanie przekazanych uprawnień

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

2. Uprawnienia do przyjmowania aktów delegowanych, o których mowa w art. 5 ust. 13 i art. 22 ust. 1, powierza się Komisji na czas nieokreślony od dnia 23 czerwca 2022 r.

3. Przekazanie uprawnień, o którym mowa w art. 5 ust. 13 i art. 22 ust. 1, 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 późniejszym terminie określonym w tej decyzji. 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. 13 lub art. 22 ust. 1 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 33

Procedura komitetowa

1. Komisję wspomaga komitet. Komitet ten jest komitetem 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 odesłania do niniejszego ustępu stosuje się art. 5 rozporządzenia (UE) nr 182/2011.

ROZDZIAŁ IX

Przepisy końcowe i przejściowe

Artykuł 34

Kary

1. Państwa członkowskie ustanawiają przepisy dotyczące kar mających zastosowanie w przypadku naruszeń obowiązków dotyczących przekazywania danych nieosobowych do państw trzecich zgodnie z art. 5 ust. 14 i art. 31, obowiązku dostawców usług pośrednictwa danych dotyczącego zgłoszeń zgodnie z art. 11, warunków świadczenia usług pośrednictwa danych zgodnie z art. 12 oraz warunków rejestracji jako uznana organizacja altruizmu danych zgodnie z art. 18, 20, 21 i 22 oraz podejmują wszelkie niezbędne środki w celu zapewnienia ich wykonywania. Przewidziane kary muszą być skuteczne, proporcjonalne i odstraszające. W przepisach dotyczących kar państwa członkowskie uwzględniają zalecenia Europejskiej Rady ds. Innowacji w zakresie Danych. Państwa członkowskie powiadamiają Komisję o tych przepisach i środkach do dnia 24 września 2023 r., a także powiadamiają ją niezwłocznie o wszelkich późniejszych zmianach, które ich dotyczą.

2. Przy nakładaniu na dostawców usług pośrednictwa danych i uznane organizacje altruizmu danych kar za naruszenia przepisów niniejszego rozporządzenia, państwa członkowskie – stosownie do przypadku – uwzględniają następujące niewyczerpujące i orientacyjne kryteria:

a) charakter, wagę, skalę i czas trwania naruszenia;

b) działania podjęte przez dostawcę usług pośrednictwa danych lub uznaną organizację altruizmu danych, aby złagodzić lub naprawić szkodę spowodowaną naruszeniem;

c) wcześniejsze naruszenia ze strony dostawcy usług pośrednictwa danych lub uznanej organizacji altruizmu danych;

d) korzyści majątkowe uzyskane przez dostawcę usług pośrednictwa danych lub uznaną organizację altruizmu danych lub straty, których uniknęli, wskutek naruszenia, o ile takie korzyści lub straty można oszacować w sposób wiarygodny;

e) inne czynniki obciążające lub łagodzące mające zastosowanie w okolicznościach danej sprawy.

Artykuł 35

Ocena i przegląd

Do dnia 24 września 2025 r. Komisja przeprowadzi ocenę niniejszego rozporządzenia i przedłoży Parlamentowi Europejskiemu i Radzie, a także Europejskiemu Komitetowi Ekonomiczno-Społecznemu sprawozdanie na temat głównych ustaleń. W razie potrzeby sprawozdaniu towarzyszą wnioski ustawodawcze.

W sprawozdaniu ocenia się w szczególności:

a) stosowanie i funkcjonowanie przepisów dotyczących kar ustanowionych przez państwa członkowskie zgodnie z art. 34;

b) poziom przestrzegania niniejszego rozporządzenia przez przedstawicieli prawnych niemających jednostki organizacyjnej w Unii dostawców usług pośrednictwa danych lub uznanych organizacji altruizmu danych oraz poziom egzekwowania kar nałożonych na tych dostawców i te organizacje;

c) rodzaj organizacji altruizmu danych zarejestrowanych zgodnie z rozdziałem IV oraz przegląd celów leżących w interesie ogólnym, którym służy dzielenie się danymi, z myślą o ustanowieniu jasnych kryteriów w tym zakresie.

Państwa członkowskie przekazują Komisji informacje niezbędne do przygotowania tego sprawozdania.

Artykuł 36

Zmiana rozporządzenia (UE) 2018/1724

W tabeli w załączniku II do rozporządzenia (UE) 2018/1724 wpis „Rozpoczęcie, prowadzenie i zakończenie działalności gospodarczej" otrzymuje brzmienie:

Zdarzenia życiowe	Procedury	Oczekiwany wynik z zastrzeżeniem, w stosownych przypadkach, oceny wniosku przez właściwy organ zgodnie z prawem krajowym
Rozpoczęcie, prowadzenie i zakończenie działalności gospodarczej	Powiadomienie o działalności gospodarczej, zezwolenie na prowadzenie działalności gospodarczej, zmiana działalności gospodarczej i zakończenie takiej działalności nieobejmujące procedur dotyczących niewypłacalności lub likwidacji, z wyłączeniem procedur dotyczących początkowej rejestracji działalności gospodarczej w rejestrze przedsiębiorców oraz z wyłączeniem procedur dotyczących zakładania spółek oraz późniejszego zgłaszania składania dokumentów przez spółki, w rozumieniu art. 54 akapit drugi TFUE	Potwierdzenie otrzymania zgłoszenia lub zmiany działalności gospodarczej, lub wniosku o zezwolenie na prowadzenie działalności gospoda
	Rejestracja pracodawcy (osoby fizycznej) w obowiązkowych systemach emerytalno-rentowych i ubezpieczeniowych	Potwierdzenie rejestracji lub numer rejestracyjny ubezpieczenia społecznego
	Rejestracja pracowników w obowiązkowych systemach emerytalno-rentowych i ubezpieczeniowy	Potwierdzenie rejestracji lub numer rejestracyjny ubezpieczenia społecznego
	Złożenie deklaracji podatkowej dotyczącej podatku od osób prawnych	Potwierdzenie przyjęcia deklaracji podatkowej
	Zgłoszenie w systemach zabezpieczenia społecznego rozwiązania umowy z pracownikiem, z wyłączeniem procedur grupowego rozwiązywania umów z pracownikami	Potwierdzenie otrzymania zgłoszenia
	Płatność składek na ubezpieczenia społeczne pracowników	Pokwitowanie lub inna forma potwierdzenia płatności składek na ubezpieczenia społeczne pracowników
	Zgłoszenie dostawcy usług pośrednictwa danych	Potwierdzenie przyjęcia zgłoszenia
	Rejestracja jako uznana w Unii organizacja altruizmu danych	Potwierdzenie rejestracji

Artykuł 37

Przepisy przejściowe

Podmioty świadczące w dniu 23 czerwca 2022 r. usługi pośrednictwa danych, o których mowa w art. 10, muszą spełnić obowiązki określone w rozdziale III do dnia 24 września 2025 r.

Artykuł 38

Wejście w życie i rozpoczęcie stosowania

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

Niniejsze rozporządzenie stosuje się od dnia 24 września 2023 r.

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

Sporządzono w Brukseli dnia 30 maja 2022 r.

W imieniu Parlamentu Europejskiego	*W imieniu Rady*
Przewodnicząca	*Przewodniczący*
R. METSOLA	B. LE MAIRE