ROZPORZĄDZENIE W SPRAWIE EUROPEJSKIEGO ZARZĄDZANIA DANYMI (DGA)

Komentarz

redakcja naukowa
Agnieszka Piskorz-Ryń, Marlena Sakowska-Baryła

Michał Czerniawski, Bogdan Fischer
Krzysztof Izdebski, Mariusz Jabłoński, Natalia Kohtamäki
Dominika Kuźnicka-Błaszkowska, Iga Małobęcka-Szwast
Agnieszka Piskorz-Ryń, Marlena Sakowska-Baryła
Krzysztof Wygoda

KOMENTARZE

Wolters Kluwer

ROZPORZĄDZENIE W SPRAWIE EUROPEJSKIEGO ZARZĄDZANIA DANYMI (DGA)

Komentarz

redakcja naukowa
Agnieszka Piskorz-Ryń, Marlena Sakowska-Baryła

Michał Czerniawski, Bogdan Fischer
Krzysztof Izdebski, Mariusz Jabłoński, Natalia Kohtamäki
Dominika Kuźnicka-Błaszkowska, Iga Małobęcka-Szwast
Agnieszka Piskorz-Ryń, Marlena Sakowska-Baryła
Krzysztof Wygoda

KOMENTARZE

Wolters Kluwer

WARSZAWA 2025

Stan prawny na 10 lipca 2025 r.

Recenzentka
dr hab. Agnieszka Grzelak, prof. Akademii Leona Koźmińskiego w Warszawie

Wydawczyni
Anna Kubuj-Kacperek

Redaktorka prowadząca
Paulina Staniszewska-Chudzik

Opracowanie redakcyjne
Dagmara Wachna

Projekt okładek serii
Wojtek Janikowski, Przemek Dębowski

Poszczególne części opracowali:
Michał Czerniawski – art. 27–28; art. 31; art. 34–35
Bogdan Fischer – art. 2 podrozdz. 20, art. 3 podrozdz. 5–6; art. 5 podrozdz. 10
Krzysztof Izdebski – art. 3 podrozdz. 10; art. 4
Krzysztof Izdebski, Agnieszka Piskorz-Ryń – art. 2 podrozdz. 19
Mariusz Jabłoński, Krzysztof Wygoda – art. 2 podrozdz. 10, 15, 17; art. 15–17; art. 25–26
Natalia Kohtamäki – art. 1 podrozdz. 7; art. 13; art. 29–30
Dominika Kuźnicka-Błaszkowska – art. 18–21; art. 23–24
Iga Małobęcka-Szwast – art. 2 podrozdz. 11–12, 16, 21; art. 10–12; art. 32–33
A. Piskorz-Ryń – art. 1 podrozdz. 1–5, art. 2 podrozdz. 1–2, 14, 18; art. 3 podrozdz. 1–3, 7–9; art. 5 podrozdz. 1–2; art. 6–9
Marlena Sakowska-Baryła – art. 1 podrozdz. 6, 8; art. 2 podrozdz. 3–9, 13; art. 3 podrozdz. 4; art. 5 podrozdz. 3, 5–9; art. 14; art. 22
Marlena Sakowska-Baryła, Bogdan Fischer – art. 5 podrozdz. 4

ISBN 978-83-8390-769-7 *ISBN PDF-a: 978-83-8390-889-2*

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. +48 728 313 462
e-mail: PL-ksiazki@wolterskluwer.com
księgarnia internetowa www.profinfo.pl

Spis treści

Wykaz skrótów

Akty prawne

DGA, rozporządzenie	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/868 z 30.05.2022 r. w sprawie europejskiego zarządzania danymi i zmieniające rozporządzenie (UE) 2018/1724 (akt w sprawie zarządzania danymi) (Dz.Urz. UE L 152, s. 1, ze zm.)
dyrektywa 2019/1024, dyrektywa o otwartych danych	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.06.2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.Urz. UE L 172, s. 56)
dyrektywa DSM	–	dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130, s. 92)
k.k.	–	ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2025 r. poz. 383)
k.p.a.	–	ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2024 r. poz. 572 ze zm.)
Konstytucja RP	–	Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. Nr 78, poz. 483 ze zm.)
RODO	–	rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1, ze zm.)
TFUE	–	Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 7.06.2016, s. 47)
TUE	–	Traktat o Unii Europejskiej (wersja skonsolidowana: Dz.Urz. UE C 202 z 7.06.2016, s. 13)
u.f.p.	–	ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2024 r. poz. 1530 ze zm.)

u.o.d.p.w., ustawa o otwartych danych – ustawa z 11.08.2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2023 r. poz. 1524)
u.s.p. – ustawa z 29.06.1995 r. o statystyce publicznej (Dz.U. z 2024 r. poz. 1799)
u.z.n.k. – ustawa z 16.04.1993 r. o zwalczaniu nieuczciwej konkurencji (Dz.U. z 2022 r. poz. 1233 ze zm.)

Czasopisma i publikatory

ONSAiWSA – Orzecznictwo Naczelnego Sądu Administracyjnego i wojewódzkich sądów administracyjnych
OSNC – Orzecznictwo Sądu Najwyższego. Izba Cywilna
OTK-A – Orzecznictwo Trybunału Konstytucyjnego; zbiór urzędowy, Seria A

Inne

EROD – Europejska Rada Ochrony Danych
i.s.p. – informacja sektora publicznego
MŚP – małe i średnie przedsiębiorstwa
NSA – Naczelny Sąd Administracyjny
PSP – podmioty sektora publicznego
PUODO – Prezes Urzędu Ochrony Danych Osobowych
SA – Sąd Apelacyjny
SN – Sąd Najwyższy
TK – Trybunał Konstytucyjny
TS – Trybunał Sprawiedliwości
WSA – Wojewódzki Sąd Administracyjny

Wstęp

Akt w sprawie zarządzania danymi – powszechnie znany jako DGA (Data Governance Act), jest jednym z kluczowych elementów strategii Unii Europejskiej dotyczącej tworzenia jednolitego rynku danych. Celem DGA jest zwiększenie dostępności danych oraz ułatwienie ich ponownego wykorzystywania przy jednoczesnym zapewnieniu wysokiego poziomu zaufania i ochrony danych osobowych oraz tajemnic, oraz innych kategorii informacji chronionych. Niniejszy komentarz zawiera analizę poszczególnych przepisów rozporządzenia, co powinno ułatwić jego bezpośrednie stosowanie w polskim porządku prawnym zarówno przez administrację publiczną, jak i przedsiębiorców zainteresowanych pozyskiwaniem danych dla potrzeb nowych technologii, w tym sztucznej inteligencji. Celem opracowania jest popularyzacja koncepcji altruizmu danych i wyjaśnienie zasad jej realizacji, więc jest ono adresowane również do osób fizycznych i organizacji zainteresowanych tym modelem dzielenia się danymi w interesie publicznym i dla dobra wspólnego.

Treść rozporządzenia odnosi się do różnych zagadnień, łącząc w sobie prawo informacyjne, w tym otwartość danych, z tematyką danych osobowych i zagadnieniami praw własności intelektualnej, tajemnic prawnie chronionych oraz problematyki świadczenia usług pośrednictwa danych. Publikacja obejmuje szczegółową analizę tego, w jaki sposób w przepisach DGA realizowane jest założenie stworzenia ram zaufania, przejrzystości i współpracy między podmiotami publicznymi i prywatnymi, a także między państwami członkowskimi UE.

Akt w sprawie zarządzania danymi ma wspierać innowacyjność, ochronę danych oraz rozwój jednolitego rynku danych, który ma być podstawą konkurencyjnej i zrównoważonej gospodarki cyfrowej w Europie. W komentarzu dokonano drobiazgowego umówienia przepisów, które służą wykonaniu tych założeń. DGA ma na celu stworzenie solidnych podstaw dla gospodarki opartej na danych poprzez zwiększenie zaufania do ich udostępniania – poprzez

ustanowienie przejrzystych zasad udostępniania danych, szczególnie tych, które są chronione z uwagi na tajemnice prawnie chronione, prawo własności intelektualnej, ochronę danych osobowych czy interes publiczny.

Dzięki DGA łatwiejsze ma być ponowne wykorzystywanie danych sektora publicznego, wspieranie powstawania nowych usług pośrednictwa danych, promowanie altruizmu danych – czyli dobrowolnego udostępniania danych przez obywateli lub organizacje w celu wspierania badań naukowych lub działań służących dobru wspólnemu. Wszystkie te kwestie zostały szczegółowo omówione w komentarzu wraz ze wskazaniem otoczenia regulacyjnego, analizą zagadnień praktycznych, wskazaniem relacji pomiędzy DGA a przepisami innych aktów, których unormowania dotyczą podobnych obszarów. DGA ma ogromne znaczenie zarówno dla administracji publicznej, jak i sektora prywatnego. Organy administracji mogą w nowy sposób wykorzystywać posiadane dane do wspierania innowacji, przedsiębiorstwa zyskują dostęp do nowych zasobów danych w sposób bezpieczny i zgodny z przepisami, osoby fizyczne natomiast mogą mieć większą kontrolę nad swoimi danymi i pewność, że są one przetwarzane w sposób zgodny z zasadami etyki i prawa.

Akt w sprawie zarządzania danymi to przełomowa regulacja, która ma stanowić fundament dla europejskiej gospodarki danych, a także tworzyć ramy zaufania, przejrzystości i współpracy między podmiotami publicznymi i prywatnymi. W publikacji wiele miejsca poświęcono zatem praktycznej stronie realizacji tych celów. Lektura komentarza powinna pomóc w zrozumieniu tego, w jaki sposób DGA ma wspierać innowacyjność, ochronę danych oraz rozwój jednolitego rynku danych, który ma być podstawą konkurencyjnej i zrównoważonej gospodarki cyfrowej w Europie.

Opracowanie jest adresowane do osób odpowiedzialnych za zarządzanie danymi, ochronę danych osobowych, otwieranie danych i ponowne wykorzystywanie informacji sektora publicznego, a także za pozyskiwanie danych osobowych i nieosobowych do różnych celów, w tym do budowania innowacyjnych usług oraz tworzenia modeli sztucznej inteligencji. Książka zawiera cenne wskazówki dla tych, którzy chcieliby dowiedzieć się więcej na temat altruizmu danych oraz usług pośrednictwa, wytyczne dla inspektorów ochrony danych, osób odpowiedzialnych za transformację cyfrową, ochronę baz danych, własności przemysłowej i praw autorskich, jak również specjalistów ds. bezpieczeństwa informacji oraz przetwarzania danych nieosobowych. To lektura dla sędziów, radców prawnych, adwokatów, naukowców i studentów zajmujących się zagadnieniami z zakresu zarządzania danymi, prawa ochrony danych osobowych, nowych technologii, prawa europejskiego, osób odpowiedzialnych za współpracę w biznesie i administracji publicznej.

Publikacja powstała dzięki współpracy licznej grupy autorów zajmujących się tematyką ochrony danych osobowych, nowymi technologiami, bezpieczeństwem informacji, prawem europejskim, informacyjnym, administracyjnym oraz konstytucyjnym – znanych i cenionych ekspertów oraz praktyków mających ogromne doświadczenie w prawnej obsłudze procesów zarządzania danymi – zarówno w sektorze prywatnym, jak i publicznym.

Jako redaktorki naukowe komentarza wszystkim Autorkom i Autorom składamy serdeczne podziękowania za zaangażowanie i wkład w jego powstanie oraz za bardzo dobrą współpracę.

dr hab. Agnieszka Piskorz-Ryń, prof. UKSW
dr hab. Marlena Sakowska-Baryła, prof. UŁ

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)

(Dz.Urz.UE L z dnia 3 czerwca 2022 r.)

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 startup – 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.
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.

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 danyc h) 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.

(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 nie- osobowe 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.

(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.

(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 startup. 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.

(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 nie- osobowe 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 przechowywanych na terenie Unii uzyskiwany w państwach trzecich lub przekazywanie tych danych do państw trzecich miały miejsce wyłącznie zgodnie z prawem Unii lub prawem krajowym danego państwa członkowskiego.[27]

(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 startup, 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 startup 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[28] 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[29] 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 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 startup 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 MŚP, przedsiębiorstw typu startup 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 interesa- riuszy 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[30]. 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.

(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[31]. 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 nie- osobowych 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[32].

(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[33] i (UE) 2019/882[34]. 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,

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

[1] Dz.Urz. UE C 286 z 16.7.2021, s. 38.

[2] Stanowisko Parlamentu Europejskiego z 6.04.2022 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz decyzja Rady z 16.05.2022 r.

[3] Zalecenie Komisji 2003/361/WE z 6.05.2003 r. w sprawie definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.Urz. UE L 124 z 20.5.2003, s. 36).

[4] Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z 9.03.2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej (Dz.Urz. UE L 88 z 4.4.2011, s. 45).

[5] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/1239 z 20.06.2019 r. ustanawiające europejski system morskich pojedynczych punktów kontaktowych i uchylające dyrektywę 2010/65/UE (Dz.Urz. UE L 198 z 25.7.2019, s. 64).

[6] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2020/1056 z 15.07.2020 r. w sprawie elektronicznych informacji dotyczących transportu towarowego (Dz.Urz. UE L 249 z 31.7.2020, s. 33).

[7] Dyrektywa Parlamentu Europejskiego i Rady 2010/40/UE z 7.07.2010 r. w sprawie ram wdrażania inteligentnych systemów transportowych w obszarze transportu drogowego oraz interfejsów z innymi rodzajami transportu (Dz.Urz. UE L 207 z 6.8.2010, s. 1).

[8] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z 11.03.2009 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.Urz. UE L 87 z 31.3.2009, s. 164).

[9] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/858 z 30.05.2018 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.Urz. UE L 151 z 14.6.2018, s. 1).

[10] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.Urz. UE L 303 z 28.11.2018, s. 59).

[11] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L 178 z 17.7.2000, s. 1).

[12] Dyrektywa 2001/29/WE Parlamentu Europejskiego i Rady z 22.05.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz. UE L 167 z 22.6 2001, s. 10).

[13] Dyrektywa 2004/48/WE Parlamentu Europejskiego i Rady z 29.04.2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.Urz. UE L 157 z 30.4.2004, s. 45).

[14] Dyrektywa 2007/2/WE Parlamentu Europejskiego i Rady z 14.03.2007 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 20.05.2015 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.Urz. UE L 141 z 5.6.2015, s. 73).

[16] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.06.2016 r. w sprawie ochrony niejawnego know-how i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.Urz. UE L 157 z 15.6.2016, s. 1).

[17] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2017/1132 z 14.06.2017 r. w sprawie niektórych aspektów prawa spółek (Dz.Urz. UE L 169 z 30.6.2017, s. 46).

[18] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130 z 17.5.2019, s. 92).

[19] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.06.2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.Urz. UE L 172 z 26.6.2019, s. 56).

[20] Dyrektywa Parlamentu Europejskiego i Rady 2009/81/WE z 13.07.2009 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.Urz. UE L 216 z 20.8.2009, s. 76).

[21] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119 z 4.5.2016, s. 1).

[22] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 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.Urz. UE L 295 z 21.11.2018, s. 39).

[23] Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 201 z 31.7.2002, s. 37).

[24] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 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.Urz. UE L 119 z 4.5.2016, s. 89).

[25] Rozporządzenie Komisji (UE) nr 557/2013 z 17.06.2013 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.Urz. UE L 164 z 18.6.2013, s. 16).

[26] Dyrektywa 96/9/WE Parlamentu Europejskiego i Rady z 11.03.1996 r. w sprawie ochrony prawnej baz danych (Dz.Urz. UE L 77 z 27.3.1996, s. 20).

[27] Motyw 22 zmieniony przez sprostowanie z 21.12.2023 r. (Dz.Urz. UE L z 2023 r. poz. 90204) zmieniające nin. rozporządzenie 23.06.2022 r.

[28] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z 15.05.2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012 (Dz.Urz. UE L 173 z 12.6.2014, s. 84).

[29] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z 25.11.2015 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.Urz. UE L 337 z 23.12.2015, s. 35).

[30] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1724 z 2.10.2018 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.Urz. UE L 295 z 21.11.2018, s. 1).

[31] Dz.Urz. UE L 123 z 12.5.2016, s. 1.

[32] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z 16.02.2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.Urz. UE L 55 z 28.2.2011, s. 13).

[33] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/2102 z 26.10.2016 r. w sprawie dostępności stron internetowych i mobilnych aplikacji organów sektora publicznego (Dz.Urz. UE L 327 z 2.12.2016, s. 1).

[34] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/882 z 17.04.2019 r. w sprawie wymogów dostępności produktów i usług (Dz.Urz. UE L 151 z 7.6.2019, s. 70).

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.

Agnieszka Piskorz-Ryń

1. Cele i wartości DGA

1. Komentowane rozporządzenie reguluje częściowo odrębne zakresy spraw, ale ich wspólnym mianownikiem są dane i ich dostępność. Służy ono solidarności cyfrowej[1] i ma na celu wzmocnienie unijnej infrastruktury danych[2], czyniąc krok ku stworzeniu europejskiej przestrzeni danych. Rozporządzenie jest częścią szerszych ram regulacyjnych UE w obrębie cyfryzacji, gospodarki opartej na danych, sztucznej inteligencji i innych ważnych celów politycznych, często określanych mianem suwerenności cyfrowej[3].

Termin „dane" zostanie omówiony w komentarzu do art. 2 pkt 1. W tym miejscu wskazać należy jedynie, że Unia Europejska od lat dostrzega potencjał danych wytwarzanych przez sektor publiczny dla rozwoju gospodarki europejskiej. Rozporządzenie to traktować należy jako dopełnienie dotychczasowej aktywności w zakresie ponownego wykorzystywania, która zaowocowała najpierw uchwaleniem dyrektywy 2003/98/WE Parlamentu Europejskiego i Rady z 17.11.2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego[4], a później jej zmianami, aż wreszcie przyjęciem dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.06.2019 r.

[1] Na temat związku DGA z solidarnością cyfrową zob. P. Hajduk, V.O. Chukwuma, *Digital Solidarity Through Spatial Data – an EU and African Perspective*, GIS Odyssey Journal 2024/4 (2), s. 107 i n.

[2] M. Maroni, *The Idea of Data and European Constitutional Imaginaries: An Immanent Critique of the Data Governance Act*, EU Data Institutionalism 2024/2, aprile/giugno, Serie V (special issue), s. 13.

[3] J. Ruohonen, S. Mickelsson, *Reflections on the Data Governance Act*, Digital Society 2023/2 (10), https://link.springer.com/article/10.1007/s44206-023-00041-7 (dostęp: 30.04.2025), s. 2.

[4] Dz.Urz. UE L 345, s. 90, ze zm. Na temat genezy ponownego wykorzystywania oraz celów i wartości, jakie stały za jej uchwaleniem, zob. A. Piskorz-Ryń, *Ponowne wykorzystywanie informacji sektora publicznego. Zagadnienia administracyjnoprawne*, Warszawa 2018, s. 78–106 oraz A. Piskorz-Ryń, *Jawność działania administracji publicznej z perspektywy „otwartego rządu"*

w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego[5].

DGA stanowi uzupełnienie regulacji w zakresie ponownego wykorzystywania danych chronionych, które nie są regulowane w dyrektywie 2019/1024, o czym szerzej mowa w komentarzu do art. 3. Rozporządzenie to jest jednym z filarów Europejskiej Strategii Danych[6]. Zapowiedziała ona dwie główne inicjatywy legislacyjne mające na celu realizację ambicji dotyczących europejskiej gospodarki danych przyszłości: rozporządzenie o danych (DA)[7] i rozporządzenie o zarządzaniu danymi (DGA). Mają one na celu usprawnienie udostępniania i ponownego wykorzystywania danych przy jednoczesnej ochronie prywatności i praw do ochrony danych obywateli UE[8]. Celem rozporządzenia jest rozwijanie wewnętrznego rynku cyfrowego wolnego od granic oraz opartego o dane społeczeństwa i opartej o dane gospodarki, ukierunkowanych na człowieka, godnych zaufania i bezpiecznych[9]. Ma ono zapewnić zwiększenie dobrowolnej wymiany danych z korzyścią dla przedsiębiorstw i obywateli poprzez ułatwienie udostępniania danych w zaufany i bezpieczny sposób. Rozporządzenie jest jednym ze środków w proponowanej strategii, które pomogą uwolnić pełny potencjał danych, zmierzając do stworzenia jednolitego unijnego rynku danych, na którym dane mogą płynnie przepływać między sektorami i granicami. Według UE będzie to potężna siła napędowa dla innowacji i tworzenia miejsc pracy. Jednocześnie dane są kluczowym zasobem dla rozwoju wszystkich organizacji, zwłaszcza start-upów i MŚP. Beneficjentami tej regulacji powinny być zarówno przedsiębiorstwa, jak i obywatele, organizacje prywatne i publiczne. Ponowne wykorzystywanie danych chronionych ma szczególne znaczenie dla wykorzystania danych do celów badawczych.

[w:] *Władza – obywatele – informacja. Ku nowemu porządkowi prawnemu. Księga pamiątkowa ku czci Profesor Teresy Górzyńskiej*, red. I. Lipowicz, Warszawa 2014, s. 112 i n.

[5] Dz.Urz. UE L 172, s. 56.

[6] Europejska strategia w zakresie danych, COM(2020) 66 final, OJ L 345, 31/12/2003, s. 0090–0096, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52020DC0066 (dostęp: 30.04.2025).

[7] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2023/2854 z 13.12.2023 r. w sprawie zharmonizowanych przepisów dotyczących sprawiedliwego dostępu do danych i ich wykorzystywania oraz w sprawie zmiany rozporządzenia (UE) 2017/2394 i dyrektywy (UE) 2020/1828 (akt w sprawie danych) (Dz.Urz. UE L 2854, ze zm.).

[8] F. Vogelezang, *Four Questions for the European Strategy for Data*, April 12, 2022, https://openfuture.eu/blog/four-questions-for-the-european-strategy-for-data/ (dostęp: 30.04.2025).

[9] Motyw 3 DGA.

2. Drugim zakresem spraw regulowanym w DGA są ramy dotyczące zgłaszania i nadzoru w odniesieniu do świadczenia usług pośrednictwa danych. Termin „usługi pośrednictwa danych" reguluje art. 2 pkt 11 DGA. Usługi te odgrywają kluczową rolę w gospodarce dzielenia się danymi. Są one istotne przede wszystkim gdy chodzi o wspieranie i promowanie praktyk dobrowolnego dzielenia się danymi między przedsiębiorstwami czy ułatwianie dzielenia się danymi w związku z obowiązkami ustanowionymi w prawie Unii lub prawie krajowym. Mogą stać się narzędziem wspomagającym wymianę znacznych ilości istotnych danych[10]. Wyspecjalizowane usługi pośrednictwa danych mogą umożliwiać powstawanie nowych ekosystemów opartych o dane. Stanowią one formę kontaktu między podażą danych a popytem na nie. Gromadzą zbiory danych i umożliwiają ich znalezienie i udostępnienie[11], wyznaczają również standardy w odniesieniu do specyfikacji technicznych. Bez nich nie będzie możliwe ustanowienie wspólnych europejskich przestrzeni danych służących dzieleniu się danymi lub ich wspólnemu przetwarzaniu na potrzeby m.in. opracowywania nowych produktów i usług, badań naukowych lub inicjatyw społeczeństwa obywatelskiego. Usługi pośrednictwa danych mogą obejmować np. dwustronne i wielostronne dzielenie się danymi, tworzenie platform lub baz danych umożliwiających dzielenie się danymi albo ich wspólne wykorzystywanie, a także tworzenie specjalnej infrastruktury do nawiązywania powiązań między osobami, których dane dotyczą, i posiadaczami danych a użytkownikami tych danych.

3. Trzecim zakresem spraw jest altruizm danych. Dotyczy on danych osobowych i nieosobowych. Termin ten 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,

[10] Motyw 27 DGA.

[11] S. Marx, *Verhaltenspflichten für Anbieter von Datenvermittlungsdiensten*, Zeitschrift für Datenschutzrecht 2023/8, s. 430.

lub do celów badań naukowych leżących w interesie ogólnym (art. 2 pkt 16). DGA określa kwestie dotyczące krajowych rozwiązań organizacyjnych lub technicznych sprzyjających altruizmowi danych, rejestracji uznanych organizacji altruizmu danych, wymogi dotyczące przejrzystości oraz zabezpieczenia praw i interesów osób, których dane dotyczą, a także posiadaczy danych w odniesieniu do ich danych.

Agnieszka Piskorz-Ryń

2. Wybór instrumentu prawnego

1. Polityka cyfrowa jest kompetencją dzieloną między UE a jej państwa członkowskie. Artykul 4 ust. 2 i 3 TFUE[12] stanowi, że w dziedzinach jednolitego rynku i rozwoju technologicznego UE może prowadzić określone działania bez uszczerbku dla aktywności państw członkowskich w tych samych dziedzinach.

2. Prawodawca europejski zdecydował się na wybór rozporządzenia jako instrumentu prawnego, co było uzasadnione przewagą elementów wymagających jednolitego stosowania, które nie pozostawiają państwom członkowskim marginesu swobody pod względem wykonania i które tworzą w pełni horyzontalne ramy[13]. Ze statusu rozporządzeń w systemie źródeł prawa UE wynikają dla państw członkowskich pewne konsekwencje, a mianowicie: zakaz precyzowania lub modyfikowania treści rozporządzenia przez organy krajowe; zakaz powtarzania treści rozporządzenia w aktach prawa krajowego; dopuszczalność (nakaz) działań regulacyjnych na poziomie krajowym w celu zapewnienia efektywności rozporządzenia[14]. Kwestie te wpływają bezpośrednio na zakres ingerencji ustawodawcy krajowego. Jest on zobowiązany podjąć działania regulacyjne w celu zapewnienia skuteczności rozporządzenia. DGA zostało implementowane do polskiego porządku prawnego ustawą o zarządzaniu danymi[15].

[12] Traktat o Funkcjonowaniu Unii Europejskiej (Dz.U. z 2004 r. Nr 90, poz. 864/2 ze zm.).

[13] Wniosek Rozporządzenie Parlamentu Europejskiego i Rady w sprawie europejskiego zarządzania danymi (akt w sprawie zarządzania danymi), COM(2020) 767 final, https://eur-lex.europa.eu/legal-content/PL/TXT/HTML/?uri=CELEX:52020PC0767, pkt 2 (dostęp: 30.04.2025).

[14] M. Baran, *Rozporządzenie* [w:] *System Prawa Unii Europejskiej*, t. 1, *Podstawy i źródła prawa Unii Europejskiej*, red. S. Biernat, Warszawa 2020, s. 981.

[15] Projekt ustawy jest przygotowywany przez Ministra Cyfryzacji. Szerzej na temat przygotowania projektu oraz jego treści wraz z uzasadnieniem na stronie: https://legislacja.rcl.gov.pl/projekt/12389302/katalog/13079809#13079809 (dostęp: 30.04.2025).

Agnieszka Piskorz-Ryń

3. Zakres DGA

1. Rozporządzenie w sprawie zarządzania danymi reguluje cztery zakresy spraw. Przed ich opisem poczynić należy uwagę o charakterze ogólnym. Widoczny jest mianowicie brak spójności między art. 1 ust. 1 lit. a DGA, zgodnie z którym: „W niniejszym rozporządzeniu ustanawia się: warunki ponownego wykorzystywania w Unii niektórych kategorii danych będących w posiadaniu podmiotów sektora publicznego", a tytułem rozdziału 2 rozporządzenia: „Ponowne wykorzystywanie niektórych kategorii chronionych danych będących w posiadaniu podmiotów sektora publicznego". Wydaje się, że materia uregulowana w rozdziale 2 nie mieści się w przyjętym brzmieniu art. 1 ust. 1 lit. a rozporządzenia. Wykracza ona poza określenie warunków ponownego wykorzystywania niektórych kategorii danych będących w posiadaniu PSP. W rozdziale 2 uregulowano m.in. opłaty za ponowne wykorzystywanie, kwestie proceduralne oraz podmioty wspierające PSP w realizacji ich zadań, takie jak organy właściwe oraz pojedyncze punkty informacyjne.

Rozporządzenie posługuje się pojęciem „warunki ponownego wykorzystywania" w art. 1 ust. 1 lit. a, a następnie w tytule art. 5. Rozumienie tych pojęć jest jednak w obu tych przepisach różne, inaczej bowiem należałoby przyjąć, że brak właściwej korelacji między art. 1 ust. 1 lit. a a treścią rozdziału 2 DGA. Powyższe rozumowanie opiera się więc na założeniu, że pojęcia identyczne są wyrażane za pomocą tych samych terminów. Spójność terminologii oznacza, iż te same terminy należy stosować do wyrażenia tych samych pojęć, a różne pojęcia nie mogą być wyrażane za pomocą identycznych terminów. Dzięki temu unika się wieloznaczności, sprzeczności lub wątpliwości co do znaczenia używanego pojęcia. Dany termin należy zatem stosować jednolicie w odniesieniu do tego samego pojęcia, a inne pojęcie należy wyrazić innym terminem[16].

2. Pierwszą z kwestii regulowanych w rozporządzeniu jest ponowne wykorzystywanie niektórych kategorii danych (danych chronionych) będących w posiadaniu podmiotów sektora publicznego. Pojęcie danych chronionych zostanie omówione w komentarzu do art. 3, a pojęcie podmiotów sektora publicznego – w komentarzu do art. 2 pkt 18. W tym miejscu warto zwrócić

[16] *Wspólny przewodnik praktyczny Parlamentu Europejskiego, Rady i Komisji przeznaczony dla osób redagujących akty prawne Unii Europejskiej*, polska wersja językowa, Unia Europejska 2015, pkt 6.2.

uwagę, że DGA nie przyznaje prawa do ponownego wykorzystywania danych chronionych, a jedynie określa warunki ich ponownego wykorzystywania i zagadnienia proceduralne związane z realizacją ponownego wykorzystywania. Kwestia ta zostanie szerzej wyjaśniona w pkt 3.

3. Drugą kategorią spraw uregulowanych w DGA są ramy prawne dotyczące zgłaszania i nadzoru w odniesieniu do świadczenia usług pośrednictwa danych. Pojęcie usługi pośrednictwa danych zostało zdefiniowane w art. 2 pkt 11 DGA. Zgodnie z zawartą tam definicją „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: 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; usług skoncentrowanych na pośrednictwie treści chronionych prawem autorskim; 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; usług dzielenia się danymi oferowanych przez podmioty sektora publicznego, które to usługi nie mają na celu ustanowienia stosunków handlowych. Szczegółowe wymogi dotyczące usług pośrednictwa danych zawiera rozdział 3, a wymogi proceduralne rozdział 5.

4. Trzecią grupę tworzą kwestie dotyczące dobrowolnej rejestracji podmiotów, które gromadzą i przetwarzają dane udostępniane z pobudek altruistycznych. Definicje legalną altruizmu danych zawiera art. 2 pkt 16 DGA. Oznacza on 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. Kwestie szczegółowe dotyczące altruizmu danych zawiera rozdział 4, a przepisy proceduralne rozdział 5.

5. Ostatnią kwestią poruszaną w DGA jest ustanowienie Europejskiej Rady ds. Innowacji w zakresie Danych jako 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 Europejskiej, 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[17]. Jej celem jest pomyślne wdrożenie ram zarządzania danymi w UE[18]. Rada 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[19]. Strukturę oraz zadania Rady określa rozdział 6 rozporządzenia. Kwestie szczegółowe zostaną omówione w komentarzu do tego rozdziału

[17] Art. 29 ust. 1 DGA.
[18] Motyw 53 DGA.
[19] Zob. również motyw 54 DGA.

Agnieszka Piskorz-Ryń

4. Relacja rozporządzenia do przepisów szczególnych

1. Rozporządzenie to pozostaje bez uszczerbku zarówno dla 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 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. W tym zakresie z art. 1 ust. 2 DGA wyraźnie wynika, że rozporządzenie to nie modyfikuje istniejących przepisów – zarówno odnoszących się do dostępu do niektórych kategorii danych, jak i ponownego wykorzystywania. Nie wpływa ono także na kształt przepisów dotyczących dostępu do dokumentów urzędowych.

2. W polskim porządku prawnym zasady ponownego wykorzystywania określa ustawa z 11.08.2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego (Dz.U. z 2023 r. poz. 1524). Określa ona zasady otwartości danych, zasady i tryb udostępniania i przekazywania informacji sektora publicznego w celu ponownego wykorzystywania oraz podmioty, które udostępniają lub przekazują te informacje[20]. Jej przepisów nie stosuje się do informacja sektora publicznego, których udostępnianie lub przekazanie zostało uzależnione od wykazania przez użytkowników interesu prawnego lub faktycznego na podstawie odrębnych przepisów[21]. Kwestie związane z dostępem do informacji publicznej, będącej odpowiednikiem używanego na gruncie europejskim pojęcia dokumentów urzędowych, reguluje ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2022 r. poz. 902). Zgodnie z art. 1 ust. 2 tej ustawy jej przepisy nie naruszają przepisów innych ustaw określających odmienne zasady i tryb dostępu do informacji będących informacjami publicznymi.

3. Rozporządzenie to pozostaje bez uszczerbku dla prawa UE, w tym następujących rozporządzeń i dyrektyw:
- rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 223/2009 z 11.03.2009 r. w sprawie statystyki europejskiej oraz uchylającego rozpo-

[20] Art. 1 u.o.d.p.w.
[21] Art. 4 ust. 2 u.o.d.p.w.

rządzenie 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.Urz. UE L 87, s. 164, ze zm.);
- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/858 z 30.05.2018 r. w sprawie homologacji i nadzoru rynku pojazdów silnikowych i ich przyczep oraz układów, komponentów i oddzielnych zespołów technicznych przeznaczonych do tych pojazdów, zmieniającego rozporządzenie (WE) nr 715/2007 i (WE) nr 595/2009 oraz uchylającego dyrektywę 2007/46/WE (Dz.Urz. UE L 151, s. 1, ze zm.);
- rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z 14.11.2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej (Dz.Urz. UE L 303, s. 59);
- dyrektywy 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. UE L 178, s. 1, ze zm.);
- dyrektywy 2001/29/WE Parlamentu Europejskiego i Rady z 22.05.2001 r. w sprawie harmonizacji niektórych aspektów praw autorskich i pokrewnych w społeczeństwie informacyjnym (Dz.Urz. UE L 167, s. 10, ze zm.);
- dyrektywy 2004/48/WE Parlamentu Europejskiego i Rady z 29.04.2004 r. w sprawie egzekwowania praw własności intelektualnej (Dz.Urz. UE L 157, s. 45);
- dyrektywy 2007/2/WE Parlamentu Europejskiego i Rady z 14.03.2007 r. ustanawiającej infrastrukturę informacji przestrzennej we Wspólnocie Europejskiej (INSPIRE) (Dz.Urz. UE L 108, s. 1, ze zm.);
- dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/849 z 20.05.2015 r. w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniającej rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylającej dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz.Urz. UE L 141, s. 73, ze zm.);
- dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/943 z 8.06.2016 r. w sprawie ochrony niejawnego *know-how* i niejawnych informacji handlowych (tajemnic przedsiębiorstwa) przed ich bezprawnym pozyskiwaniem, wykorzystywaniem i ujawnianiem (Dz.Urz. UE L 157, s. 1);

– dyrektywy Parlamentu Europejskiego i Rady (UE) 2017/1132 z 14.06.2017 r. w sprawie niektórych aspektów prawa spółek (Dz.Urz. UE L 169, s. 46, ze zm.);
– dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/790 z 17.04.2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz.Urz. UE L 130, s. 92);
– dyrektywy Parlamentu Europejskiego i Rady (UE) 2019/1024 z 20.06.2019 r. w sprawie otwartych danych i ponownego wykorzystywania informacji sektora publicznego (Dz.Urz. UE L 172, s. 56) oraz innego sektorowego prawa Unii regulującego dostęp do danych i ich ponowne wykorzystywanie.

Agnieszka Piskorz-Ryń

5. Kwestie bezpieczeństwa

1. Kwestie bezpieczeństwa są kompetencją współdzieloną z UE[22]. Rozporządzenie nie ma zastosowania do danych będących w posiadaniu podmiotów sektora publicznego, które są chronione ze względów bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego. Jego treść w tym zakresie jest spójna z art. 3 ust. 2 lit. d oraz motywem 3. Zgodnie z tym ostatnim niniejsze rozporządzenie nie powinno naruszać kompetencji państw członkowskich w odniesieniu do ich działań z zakresu bezpieczeństwa publicznego, obrony i bezpieczeństwa narodowego. Nie powinno obejmować ono 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 z 13.07.2009 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.Urz. UE L 216, s. 76, ze zm.). W polskim systemie prawnym dyrektywa ta jest wykonywana przez ustawę z 11.09.2019 r. – Prawo zamówień publicznych (Dz.U. z 2024 r. poz. 1320 ze zm.). Zawiera ona w art. 12–14 przepisy dotyczące włączeń stosowania ustawy do zamówień i konkursów wskazanych w tych przepisach. Dane pochodzące z wymienionych tam procedur są wyłączone spod stosowania DGA.

[22] Art. 4 ust. 2 lit. j TFUE.

2. Jednocześnie DGA nie ma zastosowania do innych danych, które są chronione ze względów bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego. W polskim porządku prawnym będzie to obejmowało przede wszystkim informacje kwalifikowane jako informacje niejawne. Do tej kategorii należą informacje, których nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania[23]. Informacjom tym nadaje się klauzulę od zastrzeżone do ściśle tajne[24]. Do tej kategorii zaliczyć należy także informacje, które z jakichś powodów nie otrzymały odpowiedniej klauzuli, ale zaliczyć można je do informacji niejawnych. Będą to m.in. informacje będące w posiadaniu służb specjalnych, o których mowa w art. 11 ustawy z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dz.U. z 2024 r. poz. 812 ze zm.). Zwrócić bowiem należy uwagę, że służby te nie zostały wyłączone podmiotowo ze stosowania rozporządzenia. W ustawie o ABW brak wyłączenia analogicznego do tego z art. 6 pkt 2 ustawy z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781). Do posiadanych przez te służby informacji będzie miało zaś zastosowanie wyłączenie, o którym mowa w art. 3 ust. 2 lit. d. Ma ono charakter przedmiotowy. Oznacza to więc, że można wyłączyć stosowanie DGA, a nie odmówić dostępu do tych informacji ze względu na ich chroniony charakter. W tym przypadku więc ochrona informacji niejawnych nie będzie podstawą odmowy, jak by to miało miejsce w odniesieniu do ustawy o otwartych danych, ale do informacji nią objętych nie ma zastosowanie DGA. Trzeba jednak pamiętać, że musi tu być spełniony pewien warunek, a mianowicie dane muszą być chronione ze względów bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego. Musi więc istnieć w polskim porządku prawnym przepis prawa, który chroni te dane. Nie wystarczy samo ich zakwalifikowanie jako odnoszących się do bezpieczeństwa publicznego, obronności lub bezpieczeństwa narodowego.

[23] Art. 1 ust. 1 ustawy z 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. z 2024 r. poz. 632 ze zm.).

[24] Art. 5 ustawy o ochronie informacji niejawnych.

Marlena Sakowska-Baryła

6. Stosunek do ochrony danych osobowych

1. W art. 1 ust. 3 DGA ustalony został stosunek tego aktu do regulacji, którą zbiorczo można określić jako prawo ochrony danych osobowych. Z lektury tego przepisu wynika, że prawodawca unijny wyraźnie postawił sobie za cel uregulować zarówno to, jak się ma kwestia zarzadzania danymi na gruncie DGA do przetwarzania danych osobowych, jak i to, jak wygląda nadzór instytucjonalny nad procesem takiego przetwarzania. Nie ulega bowiem wątpliwości, że zarządzanie danymi w znacznej mierze odnosi się do danych osobowych. Bez danych osobowych nie sposób się przecież obyć, gdy weźmiemy pod uwagę koncepcję altruizmu danych i samą mechanikę realizacji tej idei. Dane osobowe to również istotny zasób informacyjny, któremu trzeba poświęcić należytą uwagę, gdy w rachubę wchodzi ustalenie dopuszczalności ich ponownego wykorzystywania na podstawie DGA, relacji tego ponownego wykorzystywania względem wykorzystywania odbywającego się na podstawie przepisów o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego, a więc dyrektywy 2019/1024 oraz ustawy o otwartych danych (szerzej zob. komentarz do art. 3 ust. 1 lit. d DGA). Wreszcie dane osobowe pozostają w obszarze zainteresowania, gdy chodzi o usługi pośrednictwa danych.

2. W relacji pomiędzy zarządzaniem danymi na podstawie DGA a ochroną danych osobowych ustanawia się następujące zasady:

1) do danych osobowych przetwarzanych w związku z DGA zastosowanie mają prawo Unii i prawo krajowe w dziedzinie ochrony danych osobowych, a w szczególności DGA pozostaje bez uszczerbku dla:
   – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1, ze zm.) – RODO,
   – rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1725 z 23.10.2018 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.Urz. UE L 295, s. 39),

– dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 201, s. 37, ze zm.),
– dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 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 uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89, ze zm.);

2) przy stosowaniu DGA uwzględnia się kompetencje i uprawnienia organów nadzorczych, o których mowa w przywołanych w poprzednim punkcie rozporządzeniach i dyrektywach, a co za tym idzie na gruncie polskich przepisów prawa w sprawie przetwarzania danych osobowych w związku ze stosowaniem DGA właściwy jest Prezes Urzędu Ochrony Danych Osobowych (w motywie 4 DGA wskazuje się dodatkowo, że należy zapewnić możliwość uznawania organów ochrony danych za właściwe organy do celów niniejszego rozporządzenia, a w przypadku gdy inne organy działają jako właściwe organy do celów DGA, powinny to robić to bez uszczerbku dla nadzorczych uprawnień i kompetencji organów ochrony danych na podstawie RODO);
3) w przypadku kolizji pomiędzy DGA a prawem Unii w dziedzinie ochrony danych osobowych lub prawem krajowym przyjętym zgodnie z takim prawem Unii pierwszeństwo ma odpowiednio prawo Unii lub prawo krajowe w dziedzinie ochrony danych osobowych;
4) DGA 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;
5) w przypadku gdy dane osobowe i nieosobowe w zbiorze danych są ze sobą nierozerwalnie powiązane, do tych danych mają zastosowanie powyższe zasady, a więc – jak wskazuje się w motywie 4 preambuły DGA – przepisy te stosuje się bez uszczerbku dla wyżej wskazanych regulacji z zakresu ochrony danych osobowych oraz odpowiednich przepisów prawa krajowego.

W ten sposób w DGA wyraźnie wyznaczony został kierunek godzenia dwóch wartości, a mianowicie prywatności i związanej z nią autonomii jednostki dotyczącej jej własnej sfery informacyjnej oraz możliwości korzysta-